Gesellschaft für Informatik e.V. (GI)

publishes this series in order to make available to a broad public recent findings in informatics (i.e. computer science and information systems), to document conferences that are organized in cooperation with GI and to publish the annual GI Award dissertation.

Broken down into
• seminars
• proceedings
• dissertations
• thematics
current topics are dealt with from the vantage point of research and development, teaching and further training in theory and practice. The Editorial Committee uses an intensive review process in order to ensure high quality contributions.

The volumes are published in German or English.

Information: http://www.gi.de/service/publikationen/lni/

ISSN 1617-5468
ISBN 978-3-88579-651-0

The 9. DFN-Forum Communication Technologies 2015 is taking place in Rostock, Germany, from May 30th to June 1st.
This volume contains 12 papers selected for presentation at the conference.
To assure scientific quality, the selection was based on a strict and anonymous reviewing process.

P. Müller, B-Neumair, H. Reiser, G. Dreo Rodosek (Hrsg.): 9. DFN-Forum 2016

257

GI-Edition

Lecture Notes in Informatics

Paul Müller, Bernhard Neumair, Helmut Reiser, Gabi Dreo Rodosek (Hrsg.)

9. DFN-Forum Kommunikationstechnologien

31. Mai – 01. Juni 2016
Rostock

Proceedings

Paul Müller, Bernhard Neumair, Helmut Reiser,
Gabi Dreo Rodosek (Hrsg.)

9. DFN-Forum Kommunikationstechnologien

Beiträge der Fachtagung

31. Mai – 01. Juni 2016
Rostock, Deutschland

Gesellschaft für Informatik e.V. (GI)

Lecture Notes in Informatics (LNI) - Proceedings
Series of the Gesellschaft für Informatik (GI)

Volume P-257

ISBN 978-3-88579-651-0
ISSN 1617-5468

Volume Editors
Prof. Dr. Paul Müller (pmueller@informatik.uni-kl.de)
Technische Universität Kaiserslautern
Postfach 3049, 67653 Kaiserslautern
Prof. Dr. Bernhard Neumair (bernhard.neumair@kit.edu)
Karlsruher Institut für Technologie (KIT)
Hermann-von-Helmholtz-Platz 1, 76344 Eggenstein-Leopoldshafen
Prof. Dr. Gabi Dreo Rodosek (Gabi.Dreo@unibw.de)
Universität der Bundeswehr Münnchen
Werner-Heisenberg-Weg 39, 85577 Neubiberg

printed by Köllen Druck+Verlag GmbH, Bonn

Vorwort

Der DFN-Verein ist seit seiner Gründung dafür bekannt, neueste Netztechnologien und innovative netznahe Systeme anwendungsorientiert zu erforschen und einzusetzen, um damit die Leistungen für seine Mitglieder laufend zu erneuern und zu optimieren. Beispiele dafür sind die aktuelle Plattform des Wissenschaftsnetzes X-WiN und Dienstleistungen für Forschung und Lehre wie die DFN-PKI, DFN-AAI und föderierte Cloud-Dienste. Um diese Technologien einerseits selbst mit zu gestalten und andererseits frühzeitig die eigenen Forschungsergebnisse mit den Entwicklungen anderer Wissenschaftler abzugleichen, veranstaltet der DFN-Verein seit vielen Jahren wissenschaftliche Tagungen zu Netztechnologien. Mit den Zentren für Kommunikation und Informationsverarbeitung in Forschung und Lehre e.V. (ZKI) und der Gesellschaft für Informatik e.V. (GI) gibt es in diesem Bereich eine langjährige und fruchtbare Zusammenarbeit.

Das 9. DFN-Forum Kommunikationstechnologien „Verteilte Systeme im Wissenschaftsbereich“ steht in dieser Tradition. Nach den sehr erfolgreichen Vorgängerveranstaltungen in Kaiserslautern, München, Konstanz, Bonn, Regensburg, Erlangen, Fulda und Lübeck wird die diesjährige Tagung vom DFN-Verein und der Universität Rostock gemeinsam mit dem ZKI e.V. und der GI am 31. Mai und 1. Juni 2016 in Rostock veranstaltet und soll eine Plattform zur Darstellung und Diskussion neuer Forschungs- und Entwicklungsergebnisse aus dem Bereich TK/IT darstellen. Das Forum dient dem Erfahrungsaustausch zwischen Wissenschaftlern und Praktikern aus Hochschulen, Großforschungseinrichtungen und Industrie.

Aus den eingereichten Beiträgen konnte ein hochwertiges und aktuelles Programm zusammengestellt werden, das sich neben Fragen von Netztechnologien und IT-Infrastrukturen auch mit Infrastrukturen für eResearch befasst. Traditionell ist auch die IT- und Netz-Sicherheit ein wichtiges Thema des Forums, das auch in diesem Jahr intensiv und breit behandelt wird. Eingeladene Beiträge runden das Programm ab. So wird der DFN globale Trends in der Kooperation zwischen Wissenschaftsnetzen präsentieren. Die Zentralstelle Cybercrime in Bayern wird aus der staatsanwaltschaftlichen Praxis der Verfolgung von Cybercrime berichten und eine Vertreterin des Bundesamtes für Bevölkerungsschutz und Katastrophenschutz wird Kritische Infrastrukturen und IT-Sicherheit beleuchten.

Wir möchten uns bei den Autoren für alle eingereichten Beiträge, beim Programmkomitee für die Auswahl der Beiträge und die Zusammenstellung des Programms, bei den Mitarbeiterinnen und Mitarbeitern für die umfangreichen organisatorischen Arbeiten und beim Gastgeber für die Unterstützung des Forums sowie die Gastfreundschaft bedanken. Allen Teilnehmern wünschen wir für die Veranstaltung interessante Vorträge und fruchtbare Diskussionen.

Rostock, April 2016

Gabi Dreo Rodosek
Paul Müller
Bernhard Neumair
Helmut Reiser

Programmkomitee

Rainer Bockholt, Universität Bonn

Alexander Clemm, Cisco USA

Gabriele Dobler, Universität Erlangen-Nürnberg

Gabi Dreo Rodosek (Co-Chair), Universität der Bundeswehr München

Thomas Eickermann, Forschungszentrum Jülich

Alfred Geiger, T-Systems SfR

Wolfgang Gentzsch, The UberCloud

Andreas Hanemann, KIT

Peter Klingebiel, Hochschule Fulda

Ulrich Lang, Universität zu Köln

Paul Müller (Co-Chair), Technische Universität Kaiserslautern

Bernhard Neumair (Co-Chair), KIT

Gerhard Peter, Hochschule Heilbronn

Christa Radloff, Universität Rostock

Helmut Reiser (Co-Chair), LRZ München

Sebastian Rieger, Hochschule Fulda

Harald Roelle, Siemens AG

Peter Schirmbacher, Humboldt-Universität zu Berlin

Uwe Schwiegelshohn, TU Dortmund

Manfred Seedig, Universität Kassel

Marcel Waldvogel, Universität Konstanz

René Wies, BMW Group

Martin Wimmer, Universität Regensburg

Inhaltsverzeichnis

Netztechnologien und Infrastruktur

Infrastrukturen für eResearch

Sicherheit

Netztechnologien und Infrastruktur

Aufbau einer High Density WLAN-Infrastruktur für Hochschullehre und Veranstaltungen

Markus Speer[1], Jamaldin Chakoh[2], Andre Forsmann[3] und Dieter Frieler[4]

Abstract: Für die Nutzung mobiler Endgeräte in Hörsälen und Seminarräumen ist eine gut ausgebaute WLAN-Infrastruktur eine unverzichtbare Voraussetzung. Bereits 2010 wurde an der Westfälischen Wilhelms-Universität Münster (WWU) in den genannten Räumlichkeiten eine lückenlose WLAN-Grundversorgung realisiert. Die zunehmende Verbreitung mobiler Endgeräte und die Möglichkeit der systematischen Nutzung im Rahmen der Lehre erfordert inzwischen jedoch eine massive Erhöhung der WLAN-Versorgungsdichte zu einem „High Density WLAN". Dieses stellt eine hochwertige Nutzungserfahrung für eine steigende Anzahl gleichzeitig aktiver WLAN-Endgeräte sicher und eignet sich auch für Foyers und exponierte Außenbereiche. An der WWU wurde der Aufbau einer umfangreichen HD-WLAN-Infrastruktur für die Hochschullehre insb. in großen Hörsälen und für Veranstaltungen projektiert. Ziel war es, ein HD-WLAN-Design zu entwickeln und umzusetzen, das ein Roll-Out in großem Umfang mit einigermaßen überschaubaren Aufwänden und kalkulierbaren Ergebnissen ermöglicht. Dieses Design wurde bereits in substanziellem Umfang realisiert. In diesem Paper werden die besonderen Herausforderungen, die getroffenen Entscheidungen, die Vorgehensweise und gemachten Erfahrungen dargestellt.

Keywords: WLAN, Wireless, Infrastruktur, High Density, HD, Hörsäle, Veranstaltungen

1 Projektziele

An der WWU und am Universitätsklinikum Münster (UKM) ist eine umfangreiche WLAN-Infrastruktur mit ca. 2.250 WLAN Access Points (APs) in ca. 200 Gebäuden im Einsatz. Hierzu zählt auch eine bereits im Jahr 2010 erfolgte lückenlose Versorgung von Hörsälen und Seminarräumen für ca. 43.000 Studierende. Für eine systematische Nutzung des WLAN in großen, vollbesetzten Hörsälen durch alle Hörer wurde diese Grundversorgung allerdings nicht ausgelegt. Um hier eine qualitativ hochwertige Nutzungserfahrung zu gewährleisten, muss für solche HD-WLAN-Umgebungen ein neues Design entwickelt und implementiert werden. Dafür wurde Anfang August 2014 an der WWU der Aufbau einer umfangreichen HD-WLAN-Infrastruktur für die Hochschullehre in den ca. 50 Hörsälen mit über 100 Plätzen und auch für Foyers und exponierte Außenbereiche für Veranstaltungen projektiert. Es ging um insg. 12.400 Sitzplätze in Hörsälen mit bis zu 800 Sitzplätzen.

[1] Westfälische Wilhelms-Universität Münster - ZIV, Röntgenstr. 7 - 13, 48149 Münster, speer@wwu.de
[2] Westfälische Wilhelms-Universität Münster - ZIV, Röntgenstr. 7 - 13, 48149 Münster, chakoh@wwu.de
[3] Westfälische Wilhelms-Universität Münster - ZIV, Röntgenstr. 7 - 13, 48149 Münster, forsmaa@wwu.de
[4] Westfälische Wilhelms-Universität Münster - ZIV, Röntgenstr. 7 - 13, 48149 Münster, frieled@wwu.de

Die zu implementierende WLAN-Infrastruktur sollte für sämtliche Hörer eines vollbesetzten Hörsaals gleichzeitig für interaktive Anwendungen und mindestens niedrigbandbreitige Datenströme nutzbar sein. Die zu installierende HD-WLAN-Infrastruktur sollte primär eine hohe Robustheit und nicht so sehr eine sehr hohe Bandbreite bieten. Außerdem standen überschaubare Kosten und Aufwände für die Installation im Vordergrund, um ein einheitliches „Massenrollout nach Schema F“ ohne umfangreiche Einzelfallbetrachtung zu ermöglichen.

2 Herausforderungen

Bei Projektstart lagen beim Zentrum für Informationsverarbeitung (ZIV) keine Erfahrungen im Bereich HD-WLAN vor. Auch im Bereich des damals relativ neuen ausschließlich im 5 GHz-Band arbeitenden WLAN-Standards IEEE 802.11ac gab es kaum Erfahrungen. Es wurde davon ausgegangen, dass sich der ac-Standard in Bezug auf Designfragestellungen nicht wesentlich von der 5 GHz-Variante des Vorgängerstandards IEEE 802.11n unterscheidet. Eine Orientierung bzgl. Designfragestellungen bot [Fl13].

Eine hohe Dichte von WLAN-Clients in einem vollbesetzten großen Hörsaal erfordert eine entsprechend **hohe Dichte an APs**. Eine hohe Anzahl an APs ist aber nur dann hilfreich, wenn es gelingt die Clients einigermaßen gleichmäßig auf die APs zu verteilen.

Wenn für einen Client mehrere „brauchbare“ APs sichtbar sind, ist im Rahmen der WLAN-Technologie nicht zuverlässig steuerbar, mit welchem AP sich ein WLAN-Client verbindet („assoziiert“). Die IEEE-WLAN-Standards sehen keine Mechanismen vor, einem Client vorzugeben, mit welchem AP er sich verbinden soll. **Diese letztendliche (Roaming-)Entscheidung trifft allein der WLAN-Client.** Es ist aber naheliegend, davon auszugehen, dass ein WLAN-Client seine Entscheidung, sich mit einem bestimmten AP zu verbinden, primär von der empfangenen Sendeleistung des APs abhängig macht.

Wenn mehrere APs für die lückenlose Versorgung eines größeren Bereichs installiert werden, bedeutet das, dass sich die Funkfelder verschiedener APs überlappen. In diesen Überlappungsbereichen müssen die APs auf verschiedenen Funk-Kanälen arbeiten, um gegenseitige Störungen zu vermeiden. In den im 2,4 GHz-Band arbeitenden WLAN-Technologien IEEE 802.11b/g/n stehen nur drei überlappungsfreie Kanäle zur Verfügung. Hier stellt die Vermeidung der sog. Co-Channel-Interference (Interferenzen verschiedener Geräte auf einem Übertragungskanal) eine große Herausforderung dar. **Diese Gefahr der Co-Channel-Interference ist natürlich umso größer, je dichter die APs platziert sind.** In den im 5 GHz-Band arbeitenden WLAN-Technologien (IEEE 802.11a/n/ac) stehen bis zu 16 Kanäle zur Verfügung. Hier hat man deutliche bessere Möglichkeiten eine Co-Channel-Interference zu vermeiden. Von den 5GHz-Technologien wird dabei auch eine Erhöhung der Kanalbreite von 20 MHz auf 40, 80 oder auch 160 MHz zur Geschwindigkeitssteigerung unterstützt. Allerdings bedeutet

beispielsweise die Verdoppelung der Kanalbreite von 20 auf 40 MHz eine Halbierung der verfügbaren Kanalzahl. Auch mit speziellen Antennen kann der Problematik der Co-Channel-Interference begegnet werden.

Beim WLAN handelt es sich um eine „Shared Medium"-Technologie; d.h. dass sich alle beteiligten Geräte (APs und WLAN-Clients) die zur Verfügung stehende Bandbreite teilen. Natürlich ist eine hohe Bandbreite für die WLAN-Clients wünschenswert. **Im WLAN und insb. in einer HD-WLAN-Umgebung ist es aber auch von Bedeutung, welche Mindestbandbreite von den APs überhaupt unterstützt wird.** Werden niedrige Mindestbandbreiten unterstützt, kann das bedeuten, dass Clients, die sich mit einer geringen Bandbreite verbinden die Performance der gesamten Funkzelle eines APs verringern, da sie das gemeinsame Übertragungsmedium lange belegen. Hohe Mindestbandbreiten sorgen also dafür, dass das Übertragungsmedium schnell für andere Geräte wieder frei wird. Außerdem sorgen hohe Mindestbandbreiten dafür, dass Clients sich mit APs verbinden, die sich in ihrer Nähe befinden.

Eine weitere Herausforderung war der **Test einer implementierten HD-WLAN-Infrastruktur** unter Bedingungen, die einem Produktivszenario „aktiv genutztes WLAN in einem gut gefüllten großen Hörsaal" einigermaßen nahe kommt. Große Installationsmaßnahmen waren nur in vorlesungsfreien Zeiten möglich.

3 Design der HD-WLAN-Infrastruktur

3.1 HD-WLAN-Hardware

An der WWU und dem UKM wird vom ZIV eine WLAN-Infrastruktur mit Geräten des Herstellers Cisco eingesetzt. Für die Realisierung sollte ein Access Point Typ eingesetzt werden, der den aktuellen WLAN-Standard IEEE 802.11ac unterstützt. Zum Entscheidungszeitpunkt kamen dabei die beiden Access Point Typen C2700 und C3700 in Frage. Die Entscheidung fiel dabei zugunsten des kostengünstigeren C2700. Der um Module erweiterbare C3700 bot zwar mit der 4x4:3 MIMO-Technik gegenüber der 3x4:3 MIMO-Technik des C2700 die leistungsfähigere WLAN-Hardware, jedoch war nach eigener Einschätzung in der Praxis hierdurch nahezu kein Qualitätsunterschied im WLAN zu erwarten.

In Hörsälen muss pro Sitzplatz mindestens ein für Vorlesungszwecke aktives WLAN-Endgerät kalkuliert werden. Außerdem müssen neben den tatsächlich aktiv genutzten WLAN-Endgeräten an einem Sitzplatz auch die nicht genutzten aber evtl. im WLAN assoziierten WLAN-Endgeräte (z.B. Smartphone in der Hosen-/Handtasche) von den APs verwaltet werden. Für die Kalkulation des Mengengerüsts wurde einer Herstellerempfehlung entsprechend davon ausgegangen, dass für die Versorgung von je ca. 50 Sitzplätzen ein AP erforderlich ist. Insgesamt ergab sich für das Projekt (inkl. Foyers und exponierter Außenbereiche) ein Bedarf von ca. 300 APs.

Die WLAN-Infrastruktur von WWU und UKM ist eine zentralisierte, controllerbasierte Lösung mit nicht-autonomen APs. Insb. die Nutzdaten werden vom AP über einen Tunnel zum WLAN-Controller geführt. Die APs der HD-WLAN-Infrastruktur wurden sämtlich von zwei Controllern (WISM2-Module für Cisco Catalyst 6500 in einer High Availability Konfiguration, Software Ver. 7.6) verwaltet. Für das Management wurde Cisco Prime Infrastructure (Ver 2.2) eingesetzt. Die Abbildungen in Kapitel 5 wurden mit Cisco Prime Infrastructure erstellt.

Auf den Einsatz externer Antennen wurde verzichtet. In der Theorie (und vermutlich auch in der Praxis) können natürlich mit externen Antennen insb. in HD-WLAN Umgebungen bessere Ergebnisse in der Gestaltung des Funkfeldes erzielt werden. Dennoch wurde aus folgenden Gründen auf den Einsatz externer Antennen verzichtet: erhöhte Kosten, aufwändige Installation (steife, dicke Kabel; Antennenausrichtung), erhöhte Betriebsaufwände, optischer Störfaktor.

Ende 2014 / Anfang 2015 durchgeführte Recherchen haben gezeigt, dass kaum Firmen mit einer tatsächlich belastbaren Expertise im Bereich Ausleuchtung für eine HD-WLAN-Infrastruktur existieren. Daher wurde zu Projektbeginn auf die Einbeziehung externer Firmen für die WLAN-Ausleuchtung verzichtet. Eine selbst vorgenommene simulierte Ausleuchtung der zu versorgenden Bereiche wurde nur bei der ersten Test/Pilotinstallation durchgeführt (Produkt „Ekahau Site Survey“). Aufgrund der dabei gemachten Erfahrungen im Rahmen von Tests (vgl. Kapitel 4) in einem Funkfeld ohne Wände und ohne Reichweitenprobleme durch Dämpfung wurde anschließend bei den nachfolgenden Maßnahmen auf eine Ausleuchtung verzichtet. Es wurde beschlossen, eine an der Bestuhlung orientierte, gleichmäßige, geometrische Platzierung der APs im Deckenbereich vorzunehmen. Diese Vorgehensweise führt in der Regel zu einfachen Kabelwegen für die Tertiärverkabelung zur Netzanbindung der APs. Die Stromversorgung der APs erfolgt mittels PoE+ über die Tertiärverkabelung. Für die Netzanbindung eines APs sollte eine produktive Anbindung und eine (noch) ungenutzte Reserveanbindung verlegt werden, um ggf. zusätzliche APs anschließen zu können.

Insgesamt wurde ein Design für eine HD-WLAN-Hardwareinfrastruktur entworfen, das auf den Einsatz von Spezialhardware verzichtet und dadurch einfach umzusetzen und mit Standardmaßnahmen auch einfach erweiterbar ist („Skalierbarkeit“).

3.2 Konfiguration des HD-WLAN

Es wurde ein Designansatz verfolgt, der bewusst auf Komplexität verzichtet. Der Ansatz ist für Hörsäle bis zu einer Größe von 800 Sitzplätzen weitgehend problemlos und effizient umsetzbar. Für große Veranstaltungshallen oder Fußballstadien skaliert dieser Ansatz allerdings nicht. Ein weiterer Leitgedanke war es, sich auf Maßnahmen zu beschränken, die bei den WLAN-Produkten möglichst vieler Hersteller umsetzbar sind. Die Nutzung herstellerspezifischer Features sollte vermieden werden. Folgende Konfigurationsmaßnahmen wurden für das HD-WLAN vorgenommen:

Die Kanalbreite im 5 GHz-Band wurde auf 20 MHz beschränkt, um die maximale Zahl von 16 Kanälen für eine grundsätzliche Vermeidung der Co-Channel-Interference zur Verfügung zu haben. Die Kanalzahl reicht für Hörsäle mit bis zu 800 Sitzplätzen. Damit wurde auf eine höhere max. Bandbreite für einen einzelnen Client verzichtet. Die theoretische Maximalbandbreite beträgt bei dieser Konfiguration 260 Mbit/s im IEEE 802.11ac Standard. Das eingesetzte Produkt unterstützt maximal 217 Mbit/s.

Der Verzicht auf breitere Kanäle macht nur Sinn, wenn es gelingt, möglichst viele Clients dazu zu bringen, eine Verbindung im 5 GHz-Band aufzubauen. Dafür wurde im 5 GHz-Band eine höhere Sendeleistung als im 2,4 GHz-Band konfiguriert.

Erfahrungen aus Tests (vgl. Kapitel 4) haben dazu geführt, dass keine dynamische sondern eine statische Konfiguration der Kanäle vorgenommen wurde.

Die eingesetzten APs unterstützen sowohl das 2,4 GHz-Band als auch das 5 GHz-Band. Da im 2,4 GHz-Band nur drei überlappungsfreie Kanäle zur Verfügung stehen, wurde in Hörsälen mit mehr als drei APs auf einigen APs das 2,4 GHz-Band abgeschaltet (vgl. Abb. 1), um die im wandlosen, dämpfungsarmen Raum bei dichter AP-Montage unvermeidbare Co-Channel-Interference zu reduzieren. Hierfür muss für jeden Hörsaal eine Einzelfallbetrachtung anhand der Montagepositionen der APs durchgeführt werden.

Es wurde eine Maximalzahl von Clients pro Frequenzband eines APs konfiguriert:

- 2,4 GHz-Band: max. 60 Clients
- 5 GHz-Band: max. 50 Clients

Im 5 GHz-Band bedeutet das bei gleichzeitiger Aktivität aller Clients eine theoretische mittlere Bandbreite von ca. 4 Mbit/s pro Client.

Für die HD-WLAN-Infrastruktur wurde kein neuer Funkzellenname („SSID“) eingerichtet, um zusätzlichen Konfigurationsaufwand für die Nutzer zu vermeiden. Grundsätzlich wäre eine separate SSID im 5 GHz-Band denkbar gewesen, um Clients die Möglichkeit zu bieten, sich dediziert in das 5 GHz-Band einzuwählen. Aus Gründen der Usability und um zusätzliche Supportaufwände zu vermeiden, wurde darauf verzichtet. Außerdem bedeutet jede weitere SSID einen zusätzlichen Overhead, der sich negativ auf die WLAN-Performance auswirkt. Es gibt die herstellerübergreifende Empfehlung, möglichst ein „Single SSID Design“ anzustreben.

Es wurden Mindestwerte für die von den APs unterstützten Bandbreiten konfiguriert. Der Standard IEEE 802.11b mit Bandbreiten bis max. 11 Mbit/s wurde bereits Anfang 2013 abgeschaltet. Für die Standards IEEE 802.11a und IEEE 802.11g wurde eine Konfiguration vorgenommen, die eine WLAN-Assoziierung (Verbindungsaufbau) des Clients mit einer Bandbreite von mindestens 36 Mbps erzwingt und Bandbreiten unterhalb von 18 Mbps nicht unterstützt:

- Bandbreiten kleiner 18 Mbps: Disabled
- 18 Mbps: Supported

- 24 Mbps: Supported
- 36 Mbps: Mandatory (für Assoziierung/Verbindungsaufbau)
- 48 Mbps: Supported
- 54 Mbps: Supported

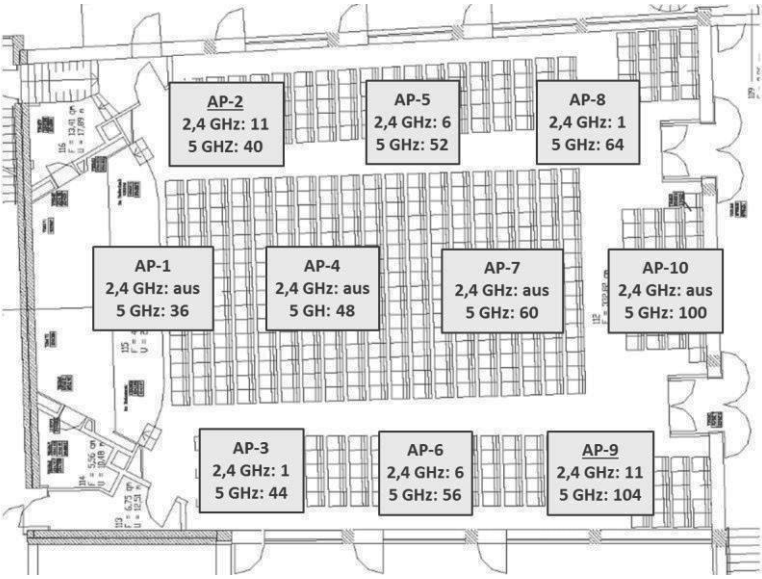


Abb. 1: Konfiguration der Kanäle auf den Access Points im Hörsaal „F1 im Fürstenberghaus“

4 Projektablauf, Tests und Projektstatus

Eine erste Test-/Pilotinstallation wurde in der Aula des Vom-Stein-Haus (Schlossplatz 34) mit 300 Sitzplätzen vorgenommen. Für diese Installation wurde eine Ausleuchtungssimulation für die Platzierung von 7 APs durchgeführt. Für einen darauffolgenden Test wurden 69 den Standard IEEE 802.11ac noch nicht unterstützende iPADs ausgeliehen, auf den Stühlen platziert und mit dem WLAN verbunden und auf jedem Gerät ein Dauervideostreamabruf von einem Medienportal gestartet. Im Mittel wurde pro Client eine Bandbreite von 2 Mbit/s beobachtet. Bei den Tests wurde mehrfach beobachtet, dass bei einer dynamischen Kanalzuweisung, wie sie im Standard-WLAN der WWU im Einsatz ist, nach einer gewissen Laufzeit viele Kanäle im 5 GHz-Band von mehreren APs gleichzeitig verwendet wurden. Dem Problem wurde nicht weiter nachgegangen, sondern es wurde entschieden, für die HD-WLAN-Infrastruktur in beiden Frequenzbändern eine feste Kanalzuordnung vorzunehmen. Insgesamt gab es keine auffälligen Probleme bei den Clients. Bei den Tests wurden auch 2,4 GHz-only-Konfigurationen untersucht, bei denen nur 3 APs aktiv waren, um eine hierfür

funktionierende Konfiguration (bzgl. der Co-Channel-Interference) für die Sendeleistung zu ermitteln. Nach Abschluss der Tests wurde die Installation im Rahmen der Feierlichkeiten zum 50-jährigen Jubiläum des ZIV Ende September 2014 erfolgreich als Veranstaltungsinfrastruktur genutzt.

Die zweite Installation wurde im Fürstenberghaus (Domplatz 20 – 22) in einer Vielzahl von großen und kleinen Hörsälen und Foyerbereichen vorgenommen. Im Hörsaal F1 mit 499 Sitzplätzen wurden in Absprache mit dem Dozenten im Anschluss an eine Vorlesung spontane HD-WLAN-Tests mit den WLAN-Endgeräten der Hörer im Hörsaal durchgeführt. Ende Mai 2015 wurde die HD-WLAN-Infrastruktur im Fürstenberghaus äußerst erfolgreich im Rahmen der „23rd European Conference on Information Systems (ECIS 2015)“ genutzt. Es wurden bis zu 370 Clients im Hörsaal F1 beobachtet.

Tabelle 1 listet die Hörsäle mit mindestens 100 Sitzplätzen und Foyers auf, die bis Anfang 2016 mit einer HD-WLAN-Infrastruktur versorgt wurden. Es wurden also bereits ca. 40 % der geplanten Räumlichkeiten versorgt. In den jeweiligen Gebäuden wurde aus Effizienzgründen oft auch eine Vielzahl kleinerer Hörsäle und Seminarräume mit berücksichtigt.

Gebäude	Räumlichkeit	Größe (m²)	Sitzplätze	APs
Domplatz 20-22, Fürstenberghaus	**F1**	**332**	**499**	**10**
	F2	169	195	4
	F4	126	155	4
	F5	171	177	4
	Foyer im EG	-	-	4
	Foyer im 1. OG	-	-	4
	Foyer im 2. OG	-	-	2
Scharnhorststr. 100	**Aula am Aasee**	**489**	**650**	**13**
	SCH 100.2	180	175	4
	SCH 100.3/H319	151	154	4
Scharnhorststr. 109 und 121	SCH 109.6	271	250	6
	SCH 121.5	329	350	6
Schlossplatz 2, Schloss	S 1	149	200	4
	S 2	145	186	4
	S 8	157	210	5
	S 9	128	124	3
	S 10	220	289	6
	Foyer	-	-	4
Schlossplatz 34, Vom-Stein-Haus	VSH 219 Aula	314	300	7
Schlossplatz 46	H 1	634	806	16
	H 2	154	120	2
	H 3	209	192	4
	H 4	154	120	2
	Foyer im EG	-	-	4

Tab. 1: Anfang 2016 mit einer HD-WLAN-Infrastruktur ausgestattete große Hörsäle und Foyers

5 Erfahrungen mit der HD-WLAN-Installation

5.1 Client-Verteilung auf die 2,4 GHz- und 5 GHz-Bänder

Es wurde untersucht, inwieweit es durch die vorgenommene HD-WLAN-Konfiguration tatsächlich gelungen ist, die Clients dazu zu bringen, möglichst eine Verbindung im 5 GHz-Band aufzubauen. Hierzu wurde zunächst ein Hörsaal („Aula am Aasee“) betrachtet, bei dem zwar die installierten APs schon gemäß einer HD-Konstellation eingebaut waren, aber noch nicht mit der speziellen HD-Konfiguration (vgl. Kapitel 3.2) sondern noch mit einer Standard-WLAN-Konfiguration versehen waren. Außerdem wurde ein Hörsaal („F1 im Fürstenberghaus“) betrachtet, der komplett gemäß HD-WLAN-Standard konfiguriert war. Wie die folgenden beiden Abbildungen zeigen gab es bei der Standard-WLAN-Konfiguration einen Client-Anteil von ca. 26% und bei der HD-WLAN-Konfiguration einen Anteil von ca. 71 % von Verbindungen im 5 GHz-Band. Die HD-WLAN-Konfiguration bewirkte also tatsächlich eine Bevorzugung des 5 GHz-Bandes durch die Clients.

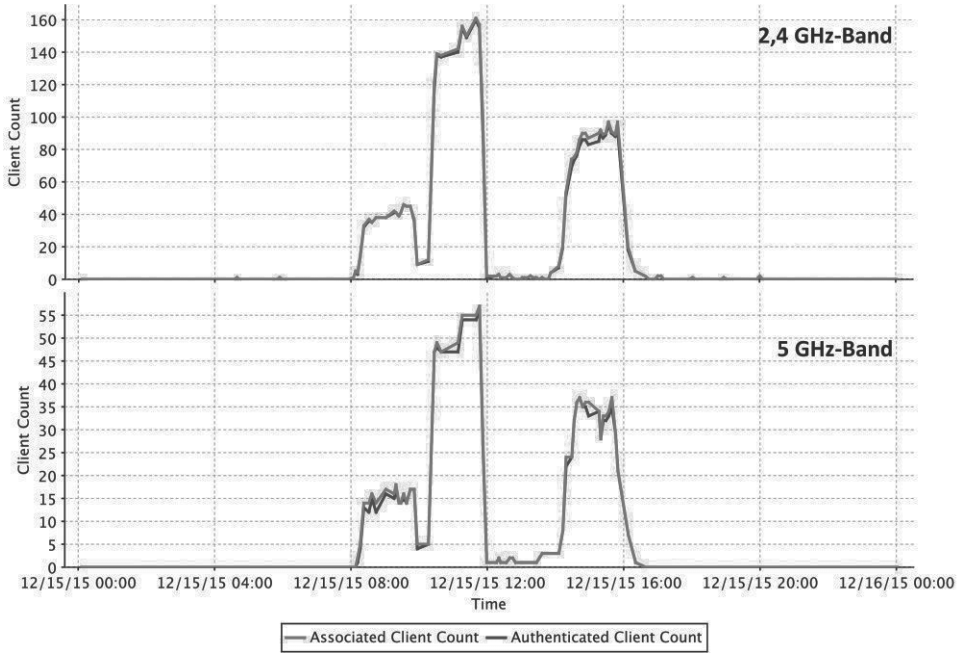


Abb. 2: Client-Anzahl in der „Aula am Aasee“ mit einer **Standard-WLAN-Konfiguration**

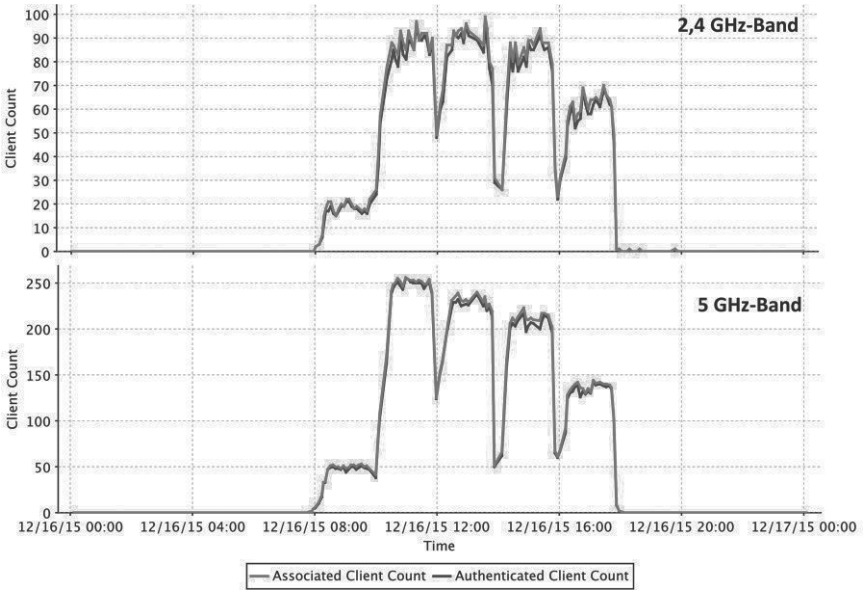


Abb. 3: Client-Anzahl im Hörsaal „F1 im Fürstenberghaus“ mit einer **HD-WLAN-Konfiguration**

5.2 Verteilung der WLAN-Clients auf die verschiedenen Access Points

Tabelle 2 zeigt, dass im Hörsaal F1 eine einigermaßen gleichmäßige Verteilung der Clients auf die Frequenzbänder der APs erzielt wurde. Dargestellt wird die maximale Client-Anzahl an einem Tag, an dem zu Spitzenzeiten ca. 350 Clients assoziiert waren. Bei diesen Maximalwerten hat man einen Anteil von 68 % Clients im 5 GHz-Band.

AP	2,4 GHz-Band	5 GHz-Band	AP	2,4 GHz-Band	5 GHz-Band
AP-1	-	25	AP-6	28	30
AP-2	**20**	**24**	AP-7	-	27
AP-3	20	21	AP-8	28	31
AP-4	-	46	**AP-9**	**23**	**51**
AP-5	33	34	AP-10	-	30

Tab. 2: Maximalwerte für die Client-Anzahl der einzelnen APs im Hörsaal F1 am 16.12.2015

5.3 Co-Channel-Interference, Channel Utilization

Um zu ermitteln, ob es gelungen ist, eine möglichst niedrige Co-Channel-Interference (CCI) zu erzielen, wurde die Channel Utilization (CU) betrachtet. In Abb. 4 ist die CU durch alle zur CCI beitragenden WLAN-Geräte rot dargestellt. Die anteilige Belegung durch die Empfangseinrichtung des betrachteten APs (Rx Utilization) ist blau, die Belegung durch die Sendeeinrichtung (Tx Utilization) ist grün dargestellt. Im 2,4 GHz-

Band wurde außerhalb der Nutzungszeiten eine als unproblematisch angesehene CU zwischen ca. 3% und 10% beobachtet. Im 5 GHz-Band wurde bei der Verwendung von 10 verschiedenen Kanälen für 10 APs eine zu erwartende CU von 0% beobachtet.

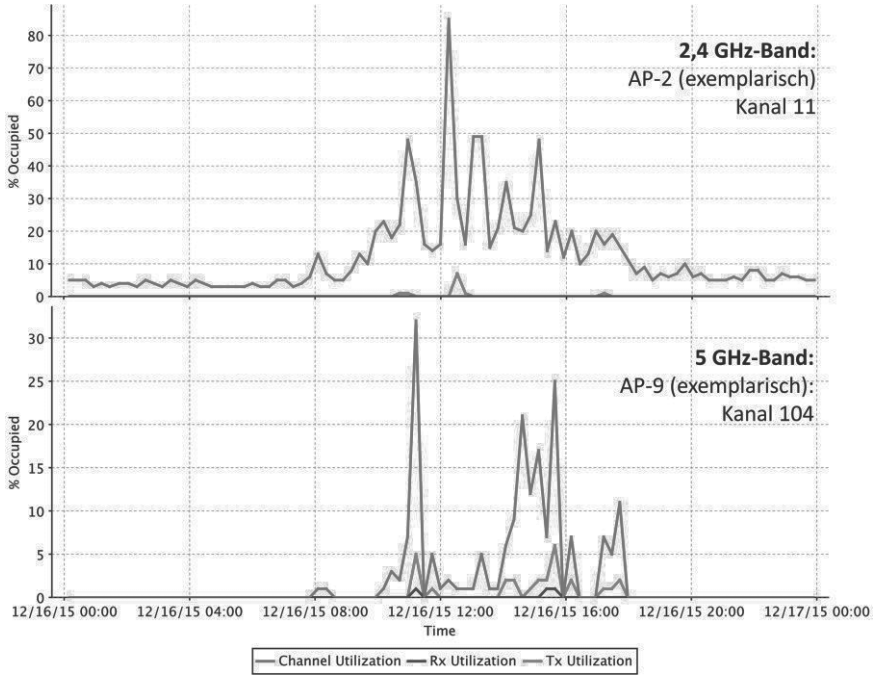


Abb. 4: Von APs (exemplarisch) beobachtete Kanalbelegung im Hörsaal F1

6 Fazit, Ausblick

Insgesamt wurde ein Designansatz verfolgt, der auf Komplexität verzichtet, sich aber als äußerst praktikabel erwiesen hat. Die Designziele (möglichst viele Clients im 5 GHz-Band, gleichmäßige Verteilung der Clients auf die APs, geringe Co-Channel-Interference) wurden erreicht. Mit externen Antennen gibt es ein Optimierungspotenzial für die Gestaltung des Funkfeldes. Das soll zukünftig im Auge behalten werden. Bislang wurden noch keine intensiven Betrachtungen von Interferenzen mit der vorhandenen, benachbarten normalen (d.h. Nicht-HD-)WLAN-Infrastruktur vorgenommen.

Literaturverzeichnis

[Fl13] J. Florwick; J. Whiteaker; A. Cuellar Amrod; J. Woodhams: Cisco Wireless LAN Design Guide for High Density Client Environments in Higher Education; Nov 2013

Verteilte Messung und Vorhersage von Kanalauslastung in IEEE 802.11 Wireless LAN

Till Wollenberg[1]

Abstract: Aufgrund der hohen Verbreitung und intensiven Nutzung von WLAN kommt es insbesondere in Bereichen mit hoher Gerätedichte (wie z. B. universitären Lehrgebäuden) schon heute zu Kapazitätsengpässen, die durch ausgelastete Funkkanäle verursacht werden. Eine Vorhersage der Funkkanalauslastung kann die Probleme durch bessere Nutzung der vorhanden Spektrumsressourcen und proaktive Anpassung genutzter Dienste abmildern. Hierfür müssen Verfahren zur Messung der Kanalauslastung, Unterscheidung von Signalquellen, Vorhersage und Austausch von Messdaten kombiniert und weiterentwickelt werden. Der vorliegende Artikel stellt ein Konzept hierzu vor.

1 Einleitung

Drahtlose Netze nach dem Standard IEEE 802.11 Wireless LAN (WLAN) sind allgegenwärtig im Büro-, Privat- und Industrie-Umfeld. Die Anzahl WLAN-fähiger Geräte steigt weiterhin kontinuierlich, während gleichzeitig die je Gerät übertragenen Datenvolumina wachsen. Aufgrund des begrenzten, für WLAN nutzbaren Frequenzspektrums steigt hierdurch die Spektrumsnutzung sowohl in räumlicher wie auch zeitlicher Dimension.

Dieser Anstieg wird zusätzlich verstärkt durch andere Funkdienste, die im selben Frequenzbereich wie WLAN arbeiten, u. a. Bluetooth, IEEE-802.15.4-basierte Systeme (z. B. ZigBee), Audio/Video-Übertragungssysteme und schnurlose Telefone. Hierdurch erreicht WLAN an Orten mit einer hohen Zahl aktiver Geräte oder Geräten mit hoher Nutzungsintensität schon heute Kapazitätsgrenzen.

Die mit einer WLAN-Übertragung erzielbare Leistung wird einerseits durch die Auslastung des Funkkanals und andererseits durch die Signalqualität und Ausbreitungsbedingungen bestimmt. Auf den unteren Netzwerkschichten werden hierdurch die Wahrscheinlichkeit einer erfolgreichen Frame-Übertragung und die nutzbaren *Modulation and Coding Schemes* (MCS) limitiert. Auf Ebene der Vermittlungsschicht ergibt sich hieraus die Übertragungsqualität (messbar im Sinne von Datendurchsatz, Paketverlust, Latenz und Jitter), wodurch letztlich auf den oberen Netzwerkschichten Eigenschaften wie Sprach- oder Bildqualität, Download-Geschwindigkeit oder das Reaktionsverhalten interaktiver Anwendungen limitiert werden.

Um in Situationen mit hoher Kanalauslastung dennoch jedem Gerät einen fairen Anteil an Sendezeit einzuräumen und Kollisionen zu vermeiden, erscheint eine zentrale Koordination sinnvoll. Berücksichtigt man jedoch die große Menge inkompatibler Kommunikations-

[1] Universität Rostock, Fakultät für Informatik und Elektrotechnik, Institut für Informatik, Lehrstuhl für Informations- und Kommunikationsdienste, 18051 Rostock, till.wollenberg@uni-rostock.de

systeme, die verschiedenen administrativen Bereiche, zu denen WLANs gehören, und die Tatsache, dass es sich bei manchen Spektrumsnutzern überhaupt nicht um Kommunikationssysteme handelt, erscheint die Durchführbarkeit eines solchen Ansatzes fragwürdig.

Der im folgenden vorgestellte, dezentrale Ansatz zur Verringerung der Problemfolgen basiert stattdessen darauf, dass jedes WLAN-Gerät versucht, den negativen Einfluss von Emissionen Dritter auf die eigenen Übertragungen zu minimieren und/oder sich an die gegebenen Umstände bestmöglich anzupassen. Je nach Netzwerkschicht können verschiedene Parameter angepasst werden:

- Auf Ebene der *Bitübertragungsschicht* kann ein WLAN-Gerät auf einen Funkkanal wechseln, der in naher Zukunft eine geringere Auslastung und/oder geringeres Interferenzniveau erwarten lässt. Ferner kann es MCS wählen, die zu kürzeren Übertragungen führen, um die Wahrscheinlichkeit von Kollisionen zu verringern sowie die genutzte Kanalbreite anpassen (z. B. keine Nutzung von 40-MHz-Kanälen). Bei erwartbarem anhaltend hohen Rauschpegel kann das Gerät zudem die für das Kanalfrei-Beurteilung genutzten Grenzwerte anheben.
- Auf Ebene der *Sicherungsschicht* von 802.11 können Parameter wie die Größe des Contention Window, Grenzwerte für die Frame-Fragmentierung und -Aggregation sowie die Strategie für Sendewiederholungen angepasst werden.
- Auf Ebene der *Darstellungsschicht* können Probleme, welche auf tiefer liegenden Schichten entstehen, in gewissen Grenzen ausgeglichen oder kaschiert werden, indem z. B. beim Media Streaming das verwendete Codec, die Quantisierung, Fehlertoleranz, Puffergrößen und/oder Paketierungsstrategie angepasst werden.
- Auf Ebene der *Anwendungsschicht* kann die Auswahl der Dienste und Anwendungen auf solche beschränkt werden, die unter den gegebenen bzw. erwartbaren Netzwerkbedingungen sinnvoll nutzbar sind. Zudem können nicht-interaktive bzw. Stapeldienste wie z. B. automatische Softwareupdates gezielt in Zeitbereiche mit erwartbar niedriger Kanalauslastung verschoben werden.

Obwohl o. g. Anpassungen grundsätzlich immer reaktiv erfolgen können, ist im Sinne der Nutzererfahrung eine proaktive Anpassung wünschenswert. So sollte bei erwartbar stark ausgelastetem Funkkanal für eine Videoübertragung von vornherein eine Kodierung mit niedriger Bitrate ausgewählt werden statt z. B. erst nach Unterbrechungen von einer hochbitratigen auf eine niederbitratige Kodierung zu wechseln.

Für eine **proaktive Anpassung** benötigen die beteiligten WLAN-Geräte neben Informationen über die aktuellen Signalbedingungen vor allem eine Vorausschau auf die zu erwartende Kanalauslastung. Diese sollte im Idealfall für alle verfügbaren WLAN-Funkkanäle vorliegen und die je nach Anwendung nutzbringenden Zeitspannen abdecken.

Um die zukünftige Kanalauslastung abzuschätzen, muss die Auslastung gemessen und im Zeitverlauf erfasst werden. Aufgrund des unterschiedlichen Einflusses auf WLAN-Übertragungen müssen hierbei verschiedene Quellen der Auslastung erkannt und unterschieden werden. In Abschnitt 2 wird ein Ansatz hierzu vorgestellt.

Die im Rahmen dieser Arbeit durchgeführten Untersuchungen fokussieren auf das u. a. für WLAN genutzte **2,4-GHz-ISM-Band**, da in diesem die Kanalauslastung aufgrund der hohen Verbreitung entsprechender WLAN-Geräte besonders problematisch ist. Die Mehrheit der in diesem Band verwendeten Funksysteme werden entweder direkt von Menschen bedient oder stehen in Zusammenhang mit menschlichen Aktivitäten. Da diese Aktivitäten typischerweise Regeln folgen (z. B. Tageszeit, Wochentag etc.) sind Muster in der Kanalauslastung zu erwarten, die sich für eine Vorhersage nutzten lassen. In Abschnitt 3 wird hierauf eingegangen.

Da die Kanalauslastung aufgrund der typischerweise geringen Reichweite von WLAN ein lokales Phänomen ist, müssen Messdaten für eine nutzbringende Vorhersage möglichst feingranular erhoben werden. In Abschnitt 4 wird ein Weg vorgestellt, um den Aufwand hierbei gering zu halten. Aus dem gewählten Weg der Teilung von Messergebnissen ergeben sich neue Herausforderungen im Bezug auf Datenschutz und Datensicherheit, welche ebendort umrissen werden, bevor in Abschnitt 5 ein Fazit gezogen wird.

2 Messung der Kanalauslastung

Historische Messdaten bilden die Grundlage für eine Vorhersage der Kanalauslastung. Daher muss die aktuelle Auslastung an jedem Ort, für den später eine Vorhersage erstellt werden soll, gemessen und im Zeitverlauf aufgezeichnet werden. Die Auslastung wird neben WLAN durch eine Vielzahl anderer Funksysteme verursacht. Während das für WLAN verwendete Kanalzugriffsverfahren (Carrier Sense Multiple Access with Collision Avoidance, CSMA/CA) durch logische[3] und physikalische Kanalfrei-Erkennung versucht, die Sendezeit zwischen sendewilligen Stationen fair aufzuteilen und Kollisionen (gleichzeitiges Senden mehrerer Stationen) zu vermeiden, gilt dies für andere Funksysteme nicht zwangsläufig. Einfache Messansätze wie z. B. auch das in 802.11k eingeführte *Channel Load*-Element geben nur die gesamte (mittlere) Kanalauslastung über einen gewissen Zeitbereich an.

Um eine Messung der Kanalauslastung zu erhalten, die der Kanalfrei-Wahrnehmung einer WLAN-Station nahe kommt, müssen jedoch die jeweiligen Quellen unterschieden werden. Dies ist bei Einsatz von Labormessgeräten [WM10], Software Defined Radios (SDR) [De10] oder begrenzt mit speziellen Funktionen einiger WLAN-Chipsätze möglich [RPB12]. Um eine breite Basis an datenerfassenden Geräten zu erhalten, sind demgegenüber jedoch geringe Hardwareanforderungen an die messenden Geräte wünschenswert. Im Rahmen der hier vorgestellten Arbeit wurde daher ein Ansatz gewählt, der zwei Datenquellen verbindet und geringe Hardwareanforderungen stellt:

1. Unter Einsatz seiner **WLAN-Empfangshardware** erfasst jedes teilnehmende Gerät die durch *WLAN-Aussendungen* auf dem aktuell vom Gerät verwendeten WLAN-Kanal verursachte Kanalauslastung. Hierbei wird ausgenutzt, dass jede WLAN-Station zunächst jeden korrekt empfangenen 802.11-Frame dekodiert und erst danach ggf. verwirft, falls er nicht für sie relevant oder fehlerhaft ist. Daher liegen

[3] Konzept des *Network Allocation Vector* (NAV), vgl. 802.11-2012 Kapitel 9.3

Informationen wie Zeitpunkt des Empfangs, Absender, Typ und Funktion des Frames sowie Kanal und Dauer der Aussendung grundsätzlich für jeden empfangbaren Frame vor bzw. können abgeleitet werden. Zusätzlich muss das Gerät die durch eigene Aussendungen verursachte Auslastung berücksichtigen.

2. Geräte, die die Möglichkeit dazu haben, erfassen zusätzlich den Signalpegel auf dem aktuellen und/oder weiteren Funkkanälen ähnlich einem **Spektrumanalysator**. Anhand des gemessenen Pegels kann dann entschieden werden, ob ein Nutzsignal (gleich welchen Ursprungs) oder Hintergrundrauschen vorliegt. Da hierbei keine hohe Genauigkeit erforderlich ist, können für diese Messung preisgünstige und energiesparende Ein-Chip-Lösungen für Schmalband-Anwendungen im 2,4-GHz-Band verwendet werden, die unabhängig vom WLAN-Interface betrieben werden.

Um die **durch WLAN verursachte Auslastung** zu ermitteln, wird getrennt nach Funkkanal für jeden Frame die Übertragungsdauer berechnet, wobei logische Größe, MCS, Guard-Interval, Präambeltyp und Frame-Aggregation berücksichtigt werden müssen. Aus der Summe der Übertragungsdauern im Verhältnis zur Anwesenheitszeit auf dem jeweiligen Funkkanal ergibt sich die durch WLAN-Übertragungen verursachte Kanalauslastung. Berücksichtigt werden müssen hierbei jedoch:

- Die Unterabtastung, welche bei WLAN-Clients durch Wechseln der Kanäle und durch zeitweises Abschalten der Empfangshardware (Energiesparfunktionen) entsteht. Sie betrifft vorwiegend Client-Geräte und muss in Form einer verringerten Gewissheit der Messergebnisse berücksichtigt werden.
- Interferenz von benachbarten Funkkanälen (Adjacent Channel Interference, ACI), welche im 2,4-GHz-Band aufgrund der überlappend definierten WLAN-Kanäle besonders relevant ist. Je nach Modulationsverfahren werden auf Nachbarkanälen ausgesandte Frames noch empfangen (bei DSSS, mit verringertem Signal-Rausch-Verhältnis) oder wirken wie eine Interferenz-Störung (bei OFDM).
- Frames, die aufgrund zu eines geringen Signalpegels oder einer Kollision nicht mehr empfangbar sind, werden in der Berechnung der durch WLAN verursachten Kanalauslastung nicht berücksichtigt.
- Dies gilt ebenso für Frames, deren Übertragungsverfahren vom messenden Gerät nicht unterstützt werden (MCS, Kanalbreite, Kodierung, Anzahl MIMO-Ströme).

Für die Ermittlung der **Gesamtkanalauslastung** mit Hilfe des Spektrumanalysators wird der verwendete Empfänger-IC auf eine geeignete Bandbreite konfiguriert (typisch zwischen 100 kHz und 500 kHz) und anschließend schrittweise so auf verschiedene Mittenfrequenzen abgestimmt, dass das gesamte Frequenzband abgedeckt wird. Zwischen den Neuabstimmungen wird jeweils der aktuelle Signalpegel ausgelesen. Im Versuch des Autors wurde hierfür ein CC2500 von Texas Instruments eingesetzt. Bei einer Bandbreite von 500 kHz wurden bei Abtastung des Bereiches 2.399–2.485 MHz ca. 3,7 Abtastungen je Sekunde erreicht, wobei der Signalpegel mit einer Auflösung von 1 dBm erfasst wurde.

Berücksichtigt werden müssen bei dieser Art der Erfassung:

- Der Zustand des Kanals (frei, belegt) muss anhand des gemessenen Signalpegels geschätzt werden. Hierzu muss ein geeignetes Modell eingesetzt werden, dass (ggf. adaptiv) Hintergrundrauschen und Nutzsignale trennt.
- Die Quelle des Nutzsignals kann nicht bzw. nur in geringem Umfang detektiert werden. In [Bl12] wird ein Ansatz hierzu vorgestellt.
- Die Empfangswege (Antenne, Vorverstärker etc.) von WLAN-Modul und Zusatz-IC unterscheiden sich, was sich u. a. in abweichenden Signal- und Rauschpegeln niederschlagen kann.

Im Ergebnis liegen bei geringem zusätzlichen **Hardware-, Kosten- und Energieaufwand** Messwerte sowohl für die durch WLAN verursachte als auch die gesamte Kanalauslastung vor, wodurch sich die durch sonstige (nicht als WLAN erkennbare) Übertragungen verursachte Auslastung rechnerisch ermitteln lässt. Die Zeitauflösung der WLAN-Messung ist hierbei sehr hoch; die Zeitauflösung für die Gesamtauslastung vom verwendeten Empfangs-IC abhängig.

Problematisch ist die Erfassung von Funksystemen, die selbst adaptiv arbeiten, d. h. bei erkannten WLAN-Transmissionen selbst nicht senden (z. B. Bluetooth mit Adaptive Frequency Hopping, AFH). Bei einer Vorhersage der Kanalauslastung äußert sich dies in einer Überschätzung der durch Nicht-WLAN-Systeme verursachen Auslastung. Ferner stößt das Verfahren an Grenzen, wenn WLAN-Module zum Einsatz kommen, die das in 802.11 definierte Verfahren zur Beurteilung der Kanalfreiheit i. d. R. auf Kosten anderer WLAN-Stationen abändern, um z. B. trotz hohen Interferenzpegels senden zu können.[4]

Um eine Vorhersage für die zukünftige Kanalauslastung zu erstellen, sind möglichst lückenlose historische Messdaten nötig, die möglichst viele Orte und WLAN-Kanäle abdecken. Um trotz der begrenzten Messmöglichkeiten *eines* WLAN-Geräts eine gute Datenabdeckung zu erhalten, können die Messungen verschiedener Geräte, wie in Abschnitt 4 dargestellt, kombiniert werden.

3 Analyse und Vorhersage

Im Ergebnis der im vorangegangenen Abschnitt beschriebenen Messung sowie nach Kombination mit Messdaten anderer Geräte wie in Abschnitt 4 beschrieben verfügt jedes am Verfahren teilnehmende WLAN-Gerät für seinen aktuellen Standort und jeden WLAN-Kanal über Informationen bzgl. der Kanalauslastung in der Vergangenheit in Form einer Zeitreihe, getrennt nach WLAN- und sonstiger Auslastung. Die Zeitreihe kann hierbei Lücken aufweisen und ist mit Unsicherheiten behaftet.

Es handelt sich typischerweise um eine **periodische Zeitreihe**, d. h. es treten sich wiederholende Muster auf und es gibt keinen globalen Trend. Für derartige Systeme bietet

[4] vgl. US-Patent 7.522.669

sich eine Analyse der Reihe im Frequenzbereich an. Bei den vom Autor im Rahmen von Langzeitmessungen der WLAN-Kanalauslastung in universitären Lehrgebäuden erhobenen Messdaten (siehe Abschnitt 4) zeigen sich in der Praxis eine Vielzahl relevanter Spektralkomponenten vom sehr hochfrequenten Millisekundenbereich (Folge des typischen Burst-Charakters paketorientierter Datenübertragungen) bis hin zu sehr niederfrequenten Komponenten (Tagesrhythmen, Wochentag/-ende, Semesterferien). Es überlagern sich eine Vielzahl von Effekten, so dass bei einer Analyse der Zeitreihe der Gesamtkanalauslastung mittels klassischer Ansätze wie z. B. der ARMA-Modellierung ein größerer Anteil an nicht durch das Modell erklärter Auslastung verbleibt, was die Qualität einer darauf aufbauenden Vorhersage verschlechtert.

Dieses Problem kann durch eine **Dekomposition der Zeitreihe** deutlich verringert werden. Hierbei wird die Zeitreihe unter Verwendung der zur Verfügung stehenden Zusatzinformationen in einzelne Komponenten zerlegt, welche jeweils besser durch Modelle beschrieben werden können, wodurch letztlich die Vorhersagequalität steigt. Als Grundlage der Zerlegung bieten sich Informationen aus den WLAN-Übertragungen selbst an, da sämtliche Kontrollinformationen unabhängig vom Datenteil der 802.11-Frames grundsätzlich unverschlüsselt übertragen werden und somit für jede empfangende WLAN-Station auswertbar sind. Konkret wurde folgende Zerlegung vorgenommen:

1. Die von jedem Access-Point ausgesandten *Beacon-Frames* haben eine feste Periode und nahezu konstante Größe, so dass ihr Anteil an der zukünftigen Gesamtauslastung leicht geschätzt werden kann.
2. Sonstige *Management-* und *Control-Frames*. Diese korrelieren stark mit der Anzahl der anwesenden Geräte. Die Geräteanzahl selbst kann aus den Messdaten rekonstruiert werden und weist i. d. R. ausgeprägte Muster im Zeitbereich auf.
3. *Datenframes* und direkt damit verbundene Control-Frames bilden eine eigene Komponente. Diese kann weiter nach einzelnen WLAN-Stationen zerlegt werden, welche besonders ausgeprägte Muster oder ein homogenes Verhalten zeigen.
4. Da die entstehende Kanalauslastung bei konstantem Datenvolumen signifikant vom gewählten Übertragungsverfahren (MCS, Anzahl MIMO-Datenströme etc.) abhängt, kann eine *Bereinigung* hierzu zusätzlich die Zerlegung verbessern.

Es gibt Situationen, die nur selten oder unregelmäßig auftreten (Feiertage, Semesterferien), so dass sie nicht oder nur bei Vorliegen sehr weitreichender Daten erkannt werden können. Hier kann die Zuhilfenahme von **Kontextfaktoren** wie z. B. Kalenderinformationen, Raumbelegungsplänen oder Wissen über Ferienzeiträume die Vorhersage verbessern, indem die Vorhersage für verschiedene Situationen (diskrete Zustände) getrennt erfolgt. Neben dem Problem der Verfügbarkeit maschinell auswertbarer Kontextinformationen ergeben sich hierbei jedoch im Hinblick auf die im folgenden Abschnitt beschriebene Verteilung entsprechender Informationen zusätzliche Fragen zum Datenschutz.

Bei einer Vorhersage der Kanalauslastung auf Basis wesentlicher Spektralkomponenten bleibt jedoch immer die Möglichkeit von Situationen, die von den bisherigen Mustern abweichen. Daher ist eine **Fehlererkennung** nötig, die ggf. die Vorhersage aussetzt und

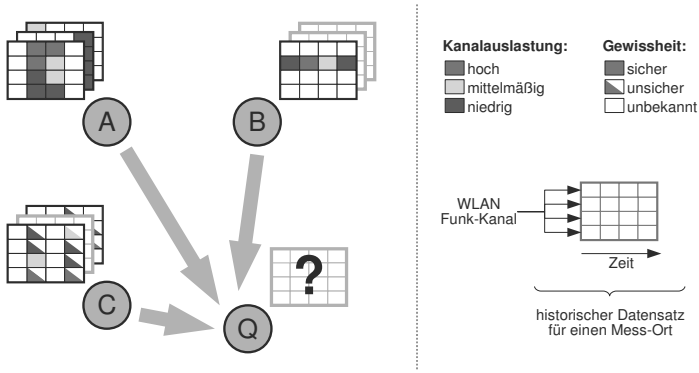


Abb. 1: Illustration zum Austausch historischer Messdaten zur Kanalauslastung zwischen WLAN-Geräten. Die Geräte A–C verfügen über lückenhafte Messdaten für verschiedene Mess-Orte. Die Daten unterscheiden sich in Zeitbereich, WLAN-Kanälen und der Gewissheit. Das neu hinzukommende Gerät Q verfügt nicht über eigene Messdaten. Es fragt daher die Daten von A–C ab und muss entscheiden, welche Daten genutzt und wie sie zu einem Gesamtbild kombiniert werden.

nötigenfalls historische Messdaten verwirft. Die Vorhersage kann zudem **Verdrängungseffekte**, die beim konkurrierenden Kanalzugriff verschiedener WLAN-Stationen und anderer (adaptiver) Spektrumsnutzer bei gesättigten Kanälen entstehen, nicht erfassen. Nutzt ein Großteil der anwesenden WLAN-Stationen eine Vorhersage auf ähnlicher Datengrundlage, können ebenfalls **Synchronisationseffekte** auftreten (mehrere Stationen beginnen simultan, einen als gering ausgelastet vorhergesagten Kanal zu nutzen), die durch Erweiterungen des Austausch- hin zu einem Koordinationsverfahren aufgefangen werden müssen.

4 Verteilte Messung und Datenaustausch

Mit dem in Abschnitt 2 beschriebenen Verfahren kann ein einzelnes WLAN-Gerät Messdaten zur Kanalauslastung erheben. Aufgrund der geringen typischen Reichweite von WLAN als Ergebnis geringer Sendeleistung und Dämpfung durch Wände etc. ist die Kanalauslastung jedoch nur am Messort bzw. in geringer Distanz zu diesem gültig. Um die zukünftige Auslastung an einem beliebigen Ort abzuschätzen, müssen daher Messdaten an möglichst vielen Ort aufgenommen werden. Da eine Installation dedizierter Mess-Systeme wie z. B. in [Zh13] vorgeschlagen mit hohen Kosten und/oder einer langsamen Verbreitung einhergeht, wird im folgenden ein alternativer Ansatz vorgeschlagen.

Hierbei nimmt jedes WLAN-Gerät, welches am Messverfahren teilnimmt, selbst Messdaten auf, soweit es seine Funktion nicht beeinträchtigt und mit Energiesparanforderungen vereinbar ist. Fest installierte Mess-Punkte können das System ergänzen. Die am Messverfahren teilnehmenden Geräte **tauschen dann untereinander ihre Messdaten aus**, so dass jedes Gerät seine Datensätze historischer Kanalauslastung vervollständigen kann. In Abbildung 1 wird das Konzept dargestellt: Hier erhält ein Gerät *Q* ohne historisches Wissen Informationen von drei verschiedenen Geräten, die jeweils Messdaten mit unterschiedlicher Zeit-, Kanal- und Ortsabdeckung sowie unterschiedlicher Gewissheit besitzen. *A* ist

mobil und kann auf allen WLAN-Kanäle Daten mit hoher Verlässlichkeit erfassen. *B* könnte z. B. ein Access-Point sein, der ortsfest ununterbrochen auf einem bestimmten WLAN-Kanal arbeitet; *C* ein mobiles Gerät mit begrenztem Energievorrat, das nur lückenhaft Daten erfassen konnte. *Q* muss diese Daten zu einem Gesamtbild kombinieren und über die Anwendbarkeit auf seinen aktuellen Aufenthaltsort entscheiden.

Hierbei müssen vier wesentliche Teilprobleme gelöst werden:

1. Jedes Gerät muss seinen **Aufenthaltsort** bestimmen können.
2. Die Ähnlichkeit zweier Messorte im Sinne der **Ähnlichkeit** der Messdaten zur Kanalauslastung muss ermittelbar sein.
3. Die Messdaten müssen in einem einheitlichen **Format** beschrieben sein.
4. Es muss ein **Verfahren zum Auffinden und Austauschen** von Messdatensätzen definiert sein.

Ferner ergeben sich im Bezug auf die praktische Umsetzbarkeit Forschungsfragen:

- Sind an einem Ort typischerweise ausreichend viele WLAN-Geräte präsent, um die Kanalauslastung lückenlos zu erfassen?
- Erlauben die Aktivitätsmuster der präsenten Geräte eine ausreichende Erfassung aller nutzbaren WLAN-Kanäle?
- Entsteht durch die Mobilität der Geräte ausreichend Austauschpotential für Messdaten?

Für die Orts- und Nähebestimmung bieten sich zunächst etablierte Positionsbestimmungssysteme wie z. B. GPS an. Neben dem Problem der schlechten Verfügbarkeit in Innenräumen ergibt sich primär das Problem, dass geographisch nahe Orte nicht zwangsläufig ähnliche Messergebnisse aufweisen. So werden zwei Messorte im Abstand von 2 m im freien Feld mit sehr hoher Wahrscheinlichkeit eine nahezu identische Situation aufweisen, während die Kanalbelegung völlig unterschiedlich ausfallen kann, wenn zwischen beiden Punkten eine Metall- oder Stahlbetonwand abschirmend wirkt.

Ziel muss daher eine **Nähedefinition** sein, die auf Ähnlichkeit der Beobachtungen abzielt und idealerweise geringe Anforderungen an die messenden Geräte stellt. Aufgrund der Tatsache, dass alle teilnehmenden Geräte mindestens über eine WLAN-Schnittstelle verfügen, bieten sich Fingerprint-basierte Verfahren an. Hierbei wird ein Ort über die dort empfangbaren WLAN-Stationen identifiziert. Access-Points und Clients können dabei unterschiedlich gewichtet werden, da erstere zumeist ortsfest sind.

Zur Bewertung dieses Ansatzes wurden in einer im Rahmen des Dissertationsvorhabens des Autors in einem universitären Büro- und Lehrgebäude durchgeführten Studie in zehn benachbarten Räumen Messgeräte installiert, die Daten zur Kanalauslastung auf WLAN-[5]

[5] erfasst wurden WLAN-Aussendungen nach den Standards 802.11b/g/n mit max. 2 MIMO-Datenströmen

und Spektrumsebene sowie die anwesenden WLAN-Geräte über drei Monate hinweg erfasst haben. Bewertet wurde u. a. die paarweise Ähnlichkeit der festgestellten Kanalbelegung in Abhängigkeit von euklidischer Distanz und Ähnlichkeit der Fingerprint-Mengen. Die in [WD13] ausführlich beschriebene Studie kommt zu dem Ergebnis, dass Fingerprint-basierte Nähedefinitionen grundsätzlich geeignet sind und bessere Ergebnisse im Bezug auf die Ähnlichkeit der Messdaten ergeben als der euklidische Abstand. Die Auswertung der Daten zu **anwesenden WLAN-Geräten** und deren Nutzungsverhalten aus der vorgenannten sowie einer weiteren, im selben Gebäude durchgeführten Studie ergab darüber hinaus eine hohe potentielle Mess-Abdeckung des Zeitbereichs sowie der WLAN-Kanäle.

Zum **Austausch von Messdaten** sind grundsätzlich verschiedene Ansätze mit individuellen Vor- und Nachteilen möglich:

- Ein Austausch *auf Ebene der 802.11-Sicherungsschicht*, d. h. zwischen WLAN-Stationen, die sich in Empfangsreichweite befinden. Da die austauschenden Geräte hierfür nicht zum selben (administrativen) Netz gehören müssen und insbesondere keine gemeinsame Konfiguration (Passwörter, Schlüssel, IP-Adressen) nötig ist, wird die Verbreitung der Messinformationen erleichtert.
- Ein Austausch *im lokalen Netz* auf Ebene der Netzwerk- oder Transportschicht. Dies schränkt den Austausch auf Geräte ein, die zum selben (administrativen) Netz gehören, bietet aber Vorteile im Bezug auf den Datenschutz (s. u.) und erlaubt überdies die Weiterleitung an Geräte, die sich nicht in unmittelbarer Nähe befinden, wodurch die Verbreitung der Messdaten innerhalb des Netzes beschleunigt werden kann.
- Ein *globaler Austausch* über das Internet, d. h. über einen oder mehrere zentrale Dienstanbieter[6], die Server zum Sammeln der Messdaten bereitstellen. Dies erlaubt eine schnelle Verbreitung der Messdaten, bedingt jedoch einen Internetzugang für jedes nutzungswillige WLAN-Gerät und verstärkt durch die zentrale Sammlung von Daten die nachfolgend umrissenen Datenschutzprobleme.

Der Austausch von Messdaten wirft Fragen zu **Datenschutz und -sicherheit** auf: So können aus den Messdaten u. a. Rückschlüsse auf Nutzungsmuster gezogen, Anwesenheitsprofile von WLAN-Geräten erstellt und anhand der Ortsbeschreibungen der Datensätze in gewissem Umfang Bewegungsprofile der Gerätenutzer rekonstruiert werden. Vorgesetzte könnten z. B. die Anwesenheitszeiten ihrer Mitarbeiter anhand der Präsenz persönlicher WLAN-Geräte ermitteln oder Einbrecher „gute“ Zeitpunkte für Straftaten bestimmen. Ferner kann ein Angreifer durch gezielte Verbreitung falscher Auslastungsinformationen den Betrieb legitimer Geräte beeinträchtigen (Denial-of-Service-Angriff) und/oder sich selbst Vorteile verschaffen. Diesen Problemen kann einerseits durch Pseudonymisierung und Anonymisierung in den Messdaten (Schutz der Privatsphäre Dritter) sowie andererseits durch kryptographische Verfahren wie Signaturen und Web-of-Trust-basierte Vertrauensmodelle (Authentisierung von Messdaten als Schutz vor Manipulationen) begegnet werden.

[6] ähnlich netzbasierter Ortsbestimmungsdienste wie *Google Location Services* und *Mozilla Location Service*

5 Zusammenfassung

Der Ansatz, mit WLAN-Geräten verteilt Messdaten zur Kanalauslastung zu erheben und untereinander auszutauschen, erscheint geeignet, um mittels Vorhersage vielfältige proaktive Optimierungen vornehmen, die schließlich zu einer besseren Spektrumnsnutzung und Verbesserung des Nutzererfahrung führen. Zusätzlich können die erfassten Informationen im **Monitoring** von WLAN-Installationen eingesetzt werden, wobei mit dem vorgestellten Ansatz trotz geringem Hardware-Aufwand eine höhere Orts- und Kanalabdeckung erreicht werden kann als mit den integrierten Diagnosefunktionen marktüblicher Enterprise-WLAN-Systeme. Die vorgeschlagene kosten- und energiesparend umsetzbare Messmethode erlaubt die Trennung von WLAN- und Nicht-WLAN-bedingter Kanalauslastung und bildet die Grundlage für spektrale Vorhersagemodelle. Den durch den Austausch von Messdaten entstehenden Vorteilen stehen Fragen des Datenschutzes gegenüber, die vor dem Einsatz sorgfältig abgewogen werden müssen. Das vorgestellte Gesamtkonzept kann aktuell verwendete, reaktive Optimierungsstrategien auf Basis lokalen Wissens entscheidend verbessern, jedoch ohne Erweiterungen bei starker Verbreitung durch Rückkopplungs- und Synchronisationseffekte an Grenzen stoßen. Eine Weiterentwicklung des Verfahrens hin zu einem konkreten Protokollvorschlag und ggf. einer Standardisierung ist wünschenswert.

Literaturverzeichnis

[Bl12] Bloessl, Bastian; Joerer, Stefan; Nordin, Noorsalwati; Sommer, Christoph; Dressler, Falko: SaFIC: A Spectrum Analysis Framework for Interferer Classification in the 2.4 GHz Band. In: 31st IEEE Conference on Computer Communications (INFOCOM 2012). IEEE, Orlando, USA, 2012.

[De10] Denkovski, D.; Pavloski, M.; Atanasovski, V.; Gavrilovska, L.: Parameter settings for 2.4GHz ISM spectrum measurements. In: 3rd International Symposium on Applied Sciences in Biomedical and Communication Technologies (ISABEL). Nov 2010.

[RPB12] Rayanchu, Shravan; Patro, Ashish; Banerjee, Suman: Catching Whales and Minnows using WiFiNet: Deconstructing Non-WiFi Interference using WiFi Hardware. In: Proceedings of the 9th USENIX conference on Networked Systems Design and Implementation. USENIX Association, S. 57–70, 2012.

[WD13] Wollenberg, Till; Dähn, Andreas: Empirical Study on Local Similarity of Spectrum Occupancy in the 2.4 GHz ISM Band. In (Jonsson, Magnus; Vinel, Alexey; Bellalta, Boris; Marina, Ninoslav; Dimitrova, Desislava; Fiems, Dieter, Hrsg.): Multiple Access Communcations, Jgg. 8310 in Lecture Notes in Computer Science, S. 113–127. Springer International Publishing, 2013.

[WM10] Wellens, Matthias; Mähönen, Petri: Lessons learned from an extensive spectrum occupancy measurement campaign and a stochastic duty cycle model. Mobile networks and applications, 15(3):461–474, 2010.

[Zh13] Zhou, Ruogu; Xing, Guoliang; Xu, Xunteng; Wang, Jianping; Gu, Lin: WizNet: A ZigBee-based sensor system for distributed wireless LAN performance monitoring. In: Pervasive Computing and Communications (PerCom), 2013 IEEE International Conference on. IEEE, S. 123–131, 2013.

Energy Efficient Ethernet in der Praxis

Sebastian Porombka[1], Gudrun Oevel[2]

Abstract: Der Beitrag untersucht die Fragestellung, zu welchen Energieeinsparungen die Verwendung des Protokolls Energy Efficient Ethernet (EEE) zusammen mit einer verbrauchsorientierten Optimierung der Anschlussgeschwindigkeit in einem typischen Campus-Netzwerks führen kann. Er zeigt, dass nach wie vor erhebliche Anstrengungen notwendig sind, um eine energie-effiziente Netzinfrastruktur zu implementieren.

Keywords: Studie, Netzwerk, Campus, Energieeinsparungen, Energy Efficient Ethernet, EEE, ALR, verbrauchsorientierte Optimierung

1 Einführung

Bei der Diskussion um Energieeinsparungen zur Stabilisierung des Weltklimas wird mittlerweile auch regelmäßig darauf hingewiesen, dass die zunehmende Vernetzung im Sinne der Stichpunkte „Always Online“ und „Internet of Things“ zu zusätzlichen Energiebedarf führt. Grundlegend dafür ist nicht nur die ständig wachsende Anzahl von Clients, sondern selbstverständlich auch der Energieverbrauch der dazugehörigen Netz-Infrastruktur [Ch08]. Für Hochschulen ist dieses Thema aber nicht nur auf der globalen politischen Ebene interessant, sondern auch ganz konkret vor dem Hintergrund von steigenden Anforderungen an die Infrastruktur bei maximal konstanten Finanzmitteln.

Im vom BMWi im Rahmen der Ausschreibung IT2GREEN (`http://www.it2green.de`) von Juni 2011 bis Mai 2014 geförderten Projekt GreenPAD (`http://www.green-pad.de`) haben sich die Autoren aus diesen Gründen intensiv mit dem Thema Energie-Management von Netzwerkkomponenten beschäftigt. Es konnte damals nachgewiesen werden [Oe14], dass Netzkomponenten im Gegensatz zu Clients und Servern (noch) nicht energieeffizient betrieben werden können, da sie über keine lastabhängige Energie-Optimierung verfügen. Dazu wurde gezeigt, dass der Energieverbrauch beim Betrieb von Netzkomponenten auch wesentlich abhängig ist von der Belegung der Switche.
Der Energieverbrauch setzt sich zusammen aus einem festen Grundverbrauch und zusätzlich einem geschwindigkeitsabhängigen Verbrauch pro belegtem Port [OP12]. Der Grundverbrauch hängt von der gewählten Architektur und der verbauten Switche bzw. deren Netzteilen ab. Der Energieverbrauch am Port ist extrem von der konfigurierten, aber nicht von der tatsächlich genutzten, Geschwindigkeit abhängig. Als Quintessenz wurde in den Untersuchungen von 2012 [OP12] daher festgehalten, dass man Energie beim Betrieb von

[1] Universität Paderborn, Zentrum für Informations- und Medientechnologien (IMT), Warburger Straße 100, 33100 Paderborn, sebastian.porombka@uni-paderborn.de
[2] Universität Paderborn, Zentrum für Informations- und Medientechnologien (IMT), Warburger Straße 100, 33100 Paderborn, gudrun.oevel@uni-paderborn.de

Netzinfrastruktur derzeit nur einsparen kann, wenn man konsequent nur das in Betrieb nimmt (Gesamtarchitektur, Anzahl der Ports, Geschwindigkeit pro Port), was man wirklich braucht und Überkapazitäten strikt vermeidet. Als Anforderung an die Hersteller wurde damals gefordert

- Ports müssen einzeln abschaltbar sein.
- Maßnahmen, um Energie bei niedrigen Auslastungen zu sparen, müssen flächendeckend umgesetzt werden. Als Beispiel wurde der Standard 802.3az Energy Efficient Ethernet (EEE) genannt.

Die Einsparung durch Änderung der Architektur und Verzicht auf Überkapazitäten wurde in [OP12] ausführlich behandelt. Da es damals in der Fläche noch keine Switche und Clients mit EEE-Implementierung gab, konnten an dieser Stelle noch keine Vergleichsanalysen in der Praxis ermittelt werden. Auch heute ist EEE in der Fläche noch nicht angekommen, so dass im vorliegenden Bericht insbesondere die Nutzung des Access-Netzes analysiert und versucht wurde die Verbindungsgeschwindigkeiten nach Bedarf einzuschränken. Dieses Verfahren wird im Folgenden als verbrauchsorientierte Optimierung bezeichnet.

2 Energy Efficient Ethernet

Der Verbrauch an elektrischer Energie durch Informations- und Telekommunikationstechnologien (IKT) steigt stetig. [La12] [La13] Offensichtlich ist das einerseits durch die stetig engere Vernetzung sowie durch stetig steigenden Datenverkehr [Ci08] [St09] und höhere Verbindungsbandbreiten zu erklären. Weltweit betrachtet wurde 2012 von einem Energieverbrauch von 42TWh für drahtgebundene und drahtlose Büronetzwerke ausgegangen [La12], [LNB12] sowie stetiger Wachstum bei fast allen Gerätetypen beobachtet. Ausnahmen waren 10/100 Mbit Switches. Scheinbar wurden alte Geräte für neuere Bandbreitenanforderungen außer Betrieb genommen und durch neue Komponenten ersetzt. Um diesen Trend zu dämpfen hat die IEEE im November 2006 [Be07] eine Studiengruppe „Energy Efficient Ethernet Study Group (EEESG)“ einbestellt, die Wege erarbeiten soll, den Energieverbrauch von Netzwerkverbindungen zu verringern. Mehrere Studien zeigen, dass in üblichen Netzwerken (Büro / Server) die Netzwerkschnittstellen in der meisten Zeit inaktiv sind und in der Zeit die volle elektrische Leistung brauchen. Eine typische 1 Gigabit (Gbit) Schnittstelle an einem PC oder Server kostet 0,5W [Re11], eine 10-Gbit-Schnittstelle werden schon 5W [B.07] verbraucht. Studien berichten auch von durchschnittlichen Auslastungen zwischen 5% [No07] (Desktop) und 30-35% [St09] (Server). Auch bei stark ausgelasteten Backbone-Switches geht die Literatur von Auslastungen $< 30\%$ aus.

Mit diesen Annahmen ging Ende 2007 aus der EEESG die „IEEE P802.3az Energy Efficient Ethernet Task Force“ hervor. Sie baute auf die Vorarbeiten der EEESG auf und sollte schwerpunktmäßig neue Protokolle und Hardwarekomponenten entwickelt werden, die Energie in Zeiten sparen, in deren Netzwerkschnittstellen ungenutzt sind. Zwei Ideen wurden in der Taskforce beleuchtet. Die erste Idee war die aktuelle Daten-übertragungsrate

nach dem Bedarf auszuhandeln. Ziel war es, den Effekt auszunutzen, dass Verbindungen mit niedriger Datenübertragungsrate auch einen niedrigeren Energiebedarf [GCN05][OP12] haben. Ist ein Übertragungskanal in der aktuellen ausgehandelten Verbindungsgeschwindigkeit unausgelastet, sollte eine niedrigere Datenrate ausgehandelt werden. Wird eine Verbindung ausgelastet, soll neu verhandelt werden. In der Forschung und in den Arbeiten der IEEE wird dieses Verfahren als „Adaptive Link Rate (ALR)“ [GCN05] [GC06] geführt. ALR könnte einfach implementiert werden, kränkelte aber an dem Problem, dass es bei der Neuverhandlung zu einem Ausfall der Verbindung von mehreren Sekunden [Br02] kommt. Es wurde an den Problemen gearbeitet [Ch10]. Schließlich wurde die Idee aber zu Gunsten der unten aufgeführten Lösung [NRW08] [Ha08] zurückgestellt. Unabhängig davon wurde an dem Themengebiet weiter geforscht. Bilal et al. publizierten 2012 eine umfangreiche Zusammenfassung der Forschungsstände in [Bi13].

Die Erweiterung, die durch den „IEEE 802.3az Standard“ entstanden ist, beschreib den neuen Zustand „Low Power Idle (LPI)“. Befindet sich eine Ethernet-Schnittstelle (PHY) in diesem Zustand, verbraucht diese nur noch einen Bruchteil der sonst notwendigen Energie. Je nach physikalischer Implementierung und ob die Betrachtung auf Client- oder Switch-Seite geschieht, liegen die Ersparnisse bei 60-90% [Re11] [LM09] [NRW08]. Schnittstellen, die sich im Zustand LPI befinden, können weder Daten senden noch empfangen. Um die Zustandsänderungen zwischen normalen Betrieb und LPI zu koordinieren, wurden im Standard Protokolle vereinbart, die es ermöglichen beide Teilnehmer abzustimmen. Wann die Zustandsänderungen passieren sollen, lässt der Standard offen. Hersteller können so selbstständig an den Algorithmen arbeiten, die diese Entscheidungen treffen und den störungsfreien Betrieb gegen die Energieersparnis abwägen.

Eine Energieersparnis lässt sich also mit LPI nur erreichen, wenn beide Teilnehmer den Standard implementieren. Kommunikationsmuster, die wenig Bandbreite verbrauchen, aber kontinuierlich die Leitung belegen, verhindern lange Einsätze von LPI und verringern dadurch die Energieersparnis. Solche Effekte können zwar mit Gegenmaßnahmen [Zh08] abgemildert werden, vermindern aber trotzdem die Einsparungen.

3 Methoden

Im Verlauf dieser Arbeit wird untersucht, welche zusätzlichen Einsparungen sich bei einer verbrauchsorientierten Optimierung im Sinne von Abschnitt 1 ergeben würden. Um die Idee aus der Standardisierung von 802.3az zur Einsparung von Energie durch Aushandeln der aktuell benötigten Portgeschwindigkeit auf ihre Relevanz zu untersuchen, wird folgender Ansatz gewählt:

1. Ports und deren Teilnehmer im Netzwerk beobachten und maximale gebrauchte Geschwindigkeit ermitteln,
2. Verbindungsgeschwindigkeit auf Switch-Seite entsprechend drosseln,
3. periodische Beobachtung der Entwicklung.

4. Erst wenn ein Port doch überlastet ist, eine höhere Verbindungsgeschwindigkeit freischalten, und diese merken.

Betrachtet werden nur Access-Ports, an die Endgeräte wie z.B. Computer, Telefone, Accesspoints angeschlossen sind. Verbindungen im Core-Bereich und im Rechenzentrum werden nicht angetastet. Anschlüsse werden zwischen 1 Gbit und 100 Mbit verhandelt. Zur Modellierung der Effekte einer solchen Geschwindigkeitsbegrenzung wurden zwei extreme Szenarien evaluiert:

- Szenario A: Die Auslastung des Vortages wird betrachtet. Hat sie den ganzen Tag die 5% nicht überschritten, wird für 24 Stunden eine Grundeinstellung von 100 Mbit eingestellt. Ansonsten wird frei verhandelt.
- Szenario B: Für jede Stunde am Tag wird die maximal nötige Geschwindigkeit durch die 5%-Regel bestimmt. Die Verbindungsgeschwindigkeit wird in diesen Stunden auf 100 Mbit gedrosselt.

Bei der Umsetzung in die Praxis werden mit diesem Ansatz bewusst folgende Einschränkungen in der Dienstqualität hingenommen: Netzausfall bei „Neuaushandlung“, wenn die Voreinstellung nicht passte, sowie Änderungen in der Verbindungs-Latenz. Neben der Energieersparnis, hat die Umsetzung folgende positive Nebeneffekte: Access Ports bekommen die Verbindungsgeschwindigkeiten, die eher an die Realität angepasst sind. Es ermöglicht eine verbrauchsorientierte Langzeit-Planung.

4 Ausgangssituation

Bei den Projektergebnissen aus GreenPAD hatte sich gezeigt, dass vollbelegte Switche pro Port energieeffizienter sind als nur teilbelegte Switche. Es stellt sich daher die Frage, wie viele Switchports in einer Netzinfrastruktur tatsächlich in Benutzung sind. Diese Frage ist auch beim Einsatz von EEE von zentraler Bedeutung.

Als Fallbeispiel demonstrieren wir ein typisches Bürogebäude, Bauteil O, an der Universität Paderborn, in dem Teile der Informatik mit hohen Anforderungen an die Netzinfrastruktur untergebracht sind. In jedem Mitarbeiterbüro im Bauteil O sind acht Netzwerkanschlüsse für im Schnitt zwei Mitarbeiter verlegt worden. Davon werden in der Regel zwei Anschlüsse für zwei VoIP Telefone und zwei weitere Anschlüsse für Notebook oder PC gebraucht. Der Rest ist für spätere Anforderungen, Drucker und weitere Computer vorgesehen. Diese Anschlüsse sind bereits auf Switche rangiert und üblicherweise auch schon in das passende Netz geschaltet und tauchen in der folgenden Darstellung als „nicht verbunden“ auf.

Diese Vorgehensweise hat im Betrieb den Vorteil, dass neue Netzanforderungen (z.B. neue Dose in Betrieb nehmen, Umschaltung in ein anderes VLAN) per Konfiguration auf den aktiven Komponenten vorgenommen werden können ohne dass ein Techniker vor Ort erscheinen muss. Um die tatsächliche Nutzung der Switchports zu erfassen, wurde zyklisch der Zustand aller Switchports gespeichert und ausgewertet.

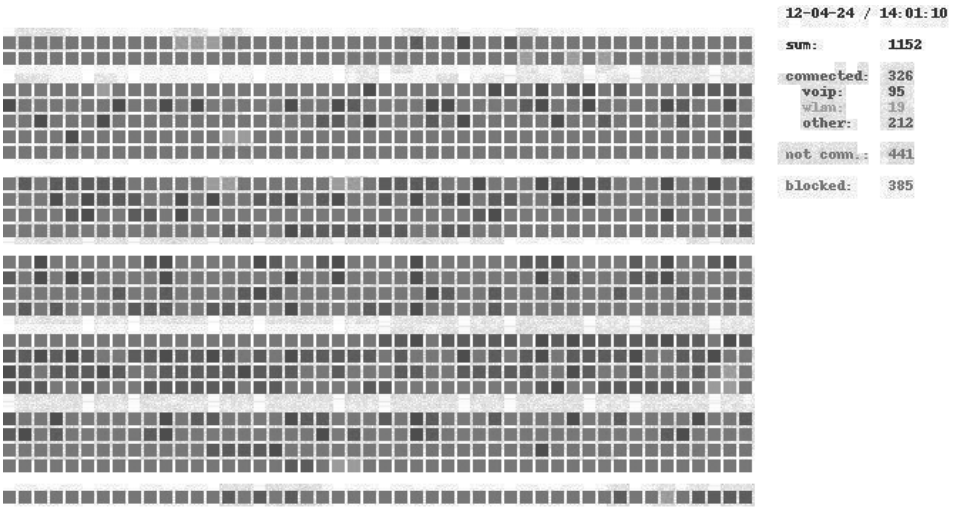


Abb. 1: Verwendung der Anschlüsse im Gebäude O während der Arbeitszeit

Abbildung 1 schlüsselt eine typische Verwendung der Switchports zur Mittagszeit auf. In diesem Moment wurden an 1.152 aufgelegten Anschlüssen 95 VoIP Telefone, 19 Accesspoints und 215 andere Geräte mit Netzwerk versorgt. Dazu gehören die PCs und Notebooks der Mitarbeiter, ein experimentelles Sensor-Netz, Drucker und andere Geräte. 438 Anschlüsse sind zwar für ein VLAN geschaltet, aber nicht verbunden. Die restlichen 385 Anschlüsse sind auf aktiven Komponenten gepatcht, aber deaktiviert. Grob gesprochen sind also von den insgesamt 1.152 Ports knapp 1/3 genutzt, ein weiteres knappes 1/3 für die Nutzung direkt vorbereitet und das restliche Drittel vorhanden, aber ungenutzt.

Abbildung 2 ist eine Momentaufnahme aus der Nacht. Offensichtlich haben (nur!) 37 Anschlüsse ihr Endgerät verloren. 178 Geräte sind noch am Netz, davon bereits abgezogen WLAN Accesspoints und VoIP Telefone. Knapp 10 Geräte haben, wahrscheinlich durch Standby-Zustände, ihre Verbindungsgeschwindigkeit auf 10 oder 100 MBit gesenkt, sind aber weiterhin online und warten darauf wieder aufgeweckt zu werden. 47 der 178 Geräte gehören zu einem experimentellen Sensor-Netz. Der Rest teilt sich auf Drucker, Mitarbeiter-Computer und Laboraufbauten auf.

Das Ergebnis überrascht, weil wir von der Arbeitshypothese ausgegangen sind, dass fast jeder Switchport, der von einem PC oder Laptop genutzt wird, nachts am Switch als inaktiv gesehen wird und entsprechend zum Stromsparen genutzt werden kann. Um im nächsten Schritt zu untersuchen, wie sich die Situation auf dem gesamten Campus darstellt, wurden alle Switchports im Abstand von 60 Sekunden an den Netzwerk-Switchen auf ihre Auslastung hin abgefragt. Durch den Vergleich mit der letzten Messung wird ein durchschnittlicher Bandbreitenverbrauch berechnet. Der Tag wird in Intervalle von 15 Minuten eingeteilt und die jeweils höchste Auslastung für jeden Switchport auf dem Campus in diesem Zeitraum vermerkt. Die Maximal-Werte im Viertelstunden-Intervall werden im Folgenden als Bandbreitennutzung bezeichnet. Anschlüsse, die mit 10 Mbit oder 100 Mbit

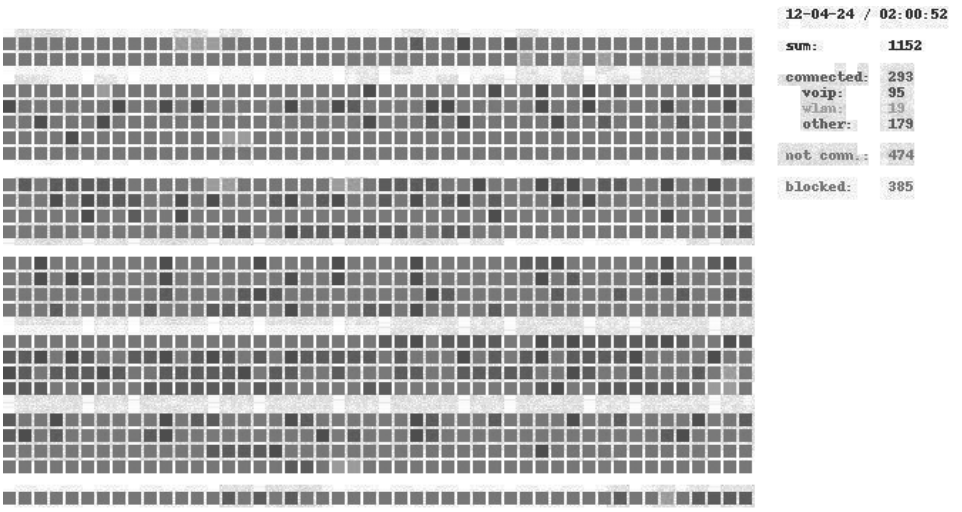


Abb. 2: Verwendung der Anschlüsse im Gebäude O in der Nacht

verbunden sind, betrachten wir als energetisch gleichwürdig genug um sie in eine Klasse für 100 Mbit einzusortieren.

Eine typische Auslastungssituation an einem Tag zeigt Abbildung 3. Aufgetragen sind alle Anschlüsse im Core-, Gebäude- und Access-Bereich. Ausgelassen sind alle Anschlüsse, die sich im Bereich des Rechenzentrums befinden. Neben den benutzten Bandbreiten sind ebenfalls die Zustände „shutdown“ und „notconnected“ verzeichnet. Ersteres beschreibt einen Anschluss, der administrativ durch die Verwaltung abgeschaltet ist und nicht benutzt werden kann. Als „notconnected“ wurden die Anschlüsse erfasst, die bereits einem Netz zugeordnet wurden und potentiell nutzbar sind. Allerdings befand sich zum Zeitpunkt der Messung kein Endgerät an dem Anschluss. In diesem Zustand befinden sich über den Tag zwischen 67% und 70% der Anschlüsse auf dem Campus.

Abbildung 4 schränkt die Sicht auf die reinen Access-Ports für Endgeräte ein, die auch aktuell verbunden sind. Neu hinzugekomme Ports sind meist per 1Gbit angeschlossen, die meisten davon davon mit einer Bandbreitennutzung < 5 Mbit. Eine Teilmenge der Anschlüsse, die mit 10/100 Mbit verbunden waren, verschwinden über den Arbeitstag. Es besteht die Vermutung, dass es sich hierbei um PCs oder Laptops handelt, die sich im Standby befinden und auf ein Wake-on-Lan-Signal warten.

Insgesamt muss in der Fläche, wie Abbildung 3 belegt, konstatiert werden, dass die Anschlussgeschwindigkeit deutlich überprovisioniert ist und fast alle Clients maximal 1% davon nutzen. Die meisten Ports sind aufgelegt, aber nicht in Nutzung. Im Tagesverlauf steigt die Anzahl der genutzten Ports, allerdings nicht signifikant. Auch hier zeigt sich also, dass die Implementierung von EEE zu erheblichen Einsparungen führen kann. Dies kann allerdings erst dann komplett umgesetzt werden, wenn alle Geräte, Switche und Clients den Standard 802.3az unterstützen.

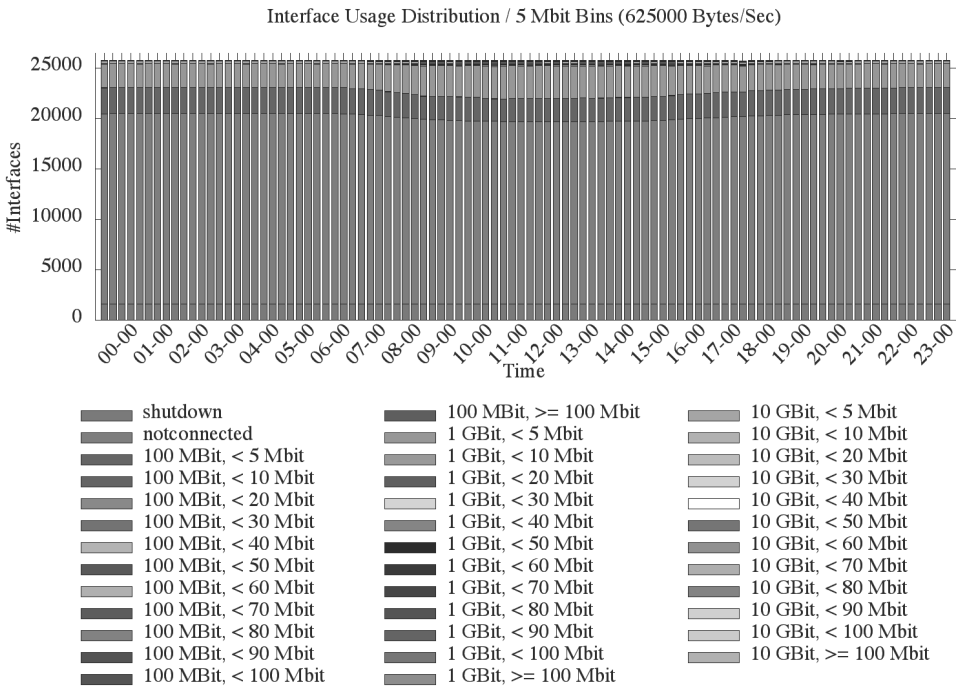


Abb. 3: Auslastung des gesamten Netzwerks über einen Tag

Dies führt zu der Fragestellung, welche Energie-Einsparungen man heute durch geschicktes verbrauchsorientiertes Provisionieren erzielen kann.

5 Einsparmöglichkeiten

Um diese Fragestellung zu eruieren, muss man zunächst wissen, welche Netzinfrastruktur im Einsatz ist und welche Effekte eine Änderung der Portgeschwindigkeit hat. Es erfolgt daher ein Überblick über die eingesetzten Geräte sowie deren Verhalten bzgl. Energieverbrauch.

Das Campus-Netz der Universität Paderborn, dessen Design an das „hierarchische Internetworking-Modell“ [Ci14] angelehnt ist, besteht aus den Bereichen „Core“, „Distribution“ und „Access“. „Core“ und „Distribution“ bilden das Grundgerüst des Netzes. In den Bereich „Access“ allen alle Komponenten, an die Endgeräte angeschlossen werden. Alle Switches im Bereich „Access“ wurden bei der letzten großen Modernisierung 2012 bis 2014 von der Firma Cisco gekauft. Aus der Produktpalette wurden modulare Switches der Baureihe Catalyst 45xx oder einzelne Geräte der Baureihe Catalyst 3560 gewählt. 77% der Switche im Access-Bereich fallen auf die Fabrikate WS-C4506-E, WS-C3560G-48PS und WS-C3560G-48TS sind. Die anderen 23% sind alte Switche, die sich in der

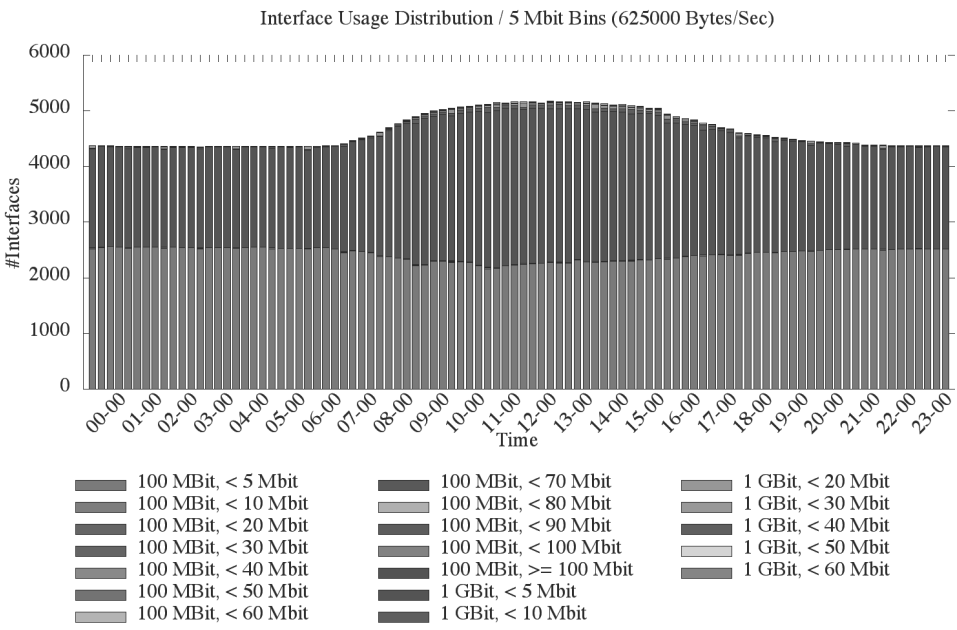


Abb. 4: Auslastung des gesamten Netzwerks über eine Tag, Eingeschränkt auf Accessports

Ablösung befinden. Die genannten 77% stellen 90% der Ports bereit. Deshalb wurden diese Fabrikate genauer untersucht und als Ziel für eine verbrauchsorientierte Optimerung genommen. Alle drei Fabrikate unterstützen im aktuellen Ausbau kein EEE. Sie wurden auf ihren Energieverbrauch in typischen Lastsituation (Belegung und Netzwerklast, siehe [OP12]) ausgemessen und zeigen als Ergebnis keine signifikante Abhängigkeit in der Energieaufnahme von der Auslastung, allerdings von der Portbelegung. Insgesamt stellen die so erhaltenen Ergebnisse die Berechnungsgrundlage zur Bewertung möglicher Einsparungspotentiale dar. Nach der großen Modernisierung wurden die neuen Catalyst 2960-x eingeführt, die nun als Ersatz für die 3560 in weiteren Modernisierungen eingesetzt werden. Ebenfalls gilt es zu prüfen, ob vielleicht Stacks aus Catalyst 2960-x als Ersatz für große Catalyst 45xx Monolithen vorstellbar sind. Diese wurden daher als Ergänzung zu [OP12] vermessen (Abbildung 5).

In Einklang mit den Herstellerangaben zeigen unsere Messungen, dass der Energieverbrauch im Vergleich zur Catalyst 3560 Serie deutlich reduziert ist. Auch identifiziert man einen Unterschied ob Endgeräte mit EEE oder ohne EEE angeschlossen werden. Man erkennt hier deutlich einen Trend in die Richtung energieeffizienter Netzwerkkomponenten. Allerdings ist es nur langfrisitg möglich den aktuellen Ausbau mit neuen Komponenten zu tauschen. Deshalb muss versucht werden in der aktuell vorherrschenden Infrastruktur kurz- bis mittelfristig Energie und damit die laufenden Kosten zu sparen. Um dieses Ziel zu erreichen, wurde der Versuch zur verbrauchsorientierten Optimerung durch das Aushandelns der Bandbreite abhängig vom Verbrauch, wird in dieser Arbeit in zwei verschiedene

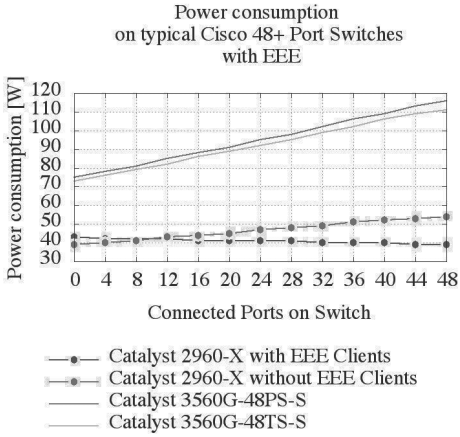


Abb. 5: Energieverbrauch Catalyst 2960-x, mit und ohne EEE kompatiblen Endgeräten

Varianten erprobt. Hierbei handelt es sich um sehr einfache Heuristiken, die ausgewählt wurden, um schnell einen Überblick über die möglichen Energiesparpotentiale zu ergattern.

Szenario A: Aus den Beobachtungen eines Anschlusses wird für 24 Stunden eine vorraussichlich maximal benötigte Verbindungsgeschwindigkeit berechnet und als maximal verhandelbare Geschwindigkeit auf der Switchseite gesetzt. Wird beobachtet, dass mit der niedrigeren Verbindungsgeschwindigkeit eine Auslastung von mehr als 5% besteht, wird diese Restriktion gelockert und eine schnellere Verbindung ausgehandelt. In diesem Moment gibt es einen Verbindungsausfall. Sinn ist es, Geräte mit durchgängig niedrigen Anforderungen auf eine niederigere Verbindungsgeschwindigkeit, und damit auf einen niedrigeren Grundverbrauch pro Port, herunterzuhandeln. Wir versuchen hiermit Teilnehmer mit sehr niedrigen Anforderungen zu identifizieren. Beispiele sind klassische Büro-Arbeitsplätze, Türterminals. Sensornetze, VoIP-Telefone usw. Im Falle einer plötzlichen Änderung des Verhaltens wird die Verschlechterung der Dienstgüte durch den Ausfall in Kauf genommen.

Szenario B: Ähnlich zu Szenario A. Allerdings wird für jede Stunde am Tag eine Voraussage getroffen, welche Verbindungsgeschwindigkeit nötig ist. Eine so genaue Vorhersage für ein Verhalten zu treffen ist relativ unwahrscheinlich. Auch macht es wahrscheinlich wenig Sinn, stündlich die Verbindung neu zu verhandeln und damit immer Ausfälle zu verursachen. Trotzdem hilft es als theoretisches Modell ein Gefühl für die Grenzen des Energiesparpotentials zu bekommen. Beide Varianten wurden in einer Simulation modelliert und wurden an einem Tag gegeneinander gerechnet.

Abbildung 6 zeigt das Ergebnis der Simulation von verbrauchsorientierter Optimierung der Portgeschwindigkeit auf den realen Daten an der Universität Paderborn. Aufgetragen sind jeweils Minimum und Maximum zu einem Zeitpunkt. Der zu erwartende reale Verbrauch liegt irgendwo zwischen den Kurven. Die rote und grüne Kurve bezieht sich auf

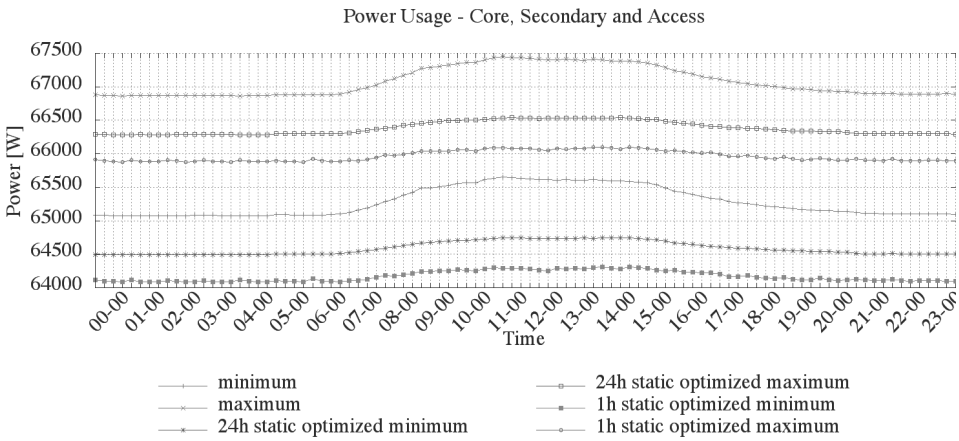


Abb. 6: Ergebnis der verbrauchsorientierten Optimierung

den Verbrauch ohne Optimierung. Die blaue und die lila Kurve zeigen die Ersparnis durch die Festlegung einer ganztägigen Beschränkung. Die hellblaue und braune Kurve visualisieren eine stündliche Anpassung auf Basis bekannter statistischer Werte. Sie bilden hier die erwähnte untere Schranke für den minimalen und maximalen Energieverbrauch. Es zeigt sich hier, dass eine verbrauchsorientierte Optimierung der Ports mit einer einfachen Heuristik – eine Größenordnung von 1.200 bis 1.800 Watt, das entspricht in etwa 50% des tatsächlich portabhängigen Verbrauchs – einsparen kann. Interessant ist auch der flachere Anstieg der Verbrauchskurve, was zur Stabilisierung der Stromnetze beitragen könnte.

6 Zusammenfassung und Fazit

Im Mittelpunkt des Beitrags stand die Frage nach der Implementierung von energieeffizienten Netzinfrastrukturen. Es konnte am realen Fallbeispiel der Universität Paderborn nachgewiesen werden, dass der Einsatz von Energy Efficient Ethernet (EEE) zu einer Senkung des Energieverbrauchs führen wird. Energetisch problematisch bleiben weiterhin die klassische Überprovisionierung beim Vorhalten von Ports und deren Anschlussgeschwindigkeit. Hier kann eine verbrauchsorientierte Optimierung heute insbesondere dabei helfen, Lastspitzen zu dämpfen. Insgesamt bleibt die energie-effiziente Implementierung von Netzinfrastruktur immer noch eine Herausforderung. Es könnte, z.B. in gut durchdachten Randfällen, ein bereits vorhandenes drahtloses Funknetz für kurzfristige Anforderungen oder Anwendungen mit geringen Bedarfen an Bandbreiten genutzt werden. Auch ist in dieser Arbeit nicht zwischen verschiedenen Verwendungszwecken von Gebäuden und Bereichen differenziert. So könnte es sein, dass es zwischen eher klassischen Bürogebäuden und Maschinenhallen unterschiedliche Verhaltensmuster gibt. Techniken aus dem Bereich SDN könnten helfen Ausfallzeiten im Moment der Neuverhandlung zu verhindern.

Literaturverzeichnis

[B.07] B. Kohl: 10GBASE-T Power Overview (Today). Energy Efficient Ethernet Study Group presentation material March 13-15, (March), 2007.

[Be07] Bennett, Mike: , IEEE 802.3 Energy Efficient Ethernet Study Group - Agenda and General Information, 2007.

[Bi13] Bilal, Kashif; Khan, Samee U.; Madani, Sajjad A.; Hayat, Khizar; Khan, Majid I.; Min-Allah, Nasro; Kolodziej, Joanna; Wang, Lizhe; Zeadally, Sherali; Chen, Dan: A survey on Green communications using Adaptive Link Rate. Cluster Computing, 16(3):575–589, 2013.

[Br02] Brown, Kevin: , 10/100/1000 Link Timing, 2002.

[Ch08] Chabarek, J; Sommers, J; Barford, P; Estan, C; Tsiang, D; Wright, S: Power Awareness in Network Design and Routing. Proc.˜of the 27th IEEE International Conference on Computer Communications (INFOCOM 2008), S. 457–465, 2008.

[Ch10] Christensen, Ken; Reviriego, Pedro; Nordman, Bruce; Bennett, Michael; Mostowfi, Mehrgan; Maestro, Juan: IEEE 802.3az: The road to energy efficient Ethernet. IEEE Communications Magazine, 48(11):50–56, 2010.

[Ci08] Cisco: Approaching the Zettabyte Era. White Paper, S. 23, 2008.

[Ci14] Cisco: Connecting Networks Companion Guide. 2014.

[GC06] Gunaratne, Chamara; Christensen, Ken: Ethernet adaptive link rate: System design and performance evaluation. Proceedings - Conference on Local Computer Networks, LCN, S. 28–35, 2006.

[GCN05] Gunaratne, Chamara; Christensen, Ken; Nordman, Bruce: Managing energy consumption costs in desktop PCs and LAN switches with proxying, split TCP connections, and scaling of link speed. International Journal of Network Management, 15(5):297–310, 2005.

[Ha08] Hays, R.: Active / idle toggling with low-power idle. IEEE 802.3az Task Force Meeting, (January):1–15, 2008.

[La12] Lambert, Sofie; Van Heddeghem, Ward; Vereecken, Willem; Lannoo, Bart; Colle, Didier; Pickavet, Mario: Worldwide electricity consumption of communication networks. Optics express, 20(26):B513–24, 2012.

[La13] Lannoo, Bart: Energy Consumption of ICT Networks. TREND Final Workshop, 2013.

[LM09] Larrabeiti, D; Maestro, J A: Performance Evaluation of Energy Efficient Ethernet. 13(9):697–699, 2009.

[LNB12] Lanzisera, Steven; Nordman, Bruce; Brown, Richard E.: Data network equipment energy use and savings potential in buildings. Energy Efficiency, 5(2):149–162, 2012.

[No07] Nordman, Bruce: , EEE Savings Estimates, 2007.

[NRW08] Nedevschi, Sergiu; Ratnasamy, Sylvia; Wetherall, David: Reducing Network Energy Consumption via Sleeping and Rate-Adaptation. S. 323–336, 2008.

[Oe14] Oevel, Gudrun: Abschlussbericht für das Projekt GreenPAD. Bericht, 2014.

[OP12] Oevel, Gudrun; Porombka, Sebastian: Zwischenbericht für das Projekt GreenPAD AP 1.3 - Energie-Management: Netzkomponenten. Bericht, 2012.

[Re11] Reviriego, P.; Christensen, K.; Rabanillo, J.; Maestro, J. A.: An initial evaluation of energy efficient ethernet. IEEE Communications Letters, 15(5):578–580, 2011.

[St09] Stobbe, Lutz; Nissen, Ing Nils F; Proske, Marina; Middendorf, Dipl Ing Andreas; Schlomann, Dipl Volksw Barbara; Friedewald, Michael; Georgieff, Dipl Volksw Peter; Leimbach, Timo: Abschätzung des Energiebedarfs der weiteren Entwicklung der Informationsgesellschaft. Computing, 7:178, 2009.

[Zh08] Zhang, Baoke Zhang Baoke; Sabhanatarajan, K.; Gordon-Ross, a.; George, a.: Real-time performance analysis of Adaptive Link Rate. 2008 33rd IEEE Conference on Local Computer Networks (LCN), S. 282–288, 2008.

Infrastrukturen für eResearch

Müller, Neumair, Reiser, Dreo Rodosek (Hrsg.): 9. DFN-Forum Kommunikationstechnologien,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2016 35

Schichtung virtueller Maschinen zu Labor- und Lehrinfrastruktur

Vitalian Danciu[1] Tobias Guggemos[1] und Dieter Kranzlmüller[1]

Abstract: Die Nutzung vieler Instanzen einer virtueller Infrastruktur für Laborversuche und Lehrveranstaltungen kann eine große Anzahl virtueller Netze und somit entsprechend hohen Managementaufwand erfordern. Diese Arbeit zeigt einen Ansatz zur Kapselung der virtuellen Komponenten und Netze einer Instanz mittels der Schichtung virtueller Maschinen. Die darin implizite Gruppierung der virtuellen Komponenten und Netze zerlegt die Gesamtmenge virtueller Entitäten in kleinere, leichter handzuhabende und dem Zweck der Instanz entsprechende Managementdomänen geringerer Komplexität. Anwendungen in der Lehre sowie in der Praxis illustrieren den Ansatz.

Keywords: virtualisierte Infrastruktur, Schichtung, Verschachtelung

1 Motivation

Der Einsatz von Virtualisierungstechnik erlaubt die Erzeugung virtueller Infrastruktur. Virtuelle Maschinen (VM) können mit virtuellen Komponenten der Sicherungsschicht verbunden werden und ergeben somit ein Netz, das für wissenschaftliche Versuche oder im Rahmen von Lehrveranstaltungen (Praktika, Demonstrationen) genutzt werden kann. Die Anzahl gleichzeitig einsatzbereiter *virtueller Labore* ist im Prinzip nur durch die verfügbaren physischen Ressourcen (Rechenleistung, Hauptspeicher, Sekundärspeicher) begrenzt, so dass sie als kosteneffiziente Alternative zu traditioneller Laborausstattung immer häufiger zum Einsatz kommen.

Während einzeln genutzte VM hauptsächlich durch ihre Konfiguration charakterisiert sind, ergeben sich die Eigenschaften des virtuellen Labors zusätzlich — und maßgeblich — durch seine Struktur (Topologie). Somit ist eine Laborinstanz enger an die spezifische *Virtualisierungsplattform* gebunden, die seine Komponenten und Verbindungen erzeugt sowie der Ausführung der Laborinstanz zugrundeliegt. Diese bietet in der Regel keine Sicht auf Strukturen, sondern Operationen zum Management einzelner Komponenten und Gruppen einzelner Komponenten. Während die Angaben zu Komponenten (z.B. Maschinenressourcen: RAM, Anzahl CPU) deklarativ vorliegen und somit einfach maschinell analysiert und bearbeitet werden können, wird die Topologie meist prozedural erzeugt, etwa durch Skripten, die die Virtualisierungsplattform ansteuern. Zudem erfordert der Betrieb virtueller Labore häufig eine große Anzahl virtueller Netzkomponenten. Diese Umstände erschweren das Management der virtuellen Labore sowie die Migration zu einer anderen Virtualisierungsplattform oder auch zu einer Instanz derselben Virtualisierungsplattform.

[1] MNM-Team, Ludwig-Maximilians-Universität München, Oettingenstr. 67, 80538 München, {danciu, guggemos, kranzlmueller}@mnm-team.org

Diese Arbeit stellt einen Ansatz zur wiederholten Anwendung von Virtualisierungstechnik vor, um die Struktur virtueller Infrastruktur zu kapseln. Abschnitt 2 analysiert ein Anwendungsszenario und formuliert Anforderungen an die Eigenschaften des Ansatzes, der in Abschnitt 3 vorgestellt wird. Abschnitt 4 beschreibt die konkrete Architektur eines Systems zur Erzeugung gekapselter virtueller Labore, ihre Umsetzung und ihren bisherigen Einsatz in der Praxis. In Abschnitt 6 werden verwandte Arbeiten gezeigt, bevor Abschnitt 7 die Arbeit abschließt und Einsatzmöglichkeiten in der Hochschullehre auf zentralen Rechenzentrumsressourcen sowie praxisrelevante Szenarien im Bereich der Network Function Virtualisation (NFV) diskutiert.

2 Analyse

Wir betrachten den Aufbau virtueller Labore anhand des Praktikums „Rechnernetze“ (RNP) am Lehrstuhl für Kommunikationssysteme und Systemprogrammierung an der Ludwig-Maximilians-Universität München. Das Curriculum beinhaltet Versuche auf der Basis von VM, wobei die einzelnen VM als Koppelkomponenten (Router) des virtuellen Labors oder als Endgeräte eingesetzt werden.

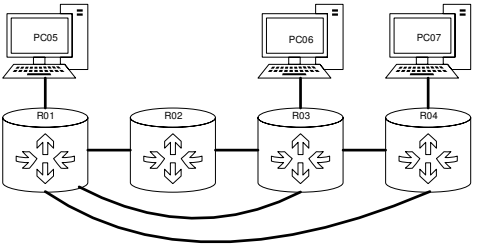


Abb. 1: Aufbau einer typischen Instanz des virtuellen Labors

Abb. 1 zeigt einen typischen Aufbau der Versuchsumgebung, die einer Gruppe von Teilnehmern zugewiesen wird. Sie besteht aus VM, die jeweils über mehrere (virtuelle) Netzschnittstellen verfügen. Jede VM ist mit einer Netzschnittstelle zum Zugang und Management („Managementschnittstelle“) ausgestattet. Die Verbindungen zwischen VM können als Portgruppen eines virtuellen Switch realisiert, oder als virtuelle Brücken/Switches umgesetzt werden. Wir bezeichnen diese Konstruktion im folgenden als *virtuelles Netz*.

Komplexitätsbetrachtung Abstrahiert von der derzeitigen Nutzungstopologie gehen wir von einem einfach vollvermaschten Netz für eine Instanz eines virtuellen Labors aus, also einem vollständigen Graphen mit $\frac{1}{2}(n^2-n)$ Verbindungen zwischen n Netzkomponenten. Hinzu kommen die Managementschnittstellen, die in einem Netz zusammengefasst werden. Für k Instanzen des virtuellen Labors ergibt sich die Gesamtzahl B an virtuellen Netzen bei n VM zu $B = \frac{k}{2}\left(n^2-n\right)+1$

Das polynomielle Wachstum der erforderlichen Anzahl virtueller Netze führt selbst bei bescheidenen Versuchsaufbauten zu unübersichtlichen Strukturen: $k = 20$ Instanzen eines virtuellen Labors mit $n = 4$ vollvermaschten Knoten (Abb. 2) benötigen der Gleichung entsprechend $B = 121$ virtuelle Netze. Bei den sieben Knoten für das Praktikum würde eine Vollvermaschung bereits $B = 421$ virtuelle Netze erfordern. Der Einsatz mehrerer physischer Maschinen zur Lastverteilung muss die Konnektivität zwischen den VM des Labors

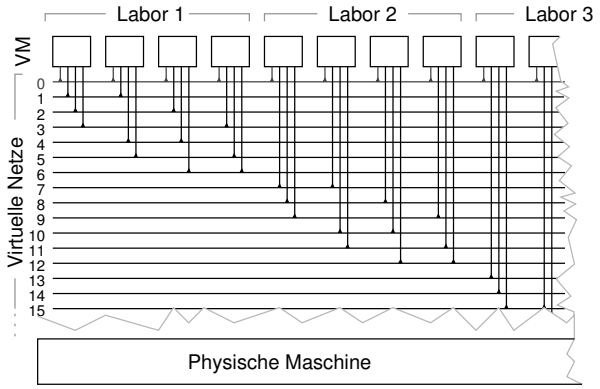


Abb. 2: Aufbau vollvermaschter virtueller Labore

gewährleisten. Gegebenenfalls müssen sich die virtuellen Netze über alle physischen Maschinen im Lastverbund hinweg erstrecken.

Betrieb Architekturbedingt stellen sich im Betrieb einige Herausforderungen. Die virtuellen Labore werden auf einem Rechnerverbund ausgeführt, der auch anderen Anwendungen dient (andere Lehrveranstaltungen, Projekte, etc.) und von einem Rechenzentrum (in diesem Fall dem Leibniz-Rechenzentrum München) betrieben wird. Es muss sichergestellt werden, dass andere parallel betriebene Anwendungen nicht gestört werden und kein unerwünschter Verkehr aus den Versuchen in das Hochschulnetz gelangt. Teilnehmer erhalten administrativen Zugang zu den Komponenten ihrer Laborinstanz, nicht aber zu der Virtualisierungsplattform, die sie erzeugt. Gelegentlich „haverierte“ Instanzen müssen somit von Lehrpersonal wiederhergestellt werden, was einen erhöhten Managementaufwand erzeugt. Die Managementdomäne der virtuellen Netze erstreckt sich über die gesamte Anzahl B dieser Netze. Managementaktivitäten wie etwa Suche und -diagnose von Fehlfunktionen können daher nicht die Partitionierung in Laborinstanzen ausnutzen, da sie sich nicht im Aufbau der virtuellen Infrastruktur widerspiegelt.

Wir formulieren folgende Anforderungen an die Konstruktion der virtuellen Labore. Die diese erfüllenden Konzepte sind in der weiteren Arbeit mit (Anf. <Nr>) gekennzeichnet.

1. *Erzeugung aus Modell.* Eine Laborinstanz soll ohne Betrachtung der Virtualisierungsplattform aus einem Modell bzw. einer Spezifikation (automatisch) erzeugt werden.
2. *Heterogene Modelle.* Die Koexistenz von Instanzen aus mehreren Modellen soll möglich sein.
3. *Wahlfreiheit der Hostplattform.* Der Aufbau soll geringe/keine Anforderungen an die Software der physischen Maschinen (Hosts) stellen.
4. *Archiv* Eine Instanz soll als Ganzes archiviert oder weitergegeben werden können.

5. *Skalierbarkeit* Die Kosten für Laborinstanzen sollen höchstens linear mit der Anzahl Instanzen wachsen. Die Skalierung bezieht sich auf die Nutzung der Ressourcen der darunterliegenden physischen Plattform, der Komplexität des Gesamtaufbaus aus allen Laborinstanzen und die Aufwendungen im Management.
6. *Isolation* Laborinstanzen sollen voneinander isoliert ausgeführt werden, so dass keine Kommunikationsartefakte "von außerhalb" durchdringen, z.B. keine Managementprotokolle der virtuellen Sicherungsschicht.
7. *Unabhängigkeit* Lastkontrolle/-verteilung auf den Hosts sollte auf der Basis der Instanzen erfolgen, statt auf der Basis einzelner Ressourcen.
8. *Beliebige Adressierung* Netze innerhalb der Laborinstanzen sollen unabhängig von der Umgebung mit beliebigen (auch in zwei Instanzen identischen) Adressen der Sicherungs- und Vermittlungsschicht versehen werden können.
9. *Nutzerzugang* Der Zugang zu jedem virtuellen Labor soll per Text- und Graphikschnittstellen möglich sein.

3 Ansatz

Der in dieser Arbeit vorgestellte Ansatz verfolgt die Erfüllung der Anforderungen aus Abschnitt 2 mittels Schichtung von Virtualisierungsumgebungen, also der Ausführung virtueller Komponenten auf der Basis darunterliegender virtueller Komponenten. Die Darstellung dieses Modells in Abb. 3 führt die folgende Notation ein:

0-VM bezeichnet die physische Maschine, die einen Hypervisor ausführt und in der Lage ist, VM und virtuelle Netze bereitzustellen. Wir nutzen die Bezeichnung „VM" für die Konsistenz der Notation.

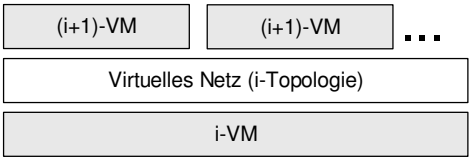


Abb. 3: Architekturprinzip

i-VM bezeichnet eine Maschine der Stufe *i*. Die VM, die direkt auf der 0-VM ausgeführt werden sind also 1-VM. Erzeugt eine 1-VM selbst virtuelle Maschinen, sind dies 2-VM, etc.

(i+1)-VM bezeichnet eine virtuelle Maschine, welche auf der Basis einer i-VM betrieben wird.

i-Topologie bezeichnet virtuelle Netze mit Netzkomponenten, die in einer i-VM erzeugt werden und (i+1)-VM verbinden.

Eigenschaften des Ansatzes Die Beziehung einer VM der Stufe $(i+1)$ zur darunterliegenden VM der Stufe *i* entspricht dabei einer Enthaltenseinrelation, also einer *Verschachtelung* der *inneren* $(i+1)$-VM in der *äußeren* *i*-VM. Diese Architektur hat die Eigenschaft, dass auch die virtuellen Netze der Labortopologie innerhalb der äußeren VM gekapselt

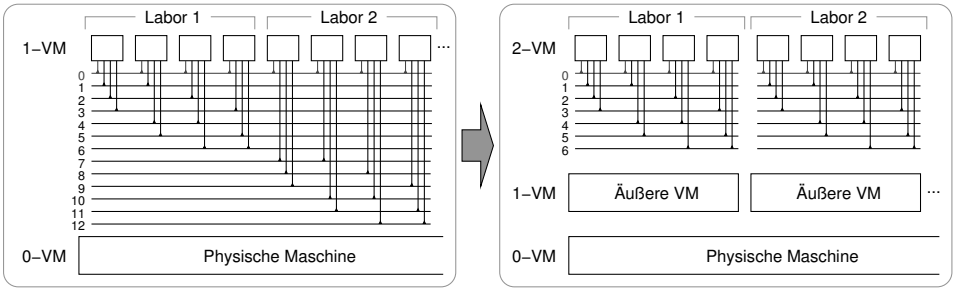


Abb. 4: Ansatz

werden (Anf. 6,7,8). Abb. 4 zeigt als Konsequenz für die Netze von in i-VM gekapselter virtueller Labore, dass die Anzahl in der identischen i-VM betriebenen Netze konstant bleibt, unabhängig von der Anzahl der Laborinstanzen (Anf. 5). Die Gesamtanzahl der Netze steigt durch die Kapselung des Managementnetzes um k, das heißt um eine zusätzliches virtuelles Netz pro Instanz.

Die ursprüngliche, alle Netze umfassende Managementdomäne zerfällt allerdings in jeweils den Instanzen entsprechenden Domänen. Eine Laborinstanz betreffende Managementaktivitäten werden somit konstruktionsbedingt auf diese eine Instanz beschränkt, was unter anderem auch heterogene Modelle ermöglicht (Anf. 2).

4 Entwurf

Wir betrachten nachstehend die prozedurale Erzeugung verschachtelter virtueller Infrastruktur sowie das Speicherkonzept für die Abbilder der sie erbringenden geschichteten virtuellen Maschinen.

Abb. 5 zeigt die Schritte zur Erstellung eines virtuellen Labors und ihre Eingabe: Die **i-Konfiguration** enthält Einstellungen einer i-VM (z.B.: IP-Adressen, Routen, Hostnamen; Konfiguration und Start von Diensten) (Anf. 9). Die **i-Topologie-Spezifikation** beschreibt Erstellung und Konfiguration virtueller Netzkomponenten innerhalb der i-VM sowie die Verbindung der (i+1)-VM mit den virtuellen Netzkomponenten. Die **(i+1)-Maschinen-Spezifikation** beschreibt die virtuelle Hardware für jede von einer i-VM verwalteten (i+1)-VM, z.B. Anzahl virtueller Prozessoren, Arbeitsspeicher, Netzschnittstellen.

1. Der *Startvorgang* beschreibt den Start einer Maschine mit *i-Konfiguration*. Falls eine i-VM keine (i+1)-VMs enthält, ist dies der einzig notwendige Schritt.

2. In der i-VM werden anhand der *i-Topologie-Spezifikation* virtuelle Netzkomponenten (Brücken/Switches) zwischen (i+1)-VMs erstellt.

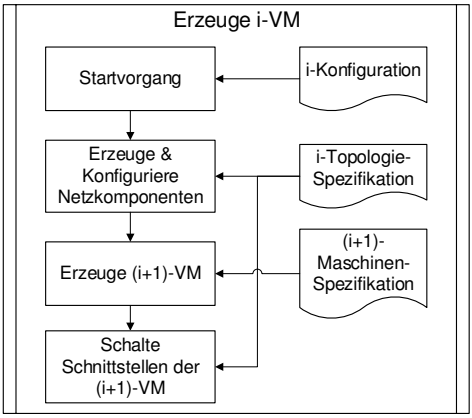
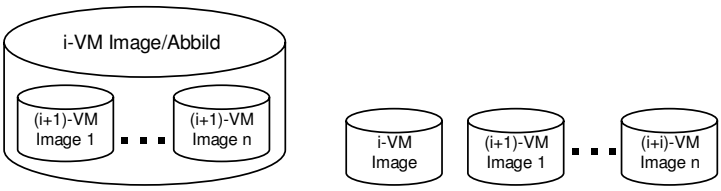


Abb. 5: Erzeugungs- und Konfigurationskonzept für VMs

3. Die in der *i-Topologie-Spezifikation* referenzierten (i+1)-VMs werden entsprechend der *(i+1)-Maschinen-Spezifikation* erzeugt und anschließend gestartet. Hier beginnt der *Startvorgang* der (i+1)-VM.

4. Entsprechend der *i-Topologie-Spezifikation* werden die Netzschnittstellen der (i+1)-VMs mit den Netzkomponenten der i-Topologie verbunden. Dieser Vorgang entspricht dem Stecken von Kabeln oder Schalten von Ports in einem physischen Netz.

Speicherkonzepte Für die Speicherung von Abbildern bzw. *Images* der (i+1)-VM innerhalb der i-VM sind zwei Ansätze denkbar (siehe Abb. 6). Bei der gekapselten Speicherung (Abb. 6a) enthält jedes i-VM-Abbild die Speicherblöcke der Abbilder „ihrer“ (i+1)-VMs. Im Gegensatz dazu sind im linearen Konzept (Abb. 6b) die Abbilder von i-VMs und (i+1) nebeneinander auf der gleichen Abstraktionsebene der Blockgeräte gespeichert.



(a) gekapselt (b) linear

Abb. 6: Speicherkonzept

Die Kapselung sichert die Konsistenz der Abbilder einer Laborinstanz auf Kosten der Einführung einer weiteren Blockabstraktion und dem damit verbundenen Leistungsverlust. Diese zusätzliche Blockabstraktion ist erforderlich, um Abbilder von (i+1)-VM, die als Dateien im Abbild der i-VM gespeichert werden, den (i+1)-VM als Blockgeräte (virtuelle Festplatten) zur Verfügung stellen zu können. Die Vor- und Nachteile des linearen An-

satzes sind invers: die ungekapselten Abbilder aller VM werden ungruppiert nebeneinander gehalten und sie können dadurch durch die gleiche Blockabstraktion genutzt werden; die Konsistenzerhaltung ist dabei nicht mehr durch die Konstruktion unterstützt sondern muss insgesamt als Managementaufgabe wahrgenommen werden. Beide Ansätze erlauben Archivierung (Anf. 4), wobei der gekapselte Ansatz diese intuitiver unterstützt.

5 Umsetzung am Beispiel RNP

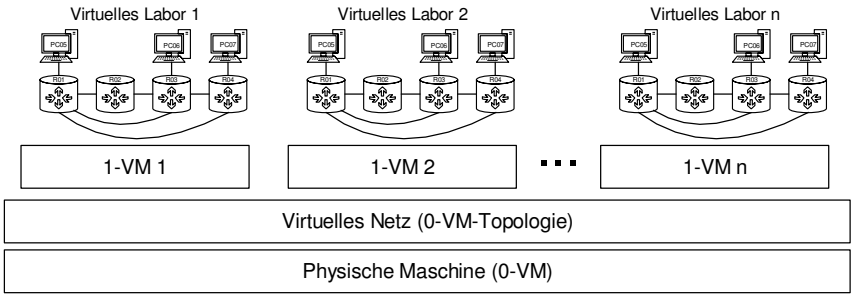


Abb. 7: Aufbau der Laborinfrastruktur für das RNP

Für das in Abschnitt 2 beschriebene RNP-Szenario wurde ein 3-stufiges System implementiert. Die 0-VM enthält für jeden Teilnehmer des Praktikums eine 1-VM, welche wiederum 2-VM mit dem im Praktikum eingesetzten virtuellen Labor enthält (siehe Abb. 7).

```
#How many routers and PCs should be created
NO_OF_ROUTERS=4
NO_OF_PCS=3

#Bridge definitions
BRIDGES="(1,2) (1,3) (1,4) (1,5) (2,3) (3,4) (3,6) (4,7)"
```

Abb. 8: Spezifikation der Verbindungen für ein virtuelles Labor

Die nötigen Topologie- und Maschinenspezifikationen (vgl. Abb. 5) werden aus einer deklarativen Angabe der Topologie generiert (Anf. 1). Aus der Angabe der Verbindungen zwischen VM (vgl. Abb. 8) kann die Anzahl erforderlichen Maschinen und die jeweilige Anzahl der Netzschnittstellen ermittelt werden. Die Maschinen werden unabhängig von ihrer Funktion als Router oder PC fortlaufend durchnummeriert, weshalb im Beispiel mit sieben Geräten Router01-04 und PC05-07 entstehen. Dies verdeutlicht die intendierte Rolle der VM aus didaktischen Gründen, ist jedoch technisch nicht erforderlich.

Die isolierten virtuelle Labore dürfen in jeder 1-VM bezüglich der Konfiguration (z.B. Adressierung) ihrer jeweiligen 2-VM identisch sein. Für jede i-VM werden die erforderlichen Konfigurationsdateien in einem Baum abgelegt, wie in Abb. 9 dargestellt. Sie werden in das Abbild der VM übertragen, bevor diese gestartet wird. Die Abbildung zeigt die

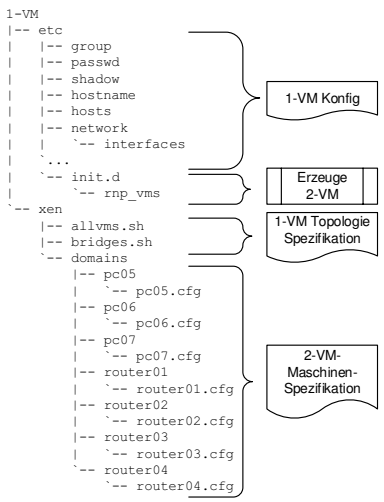


Abb. 9: Ordnerstruktur für die Konfiguration der Maschinen.

nötigen Dateien für eine 1-VM. Dies erlaubt einerseits Unterschiede zwischen VM der gleichen Stufe (z.B. verschiedene MAC- und IP-Adressen der 2-VM einer Laborinstanz) aber auch die Koexistenz verschieden bestückter 1-VM.

Szenariobedingt entschieden wir uns für das gekapselte Speicherkonzept. Im Allgemeinen scheint das gekapselte Konzept für Lehrveranstaltungen geeignet zu sein.

Auf Grund der Anforderung nach einer möglichst unangepassten 0-VM (Anf. 3), entschieden wir uns für den vom Linux-Kernel unterstützten KVM-Hypervisor in der 0-VM. Die 1-VM ist ein für Xen angepasster Linux-Kernel, da Xen einige Konfigurationsvorteile bietet. Beim Betrieb mit 25 Teilnehmern und ebensovielen Laborinfrastrukturen konnten keine für den Betrieb des Praktikums relevante Leistungseinbußen festgestellt werden.

6 Verwandte Arbeiten

Virtualisierung im Lehrbetrieb einzusetzen ist heutzutage keine Seltenheit und oft sogar organisatorisch alternativlos [Ga08]. Vor allem für systemnahe Kurse, in welchen Studenten Netzmanagement, Systemadministration oder Systemprogrammierung erlernen ist ein administrativer Zugriff oft unerlässlich. Virtuelle Maschinen bieten hier den unschätzbaren Vorteil, dass – vorausgesetzt sie sind richtig konfiguriert – viele administrative Aufgaben einfach und zentralisiert durchgeführt werden können. Vor allem ausschalten, zurücksetzen und abschotten bei Sicherheitsproblemen kann schnell und einfach vom Administrator des Hypervisors durchgeführt werden. Zusätzlich sind die Anschaffungskosten niedriger und Platz wird effizienter genutzt. Lindinger et. al [LRg08] zeigen eine nicht-geschichtete virtuelle Infrastruktur für einen praktischen Kurs in IT-Sicherheit und diskutieren die Anforderungen und Schwierigkeiten einer solchen Architektur.

In Forschungsprojekten sind virtuelle Labore wie etwa PlanetLab [Ch03] bzw. dessen europäische Variante PlanetLabEU entstanden. Dabei werden Teile einer international verteilten Infrastruktur (sogenannte *Slices*) einzelnen Forschungsvorhaben zugewiesen. Die darunterliegenden realen Netze erlauben dabei realitätsnahe Ergebnisse.

Die Idee virtuelle Umgebungen geschichtet bzw. verschachtelt (*nested*) zu implementieren ist so alt wie die Virtualisierung selbst und wird teilweise auch als rekursive Virtualisierung bezeichnet. Schon 1973 beschrieben Lauer et. al [LW73] die Möglichkeit, dass jeder Prozess seinen eigenen virtuellen Speicher definieren und verwalten könne.

Neuere Arbeiten beschäftigen sich mit der Optimierung von geschichteten Virtualisierungsumgebungen für verschiedene Plattformen und Anwendungsfälle. So verwenden Pan et al. [Pa11] KVM als Hypervisor wohingegen Ben-Yehuda et al. [Be10] und Zhang et al. [Zh11] den Xen-Hypervisor [Ba03] verwenden, der von Intel mittlerweile mit Hardwareoperationen unterstützt wird [ZD12], um die Performance zu verbessern. KVM [KI07] selbst unterstützt ebenfalls geschichtete Virtualisierung auch ohne Hardwaresupport, wird allerdings von Pan et. al auf Grund der schlechten Performance für ungeeignet im realen Betrieb betrachtet. Vor allem im Bereich des IO-Benchmarking zeigen Ben-Yehuda et. al beeindruckende Ergebnisse, wenn die IO-Zugriffe direkt an den Hypervisor auf Stufe 1 durchgereicht werden können. Alle Arbeiten gehen von einem Verlust der CPU-Performance von 4-6% aus, solange man maximal zweistufig geschichtet und entweder die Hardware oder der Hypervisor der ersten Stufe Hilfsmittel für Stufe 2 zur Verfügung stellt.

7 Zusammenfassung und Ausblick

Die praktische Arbeit im Labor ist ein wichtiger Bestandteil der Lehre und Ausbildung an Hochschulen und Universitäten und generiert eine hohe Anzahl von Einsatzmöglichkeiten. Um diese flexibel und effizient im Lehrbetrieb verwenden zu können, wird wieder einmal auf Virtualisierungstechniken zurückgegriffen. In diesem Papier wurde ein neuer Ansatz vorgestellt, mit dem sowohl die Kapselung, aber auch die Gruppierung von Netzen innerhalb einer virtuellen Infrastruktur ermöglicht und vereinfacht werden. Wir beschreiben sowohl die Anforderungen an eine solche virtuelle Laborumgebung, als auch den Aufbau und die dafür notwendigen Komponenten. Die vorgestellte Lösung wurde in der Praxis evaluiert und optimiert und wird seit einiger Zeit erfolgreich im Lehrbetrieb eingesetzt. Die damit erreichte Flexibilität und Skalierbarkeit hat sich als sehr wertvoll erwiesen, um schwankende Zahlen von Studenten in gleicher Qualität unterrichten zu können. Die Abschottung zur Außenwelt hat bisher keinerlei Beeinträchtigung des Betriebs im Wissenschaftsnetz ergeben.

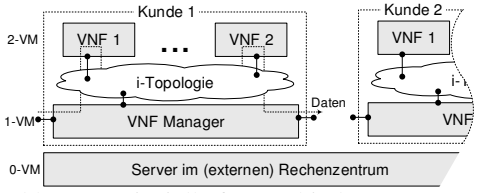


Abb. 10: Beispielhafte Architektur von geschichteter Virtualisierung für NFV.

Szenarien in der Praxis Die inhärente Kapselung der Netze einer geschichteten Infrastruktur erlaubt auch vielfältige industrielle Einsatzmöglichkeiten. Das „European Telecommunications Standards Institute“ (ETSI) beschreibt eine Architektur [ET14], in der mehrere virtuelle Netzfunktionen (VNF) miteinander verbunden und nacheinander ausgeführt und orchestriert werden, um zusammen einen Dienst zu erbringen. Die im Netz erforderlichen Dienste können aus sogenannten *Microservices* (z.B. Paketfilter, Wegewahldienste oder auch E-Mail, Spamfilter und Virenscanner) aufgebaut und von einem VNF-Manager orchestriert werden.

Legt man dieser Architektur eine zweistufig geschichtete Infrastruktur zugrunde, wie in Abb. 10 dargestellt, könnten die VNF in 2-VM instantiiert werden, durch virtuelle Switches verbunden und von einem VNF-Manager innerhalb der 1-VM orchestriert werden. Die Kapselung des so zusammengesetzten Dienstes ermöglicht sein Management als Ganzes (z.B. die Schaltung der Lebenszyklusphasen), seinen Betrieb auch in Rechenzentren dienstagnostischer, externer Betreiber (etwa Cloud/IaaS Anbieter) sowie seine Verschiebung zwischen Standorten.

Aktuell erweitern wir die bereits deklarative Topologiespezifikation um Angaben zur Konfiguration einzelner Komponenten sowie eine automatische Zuweisung von Adressräumen an die erzeugten Infrastrukturinstanzen. Ziel ist eine formale Sprache, mit der geschichtete virtuelle Infrastruktur beschrieben und anschließend erzeugt werden kann.

Literaturverzeichnis

[Ba03] Barham, Paul; Dragovic, Boris; Fraser, Keir; Hand, Steven; Harris, Tim; Ho, Alex; Neugebauer, Rolf; Pratt, Ian; Warfield, Andrew: Xen and the art of virtualization. ACM SIGOPS Operating Systems Review, 37(5):164–177, 2003.

[Be10] Ben-Yehuda, Muli; Day, Michael D. et al.: The Turtles Project: Design and Implementation of Nested Virtualization. In: 9th USENIX Symposium on Operating Systems Design and Implementation (OSDI 10). USENIX Association, Vancouver, BC, Oktober 2010.

[Ch03] Chun, Brent; Culler, David; Roscoe, Timothy; Bavier, Andy; Peterson, Larry; Wawrzoniak, Mike; Bowman, Mic: PlanetLab: an overlay testbed for broad-coverage services. ACM SIGCOMM Computer Communication Review, 33(3):3–12, 2003.

[ET14] ETSI: Network Functions Virtualisation (NFV); Architectural Framework. Group Specification RGS/NFV-002, European Telecommunication Standards Institute (ETSI), Dezember 2014.

[Ga08] Gaspar, Alessio; Langevin, Sarah; Armitage, William; Sekar, R.; Daniels, T.: The role of virtualization in computing education. ACM SIGCSE Bulletin, 40(1):131–132, 2008.

[KI07] KIVITY, Avi: KVM: The Linux Virtual Machine Monitor. In: Proceedings of the Linux Symposium. Ottawa, Ontario, 2007.

[LRg08] Lindinger, Tobias; Reiser, Helmut; gentschen Felde, Nils: Virtualizing an IT-Lab for Higher Education Teaching. In (Gesellschaft für Informatik e.V., Paderborn, Hrsg.): GI/ITG KuVS Fachgespräch "Virtualisierung". S. 97–104, 2008.

[LW73] Lauer, Hugh C.; Wyeth, David: A Recursive Virtual Machine Architecture. In: Proceedings of the Workshop on Virtual Computer Systems. ACM, New York, NY, USA, S. 113–116, 1973.

[Pa11] Pan, Z.; He, Q.; Jiang, W.; Chen, Y.; Dong, Y.: NestCloud: Towards practical nested virtualization. In: 2011 International Conference on Cloud and Service Computing (CSC). S. 321–329, Dec 2011.

[ZD12] Nested Virtualization Update From Intel, `http://docs.huihoo.com/xen/summit/2012/aug28/6a-nested-virtualization-update-from-intel.pdf`.

[Zh11] Zhang, Fengzhe; Chen, Jin; Chen, Haibo; Zang, Binyu: , CloudVisor: retrofitting protection of virtual machines in multi-tenant cloud with nested virtualization, 2011.

Müller, Neumair, Reiser, Dreo Rodosek (Hrsg.): 9. DFN-Forum Kommunikationstechnologien,
Lecture Notes in Informatics (LNI), Gesellschaft fuŕ Informatik, Bonn 2016 45

Improving Storage Performance with bcache in a Virtualization Scenario

Konrad Meier[1], Martin Ullrich[2], Dirk von Suchodoletz[3]

Abstract: The development of hard disk technology has not kept up with the general speed-up of computers and modern day technological developments like virtualization and cloud deployment. Flash storage, on the contrary, improves access speed and bandwidth significantly but at comparably higher costs. As in most scenarios only a fraction of the actual data stored on disk is ever used in arbitrary operation, a combination of both storage technologies can offer a good balance of speed and capacity. This resulted in tiered storage solutions offered by a range of commercial system providers. If the procurement of a new storage system is out of question, a Linux based flash cache approach can significantly improve performance of existing systems with moderate efforts in terms of setup and configuration.
This paper describes how an overloaded storage system primarily used as NFS based storage system for virtualization hosts could be brought back to operation by a multilayer data caching strategy to overcome high latencies and a low throughput. The resulting system design combines the benefits of high capacity slow spinning disk storage with flash only storage to a hybrid system. The presented approach was tested and evaluated in a real world productive environment. Various performance measurements and data are presented.

1 Introduction

Spinning magnetic disks were the backbone of permanent storage in computer technology for more than forty years. While the capacity was increased from some few Megabytes in the beginning to a several TeraBytes in modern day disks, this unparalleled development was not matched in terms of increased bandwidth and reduced access latency. Quite some effort was put into increasing the bandwidth and access times[4] of single disks, but the current technology has hit certain physical barriers. In particular, the access times have not changed significantly in the development of recent years [Wo09]. Storage manufacturers undertook quite some research to overcome those limits by combining multiple disks in complex configurations. But the exponential increase in storage demand and new applications like virtualization, cloud technology or big data easily outrun these developments. These applications usually generate random IO patterns, which are not handled well above a certain threshold by most traditional storage systems and appliances. This issue is fairly independent of whether directly attached disks, network attached storage (NAS) or storage area networks (SAN) are deployed. Especially, the additional layer of a network filesystem

[1] Computer Center, University of Freiburg, konrad.meier@rz.uni-freiburg.de
[2] Computer Center, University of Freiburg, martin.ullrich@rz.uni-freiburg.de
[3] Computer Center, University of Freiburg, dirk.von.suchodoletz@rz.uni-freiburg.de
[4] For a standard 15k RPM disk (e.g. Seagate Savvio 15K.3 300GB) the average latency is 2.0 ms and the disk seek-time for read operations is 2,6 ms. On everage this gives about 217 IOPS; The sequential read bandwidth depends on the position on the disk (outer edge or inner edge) and varies between 202 and 151 MByte/s.

as used with NAS can add to the problem. Nevertheless, a significant advantage of the network based solutions is a fast and easy live migration of virtual machines and a centralized data management.

In virtualization environments where a large number of virtual machines access files on the same NAS or SAN systems, traditional spinning disks are heavily challenged by the generated IO patterns. The reason is that each VM reads and writes into a different (large) file of the same storage. From the view-point of the storage system, the observed IO pattern is highly unpredictable.
Flash storage (in the form of solid state drives (SSD)) looks like the natural solution to this challenge as a single disk can easily handle multiple times of the bandwidth of spinning disks and especially since it is much more potent regarding IOPS[5] - 217 IOPS of an enterprise harddisk[6] compared to 28k (write) and 97k (read) IOPS of a SATA attached flash disk[7] (even more for special purpose devices like PCIe attached flash storage). Nevertheless, even with the evident decrease in price per Gigabyte, flash still cannot challenge magnetic hard-drives in terms of capacity.

Looking at the amount of accessed blocks on a storage system within a certain time frame reveals that most of the data is cold, meaning seldomly or never read. Only a small percentage is often accessed. Thus, transferring all data to flash is not required at all, but a proper strategy is needed to send hot data blocks to flash and keep cold blocks on magnetic mass storage. The state of the art solution to this problem is so-called tiered storage. It uses SSDs for caching to buffer data before being sent to the spinning drives [By12] [Ch15]. Actively used data is cached in flash, and cold-data is stored on spinning hard disks.

As many traditional and often expensive storage systems are still in use and cannot easily be replaced by betteperforming systems before their planned end of life, a cost-efficient but effective approach to bridge this time is required by many computer centers.

We evaluated a comparably novel multilayer caching strategy, which includes the use of memory-caching and SSD-caching. For the SSD-caching we used the block layer cache bcache[8] for which not much long term experience exists. The proposed solution is based on free open source software and utilizes commodity hardware. It is therefore usable in a wide range of applications. For example for applications like parallel storage in HPC[9], where large amounts of data, in some research workflows easily hundreds of TeraBytes, need to be stored and accessed for high performance processing. Back-end storage for cloud scenarios can be expected to profit as well.

[5] Input/Output Operations Per Second, an often used performance metric for storage devices.
[6] Seagate Savvio 15K.3 300GB; For calculation see footnote 4
[7] Samsung Enterprise SSD SM863 SATA 960GB
[8] bcache: Linux kernel block layer cache; [bc]
[9] HPC: High-Performance Computing

2 Initial Situation

The initial system without caching is given in Figure 1. As storage back end a system equipped with 56 x 3TB HDD and 4 x SSDs is used.[10] The SSDs are used as a read cache. The storage provided by the system is internally configured as a Dynamic Disk Pool [De15] and then exported as a LUN[11] over Fibre Channel. Internally every LUN is mapped to one of the two RAID controllers. The NFS server connects to the Storage System by two redundant 8 GBit/s wide Fibre Channel links. The system is using Fibre Channel multipathing provided by the Linux Device-Mapper. The imported block storage is mounted by the NFS server as an *ext4* filesystem to provide various NFS exports for the ESX Cluster over 10 GBit/s Ethernet. On the VMware ESX-Cluster[12] we have 150+ running VMs on five servers. Each host connects to the NFS server over NFSv3 and uses multiple 10 GBit Ethernet connections for redundancy[13].
The chosen setup was easy to use since new VMs could effortlessly be provided and automatically placed on the NFS datastore. The general challenge of this configuration lies in

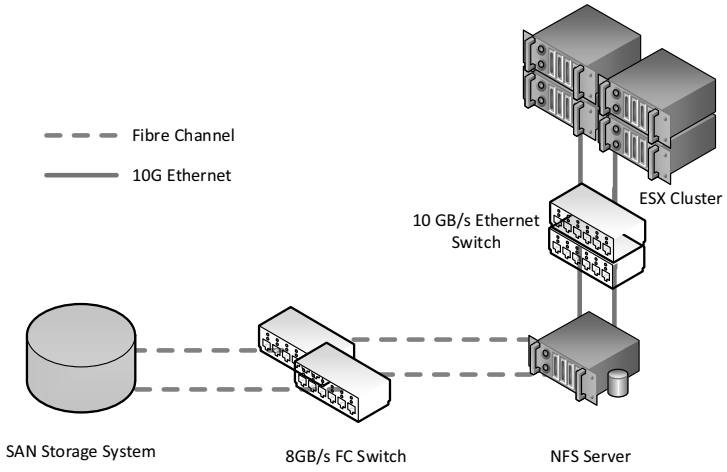


Abb. 1: Structure of the Virtualization Environment with shared NFS-based NAS

the complexity of the layered filesystem and block device setup. Within the VMs the OS is writing to a file which translates to a block IO like it would do in a physical machine. Because of virtualized hardware this block IO is translated to an IO on an open file on the storage handled by the virtualization hypervisor. This finally triggers a block IO on the network attached storage system.

[10] The system used is a DELL PowerVault-MD3660f dual-controller (active/active). The system was developed by LSI-Engenio (today NetApp) and is based on SANtricity. A widely available block storage product of similar features is offered by a number of manufacturers.
[11] LUN: A logical unit number identifies physical or virtual storage devices
[12] In this setup we used VMware ESX 5.5
[13] LACP configuration on the server and switches

A slow or delayed IO on the storage system looks like a failing block device to the operating system running inside a VM. At a certain threshold the OS is remounting the filesystem read-only (for data integrity reasons). To mitigate that scenario VMware tools (or open-vm-tools) usually increase SCSI timeouts[14] within the VM to prevent that a filesystem is remounted read-only too early. To save disk space, the container files are created using thin provisioning. Those files are constantly growing if a VM writes data to its disk. Since multiple containers are increasing in size parallelly, the container files are fragmented over time. This means that even sequential IO patterns from inside the VM do not necessarily write sequentially to the underlying storage system. For a storage system with spinning magnetic disks, fragmentation is therefore a problem since a lot of seeking operations are required to access data.

Challenges also arise from the NFS server side. In favor of performance the NFS client is often configured in *async* mode. This means that writing operations are acknowledged but not necessarily written back to storage system. Instead they are queued in RAM on the server. The opposite operation mode *sync*, ensures that every block is written, but significantly adds to latency as it has to wait for the underlying storage layer to complete the operation.
If the storage server is becoming congested, a long queue of blocks to be written builds up in the NFS server. This results in a large wait IO load that can stall the system entirely. It even might result in lost outstanding IO operations and the container files become corrupted. This corruption is much more dangerous than single files not properly written, as the files on the storage system are block devices to the virtual machines. Lost block writes may destroy filesystems and may render VMs unbootable.

The read and write pattern of the Virtualization environment is highly random. Every single VM generates only a small number of IO operations but in sum over all VMs the number of operations fluctuates between 1000 and 3000 IOPS.[15] Different problems were identified. Some VMs were configured with insufficient amount of RAM and started swapping to the storage system. Increasing the amount of RAM and removing the swap partition improved the situation to a certain degree. Moreover, the log file verbosity of some VMs generated a significant amount of (unnecessary) IO operations. In most cases it was no problem to set a less verbose logging behavior of the services.
The lack of a centralized backup system for the virtualization environment made it desirable that every VM itself writes a backup to an external backup system. This again generates a substantial amount of IOPS, especially at night during the backup runs.

The high number of IO operations leads to high IO latencies for some IO operations and could be measured within the virtual machines. An example output from the tool *fio*[16] looks like this:

[14] scsi device timeout: e.g. */sys/block/sda/device/timeout*; also refer to vmware knowledge base: http://kb.vmware.com/kb/1009465

[15] These values were readout directly from the storage system with the management tools provided by the manufacturer.

[16] Fio: Flexible I/O Benchmark; fio configuration: randread, size=8192MB; http://git.kernel.dk/?p=fio.git;a=summary

```
lat (usec) : 250=26.96%, 500=72.49%, 750=0.29%, 1000=0.07%
lat (msec) : 2=0.09%, 4=0.08%, 10=0.01%, 20=0.01%, 50=0.01%
lat (msec) : 100=0.01%, 250=0.01%, 500=0.01%, 750=0.01%, 2000=0.01%
lat (msec) : >=2000=0.01%
```

Most of the operations (>99%) are handled within one millisecond or less. But some operations require significantly more time. In some cases an operation even takes several seconds to be processed. In VMs this repeatedly led to long wait IO phases in which the VM had to wait for requested blocks. The reason for this is that for some IO patterns the spinning hard disks were not able to reposition and respond in time, causing high latencies for some IO requests in the storage system. With tools like *iotop*, *htop* and *vmstat* it was possible to analyze the situation on the NFS server. For example, a high amount of wait IO load is visible in *htop* and *vmstat*. The load was generated by the NFS kernel server waiting for block requests from the storage system.

3 Available Caching Solutions

For a SSD caching setup based on Linux, different approaches have been implemented over the last years:

- Flashcache [Fa]: Initially developed by Facebook and released as open source in 2011. It is implemented on top of the Linux kernel Device-Mapper of the Linux kernel.
- EnhanceIO [ST]: A fork based on Flashcache. In development since 2013. It implements a new write-back engine and is not based on the device mapper.
- dm-cache [dm]: Also based on the Linux kernel Device-Mapper framework. dm-cache was merged into the linux mainline kernel with version 3.9 (April 2013). It requires three devices to operate, a storage device, a caching device and a metadata device.
- bcache [bc]: Based on Linux kernel block layer. Bcache was merged into Linux mainline kernel with version 3.10 (June 2013). It is easy to use and configurable during operation through the proc filesystem. For example it is configurable if sequential IO is cached or directly written to the storage system.

Several authors have compared the different implementation approaches. The effect of Flashcache and bcache on I/O performance is evaluated in the work of Chritopher Hollowell et al. [Ho14] for a High-Energy Physics computing setup. In a white paper from Dell [AR13] the authors compare bcache and dm-cache as two caching solutions available in the Linux mainline kernel.

The possibility to cache write operations (write-back) is important in our case since random write operations were congesting our storage system. This is supported by all of the listed software solutions. To avoid a conflicting configuration, we decided not to use

dm-cache because we already used the Device-Mapper for our Fibre Channel multipath configuration. Instead we decided to use bcache because it is already in the kernel and is based on the Linux block layer.

4 Caching Setup

To overcome the poor IO performance within the virtualization environment a new NFS server with a multi-layer caching strategy was deployed. Two objectives were pursued. First, reducing the read operations in the back end storage system through a bigger read cache in the NFS server. Second, aggregating the random write operations to a more linear write pattern, by using a write cache in the NFS server.
For the first objective the amount of RAM in the storage node was increased significantly by the factor of 8 to 256 GByte. The RAM is only used as a read-cache because of its nonpermanent nature. Otherwise, in the case of power loss, data stored in RAM and not yet written would be lost.
For the second objective, Linux *bcache* is used as a read and write cache. Bcache is a kernel block layer cache, that allows to use SSDs as cache for slower hard drives. Bcache can be used as read and writeback cache at the same time.

For the new NFS server with bcache a complete new machine with the following specification was deployed: 2 x 8 Core Intel E5-2640v3 2.6 GHz; 256 GByte DDR4 RAM; Ethernet: 2 x 10 GBit/s; Fibre Channel: 2 x 8 GBit/s Fibre Channel Host Adapter; bcache Storage: 4 x 960 GByte Samsung SM863 Enterprise SATA SSD;

The additional CPU cores in the new server are used to start a high number of NFS server threads. In comparison to the old system we increased the number of server threads from 8 to 256. This allows to handle more NFS requests parallelly.
The two Ethernet interfaces are configured as LACP[17] network device. A RAID-Controller is used to configure the four SSD Drives as RAID 10[18]. RAID 10 was used because it is the best compromise between storage capacity, redundancy and performance. Choosing suitable SSD drives is a critical task. We expected a write stream of about 100 MB/s. This results in ˜8,4 TByte data written to the cache every day. A normal consumer SSD is specified for about 75-150 TBW[19]. We selected a middle class enterprise SSD Samsung SM863[20] with a specification of 6160 TBW. This gives an expected life-time of about 3 years. The connection to the storage subsystem remained unchanged (2 x 8 GBit/s Fibre Channel). The interaction of the components in the new NFS server is shown in Figure 2.

As a fast first level cache the RAM of the NFS server is used as a Linux kernel page cache. Unallocated RAM is used to cache data from the storage devices. About 236 GByte is used as file cache. Half of the file cache is marked as inactive. This means that this cache data

[17] LACP: Link Aggregation Control Protocol; IEEE specification for bonding of multiple network links.
[18] RAID 10: striped set from a series of mirrored drives
[19] TBW: TeraByte Written. Specifies the total amount of data that can be written to the disk before flash cells starts to die. For example the popular Sasmung 840 EVO 250 GB is specified for 75 TBW.
[20] Alternate SSDs considered were: Intel SSD DC S3610 800 GB with 5300 TBW; Sandisk CloudSpeed Ascend 960 GB with 1752 TBW; Toshiba HK3R2 960 GB with 1752 TBW

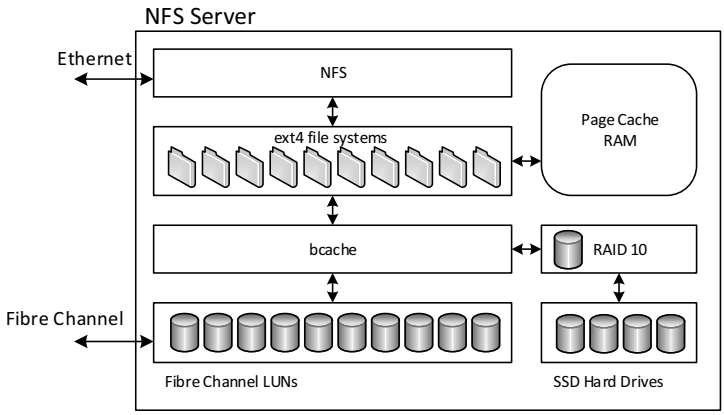


Abb. 2: NFS Server RAM and SSD caching structure

has not been accessed for a longer time period. The values are only changing slightly over time.

For bcache to work, a minimum of two block devices are necessary. A Cache-Device to store the cached data and a Backing-Device that should be cached. In our setup the RAID 10 device provided by the RAID controller is used as bcache Cache-Device. The Backing-Devices are the LUNs provided over Fibre Channel. To confine problems caused by corrupt filesystems, we decided to provide 10 x 2 TByte LUNs instead of a single 20 TByte LUN. Every LUN was then configured as Backing-Device and the resulting block device was formated with an ext4 filesystem. The resulting 10 filesystems are exported over NFS and used in the ESX cluster as NFS datastores. As shown in 2 a single Cache-Device is used to cache the 10 LUNs provided.

The default configuration of bcache can be modified by the proc filesystem. For our setup we activated the *write back* option and disabled *sequential cutoff*. With enabled *write back*, write operations are stored on the cache device (SSD) and later copied to the backing device. This allows bcache to collect write operations and write them to the backing device in a more sequential order. The *sequential cutoff* detects sequential write operations and redirects the operations directly to the Backing-Device. In our setup we disabled *sequential cutoff* to ensure that each write operation is made to the Cache-Device first. This way the number of write operations to our storage system is minimized.

5 Results

The new caching setup (RAM + bcache) reduces the IO latencies within the virtual machines significantly. The same fio test as stated before shows that the overall IO latency was reduced:

```
lat (usec) : 250=99.89%, 500=0.08%, 750=0.01%, 1000=0.01%
lat (msec) : 2=0.01%, 4=0.01%, 10=0.01%, 20=0.01%, 50=0.01%
lat (msec) : 100=0.01%
```

The amount of dirty data in the bcache fluctuates over time and is given in figure 3 for each Backing-Device. Some caching devices like bcache0 and bcache3 have to handle virtual machines with a more write intensive workload. The amount of dirty data for each caching device is limited to approximately 19 GByte[21]. It is possible to use more space as write cache, but first results show that the default configuration of bcache is sufficient. The figure shows the first eight days after start of the new caching setup. The migration of the VM Container files to the new cached datastores can be clearly seen as a spike in the figure. After this initial copy procedure, the VMs were powered back on and resumed normal operation. The read operations cache hit ratio for every cached device is given in

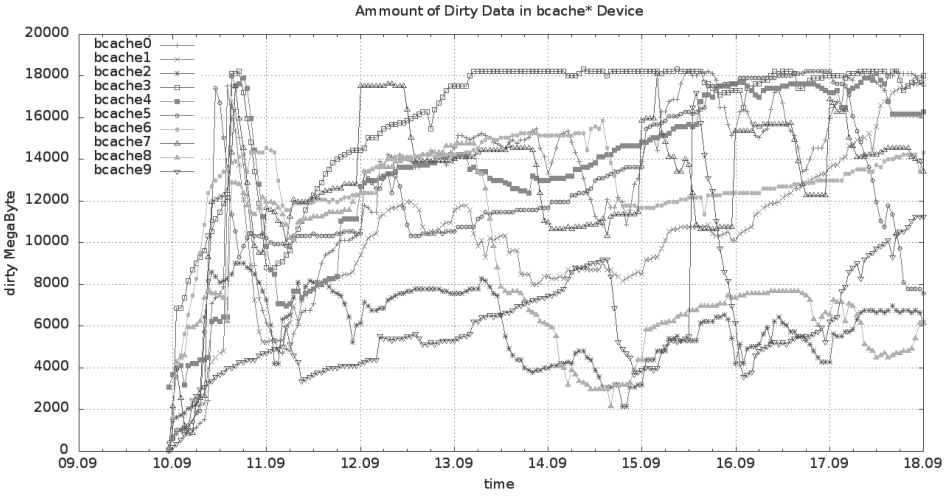


Abb. 3: Amount of dirty data in bcache devices over a period of eight days

figure 4(a-j). The ratio fluctuates heavily over time for some bcache devices. For bcache0 and bcache3 the average cache hit ratio is low, but the amount of dirty data in the cache is high. This suggests that VMs with a more write intensive workload are running on that data store.

Before the system was taken into production, several failure scenarios where tested to ensure that data written to the write back cache is not corrupted in case of an outage. For this a VM was writing a known data to a datastore and the bcache NFS server was rebooted, reset and disconnected from the power. In none of the tested scenarios data was lost or corrupted. After the server rebooted successfully the NFS client connection was restored and all write operations continued.

[21] Default bcache config: 10% of the caching device is used as write cache. This space is divided by the number of caching devices. In this setup: 1919, GByte * 0,1 / 10 = 19,193 GByte

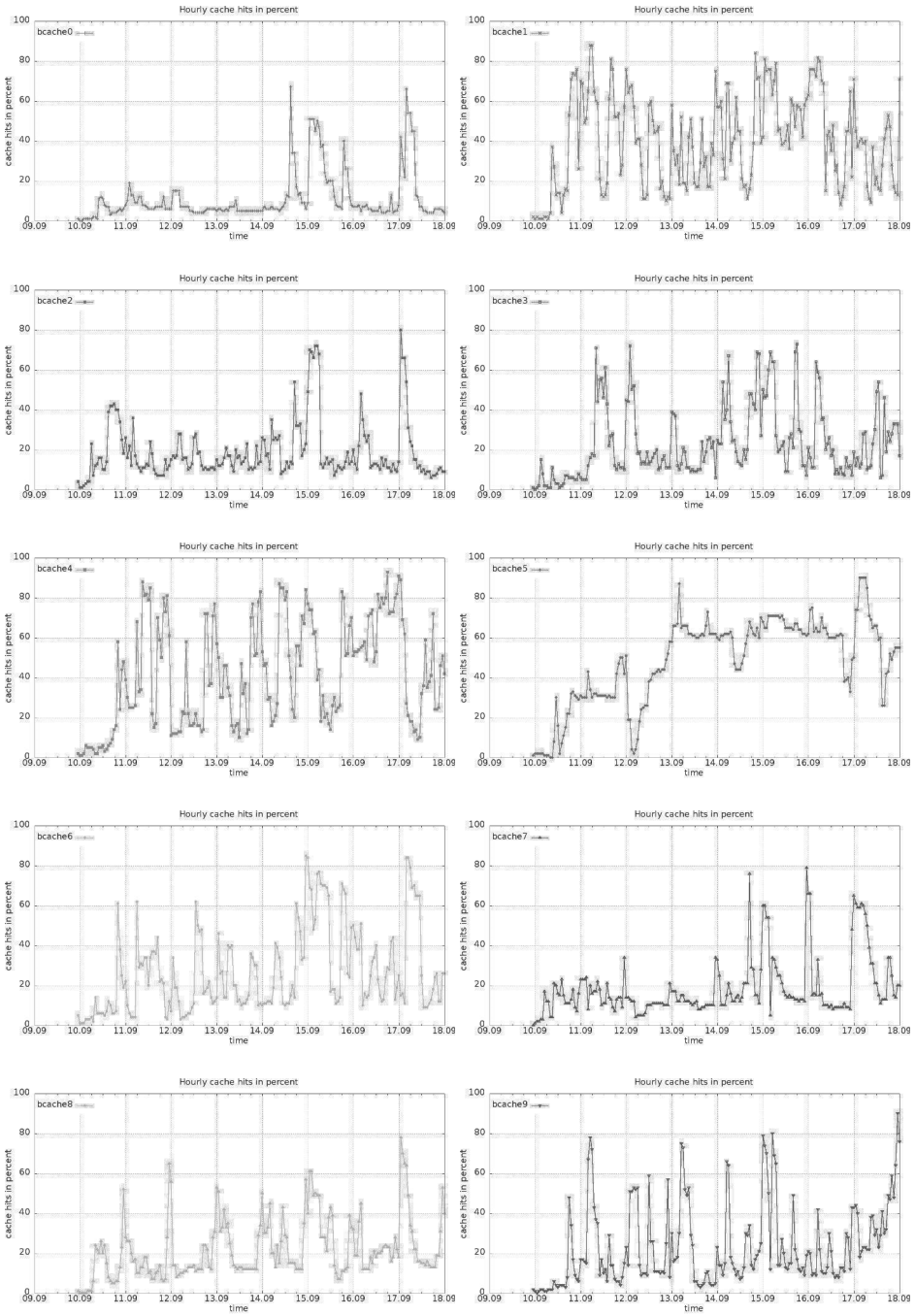


Abb. 4: Cache hit ratio for all 10 cached devices

6 Conclusion

The overall setup took less than two days to complete and migrate all data. The setup was designed in a way to allow a single SSD to fail and to get replaced without any downtime. In total we invested an amount of 10.000 Euro to bridge the gap until the new storage system is in place. The relatively moderate investment significantly improved the performance and even allowed to add new virtual machines (a process which was stopped due to the issues).
The setup has now been running for more than 4 month without any failure or data loss. The SSDs are permanently monitored to check for the amount of data written (TBW limit) and to look for possible failures. A total amount of 97.4 TB has been written to the bcache (SSD disks). This is significantly less than predicted (cf. section 4). The amount of data written by bcache corresponds to the values reported by the SMART from the disks. Due to the RAID 10 configuration every disk reports about 50 TB written.

Initial results show that the cache significantly reduces the load on the spinning disks as well as the overall I/O latency. Hot data is cached on the SSD drives and can be accessed much faster than the data on the spinning disks.

References

[AR13] Ali, Ahmad; Rose, Charles: , bcache and dm-cache - Linux Block Caching Choices in Stable Upstream Kernel. http://en.community.dell.com/cfs-file/__key/telligent-evolution-components-attachments/13-4491-00-00-20-43-81-99/LinuxBlockCaching.pdf, 2013. Accessed: 2016-1-10.

[bc] bcache. https://www.kernel.org/doc/Documentation/bcache.txt. Accessed: 2016-1-10.

[By12] Byan, S.; Lentini, J.; Madan, A.; Pabon, L.; Condict, M.; Kimmel, J.; Kleiman, S.; Small, C.; Storer, M.: Mercury: Host-side flash caching for the data center. In: Mass Storage Systems and Technologies (MSST), 2012 IEEE 28th Symposium on. pp. 1–12, April 2012.

[Ch15] Chen, X.; Chen, W.; Lu, Z.; Long, P.; Yang, S.; Wang, Z.: A Duplication-Aware SSD-Based Cache Architecture for Primary Storage in Virtualization Environment. Systems Journal, IEEE, PP(99):1–12, 2015.

[De15] Dell Storage Engineering: , Dynamic Disk Pools Technical Report. http://i.dell.com/sites/doccontent/shared-content/data-sheets/en/Documents/Dynamic_Disk_Pooling_Technical_Report.pdf, 2015. Accessed: 2016-1-10.

[dm] dm-cache. https://www.kernel.org/doc/Documentation/device-mapper/cache.txt. Accessed: 2016-1-10.

[Fa] Facebook Flashcache. https://github.com/facebook/flashcache/. Accessed: 2016-1-10.

[Ho14] Hollowell, Christopher; Hogue, Richard; Smith, Jason; Strecker-Kellogg, William; Wong, Antonio; Zaytsev, Alexandr: The Effect of Flashcache and Bcache on I/O Performance. Journal of Physics: Conference Series, 513(6):062023, 2014.

[ST] STEC EnhanceIO SSD Caching Software. https://github.com/stec-inc/EnhanceIO. Accessed: 2016-1-10.

[Wo09] Wood, Roger: Future hard disk drive systems. Journal of Magnetism and Magnetic Materials, 321(6):555 – 561, 2009. Current Perspectives: Perpendicular Recording.

Introducing Research Data Management as a Service Suite at RWTH Aachen

Thomas Eifert[1], Stephan Muckel[2], Dominik Schmitz[3]

Abstract: Research Data Management (RDM) receives more and more attention as a core component of scientific work. This importance equally stems from the scientific work with ever-increasing amounts of data, the value of this data for subsequent use, and the formal requirements of funding agencies. While these requirements are widely accepted among the researchers, the individual acceptance depends on many factors. In this paper we describe the initial steps at RWTH Aachen University to implement RDM as a widely accepted service suite. Here, service means appropriate IT solutions as well as a comprehensive training and support. The steps include the preliminary work to get the top management's awareness and the dialog with the scientists to learn the practical requirements. We present the initial solutions and solution concepts derived so far. We explain how our local approach relates to broader external initiatives. It is especially important that all these concepts together encompass a comprehensive suite of support offerings, guidelines, and various IT service modules built or planned on the underlying IT infrastructure.

Keywords: Research Data Management, Service introduction

1 Introduction

Research data is the outcome as well as the foundation of scientific work. Researchers need an environment that enables them to work efficiently and securely with their research data (cf. [KE13, EU10]. Currently, research data management (RDM) at RWTH Aachen is not as well-developed at all levels as to support the research process in an optimal way. Moreover, (inter)national research funding institutions, such as the European Union program Horizon 2020, the German Research Foundation and the Federal Ministry of Education and Research as well as various publishers (e.g. NATURE[4]), are increasingly requiring scientists and scholars to plan and execute good data management practices. An obligation to archive produced data already exists by carrying out "good scientific practice" [RW11], some even ask for the publication of primary data, e.g. the Open Data Pilot of the EU[5].

To fulfill these growing requirements and thus make research data accessible and usable for subsequent research projects has become an inevitable objective for all scientific institutions. Thus, structures and processes have to be established to relieve the scientists

[1] RWTH Aachen University, IT Center, 52056 Aachen, eifert@itc.rwth-aachen.de
[2] RWTH Aachen University, Central Administration, 52056 Aachen, Stephan.muckel@zhv.rwth-aachen.de
[3] RWTH Aachen University, University Library, 52056 Aachen, d.schmitz@ub.rwth-aachen.de
[4] http://www.nature.com/srep/journal-policies/editorial-policies
[5] http://europa.eu/rapid/press-release_IP-13-1257_en.htm

from these tasks and let them focus their primary work. For this reason, there are many (inter-)nationally coordinated activities as well as activities at federal state and local levels to tackle these questions. This contribution presents the local approach to combine and integrate these activities into the local infrastructure to prepare the path for the steps to come.

Domain Model The well-known domain model [KE13] visualized in Figure 1 has proven to be a valuable means to a common understanding and basic structuring of research data management. It distinguishes four domains where researchers act: the private domain, the group domain, the persistent domain and the public domain enabling access and reuse. Research typically starts in the private domain where a researcher mainly works alone on his or her data. Depending on the circumstances e.g. the project situation the need arises to share the data within the group domain. Typically this forces to explicitly add metadata well-known to the individual researcher but if not provided prohibiting an understanding by collaborators. Once publications have been written or, at least, at the end of a project, good scientific practice asks for long-term storage of primary research data. Again, the need to capture more descriptive information rises since it cannot be ensured that people that have produced data will be available once the data need to be accessed. This is obvious for the public domain which can be chosen to be addressed by a researcher at any time. Using the data requires a thorough understanding that is helped by an encompassing documentation with comprehensive and as far as possible standardized metadata.

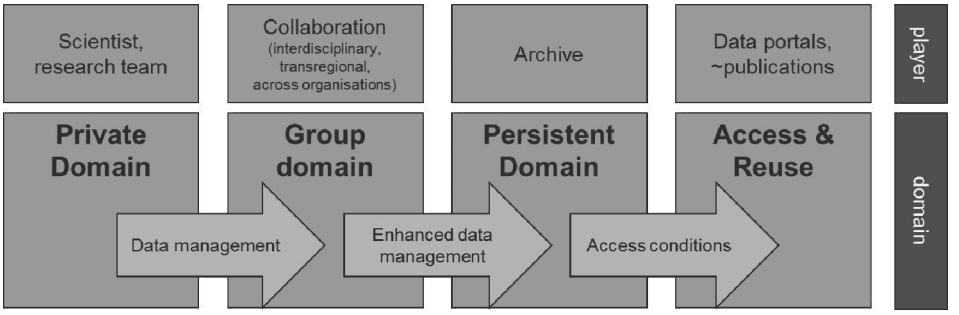


Figure 1: Domain model [KE13]

2 Initiating RDM: the Pre Project at RWTH

At the latest with the recommendations by the HRK, the German rectors' conference, [Ho14, Ho15] it has become obvious that universities as any other research institutes have to address research data management. When starting the project, we have observed similar approaches at many other places. Typically, three central institutions form the nucleus of a local project to establish research data management at an institutional level: the computing center for IT support and storage, the library for metadata and publishing

issues and the central administration in particular the part concerned with research funding. But a major concern is to get the researchers involved that are the addressees of such a service suite. Fortunately several national and international projects have been carried out or recently started, that address at least parts of these issues. We will refer to them throughout the rest of the paper.

2.1 Capture Current Situation

A typical approach to get the researchers involved is to simply ask them about their needs [Si14, Tr16]. The known surveys build on each other and the organizations are open to share their questionnaires which reduces the locally required efforts. Due to the already published survey results, we decided for the RWTH to start by a rather small sample of scientists that were interviewed in a structured manner. This analysis targeted at the creation of a starting point for planning an RDM infrastructure, to get into direct contact to communicate the aim of the project and to involve the affected scientists at the earliest point possible to address the "freedom of science" as well as fostering acceptance and awareness. Selecting the sample we took care of a broad coverage of criteria such as faculty, team size, age and gender, etc. The evaluation of the interviews later gave a good confidence that – at that level of detail – we got a reasonable coverage of all properties required.

The interviews were carried out along a self-developed guideline building on the experiences of larger surveys in particular [Tr16]. The invitation to participate in the interviews was sent by the University's top management, i.e. the rector. As a common result all scientists confirmed to already have methods for dealing with research data that accommodate their personal needs. Nonetheless, all observe a huge potential for improvement, in particular in regard to the improved capture of descriptive metadata that enable discoverability and reuse all alone. Yet they do not consider this a responsibility of their individual scientists or teams. Thus, while the survey did not bring up entirely new issues it ensured a mandate for a centrally organized service structure at RWTH.

2.2 Derived Requirements

The need for supportive services is seen consistently. But all interview partners stressed that any supportive service needs to be strictly user-oriented, intuitive to use, and easily be integrated into current research processes. In particular, we have to take into account the various discipline-specific repositories and virtual research environments that have been established over the last years. A CERN-related physicist has different processes and less local need than local laboratories with unique features. Thus, the functional and non-functional characteristics of a suitable service suite must be evaluated with respect to the local environment as well as national and international settings.

From the surveys and our own interviews we were able to derive requirements on future services for RDM support and non-functional qualities of these services that are essential

for acceptance. The different ranges of these qualities can directly be mapped onto the domain model (see Fig.1).

For the persistent domain, the predominant requirements are stability over time, an adequate metadata infrastructure to ensure discovery as well as scalability in size, since over time all research data will be stored here. Much more important than for the long term storage, the requirements to the UI for the daily “live” work, i.e., in the “private” and the “collaborative” domain, are very specific and very broad at the same time: The scientists expect traditional file system access as well as via web browser, through RDM systems or by cloud techniques, together with fast access to large resources and easy means to attach and link metadata to improve discovery, documentation, and reuse. We expect a further strong growth with respect to IT integration, for instance in the areas of experiment control and automated measurement systems, so the emerging solutions on this side will drive the way data as well as metadata is transferred to storage systems. Among these new scenarios are measurement systems which directly deliver raw data via cloud protocols and store the describing metadata in a database.

Common to all domains are the aspects of user-orientation, which means from the handling as well as from the functional perspective, and integration into existing workflows. On the other hand, the central institutions are not able to realize and maintain a homogeneous digitalized working space for each individual researcher. This will never scale. Accordingly, the challenge is to meet the right mixture of basic support and extensible infrastructure.

2.3 Support by University Top Management, Communication & Awareness

An important factor for success is that the university management – after internal discussion with all the stakeholder groups – starts by sending a clear, primarily internal, message that RDM will represent a key element of the university's ethos going forward. Publication of a "research data policy" in the form of strategic guidelines for RDM has often proven helpful in putting the subject of RDM at the top of the university agenda. Different University groups and committees are involved in the process to develop guidelines on research data management at RWTH. These guidelines, decided by rectorate in March 2016 [RW16], create awareness to take on responsibility for research data, to guarantee reproducibility, availability, and protection – including the protection of intellectual property –, and to provide functionalities concerning organizational, description/metadata, archiving, and reusability related aspects.

3 Current Project and Intended Solutions

The RWTH rectorate has taken responsibility for the implementation of HRK Recommendation of 2014-05-13 on the topic "Management of research data – a key strategic challenge for university management" [Ho14] and following the

recommendation of the RWTH Aachen CIO Advisory Board has decided to implement the following measures: establishing a holistic consultancy and support offer, a specification of resources (costs, persons), suitable awareness and acceptance activities, competence building teaching offers not only for researchers but also already for master students, strong need for prolific cooperation partners, stepwise introduction of suitable IT support, introduction of a suitable RWTH policy on research data management, and the establishment of a holistic IT support for the entire research process for at least three institutes at RWTH until mid of 2017.

3.1 Structure of the Project

To fulfill the university top management's tasks five modules have been established within the project. The module "awareness and acceptance" takes care of the very important communication activities. As also stated by the German Rectors' Conference [Ho15] this is a pivotal and major concern within a successful RDM project. As a specific part the setup of a broadly accepted "RDM policy" is established as a separate module. Further on, another major concern that is also very much related to awareness is the module on "consultancy and RDM teaching". It forms one of the central corner stones of the project. But without suitable IT support nobody will be able to establish a tangible research data management in our digital world, thus the equally urgent need for a module on "technical support". Yet, this module is not intended to resolve all problems by developing all solutions again locally. Thus, to achieve sustainable financing of RDM activities, a fifth module explicitly addresses "cooperations, partners and projects", thus building on initiatives such as the Research Data Alliance (RDA)[6] or the DINI/nestor working group on research data management[7].

In the following sub chapters we will present first glimpses on the intended solutions on consultancy and teaching offers as well as technical IT support that is embedded in the existing as well as externally developed IT infrastructure.

3.2 Consulting Services and Teaching

Already since 2014 the university library has established an introductory course for PhD students covering all basic aspects of research data management. It has been adapted to the feedback and is nowadays offered twice per semester. This introductory course serves as the foundation to elaborate an encompassing course offer that details out particular topics such as personal (meta)data management, data management plans, publishing and discovering data, collaboration, and archiving.

Regarding consulting services we currently follow two trails. On the one hand we have chosen a small number of dedicated institutes as scientific partners in the project to get

[6] http://rd-alliance.org
[7] http://www.forschungsdaten.org/index.php/AG_Forschungsdaten

real world experiences with the concrete problems researchers face during their daily work. The intention is to develop solutions for and with them during the project phase with the aim to derive more generic solution patterns that can be applied in similar institutes. The second trail is that we positioned the established Service Desk run by the IT Center as the single point of contact. The people from service desk are informed where to delegate questions as 2nd level support thereby hiding the complexity of separate institutions within the university supporting research data management (IT Center, library, central administration). For more complex problems, we plan a 3rd level that in fact realizes mini projects combining suitable forces from central institutions and the affected institute. The main purpose of this integrated set up is, to be able to scale. As more and more questions arrive at the service desk, the more repeated questions can be expected that can with growing knowledge then be answered already in the 1st level support while currently nearly all questions will be forwarded to the 2nd level.

In regard to the content of consultancy and teaching, we assist scientists with the creation of data management plans and advise them on their realization as well as on how to handle research data in their project. In particular, we help scientists to find a suitable metadata model for depicting their data or develop an appropriate solution together with them. Directories of standards and ontologies such as the RDA Metadata Standards Directory Working Group[8] typically serve as the starting point. In many cases domain specific approaches exist and are well suited to address researchers' needs.

3.3 Conceptualization of the Technical Infrastructure

The conceptualization of the technical infrastructure is driven by the observation, that a fully integrated and fully individualized monolithic digitalized working space for each individual researcher might be optimal in regard to meeting the user requirements (see Chapter 2.2) but it is unrealistic to be ever achieved by a single local institution. The span of domain- and discipline-specific requirements is simply too large. Accordingly, the solution concept foresees modularization and scaling options as the cornerstones of the technical infrastructure. In addition, only by reconsidering existing services – locally as well as provided by external partners or services at national or international level – and incrementally adding new services the introduction of a holistic service suite for research data management becomes feasible.

We basically distinguish between two aspects: for one there must be enough place to safely store the ever increasing amount of research data and on top of that we must provide suitable services that allow to work effectively and efficiently with the data.

[8] https://www.rd-alliance.org/groups/metadata-standards-directory-working-group.html

3.4 Basic Needs and Services

When figuring out where to start it has become obvious that despite the fact that the earlier encompassing metadata to research data are established the easier any later step and activity can be performed, the corresponding change in mind of researchers cannot be expected to take place too soon – many communication, consultancy and teaching activities will be needed to pave the ground. Yet the urgent need to improve the current situation has already been becoming obvious from our small local survey. In particular, researchers must be relieved from the burden of ensuring the most basic requirements of good scientific practice, mainly the requirement to ensure safe storage of research data for at least ten years after research completion, i.e. the persistent domain and optionally the access and reuse domain. Following the concept of modularization, at the same time the established IT system structure should be open and supportive to any more advanced approach to research data management also addressing the other earlier and more complex domains, the private and the group domain.

The university library has taken over the duty to cover the access and reuse domain. They provide researchers with information on where to publish their subject specific data (e.g. specific repositories as they can be found at re3data [Pa15]) also complying with funder requirements e.g. by EU. This also includes the opportunity to publish data at the already established repository[9] at RWTH Aachen if no suitable subject specific repository exists.

To address the need of a non-publishing but archiving facility, we have looked at several typical processes (data to a dissertation, data to a project, data to a publication) and have extracted a minimal process for data archiving, shown in Figure 2.

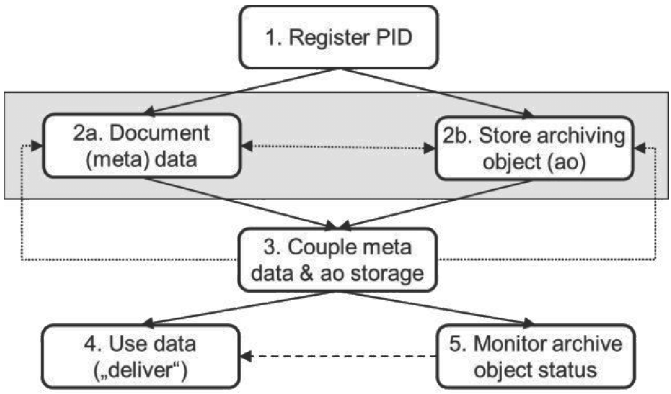


Figure 2: Basic Data Archiving Workflow

As a result, this basic workflow asks for three minimal IT services that need to be established.

[9] http://publications.rwth-aachen.de

1. An independent, highly available and performant persistent identifier (PID) service that can be addressed at any time by any researcher for as many objects as needed.

2. A storage component amenable to the needs of the researcher. While central basic solutions are offered – in particular access to the central tape archiving infrastructure –, due to the heterogeneity of research at RWTH we do not expect a single solution to be used. Thus at the PID service, any location can be registered.

3. To enable suitable subject specific and individual approaches to the description of resources, we similarly plan to register a link to additional metadata within the PID system. This builds on the RADAR schema[10] as the most basic set of metadata.

While the high amount of industrial cooperations at RWTH Aachen as well as the limitations of RADAR [Kr16] to store data related to persons[11] ask for a local solution, we consider it important to build the local solution in accordance with this national approach. In regard to the PID service, we will indeed be able to make use of the EPIC infrastructure provided by GWDG Göttingen within the EU project EUDAT[12]. Other examples for current and future service modules are Web tools for metadata libraries, version control systems and others. One particular service already in place is a university-wide identity management system [EB13] that allows account provisioning attached to person lifecycle management. With respect to RDM the knowledge about the creator of scientific data is as important as access management by identity based roles.

By this basic but open infrastructure we expect to address the urgent current needs as well as to be open enough to subject and institute specific solutions that the individual researchers plan for. In particular, more advanced data processing pipelines can be established that produce data, register them with PIDs and refer to them via the PIDs in later analyses steps as it has been proposed in the notion of the "data fabric" [Wi15].

3.5 Derived Long-Term Concept for the Storage Layer

Quantitative characteristics must be derived from the information collected in the interviews and the current storage usage for now as well as for the foreseeable development in order to create reasonably sized support and operating structures as well as technical equipment. From the storage layer perspective, we derived a 3-tier architecture to support the needs of a future RDM system as well as the currently available service modules.

The lowermost tier corresponds directly to the persistent domain and is realized by a high-capacity system (based on tape technology). The capacity is oriented at the total

[10] https://www.radar-projekt.org/download/attachments/3178555/AP3_RADAR_Metadata-Kernel__engl_v02.pdf?version=1&modificationDate=1415809915000&api=v2
[11] https://www.radar-projekt.org/display/RD/FAQ
[12] http://www.pidconsortium.eu/

amount of data that has to be kept in the context of RDM. Since there is little live access to the data stored here this tier could easily be shared with other universities when the privacy protection issues can be solved.

The mid-tier has to support all access methods depicted in Chap. 2.2. Capacity wise, we see this tier to accommodate all running projects, so it has to keep all data generated during typical project or thesis durations. It is also the place where collaborative access will be realized, either in the context of the collaborative domain as in the Access-and-reuse-domain. The most promising technologies for implementing this tier have high scaling characteristics in terms of size and speed as we see it in current disc based so-called object storage solutions.

The uppermost tier has to accommodate the performance and functionality of highly interactive work as it is carried out in the private and the group domain. For convenient user access, this tier has to realize a multitude of current and future access protocols, from fileserver to web/cloud methods. With respect to the data, this tier holds a sort of a working set of data. It is also the tier where the use-related requirements, in particular the intuitive UI and the ability to integrate with well-established processes within the scientific departments, are most important. Even more, a bad match to these "soft" requirements induces a high risk of bad acceptance by the scientists.

4 Outlook

Based on the results we gained so far we are currently developing our set of existing services in the direction of RDM. During this process we identify gaps and start projects to close these. On the other hand, now that we have a concept of how to accommodate the storage needs of RDM we cast this concept in a series of cooperative proposals in order to get funding support either for the necessary work as well as for the large scale storage components.

Acknowledgements

The depicted work has been carried out by a joint project group of the University's Library (U. Eich, S. v.d. Ropp, D. Schmitz, U. Trautwein-Bruns), IT center (B. Magrean, I. Hengstebeck, Th. Eifert, F. Krämer, A.-K. Wluka), and central administration (J. Dautzenberg, A. Haverbusch, S. Muckel) led by Prof. M. S. Müller and E. Müller.

References

[EU10] European Union: Riding the Wave. How Europe can gain from the rising tide of scientific data. Online: http://ec.europa.eu/information_society/newsroom/cf/

document.cfm?action=display&doc_id=707, Last Access: 2016-01-11, 2010.

[Ho14] Hochschulrektorenkonferenz: Management of research data – a key strategic challenge for university management. Online: http://www.hrk.de/positionen/gesamtliste-beschluesse/position/convention/management-von-forschungsdaten-eine-zentrale-strategische-herausforderung-fuer-hochschulleitungen/, Last access: 2016-01-12, 2014.

[Ho15] Hochschulrektorenkonferenz: How university management can guide the development of research data management. Orientation paths, options for action and scenarios. Online: http://www.hrk.de/positionen/gesamtliste-beschluesse/position/convention/wiehochschulleitungen-die-entwicklung-des-forschungsdatenmanagements-steuern-koennen-orientierung/, Last access: 2016-01-12, 2015.

[KE13] Klar, J., Enke, H.: Rahmenbedingungen einer disziplinübergreifenden Forschungsdateninfrastruktur, Report Organisation und Struktur. DOI: 10.2312/RADIESCHEN_005, 2013.

[Kr16] Kraft, A. et.al.: The RADAR Project—A Service for Research Data Archival and Publication. ISPRS Int. J. Geo-Inf. 5, 28. DOI: 10.3390/ijgi5030028, 2016.

[Pa15] Pampel, H. et.al.: Stand und Perspektive des globalen Verzeichnisses von Forschungsdaten-Repositorien re3data.org. In (Müller, P. et.al., eds): 8. DFN-Forum Kommunikationstechnologien: Beiträge der Fachtagung 08.06-09.06.2015 in Lübeck (GI-Edition: lecture notes in informatics; 243, pp. 13–22). Gesellschaft für Informatik, Bonn, 2015.

[RW11] RWTH Aachen University: Grundsätze zur Sicherung guter wissenschaftlicher Praxis der Rheinisch-Westfälischen Technischen Hochschule Aachen. Amtliche Bekanntmachung vom 11.01.2011. Online: http://www.rwth-aachen.de/global/show_document.asp?id=aaaaaaaaaaoyxb, Last access: 2016-01-12. 2011.

[RW16] RWTH Aachen University: Leitlinien zum Forschungsdatenmanagement für die RWTH Aachen. Rektoratsbeschluss vom 08.03.2016. Online: http://www.rwth-aachen.de/global/show_document.asp?id=aaaaaaaaaaqwpfe&download=1, Last access: 2016-03-10, 2016.

[Si14] Simukovic, E. et.al.: Was sind Ihre Forschungsdaten? Interviews mit Wissenschaftlern der Humboldt-Universität zu Berlin. Bericht, Version 1.0. Online: urn:nbn:de:kobv:11-100224755, Last access: 2016-01-12, 2014.

[Tr16] Tristram, F. et.al.: Öffentlicher Abschlussbericht von bwFDM Communities – Wissenschaftliches Datenmanagement an den Universitäten Baden Württembergs. Online: http://bwfdm.scc.kit.edu/downloads/Abschlussbericht.pdf, Last access: 2016-04-08, 2016.

[EB13] Eifert, T., Bunsen, G.: Grundlagen und Entwicklung von Identity Management an der RWTH Aachen. PIK - Praxis der Informationsverarbeitung und Kommunikation. Band 36, Heft 2, Seiten 109–116, DOI: 10.1515/pik-2012-0053, 2013.

[Wi15] Wittenburg, P.: Data Foundation & Terminology WG. Data Fabric IG. Presentation at the RDA-DE-DINI Workshop “Aktuelle Resultate der Research Data Alliance (RDA) und deren zukünftige Bedeutung” 2015-05-28/29 in Karlsruhe, Germany. Online: http://www.forschungsdaten.org/images/f/fc/RDA-DE-2015_Wittenburg_Peter_III.pdf Last access: 2016-01-12, 2015.

Sicherheit

Improving the Scalability of Identity Federations through Level of Assurance Management Automation

Michael Grabatin[1], Wolfgang Hommel[1], Stefan Metzger[2], Daniela Pöhn[2]

Abstract:

Access to remote IT services through identity federations (IFs) has solid technical foundations such as the Security Assertion Markup Language (SAML). However, reliable delegated user authentication and authorization also pose organizational challenges regarding the quality management of user data. Level of Assurance (LoA) concepts have been adapted and applied to IFs, but their inhomogeneous proliferation bears the risk of aggravating instead of simplifying the manual work steps required for providing IT services for multiple or dynamically set up IFs. This paper presents a novel LoA management approach that has been designed for a high degree of automation and gives an outlook to its application based on the GÉANT-TrustBroker toolchain.

1 Motivation

Identity federations, such as the German DFN-AAI [DFa], are a well-established key technology to enable users from one organization (the identity provider, IDP) to access IT services operated by another organization (the service provider, SP) without the need to manually set up user accounts on the SP side. By using standardized protocols like the Security Assertion Markup Language (SAML, [Ca05]), SPs can delegate the authentication step of, e. g., the login to a web-based application to the user's IDP and also request certain user profile data, referred to as user attributes, from the IDP. For example, DFN-AAI can be used by software vendors like Microsoft to make commercial software available to students of German higher education institutions (HEIs) free of charge while ensuring that the downloading user indeed belongs to a certain eligible university and is enrolled as a student there [Re].

SAML and similar protocols have initially been designed with pairs or small sets of IDPs and SPs in mind. They provide the technical basis for inter-organizational authentication and authorization (AuthNZ), but assume that additional organizational or contractual measures are in place to control whose IDP's users are allowed to access whose SP's services. However, over the past decade, DFN-AAI and other federations have attracted so many member organizations that, on a technical level and in theory, the users of hundreds of IDPs could use the services of hundreds of SPs. Inter-federations, such as eduGAIN [GÉ], which meanwhile unites 40 national federations including DFN-AAI, and dynamic federation enablers like GÉANT-TrustBroker [PMH14] further contribute to the international and cross-industry-sector use of identity federations with a significant practical impact.

[1] Universität der Bundeswehr München, 85577 Neubiberg, [michael.grabatin,wolfgang.hommel]@unibw.de
[2] Leibniz Supercomputing Centre, 85748 Garching n. Munich, [metzger,poehn]@lrz.de

With the number of federation partners rising, it becomes more and more complex and tedious to manually configure all the individual IDP $\leftrightarrow$ SP relationships. Instead, an SP might want, for example, to accept users from any IDP as long as there is a guarantee that the IDP is a state-approved HEI and the users' *student* status is reliably removed whenever a student is disenrolled. Such conditions on selected data quality management aspects have led to the concept of Levels of Assurance (LoA); for example, DFN-AAI distinguishes between the three LoAs (*Verlässlichkeitsklassen*) Test, Basic, and Advanced [DFb].

Unfortunately, technical support for different LoAs is quite limited in current identity federation standards and products, which basically leads to the situation that DFN-AAI is not one federation, but three – one federation for each LoA. Furthermore, each federation operator can define its own data quality criteria and LoAs, so SPs that accept IDPs from different federations cannot assume that, e. g., IDPs from Germany's DFN-AAI-Advanced, Switzerland's SWITCH-AAI, and Australia's AAF adhere to the same data quality standards. For example, unlike the three German DFN-AAI federations, Australia's AAF uses four LoAs that are not available as separate federations but as user attribute, i. e., similar to the user's email address in the *mail* attribute, her level of identity assurance is available as *eduPersonAssurance* attribute.

Managing LoAs therefore is crucial for the efficient and scalable use of large federations and inter-federations from an SP perspective as well as key to adequate service access from the IDPs' point of view. This paper presents a novel LoA management approach that keeps the currently established, diverse solution attempts in mind and leverages common ground with the goal of a high degree of automation in operation; its viability is discussed based on the GÉANT-TrustBroker IDP $\leftrightarrow$ SP metadata exchange service. The remainder of this paper is structured as follows: Section 2 compares selected current real-world deployments and summarizes related approaches by research as well as standardization bodies. Section 3 then presents the novel LoA management concept along with its data model and automated comparison workflow. Finally, Section 4 gives an outlook to its application within GÉANT-TrustBroker.

2 State of the Art and Requirements regarding Levels of Assurance

An LoA, such as the DFN-AAI Advanced mentioned above, basically is a set of {*LoA aspect*, *value*}-pairs. While there are no restrictions regarding which *LoA aspects* are used to compile an LoA, the following *LoA aspects* are often used in practice:

Identification: How has the user been identified by her IDP? For example, manual verification of a government-issued photo identification document can be considered as more trustworthy than web-based self-registration.

Data Management: How up-to-date and precise is the user data? For example, are accounts of retired employees removed immediately or only once per quarter?

Authentication: How are users authenticated by their IDP during login, e. g., using only passwords or based on multi-factor authentication methods such as smartcards?

Assertion Representation: How is user data transported from to IDP to the SP considering risks such as unintended information leaking and spoofing? For example, are TLS-encrypted connections used and is the data digitally signed by the IDP?

Accountability: Which state-of-the-art technical security measures does the IDP have in place to prevent, e. g., unauthorized user data modification?

Organizational Management: Which organizational security management procedures are applied on the IDP side? For example, did an independent third party perform a security audit?

For a specific LoA, a specific *value* needs to be assigned to each of the chosen *LoA aspects*. The available *values* and their semantics, i. e., their precise and binding meaning, is typically documented in human-readable prose text approved by legal experts. To enable automated machine-processing, ordered identifier sets are used: For example, in the context of the *LoA aspect* data management, the *values* 0, 1, and 2 could be used to distinguish between "no guarantees", "data is no older than 3 months", and "data is no older than 14 days". Obviously, an IDP fulfilling *value* 2 of this *LoA aspect* would also be suitable for SPs only requiring *value* 1. As a consequence, a flexible solution must support arbitrary *LoA aspects* with arbitrary *values*; as shown below, we require *values* to be ordered, i. e., they must be comparable and a higher value must implicitly also fulfill the requirements of lower values.

Several federations operated by national research and education networks as well as standardization bodies have specified LoAs, e. g., NIST in SP 800-63-2 [Bu13], ISO/IEC 29115:2013 [IS13], the electronic identification and trust services (eIDAS) [Eu14] of the European Commission, and the Kantara Identity Assurance Framework (IAF) [Ka]. Typically, 2–4 *values* are used per *LoA aspect* and an IDP is assigned to the overall LoA corresponding to the lowest *value* found in any of its *LoA aspects*. For example, if a German IDP fulfills all criteria for DFN-AAI Advanced except one, it is assigned to the Test or Basic LoA depending on the *value* of this one criterion. Although this is a simple and effective assessment procedure, it does not flexibly take into account that SPs' data quality requirements can be more fine-grained than "one of three LoA levels".

Given the rich semantics of the *LoA aspects' values* and the lack of a global overall standard, the LoAs used by different federations must initially be compared manually in a *LoA aspect*-by-*LoA aspect* manner, determining the semantic equivalence of the available *values*. For example, regarding the *LoA aspect* data management, InCommon's Bronze LoA fulfills the requirements of DFN-AAI Advanced, but no DFN-AAI LoA fulfills InCommon's Silver LoA requirements; similarly DFN-AAI Basic IDPs are not suitable to use services operated by InCommon Bronze SPs. The results of such manual comparisons lead to a simple mapping of *LoA aspect value* equivalence, which can later be used to automatically compare LoAs of arbitrary inter-federation IDP $\leftrightarrow$ SP pairs.

Especially when there is no individual contract between an SP and an IDP, LoA assignment procedures become relevant in practice. For example, using any of the DFN-AAI LoAs is tied to a legally binding, written contract between the IDP organization and DFN as federation operator, which includes a self-declaration of conformity. Other national research

federations, such as Haka in Finland and SURFnet in the Netherlands, use check-list-style maturity self assessments that must be passed, whereas industry federations, e. g., in the automotive supply chain, typically require formal third-party audits and certification processes.

The primary technical challenge related to this trustworthy and authentic assignment of LoAs to IDPs is about how the IDP's LoA is communicated to the SP and how it can be verified by the SP; as mentioned in the previous section, there are, in principle, only two approaches that can optionally be combined:

1. LoAs can be included in the federation metadata files: Federation operators provide lists of federation members including metadata such as their communication endpoints, server X.509v3 certificates, and human contact information:

   - The SAML Identity Assurance Profile [Kl10] allows to include multiple URI-styled references to LoA specifications that are fulfilled by an entity, i. e., only globally unique identifiers of LoAs that are described somewhere else are included.
   - Vectors of Trust (VoT) [RJ15], which is intended to become an IETF RFC standard, describes how an LoA's {*LoA aspect*, *value*}-pairs can be represented as a simple URN-style text string. Therefore, all LoA information is included and no external documents need to be fetched, but the SP still needs to know how to interpret the *LoA aspects* and their *values*.

   When LoA information is included in official federation metadata this way, SPs trusting the federation operator can rely on the correctness of the provided IDP LoAs.
2. LoA information can be included in each communication between an IDP and an SP about a specific user who currently logs into the service:

   - The *eduPersonAssurance* attribute is used in several research and education federations; its expressiveness is approximately equivalent to the SAML Identity Assurance Profile mentioned above.
   - SAML responses can include the so-called Authentication Context Class statement, which, however, by intention primarily covers the *LoA aspect* authentication.
   - The Vectors of Trust LoA representation could also be sent as a user attribute, although no real-world deployment of this approach is currently known to the authors.

   Unless any of this information is digitally signed by a trusted third party, the SP needs to trust the IDP regarding the correctness of the provided LoA data.

Although both approaches apparently provide similar functionality, transporting LoA information in the communication between IDP and SP, i. e., outside the federation metadata,

is highly important in practice for IDPs that have different groups of users with different LoAs (see also [TM11]). For example, a university IDP may only achieve LoA 1 for all of its students due to data up-to-dateness issues in the student administration system, but achieve the better LoA 2 for its staff and faculty due to better currentness of data in its human resources management system. LoA information therefore needs to be sent to the SP on a per-user or even per-user-attribute basis to ensure that all eligible users can access the service. Similarly, dynamic IDP/SP metadata exchange solutions, such as the Metadata Query Protocol [Yo15] and GÉANT-TrustBroker, which bypass the organizational overhead of running formal federations, motivate solutions that are not based on federation-wide, federation-operator-signed metadata.

It is furthermore important that currently only the LoAs achieved by IDPs are explicitly stated in federation metadata or SAML-based communication. SPs' LoA-specific requirements can, for example, in the case of DFN-AAI be derived implicitly from an SP's federation membership, e. g., DFN-AAI Advanced but not Basic; however, there are no other ways to inform IDPs about SP requirements yet. This can lead to situations in which IDPs send detailed user profiles to SPs although the users are not allowed to access the services; this issue clearly should be addressed when the IDP $\leftrightarrow$ SP communication is established.

3 Managing Levels of Assurance with a high Degree of Automation

The previous section has shown that, as of today, different LoA schemes have been proposed and are in real-world use but lack interoperability and apply different methods to transport *LoA aspects* and *values* between IDPs and SPs. This paper proposes a technical solution to the LoA comparison core issue: *How can be determined whether a specific IDP provides a sufficient LoA for a specific SP in an automated, efficient manner?* The proposed solution consists of three contributions that build on top of each other:

1. The SAML Identity Assurance Profile [Kl10] is combined with IETF's Vectors of Trust [RJ15] to create an LoA data model that is used to encode *LoA aspects* and their *values* as simple text string encodings.
2. A specification defines how SPs announce their LoA requirements and IDPs indicate their LoA guarantees as a part of their SAML metadata or individual SAML messages; existing deployments and good practices are accounted for in this step.
3. A workflow describes how software tools can automate the comparison between SP LoA requirements and IDP LoA guarantees either via a trusted third party, such as the GÉANT-TrustBroker service, or locally at each IDP or SP.

The proposed solution works on both, per-IDP and per-user, levels to achieve the flexibility none of the previous approaches alone enables; optionally, it can be applied on a per-user-attribute level and supports digital signatures by trusted third parties for LoA guarantee validation. The following subsections detail each of the three steps outlined above, while Section 4 then gives an outlook to the GÉANT-TrustBroker-based implementation.

3.1 LoA data model to encode LoA aspects and values

On the one hand, the SAML Identity Assurance Profile (SAML-IAP) uses URIs, such as `http://foo.example.com/assurance/loa1`, to reference unique identifiers of LoA specifications that are documented somewhere else (see [Kl10, section 2.3]). On the other hand, IETF's Vectors of Trust (VoT) uses text strings, such as `urn:ietf:param:[TBD]:P1.Cc.A3`, to encode *LoA aspect* identifiers (P, C, and A) along with their *values* (1, c, and 3) (see [RJ15, sections 4.1 and 4.3]).

The proposed solution basically combines both approaches by creating a SAML-IAP-compliant URI that uses a fixed base LoA identifier, e. g., `https://loa.geant.net/gntb`, and appends an LoA identifier as well as VoT's wire representation string as parameters `loa` and `vot`; the above example therefore results in

```
https://loa.geant.net/gntb?loa=http%3A%2F%2Ffoo.example
                           .com%2Fassurance%2Floa1&vot=P1.Cc.A3
```

Given the semantical overlap of both parameters, `loa` and `vot`, the different semantics of LoAs stated by IDPs and SPs, and the practical necessity to support multiple LoAs in parallel, the semantics of the URI parts exemplified above are defined as follows in accordance with IETF RFC 3986:

- The URI scheme and hier-part (see RFC 3986, section 3), i. e., `https://loa.geant.net/gntb` indicate the implementation variant of this approach to distinguish it from traditionally used SAML-IAP implementations.
- To state multiple LoAs that are to be used in parallel, multiple URIs must be created and used just like other multi-value attributes in SAML metadata or SAML messages.
- At least one of the two parameters `loa` and `vot` *must* be present. If both of them are used, the *values* of the *LoA aspects* encoded in the `vot` parameter *must* be the same as or higher than the *values* derived from the LoA referenced by the `loa` parameter and override them. This means that the `vot` parameter can be used to specify either additional *LoA aspects* that are not covered by the referenced LOA or the over-fulfillment of the referenced LoA, but it *must not* be misused to express shortcomings in fulfilling the referenced LoA.
- IDPs specify their LoA guarantees, while SPs specify their LoA requirements: When comparing a pair of requirements and guarantees, the requirements are fulfilled if and only if the *value* of each *LoA aspect* in the IDP LoA matches or exceeds the *value* of the same *LoA aspect* in the SP LoA. *LoA aspects* that are provided by the IDP LoA but not covered by the SP LoA are discarded. However, *LoA aspects* specified by the SP LoA but not by the IDP LoA indicate non-conformity, i. e., the requirements are not fulfilled.
- On a per-IDP level, i. e. for use in SAML metadata, IDPs can create multiple URIs with the same `loa` parameter value but different `vot` parameter values. This indicates that the IDP has different user groups with non-uniform LoA guarantees that need to be evaluated on a per-user (or per-user-attribute) level.

Based on the discussion of human-readable prose text LoA documents in Section 2, in order to enable automated tool-supported comparisons, the values of the `loa` parameter must either refer to a public document containing a VoT string or the tool needs to have an internal database (i. e., mapping tables) in which the referenced LoA's *aspects* and their *values* are defined, e. g., based on manual creation by a human interpreting the LoA document. The initial creation of these mapping tables cannot be automated unless, for example, ontology-based approaches are used that are outside the scope of this paper.

In order to restrict an LoA to selected user attributes, an optional third parameter named `attributes` can be used. For example, if an SP requires that an IDP provides a high value for the *LoA aspect* data management regarding the user attribute `mail`, i. e., the user's email address(es), but is willing to accept potentially outdated user telephone numbers, i. e., user attributes `telephoneNumber` and `mobile`, the relevant parts of the LoA URI would look like:

```
...&vot=D2&attributes=mail
...&vot=D0&attributes=telephoneNumber,mobile
```

The comma-separated user attributes can be specified either by their human-readable name as in the example above, i. e., more formally, their *SAML2 Attribute FriendlyName*, or by their globally unique OID, e. g., `0.9.2342.19200300.100.1.3` for `mail`.

3.2 Communicating encoded LoA requirements and guarantees via SAML

LoA URIs as specified above need to be embeddable into both SAML metadata and messages. Given the existing standards and practices, the following methods are to be used:

- Based on SAML-IAP, IDPs and SPs can include an arbitrary number of LoA URIs as *assurance-certification* entity attributes in their SAML metadata. This is already in real-world use for IDPs and can be applied to SPs without requiring any changes to the SAML metadata XML schema.
- IDPs that deliver per-user LoA information can transmit LoA URIs via a dedicated, multi-value user attribute. For example, the attribute *eduPersonAssurance* supports URI-style values and is therefore well suitable for this task; while it is the de-facto standard for research and education IDPs, other lines of business will likely choose or create a different user attribute with the same syntax that better fits their specific user data schema.
- SPs currently lack a proper, standardized way of sending full LoA requirements within their SAML requests. SAML-IAP specifies the use of LoA URIs as *RequestedAuthnContext* element in SAML requests, but this element's original intention was limited to the single *LoA aspect* authentication. LoA URIs as discussed above are compatible regarding their syntax and can be used, but a more generic approach as part of future SAML-IAP versions would be a better long-term solution.

It is worth noting that the only standardized way of providing LoA requirements and guarantees verifiable via a trusted third party (TTP) is by having federation-wide SAML metadata files signed digitally, which is typically done by the federation operator or an entity metadata aggregation delegate. Facilitating per-user TTP signatures is technically possible in principle, but as of today not a realistic option for real-world deployments due to the related organizational overhead; a thorough analysis will be part of our future work.

3.3 Automatically comparing LoA requirements and guarantees

To determine whether an IDP's LoA guarantees positively match an SP's LoA requirements, both parties' LoA URIs must be evaluated and compared to each other. Although this comparison is quite simple in principle, it is non-trivial due to the following four marginal conditions:

1. As both IDP and SP can have multiple LoA URIs, each IDP LoA URI must be compared with each SP LoA URI. The SP's requirements are fulfilled if there is at least one (IDP LoA, SP LOA)-pair in which the IDP LoA guarantees fulfill the SP LoA requirements.
2. If an LoA URI contains both parameters `loa` and `vot`, their *effective (LoA aspect, value)-pairs* must first be determined by combining both parameters: As specified in Section 3.1, parameter `loa` determines the basic set of *(LoA aspect, value)*-pairs, which is then extended or adjusted according to the *(LoA aspect, value)*-pairs encoded in the given VoT.
3. If both parties use different sets of *LoA aspects*, e. g., due to applying LoAs from different federations, mapping tables must be applied if available.

In pseudocode, the comparison therefore can be performed as follows:

```
1  typedef enum {NOT_FULFILLED, FULFILLED} comparison_result;
2  comparison_result compare_LOA_URIs(sp_loa_uris, idp_loa_uris) {
3    foreach sp_loa_uri in sp_loa_uris do {
4        effective_sp_loa := parse_LoA_URI(sp_loa_uri);
5        foreach idp_loa_uri in idp_loa_uris do {
6          effective_idp_loa := parse_LoA_URI(idp_loa_uri);
7          foreach sp_loa_aspect in effective_sp_loa do {
8              if (idp_loa_aspect of same type exists
9                  or can be derived via mapping table) {
10               if (idp_loa_aspect.value < sp_loa_aspect.value) {
11                 // IDP guarantee does not fulfill SP requirement
12                 continue with next idp_loa_uri;
13               }
14             }
15             else { // LoA aspect requested by SP is not known to IDP
16               continue with next idp_loa_uri;
17             }
18         }
19         return FULFILLED; // All relevant LoA aspects had suitable values
20       }
```

```
21    }
22    return NOT_FULFILLED; // No suitable (SP LoA, IDP LoA)-pair was found
23  }
```

This workflow applies to metadata-based as well as per-request-based LoA URI comparisons. Additionally, if the `attributes` parameter is used in LoA URIs, the comparison must be repeated for each respective set of user attributes. Various optimizations could be made in implementations based on eventually available additional information, such as comparing the best IDP LoA guarantees with the lowest SP LoA requirements first, but as the workflow is neither computationally intensive nor time-critical in today's real-world deployments, optimizations are out of scope of this paper.

4 Outlook: Application to GÉANT-TrustBroker

In practice, automatically comparing LoA requirements and guarantees is important in the following use cases:

- A specific IDP $\leftrightarrow$ SP pair has no other trust-building measures in place, such as membership in a common federation or a written contract.
- LoA requirements or guarantees have changed since they were checked last time.
- IDPs have different user groups with inhomogeneous LoA guarantees.

Unlike traditional national or community-specific identity federations, the TrustBroker service, which is currently being developed by the pan-European research and education network GÉANT, enables the dynamic, user-triggered, on-demand setup of virtual identity federations [PMH14]. As this implies that there are neither central, trusted federation operators nor written contracts in place, automated LoA comparisons take up a key position regarding data quality assurance.

The GÉANT-TrustBroker toolchain consists of a centrally operated SAML metadata repository, in which individual IDP and SP metadata is stored, and plug-ins for IDP and SP software products, such as Shibboleth and SimpleSAMLphp, which retrieve the opposite party's metadata on demand and integrate it into the local software configuration. Without automated LoA management, only primitive white and black lists of domain or organization names were usable to specify or restrict memberships in the created dynamic virtual federations. By implementing the approach described in Section 3, the central GÉANT-TrustBroker service can verify – to the extent of LoA information embedded in the SAML metadata – whether an IDP's data quality is sufficient for a chosen SP and can therefore prevent the unneeded exchange of SAML metadata between IDPs and SPs with unfulfilled LoA requirements, which in turn prevents the transfer of users' personal data without service in return.

Similarly, the GÉANT-TrustBroker plug-ins operated locally by IDPs and SPs can apply the LoA comparison whenever the SAML metadata of either party has changed or per-user LoA requirements and guarantees need to be handled. This also prevents unneeded

personal data leakage and assists the IDP and SP operators by precisely indicating which LoA requirements or guarantees need to be addressed to enable successful interoperation.

The required extensions to the GÉANT-TrustBroker tools will be implemented as part of GÉANT's EC-funded GN4 project with pilot operations as part of the AARC project.

References

[Bu13] Burr, William E.; Dodson, Donna F.; Newton, Elaine M.; Perlner, Ray A.; Polk, W. Timothy; Gupta, Sarbari; Nabbus, Emad A.: NIST SP 800-63-2 – Electronic Authentication Guideline. Special Publication, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, 2013.

[Ca05] Cantor, Scott; Kemp, John; Philpott, Rob; Maler, Eve (Eds.): Security Assertion Markup Language v2.0. OASIS Security Services Technical Committee Standard, 2005.

[DFa] DFN-AAI: , DFN-AAI – Authentication and authorization infrastructure. `https://www.aai.dfn.de/en/`. [Online, retrieved December 16th, 2015].

[DFb] DFN-AAI: , DFN-AAI – Degrees of reliance. `https://www.aai.dfn.de/en/der-dienst/degrees-of-reliance/`. [Online, retrieved December 16th, 2015].

[Eu14] European Parliament and the Council of the European Union: EUR-Lex – 32014R0910. Regulation of the European parliament and of the council, EU, 2014. [Online, retrieved December 16th, 2015].

[GÉ] GÉANT: , eduGAIN Service Homepage. `http://services.geant.net/edugain/Pages/Home.aspx`. [Online, retrieved December 16th, 2015].

[IS13] ISO/IEC: ISO/IEC 29115:2013 – Entity authentication assurance framework. International Standard, ISO/IEC, 2013.

[Ka] Kantara Initiative: , Identity Assurance Framework. `http://kantarainitiative.org/confluence/display/LC/Identity+Assurance+Framework`. [Online, retrieved December 16th, 2015].

[Kl10] Klingenstein, Nathan; Hardjono, Thomas; Morgan, RL Bob; Madsen, Paul; Cantor, Scott: SAML V2.0 Identity Assurance Profiles Version 1.0. OASIS Security Services Technical Committee Standard, OASIS, 2010.

[PMH14] Pöhn, Daniela; Metzger, Stefan; Hommel, Wolfgang: Géant-TrustBroker: Dynamic, Scalable Management of SAML-Based Inter-federation Authentication and Authorization Infrastructures. In: ICT Systems Security and Privacy Protection. Springer Berlin Heidelberg, pp. 307–320, 2014.

[Re] Rechenzentrum der Universität Würzburg: , StudiSoft – Webshop. `http://www.studisoft.de/`. [Online, retrieved December 16th, 2015].

[RJ15] Richer, Justin; Johansson, Leif: Vectors of Trust – draft-richer-vectors-of-trust-02. Internet-Draft (work in progress), IETF, 2015.

[TM11] Thomas, Ivonne; Meinel, Christoph: An Attribute Assurance Framework to Define and Match Trust in Identity Attributes. In: ICWS. IEEE Computer Society, pp. 580–587, 2011.

[Yo15] Young, Ian: SAML Profile for the Metadata Query Protocol — draft-young-md-query-saml-05. Internet-Draft (work in progress), IETF, 2015.

Müller, Neumair, Reiser, Dreo Rodosek (Hrsg.): 9. DFN-Forum Kommunikationstechnologien,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2016 77

Privacy-Aware Intrusion Detection in High-Speed Backbone Networks - Design and Prototypical Implementation of a Multi-Layered NIDS

Mario Golling[1], Robert Koch[1] and Gabi Dreo Rodosek[1]

Abstract: Network Intrusion Detection Systems are nowadays an integral part of network security. NIDS provide a layer of defense by monitoring and analyzing the traffic for signs of suspicious activities and alerting system administrators when potential violations are detected. In the context of large, high-speed networks, such as backbone networks, we make two observations: Firstly, devices capable of detecting intrusions on high-speed links of 10 Gbps and higher are rather expensive or must be built based on complex arrays. Secondly, legislation commonly restricts the way in which backbone network operators are allowed to analyze data. As a consequence, traditional Intrusion Detection approaches, where individual packets are scanned for suspicious patterns (commonly referred to as Deep Packet Inspection) are not applicable. Although Flow-Based Intrusion Detection offers several advantages in terms of processing requirements, the aggregation of packets into flows obviously entails a loss of information. To bridge the gap, within a previous publication, we have proposed a multi-layered approach that combines the advantages of both types of Intrusion Detection. The first layer comprises Flow-Based Intrusion Detection, making a pre-selection of suspicious traffic. Additional Packet-Based Intrusion Detection is subsequently performed on the pre-filtered packet stream to (i) facilitate in-depth detection, (ii) avoid the problem of a costly infrastructure, (iii) obey to the various legal barriers on network traffic inspection and to (iv) reduce the oftentimes high false alarm rate of Flow-Based Intrusion Detection Systems. Within this publication, we refer to our previously develop concept of Multi-Layered Intrusion Detection and extend it by demonstrating the corresponding prototype and a practical evaluation. As such. we shortly recall the underlying concept and then present a prototypical implementation and evaluate it with real data.

Keywords: Network Security, Intrusion Detection, High-Speed Networks, Flow-Based Intrusion Detection, Multi-Layered Intrusion Detection, Legal Inspection

1 Introduction

Attacks on computer systems are constantly rising throughout the last couple of years, both in terms of quality and quantity. Especially when attacks are performed in a distributed manner, their devastating power can have a significant impact on Backbone Providers, as for example seen in early 2013 when the Spamhaus project was targeted by Distributed Denial of Service (DDoS) attacks with more than 300 Gbps - enough to overload several Internet exchanges. In addition to DDoS attacks, in particular large scale activities (primarily worms and botnets) are also of special relevance for high-speed network operators, since they also consume a great amount of resources (e.g., see [Ar14, GHK14]).

[1] Munich Network Management Team (MNM-Team), Universität der Bundeswehr München, Werner-Heisenberg-Weg 39, D-85577 Neubiberg, {mario.golling, robert.koch, gabi.dreo}@unibw.de

As a result of the increase in the importance of defending against IT attacks, Intrusion Detection, *the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices* [SM07], is constantly gaining attention. Focused on *identifying possible incidents, logging information about them, attempting to stop them, and reporting them to security administrators*, Intrusion Detection Systems (IDSs) are nowadays an integral part of any IT defence strategy and as such a necessary addition to the security infrastructure of nearly every organization [SM07].
As presented in more detail in Section 2, the balance between the demands of High-Speed Backbone Providers (especially high-speed links, high throughput, the need for a low false alarm rate, a particular interest in certain *large-scale* attack types and, derived from legal standards, the necessity to stay inlined with data protection requirements) on the one hand and the capabilities of IDSs (reliable detection in high-speed backbone environments in compliance with legal requirements is currently not possible or only very limited requiring a high financial effort resp. specific situations / constellations) on the other hand is *not* in line. To improve this situation, Section 3 firstly illustrates our conceptual design. Based on this, Section 4 then implements a corresponding Proof-of-Concept (PoC), before an evaluation with the help of real-world data is presented in Section 5. Finally, Section 6 concludes this paper, giving a final summary as well as an outlook.

2 Background

Especially in relation to the subject of this publication, Intrusion Detection in High-Speed Backbone Networks, Network-Based IDSs (NIDSs), *which monitor network traffic for particular network segments or devices and analyze the network and application protocol activity to identify suspicious activity* [SM07] are of high relevance, since their counterpart, Host-Based IDSs (HIDSs), *which monitor the characteristics of a single host and the events occurring within that host for suspicious activity* [SM07] are not applicable due to the fact that High-Speed Backbone Providers are normally used to forward data and as such are neither the source nor the destination of the data.
Next to the distinction of IDSs in HIDSs and NIDSs, other subdivision can be made as well (e.g., see Debar et al. [DDW00]). Traditional Intrusion Detection approaches rely on the inspection of individual packets, often referred to as **Deep Packet Inspection (DPI)**, where individual packets are scanned for signs of suspicious activities; some of the more popular IDSs that make use of this approach are Snort, Suricata, Bro (*open source*) or from vendors such as Cisco or McAffee. However, high link speeds/throughputs, especially in backbone networks, seriously constrain this approach. With link speeds of more than 40 Gbps, DPI-Based IDSs are either very expensive (e.g., because they have to built based on complex arrays) or not even available. Furthermore, legislation, especially in the European Union, seriously restricts the use of DPI and often requires a solid legal justification *before* DPI can be applied.
To overcome both constraints, **Flow-Based Intrusion Detection** can be applied. A flow is defined as *a set of IP packets passing an observation point in the network during a certain*

time interval; all packets belonging to a particular flow have a set of common properties and focuses primarily on packet header fields and packet characteristics. Consequently, compared to DPI-Based Intrusion Detection, Flow-Based IDSs have to handle a considerable smaller amount of data, which is of advantage in terms of privacy and link speed (allowing to perform a detection in high-speed environments). Given that flow export technologies, such as NetFlow and IPFIX, aggregate packets into flows, such an IDS is usually capable of monitoring the aggregated traffic using commodity hardware. Next to this, flow export technologies are nowadays embedded in the vast-majority of high-end packet forwarding devices (Routers and Switches) and are already widely used for network management, so deploying Flow-Based IDSs comes at almost no cost which in turn makes this approach economically attractive.
However, this entails *three major drawbacks*, which currently exclude Flow-Based IDSs from their large-scale practical usage:

1. *The number of recognizable attacks is severely restricted.* In comparison to DPI-based IDSs a decision has to be made on the basis of an evaluation of a significantly lower amount of data which particularly excludes the detection of payload-based attacks except a volume-based detection wrt. abnormal behavior of the "amount" of payload.
2. *The detection time is increased.* Normally multiple flows are generated on the network components. Thereafter, these flows are exported to a Flow Collector in a certain interval before then, in the third step, an analysis can be carried out by a Flow-Based IDSs.
3. *The number of false alarms increases (partly).* Based on the fact that relatively little information can be analyzed, for certain classes of attacks, no unambiguous distinction between benign and malignant traffic can be made. Although this does not apply to all classes of attacks, it can be said that in comparison with a DPI-Based IDS, a Flow-Based IDS has a higher percentage of false positives.

As shown in Figure 1, Flow-Based IDSs are capable of detecting *those attacks* that are of high relevance for a backbone network operator. On the other hand, quite a number of different approaches are available, each of them addressing specific aspects (see [Sp10]).

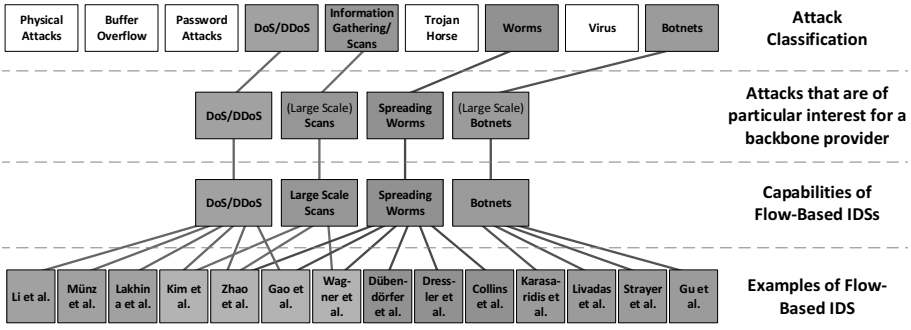


Fig. 1: Capabilities of Flow-Based IDSs vs Special Interests of Backbone Providers wrt. Intrusion Detection [GHK14]

Many of these approaches are either of theoretical nature and/or focus on very specific

cases (for example, the recognition of (non-large-scale) attacks in SSH connections which - with regard to Backbone Providers - is of secondary importance).
Nevertheless, with regard to (i) the three major drawbacks and (ii) Backbone Providers, it has to be noted, that the first two arguments (restricted number of recognizable attacks and increased detection time) are of lower importance. In addition, the compliance of Flow-Based IDSs with data privacy regulations as well as their low prize has to be emphasized, too. However, due to argument number 3 (low accuracy), Flow-Based IDSs are marginally used.

3 Design

In this Section, the design of the Multi-Layered Architecture is presented briefly. In order to be widely deployable, the architecture deliberately makes use of existing state-of-the art approaches. The main components, together with their interactions, are shown in Figure 2; the architecture is a slightly simplified version of the one already presented in [GHK14] and [GKS14] to allow for (i) a smoother introduction to the topic and (ii) to perform an appropriate implementation and evaluation. In particular, the implementation / evaluation as such is *the* main added value of this publication.

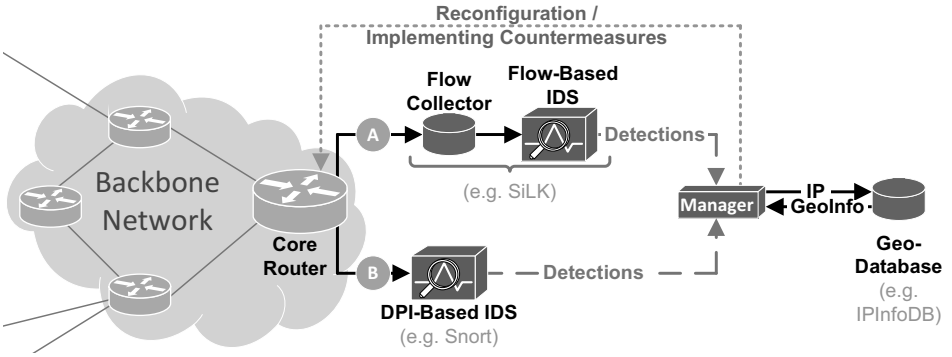


Fig. 2: Architecture for Privacy-Aware Intrusion Detection in High-Speed Backbone Networks

Components
The architecture makes use of both (i) an Flow-based IDS *and* (ii) an DPI-Based IDS. While the Flow-based IDS constantly analyzes the entire data traffic, the DPI-based IDS is activated by the Manager to investigate / analyze exactly this part of the suspicious traffic - and not more. As such, the Manager controls the data-streams, and activates / configures the DPI-based IDS. To make sure that the DPI-Based IDS receives the optimal data-stream, the Manager can reconfigure the Core Router (Reconfiguration). Upon detection of an attack, the Manager can also reconfigure (Implementing Countermeasures) the Router to drop the attack traffic (e.g., by using an Access Control List / creating a sinkhole, by load balancing requests to multiple facilities or by informing the Administrator about the suspicious traffic).

Geolocation
The knowledge of the geographical origin of an attack may also be of great importance. As for example the security company Mandiant has revealed in a study [Ma13], a large part of *all* attacks on US authorities originate from a single building in Shanghai / China. As a result, within the architecture, geo-localization (also called Geolocation), the mapping of a logical address, here the IP of a host, with the physical respectively geographic location is used, too. To this end, the architecture uses a Geolocation Service based on a Geolocation Database which is constantly updated. In particular if, due to the lack of performance of the DPI-Based IDS, not all incidents of the Flow-Based IDS can be investigated, Geolocation (next to the already existing weighting of the Flow-Based IDS) is used as an additional distinguishing feature to differentiate between the important and the less important incidents.
In this work, Geolocation is used in two ways: Static Geo-Reputation and Dynamic Geo-Correlation. In analogy to e-mail white-and blacklisting, IP addresses obtain a specific score (ip scoring mechanism), within the *Static Geo-Reputation* process. Especially for organizations with which there is a special relationship of trust, whitelisting is conceivable. Here, this implies that the probability of a large-scale attack starting from e.g., another provider who is known to have very high security standards is reduced (but not equal to zero). On the other hand, also the idea of blacklisting seems to be generally applicable to Intrusion Detection. Organizations / providers that are known to have a low level of security obtain a higher scoring.
In contrast to the static assignment of IP addresses in those that tend to be benign IP addresses (whitelist) and those that tend to be malignant (blacklisting), a correlation of IPs (to other IPs known to be malicious) can also be established dynamically (*Dynamic Geo-Correlation*). Starting from the origin of an incident and by taking into account historic data, the degree of similarity can also be defined. The Dynamic Geo-Correlation approach of this paper is build upon different presumptions, which are:

1. *Temporal correlation*. After a certain time, a Geo-Correlation shall no further be given; e.g., after a certain timer has expired.
2. *Spatial correlation*. A new connection only gets correlated to an already known, malicious connection if the distance is lower than a specific threshold.
3. *Fog of time*. The older the information (IP known to be malicious in the past), the less important shall this information be; as a consequence, the distance in which a Geo-Correlation is assumed is decreasing over time.
4. *Accuracy level*. The more accurate the Geolocation is (which is also closely linked to the density of the population), the smaller the distance for Geo-Correlation and vice versa; hence, the less precise the Geolocation, the greater the distance for Geo-Correlation.

4 Implementation

Following one of the underlying objectives of our research - to combine as many as possible *already available solutions* in an appropriate manner - for the implementation, well-established solutions are used. Referring to this, the examples of Figure 2 - written in

grey - correspond to the solutions used. To this end, the authors would like to point out in particular three aspects:

1. *Flow Collector/Flow-Based IDS*. Although - as already mentioned - in theory, a wide variety of solutions is available for the analysis of flows (see [Si15] for more details), unfortunately only a fraction of these solutions are also available as a real product / software solutions. In the open source community, there are just a few popular tools [Ma09]: nfdump (and its web component nfSen), SiLK (System for Internet-Level Knowledge, which is developed by Carnegie Mellon) and Stager (a system for aggregating and presenting network statistics).
   For the following reasons, SiLK [CE16] has been chosen:

   - All open source projects offered much better opportunities to make own modifications in comparison to commercial tools such as IBM Aurora, NetQoS Reporter Analyzer, Caligare Flow Inspector, and Arbor Peakflow (see also [Ma09]).

   - Stager, a representative of open source software, with the last update on July 8th, 2010 seems to be no longer maintained and is therefore also not considered.

   - In choosing between nfdump / nfsen and SiLK, SiLK was finally the choice, firstly because it was preferred in several web discussions (see [Op12] resp. [Op14]) and, secondly, it turned out to be better suited for the relevant use case as well as the extensions needed.

2. *DPI-Based IDS*. Here, the choice is comparatively easy. Snort, as the de facto state-of-the art in the field of open source Intrusion Detection is our solution of choice.
3. *Geo-Database*. In terms of Geolocation, we also have a state-of-the art solution in use, in this case the IPInfoDB with the use of the corresponding API.

In the first step, we have set up a new virtual machine (VirtualBox) with Ubuntu 15.10. Using a virtual machine was based on the fact that we thus are able to quickly switch between different computers and consequently are able to run this VM on a high-performance machine at a later point in time. Inside the VM, both IDSs were installed. For the actual prototype, the Manager, C was used. As Section 5 will carry out in more detail, for reasons of traceability and optimization no *live evaluation* was performed. Instead, within the first step of the evaluation, live data traffic was recorded using special hardware accelerated network interface card (here with the use of the so-called HANIC Appliance from Invea-Tech; see e.g., [Vi14] for more information about the appliance). This has the advantage that external influences (changes in traffic patterns etc.) can be excluded and / or are kept constant (ceteris paribus) and we (i) obtain a better comparison of systems / versions / parametrizations and (ii) are able to compare individual states of development of our prototype in a better way. Consequently, the communication between the Manager and the Router was not implemented with the PoC.

5 Evaluation

5.1 Evaluation Setup

As previously mentioned, (i) to simplify the evaluation and (ii) to reduce external effects as well as to (iii) to allow a better comparison of individual systems, traffic data was recorded in advance with the aid of special hardware. To this end, at the uplink of the University of Twente (40 GBit/sec uplink of the university with their parent ISP), all incoming as well as outgoing data stream was collected and recorded in September 2014, comprising a period of several days. Accordingly no filtering has been applied. Special focus has been placed on obtaining a *representative data stream*. Therefore, in advance, the authors were especially driven from the following considerations: (i) The data stream was deliberately recorded over several days (including weekends); (ii) it has been ensured that external unusual effects such as semester breaks were reduced to a minimum.
In the next step, we have enriched the data set of the University of Twente to (i) have a more solid and representative portfolio of attacks and (ii) to increase the throughput to the level that is typical for a Backbone Provider. The latter was necessary because, despite the fact that the university has a connection of 40 Gbit/s, this connection was - on average - only used at a relatively low level (low throughput). The use of synthetic attacks was also needed to have a good and typical portfolio of attacks. Here, we have especially made use of the publications of Arbor Networks (e.g., see [Ar14]).
In order to know the Ground Truth (within the scope of this PoC), we have then analyzed the original data set of Twente (slowly) with the use of (several) DPI-based IDSs for the presence of attack traces. Although the authors know that by doing so most likely not all attacks are revealed, for the lack of alternatives, the results obtained hereby are used as (relative) Ground Truth. Concerning the synthetic portion (background noise and synthetic attacks), of course, we have taken the real values as baseline.
With the help of two additional virtual machines (both also use Ubuntu 15.10) and a virtual switch (where next to the two traffic generators the evaluation machine was connected) the actual evaluation took place.
The sampling rate we used was 1-in-100 (frequency in which the packets are analyzed; on average, 1 in every 100 packets is captured and analyzed) with a polling-interval of 30 sec (timeframe in which the network device exports Flows to the collector); these settings are essentially based on a compromise of [PP09, bl15] and [nM15].

5.2 Findings

Due to brevity, we would like to discuss here especially the practical example of a Distributed Denial of Service attack. Figure 3 shows an appropriate excerpt.

Subsequently, we assume that the following factors are necessary for a positive identification:

1. A positive initial identification by the Flow-Based IDS,

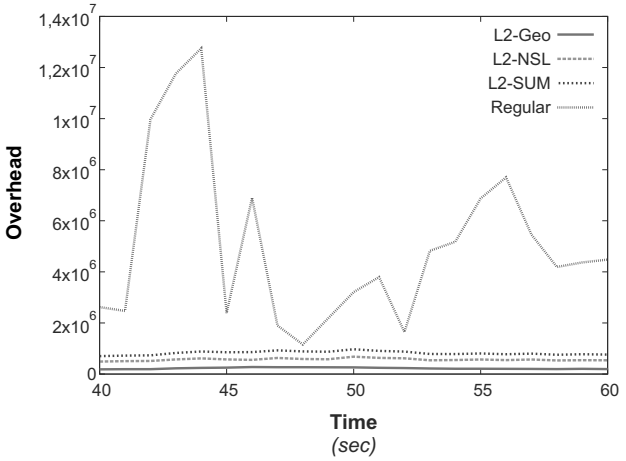


Fig. 3: Resource consumption of a DDoS; L2-Geo represents the Geolocation-time; L2-NSL refers to the NSLOOKUP-Time, L2-SUM corresponds L2-Geo + L2-NSL and Regular represents the regular overhead of the DPI-Based IDS

2. A precise geographical knowledge of both communication partners and other information (in order to consider possible contractual limitations - in particular, possible contractually guaranteed non-blocking agreements); for this, within the scope of the prototype, both NSLOOKUP resp. DIG, *and* the Geolocation of IPINFODB is used and all traffic (i) from/to Spain resp. (ii) governmental organization of the Netherlands is *never* blocked,
3. A positive verification from the DPI-Based IDS; this is particularly necessary to reduce the false alarm rate of the Flow-Based IDS. This is mainly due to the fact that the objective of a Backbone Provider is not to identify as many attacks as possible (as Intrusion Detection is not in the main focus of a Backbone Provider). Instead, a Backbone Provider rather likes to reduce the false alarm ratio to the absolute minimum possible.

Figure 3 and 4 are to be interpreted as follows: At the beginning of the detection of a DDoS attack, the overhead is relatively high, because new connections are initiated from different places. This results in a high overhead for both IDSs, but especially for the DPI-based IDS (see Figure 3 - regular). In spite of this overhead, with regard to Geolocation and NSLOOKUP the overhead is comparatively moderate, but also comprises quite high fluctuations (see Figure 4).

The reason why the overhead in Figure 4 decreases with time is because after a certain time, no new lookups are needed anymore. The real added value of the architecture is in particular (i) in the area of privacy and (ii) of maintaining contractually guaranteed obligations (in particular the non-blocking of certain communication relationships). In comparison to the direct use of a DPI-Based IDS without the Flow-Based IDS, the data load has been reduced with a factor of approx. one third, and - this is one of the main advantages - also guarantees

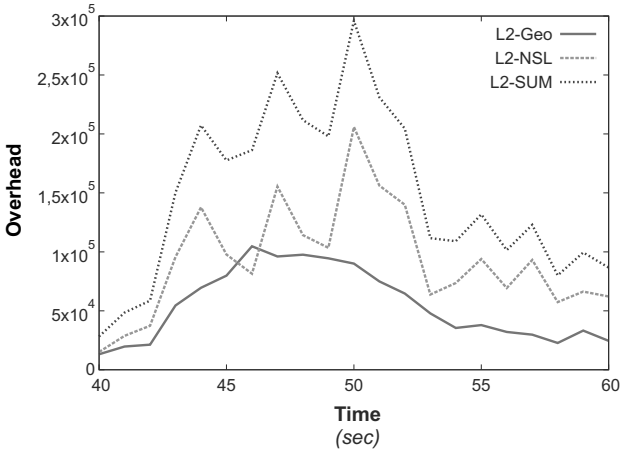


Fig. 4: Resource consumption of a DDoS; L2-Geo represents the Geolocation-time; L2-NSL refers to the NSLOOKUP-Time, L2-SUM corresponds L2-Geo

that data protection requirements are met. The use of Geolocation and NSLOOKUP also ensures a better applicability of existing business contracts.

6 Conclusions and Outlook

In this paper, we have presented an architecture for privacy-aware Multi-Layered Intrusion Detection, which aims at (i) reducing costs by being deployable on commodity hardware, (ii) overcoming legal limitations with respect to traffic analysis (a clear motivation in terms of a Flow-Based IDS alert is needed *before* DPI is performed) and (iii) compliance with specific aspects such as the contractually guaranteed non-blocking of data traffic of certain contractors. To this end, a generic architecture has been defined and a first implementation was realized. With the help of real-world traffic, the main benefits of the architecture were shown, too.

For the future, amongst other things, we plan to investigate in more detail: First, we like to examine the influence of the sampling rate; e.g. by using a sampling of 1:1 (i.e., everything is sampled), or 1:50. Second, we like to look for ways and means to consider the contracts between Backbone Provider and costumer in more detail. Third, we are trying to improve Intrusion Detection through inter-domain exchange of knowledge of attacks, both between "trusted partners" as well as between partners with whom there is no special trust relationship.

Acknowledgement

This work was partly funded by FLAMINGO, a Network of Excellence project (ICT-318488) supported by the European Commission under its Seventh Framework Programme.

References

[Ar14] Arbor Networks: , Worldwide Infrastructure Security Report - 2014 Volume IX, 2014.

[bl15] blog.sflow.com/: , sFlow Sampling rates, 2015.

[CE16] CERT/NetSA at Carnegie Mellon University: , SiLK (System for Internet-Level Knowledge). [Online]. Available: http://tools.netsa.cert.org/silk, 2016. [Accessed: January 24, 2016].

[DDW00] Debar, Hervé; Dacier, Marc; Wespi, Andreas: A revised taxonomy for intrusion-detection systems. In: Annales des télécommunications. volume 55. Springer, pp. 361–378, 2000.

[GHK14] Golling, Mario; Hofstede, Rick; Koch, Robert: Towards Multi-layered Intrusion Detection in High-Speed Backbone Networks. In: Proceedings of the 6th International Conference on Cyber Conflict (CyCon). IEEE, pp. 1–17, 2014.

[GKS14] Golling, Mario; Koch, Robert; Stiemert, Lars: Architektur zur mehrstufigen Angriffserkennung in Hochgeschwindigkeits-Backbone-Netzen. In: 7. DFN-Forum Kommunikationstechnologien, Beiträge der Fachtagung, 16.-17. Juni 2014, Fulda. LNI. GI, pp. 131–140, 2014.

[Ma09] Mansmann, Florian; Fischer, Fabian; Keim, Daniel A; Pietzko, Stephan; Waldvogel, Marcel: Interactive analysis of netflows for misuse detection in large IP networks. 2009.

[Ma13] Mandiant Corporation: , APT1 - Exposing One of China's Cyber Espionage Units. Mandiant Intelligence Center Report, 2013. http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf, last seen on 27/04/2014.

[nM15] nMon Corp: , Configuring switches to send sFlow, 2015.

[Op12] Open Discussion at www.reddit.com: , Netflow Tools... nfdump vs SiLK tool suite. Anyone have experience?, October 2012. Post filed 15 Oct 2012, http://www.reddit.com/r/netsec/comments/11iszm/netflow_tools_nfdump_vs_silk_tool_suite_anyone/, last seen on 28.07.2015.

[Op14] Open Discussion at http://www.gossamer-threads.com/: , oss netflow collector/trending/-analysis, May 2014. Post filed 2 May 2014, http://www.gossamer-threads.com/lists/nanog/users/171395, last seen on 28.07.2015.

[PP09] Phaal, Peter; Panchen, Sonia: , Packet Sampling Basics, 2009.

[Si15] Simon Leinen: , FloMA: Pointers and Software, April 2015. Last updated 11 April 2015, https://www.switch.ch/network/projects/completed/TF-NGN/floma/software.html, last seen on 28.07.2015.

[SM07] Scarfone, Karen; Mell, Peter: Guide to intrusion detection and prevention systems (idps). NIST special publication, 800(2007):94, 2007.

[Sp10] Sperotto, Anna; Schaffrath, Gregor; Sadre, Ramin; Morariu, Cristian; Pras, Aiko; Stiller, Burkhard: An overview of IP flow-based intrusion detection. Communications Surveys & Tutorials, IEEE, 12(3):343–356, 2010.

[Vi14] Viktor Pus and Lukas Kekely and Martin Spinler and Vaclav Hummel and Jan Palicka: , HANIC 100G: Hardware accelerator for 100 Gbps network traffic monitoring, 2014.

Security Awareness Kampagne als Element aktiven Lernens – ein Erfahrungsbericht

Marietta Spangenberg[1]

Abstract: Das Thema "Entwicklung von IT-Sicherheitsbewusstsein an der Hochschule Zittau/Görlitz" wurde im Modul IT-Sicherheitsmanagement der Masterausbildung Informatik als Projektaufgabe bearbeitet. Mit diesem Projekt sollten Aktivitäten im Bereich IT-Sicherheitsbewusstsein und Schulung zu IT-Sicherheitsfragen an der Hochschule initiiert und insbesondere eine Security Awareness Kampagne durchgeführt werden. Neben der Anwendung des erworbenen Wissens im Bereich IT-Sicherheitsmanagement in der Praxis waren bei der Bearbeitung des Themas weitere Kompetenzen wie beispielsweise Kreativität, Teamfähigkeit oder Kommunikation gefragt. Die Studierenden entwickelten eigenständig Ideen, etablierten ein Projektmanagement, bearbeiteten das Thema in Projektteams und realisierten eine Security Awareness Kampagne an der Hochschule mit einer abschließenden Evaluation. Das Projekt wird als Beispiel aktiven Lernens untersucht, der Aufwand für Studierende und Lehrende sowie die Projektergebnisse werden analysiert und bewertet.

Keywords: aktives Lernen, Didaktik, Hochschulausbildung, Informationssicherheitsmanagement, IT-Sicherheit, IT-Sicherheitsbewusstsein Kompetenzen, projektorientiertes Lernen, problembasiertes Lernen, Security Awareness

1 Einführung

Ständige Weiterentwicklungen der Informations- und Kommunikationstechnologien und der darauf basierenden Anwendungen verändern Gesellschaft, Wirtschaft, Wissenschaft und Ausbildung. Die zunehmende Vernetzung, die Integration der Netze, die Ubiquität der Informationsnutzung, das enorme Wachstum von Datenmengen und eine Zunahme der Komplexität bestimmen die Entwicklung. Dabei werden die Grenzen der bisherigen Informationsverarbeitung überschritten, wenn beispielsweise Smartgeräte im Haushalt zum Einsatz kommen oder autonome Fahrzeuge unterwegs sind. Andererseits werden jeden Tag neue Sicherheitsvorfälle und Bedrohungen bekannt, deren Ursachen in einer unzureichenden Informationssicherheit liegen. Nutzerdaten von Millionen von Nutzern wurden ausgespäht und missbräuchlich genutzt. Als Beispiel seien die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) Anfang 2014 publizierten Fälle des Identitätsdiebstahls von 16 bzw. 18 Millionen E-Mail-Adressen und Passwörtern genannt (vgl. [BS14], S. 29). Die wirtschaftlichen Folgen dieser Sicherheitsvorfälle sind ebenfalls gravierend, in Deutschland liegt der Schadensumfang durch Verbrechen unter Ausnutzung von Informations- und Kommunikationstechnik in der Größenordnung von

[1] Hochschule Zittau/Görlitz, Fakultät Elektrotechnik/Informatik, Theodor-Körner-Allee 16, 02763 Zittau, m.spangenberg@hszg.de

1,6 % des Bruttoinlandprodukts ([CS14]). Mit dem Stuxnet-Virus wurde die Verletzlichkeit von industriellen Steuerungssystemen verdeutlicht. Zunehmend sind diese Systeme ähnlichen Bedrohungen wie die traditionelle IT-Landschaft ausgesetzt (vgl. [BS13], S. 32-36). Die Nutzung der sozialen Netzwerke sowie aller Anwendungen, die auf der Nutzung des Internets basieren, bergen Gefahren für die Nutzer. Inwieweit ist beispielsweise Tracking im Netz mit unseren Persönlichkeitsrechten vereinbar? Damit werden neben technischen Fragen der Informationssicherheit zunehmend rechtliche, organisatorische, wirtschaftliche, finanzielle, aber auch ethische Fragen aufgeworfen, die in der modernen Hochschulausbildung adressiert werden sollten (vgl. [AC13], S. 35).

2 Herausforderungen der Informatikausbildung

Das Spannungsfeld der Beurteilung der Informatik bewegt sich zwischen der Einordnung als Hilfswissenschaft mit den daraus resultierenden „Bindestrich-Informatikern“ oder als Universalwissenschaft. Unbestritten ist in jedem Fall die Durchdringung aller Gebiete unseres Lebens durch Techniken und Methoden der Informatik mit vielen Anwendungsmöglichkeiten.

Als Schlagworte seien Big Data, Industrie 4.0, Cloud, Bring Your Own Device (BYOD) und das Internet der Dinge genannt. Die ungeheure Dynamik der Entwicklung der Informatik führt zu einem rasch verfallenden aktuellen Wissen in der Informatik. Das ist besonders für die Informatikausbildung relevant, da diese nicht von ein paar Schlagworten geprägt sein sollte, sondern Grundlagenwissen und Kompetenzen sollten derart vermittelt werden, dass die Studierenden für ihr zukünftiges Berufsleben dazu befähigt werden, sich neues Wissen eigenständig anzueignen und adäquat anzuwenden.

Bei den zu vermittelnden Inhalten ist es mittlerweile selbstverständlich, dass Informationssicherheit bzw. IT-Sicherheit in unterschiedlichen Facetten zum Fächerkanon der Informatikausbildung gehört (vgl. [AC13], S. 37). Neben konkreten Empfehlungen zur inhaltlichen Ausgestaltung der Ausbildung im Bereich der Informatik und IT-Sicherheit orientiert die Gesellschaft für Informatik (GI) für die Bachelor- und Masterausbildung im Fach Informatik zunehmend auf geforderte Kompetenzen (vgl. [GI05], S. 8ff.; [GI06], S. 4ff.). Der Fokus liegt nicht mehr auf Inhalten, sondern auf den Kompetenzen, die von einem Absolventen eines Informatikstudienganges erwartet werden.

Die genannte Problematik der großen Dynamik wird in den Bereichen IT-Sicherheit sowie IT-Sicherheitsmanagement besonders sichtbar. Täglich gibt es neue Angriffe auf Informationssysteme und IT-Infrastrukturen. IT-Sicherheit wird von der technologischen Entwicklung aber auch von der Kreativität und kriminellen Energie der Angreifer getrieben. Es kann in der Ausbildung nicht darum gehen, heute aktuelle Angriffsmethoden und Gegenmaßnahmen zu vermitteln, sondern es geht um prinzipielle Herangehensweisen und Methoden, die an aktuellen Fallbeispielen erworben und trainiert werden. Als Fallbeispiel soll ein Projekt im Modul „IT-Sicherheitsmanagement“ im Masterstudiengang Informatik der Hochschule Zittau/Görlitz dienen.

3 Modul IT-Sicherheitsmanagement

Das Modul wird im 1.Semester des Masterstudienganges Informatik angeboten und umfasst 4 Semesterwochenstunden (SWS) mit 2 SWS Vorlesung und 2 SWS Übung bzw. Seminar. Als Lehr- und Lernformen sind Vorlesung mit Präsentationen und Demonstration praktischer Beispiele, die selbstständige Erarbeitung von Stoffkomplexen, praktische Arbeit mit Risikomanagement- bzw. Sicherheitstools, Fallstudien, die eigenständige und Teamarbeit während der Projektbearbeitung, die Gestaltung von Workshops und eine exemplarische Vertiefung bestimmter Themen mittels Lösung einer komplexen Projektaufgabe mit möglichst starkem Praxisbezug vorgesehen. Neben Fachkompetenzen wie beispielsweise zu Methoden des Risikomanagement, der Methodik des IT-Grundschutzes des BSI, juristischen und wirtschaftlichen Grundkompetenzen, der Kenntnis und Anwendung von fachspezifischen Standards sollen die folgenden fachunabhängigen Kompetenzen erreicht werden ([Mo16]):

- Problemlösefähigkeit
- Planungs- und Entscheidungstechniken, Umsetzungskompetenz
- Kommunikationsfähigkeit
- Teamfähigkeit, Eigeninitiative
- Kreativität
- Leistungsbereitschaft
- Übernahme von Verantwortung

Wie bereits ausgeführt geht es um die Vorbereitung auf das berufliche Tätigkeitsfeld in der Zukunft. Hier ergibt sich die Frage, inwieweit mit traditionellen inhaltsbezogenen und lehrendenzentrierten Lehrformen die geforderten Ziele und Kompetenzentwicklung erreicht werden können oder ob aktive Lehr- und Lernformen besser geeignet sind. Gerade die Vermittlung nicht fachspezifischer Kompetenzziele, aber auch fachspezifischer Kompetenzen im Bereich des IT-Sicherheitsmanagements lassen eine weniger inhaltsorientierte und mehr projektorientierte Lehre sinnvoll erscheinen (vgl. [AC13], S. 24). Das schließt die Vermittlung von Grundlagen und aktuellen Inhalten ein, diese werden sozusagen als Mittel zum Zweck benutzt. Darauf aufbauend sollen Methoden und eigene Erfahrungen für die Zukunft entwickelt werden. Eine didaktische Zielstellung der Hochschulausbildung besteht in der Vermittlung eines möglichst anschaulichen und nachvollziehbaren Blicks auf das spätere Berufsfeld (vgl. [Wj05], S. 15). Die European Union Agency for Network and Information Security (ENISA) empfiehlt in [EN14] speziell für die Ausbildung auf dem Gebiet der Netzwerk- und Informationssicherheit konkrete Praxisbezüge und Kooperationen mit der Wirtschaft und Behörden.

4 Aktives Lernen

Der Begriff des „aktiven Lernens“ ist nicht präzise definiert. Die folgenden Merkmale werden aus pragmatischer Sicht als charakteristisch für das aktive Lernen angesehen:

- Die Studierenden sind über das reine Zuhören hinaus beteiligt.
- Die Entwicklung studentischer Fähigkeiten und Fertigkeiten ist wichtiger als die Informationsweitergabe.
- Die Studierenden werden zu höheren kognitiven Leistungen angeregt (Analyse, Synthese, Evaluation).
- Die Studierenden werden aktiviert (lesen, schreiben, diskutieren, beschreiben, …).
- Es wird größerer Wert darauf gelegt, dass die Studierenden ihre eigenen Konzepte, Einstellungen und Werte erkunden, so dass anstelle von Dozentenzentrierung eine Studierendenzentrierung erfolgt.

Nach [Rm12, S. 18 ff.] werden unterschiedliche Konzepte des aktiven Lernens wie beispielsweise handlungsorientiertes, problemorientiertes oder projektorientiertes Lernen unterschieden.

Bei dem untersuchten Fallbeispiel kommen traditionelle Lehre in Form von Vorlesung und Übung und projektorientiertes Lernen zum Einsatz. Die zu lösende Aufgabe stammt unmittelbar aus dem Berufsfeld, es erfolgt eine eigenständige Arbeit durch die Projektgruppe und es wird Wissen aus verschiedenen Bereichen verknüpft. Elemente des problemorientierten Lernens sind ebenfalls vertreten, indem unter Begleitung durch den Dozenten eine eigenständige Wissensaneignung während des Lernprozesses erfolgt. Der Wissenserwerb wird somit nach Mandl und Krause (vgl. [MK01], S. 4ff.) als aktiver, konstruktiver, situativer und sozialer Prozess realisiert.

5 Projekt IT-Security Awareness-Kampagne

Im Rahmen des zu untersuchenden Projektes „Entwicklung von IT-Sicherheitsbewusstsein an der Hochschule Zittau/Görlitz“ im Modul „IT-Sicherheitsmanagement“ sollte von den Studierenden eine Security Awareness Kampagne für die Hochschule organisiert werden. Die Awareness Kampagne war Bestandteil der Entwicklung eines Informationssicherheitsmanagementsystems (ISMS) basierend auf ISO 27001 und IT-Grundschutz (BSI) an der Hochschule. Die Ziele der Awareness Kampagne bestanden in der Sensibilisierung der Hochschulangehörigen in IT-Sicherheitsfragen und der Schaffung einer Basis für Schulungsprojekte.

Das hier dargestellte Projekt sollte sowohl matrikelübergreifend gestaltet werden als auch eine große praktische Relevanz zur Verstärkung der Elemente der aktiven Lehre aufweisen. Das Lernen sollte in einer komplexen und realitätsnahen Situation erfolgen.

In Abbildung 1 ist die Einbettung des Projektes in den Ablauf des gesamten Semesters dargestellt. Es ist ersichtlich, dass zu Beginn des Semesters traditionelle Lehrformen zur grundlegenden Wissensvermittlung und zum Kennenlernen entsprechender Methoden gewählt wurden.

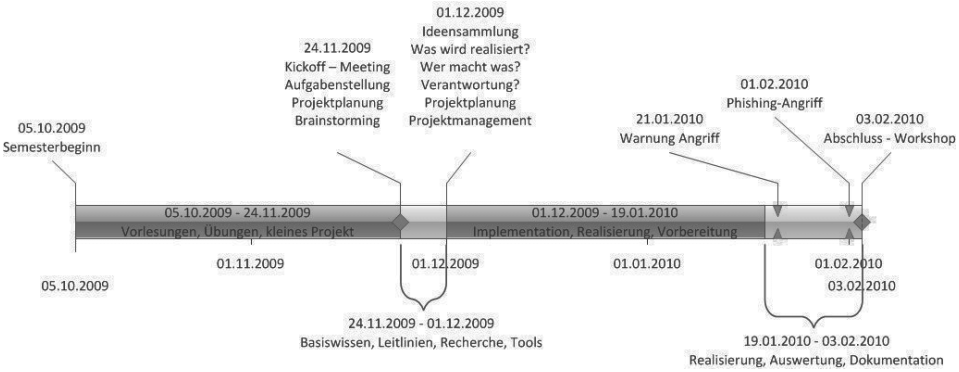


Abb. 1: Ablauf Projekt – Einordnung in das Semester

Gerade bei der Einführung von ISMS in Unternehmen klaffen Anspruch und Realität oft weit auseinander. Die Durchsetzbarkeit ist schwierig, sei es weil Ressourcen fehlen oder die Akzeptanz nicht vorhanden ist oder die Kommunikation ganz einfach schlecht oder unzureichend ist und es an IT-Sicherheitsbewusstsein mangelt. Diese Situation bereits während des Studiums kennenzulernen und Lösungsmöglichkeiten für die Praxis zu entwickeln, ist für Studierende eine große Chance, wesentliche Kompetenzen für die berufliche Arbeit zu entwickeln.

Die detaillierten Projektziele waren wie folgt formuliert:

- Lösung einer konkreten Aufgabenstellung aus dem Fachgebiet/zukünftigem Berufsfeld für ein Unternehmen (Hochschule)
- Kenntnisse aus dem Fachgebiet anwenden und weiterentwickeln
- eigenständige Bearbeitung durch Projektgruppe
- Verknüpfung von Wissen aus verschiedenen Bereichen
- Entwicklung von Eigeninitiative und Kreativität
- Auswahl geeigneter Werkzeuge, Methoden und Hilfsmittel
- Einsatz geeigneter Medien
- Projektmanagement
- Kommunikation und Teamfähigkeit

Diese Ziele stehen für projektorientiertes bzw. projektbasiertes Lernen.

Die Ideensammlung beim Kickoff-Meeting reichte vom einheitlichen Logo über die Gestaltung eines Webauftrittes, Workshops zu Sicherheitsthemen, einem Quiz, einem Video bis zu einem fingierten Phishingangriff. Aufgrund des großen Engagements der Studierenden konnten alle Ideen realisiert werden. Die Arbeit erfolgte in Gruppen mit jeweils 2 bis 4 Studierenden je nach Teilaufgabenstellung. Da alle Aktivtäten und Komponenten der Kampagne miteinander verzahnt sein sollten, waren regelmäßige Abstimmungen im gesamten Team notwendig. Dazu fand pro Woche ein Treffen des gesamten Teams zur Darstellung des Arbeitsstandes, zur Klärung und Abstimmung offener Fragen statt. Neben den Treffen wurde über ein Wiki und per E-Mail kommuniziert.

Die Kampagne umfasste die folgenden Elemente: Logo, Plakate, Flyer, Workshops mit Mitarbeitern und Studierenden inkl. Evaluation, „Beobachtungen“ zum Sicherheitsbewusstsein, Quiz, Phishingangriff, Video, Webseite, hochschulweiter Workshop. In Abbildung 2 ist ein Plakat als beispielhaftes Ergebnis dargestellt.

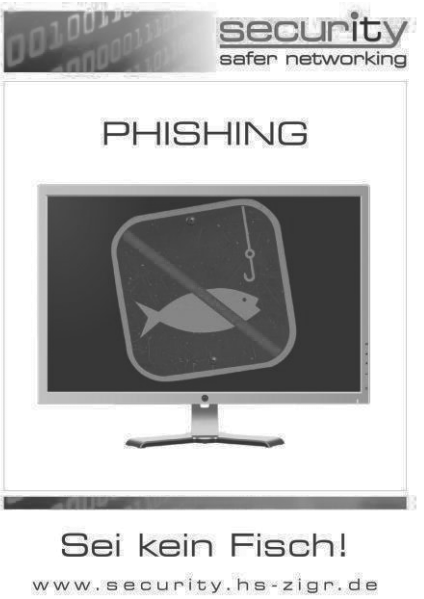


Abb.2: Beispiel eines Plakates der Kampagne

6 Elemente der Kampagne unter dem Aspekt aktiven Lernens

Alle Elemente der Kampagne waren Ergebnis des Brainstormings und stellten damit eigene Ideen der Studierenden dar. Die Bearbeitung erfolgte nach Interessenlage und persönlichen Erfahrungen, die teilweise auch aus anderen Fachgebieten stammten. Wissen wurde aktiv, selbstgesteuert und konstruktiv erworben und angewendet. Dabei

konnte auf die Inhalte der Lehrveranstaltung zurückgegriffen werden, aber auch eigene Recherchen waren erforderlich.

Bei Workshops zur Passwortsicherheit mit Mitarbeitern und Studierenden unterschiedlicher Fakultäten waren insbesondere die Kommunikation mit Nichtinformatikern und eine Ausrichtung der Inhalte auf das jeweilige Auditorium gefragt. Es wurde eine Evaluation der Ergebnisse durch Befragung der Teilnehmer durchgeführt. Mit der eingesetzten Methodik der Befragung und Auswertung erfolgte die Zusammenführung fächerübergreifender Erfahrungen. Beim Logo, den Plakaten und den Flyern mussten einerseits inhaltliche Fragen und andererseits ein ansprechendes Design beachtet werden. Der hochschulweite Phishingangriff erforderte Kenntnisse der Programmierung, zum Netzwerk, zu Anwendungen, zur IT-Sicherheit, zum Datenschutz und war eine Herausforderung in der Organisation. Auch beim Video spielten adäquate Inhalte der IT-Sicherheit, aber auch eine spannende Story eine Rolle. Es mussten Schauspieler akquiriert werden und die Videoproduktion einschließlich der technischen Voraussetzungen war zu organisieren. Die Vorbereitung des abschließenden hochschulweiten Workshops erforderte eine perfekte Organisation über Einladung, Anmeldung, Raumorganisation und Öffentlichkeitsarbeit und die ansprechende Präsentation der Ergebnisse. Damit wird deutlich, dass jedes Element der Kampagne unmittelbar aktives Lernen war und sowohl die geforderten Fachkompetenzen als auch die fachunabhängigen Kompetenzen in ihrer Entwicklung gefördert hat.

Die Rolle der Lehrenden hat trotz der unmittelbaren Studierendenzentrierung nicht an Bedeutung verloren. Ganz wichtig war die Beratung in Fachfragen und zur Organisation. Es bestand die Notwendigkeit, Abstimmungen mit den Verantwortlichen der Hochschule (Hochschulleitung, IT-Sicherheitsmanagementteam, Hochschulrechenzentrum, Dezernaten, Fakultäten) vorzunehmen. Gegenüber dem Auftraggeber war die Gesamtverantwortung für das Projekt zu übernehmen und als Ansprechpartner für alle Beteiligten zu fungieren.

7 Erfahrungen

Die Laufzeit des Projektes umfasste ca. zwei Monate, 19 Studierende waren beteiligt. Innerhalb dieses Zeitraums wurden ca. 20 Zeitstunden des Unterrichts für das Projekt aufgewendet. Der zusätzliche Aufwand pro Studierendem belief sich laut Befragung der Studierenden zwischen 30 und 200 Stunden. Das Video beanspruchte dabei die meiste Zeit. Allein die Bearbeitungszeit steht für ein weit überdurchschnittliches Engagement der Studierenden. Es ist gelungen, die Studierenden zu motivieren und zu aktivieren. Das Projekt soll nun aus unterschiedlichen Sichten eingeschätzt werden.

Sicht der Studierenden

Die studentische Arbeit kann mit den Stichwörtern: Begeisterung, Initiative, Motivation, Selbstverwirklichung, Organisation, Kooperation, Kommunikation auch mit Nichtinfor-

matikern, Kreativität, Übernahme von Verantwortung, Verlässlichkeit beschrieben werden. Das Projekt verursachte zumindest partiell einen sehr hohen Workload, der aber von den Studierenden nicht beklagt wurde. Allerdings wurden während der Bearbeitungszeit teilweise Abstriche bei anderen Modulen gemacht. Die praktische Aufgabenstellung und das unmittelbare Feedback wie beispielsweise die Reaktionen auf den Phishingangriff beflügelten die Studierenden. Unterschiede zwischen Theorie und Praxis mussten ebenfalls realisiert werden.

Sicht der Lehrenden

Die Projektbegleitung stellte aufgrund der Einbindung des Projektes in den Hochschulalltag eine neue Herausforderung dar. Es handelte sich nicht um ein fiktives Fallbeispiel, bei dem das Ergebnis für die Lehrende zu Projektbeginn feststeht, sondern um die Integration des Projektes in die Praxis mit allen Problemen der Organisation und der Abstimmung mit Verantwortlichen der Hochschule.

Sehr beeindruckend war das Erleben des herausragenden studentischen Engagements, das teilweise beim Generieren immer neuer Ideen gedrosselt werden musste. Das unmittelbare Feedback der Studierenden hinsichtlich der praktischen Relevanz der Inhalte, die in der Lehrveranstaltung vermittelt wurden, ist positiv hervorzuheben. Insgesamt war der Zeitaufwand für die Betreuung des Projektes sehr groß, da neben der Betreuung der Studierenden in einem neuen Projektumfeld die Kampagne an der Hochschule als Ansprechpartner begleitet werden musste.

Die erreichten Ergebnisse und Befragungen der Studierenden zeigen, dass diese Form der Projektarbeit und des aktiven Lernens sehr gut geeignet ist, die geforderten fachspezifischen und fachunabhängigen Kompetenzen zu erreichen. Der Wissenserwerb erfolgt sehr intensiv und nachhaltig.

Sicht des „Auftraggebers“ Hochschule

Sowohl hinsichtlich der unmittelbaren Wirkung als auch der Nachhaltigkeit hat die Security Awareness Kampagne alle Ziele erreicht. Mitarbeiter und Studierende wurden für IT-Sicherheitsprobleme sensibilisiert und motiviert, sich mit der Problematik auseinanderzusetzen. Gerade die Erfahrung mit dem Phishingangriff hat zu kritischen Reflexionen der eigenen Handlungsweise angeregt. Die Studierenden erstellten viele unmittelbar nachnutzbare Materialien, die als Basis für weitere Entwicklungen im Bereich Security Awareness genutzt werden konnten.

8 Fazit

Die Studierenden des Projektteams konnten beim Projektstart auf dem Gebiet der IT-Sicherheit auf eine fundierte Ausbildung im Rahmen ihres Bachelor- und Masterstudiums aufbauen. Sie waren aber bis dato keine Spezialisten in Awareness Kampagnen, im Management oder in der Kommunikation von IT-Sicherheitskonzepten. Trotzdem ist es gelungen, eine sehr komplexe Projektaufgabe aus dem Bereich Security Awareness zu

lösen und an der Hochschule mit ca. 4000 Studierenden und 400 Mitarbeitern wirksam werden zu lassen. Sehr positiv ist die Möglichkeit des bewussten Einbringens persönlicher Erfahrungen aus anderen Fachgebieten und die Integration persönlicher Interessen der Studierenden in die Projektarbeit zu bewerten. Darin werden wesentliche Gründe für die starke Motivation, die Effektivität und Effizienz der Projektbearbeitung gesehen. Zusammenfassend ist einzuschätzen, dass diese Form der Lehre und Projektbearbeitung sehr gut geeignet ist, die geforderten Lernziele zu erreichen und Kompetenzen zu entwickeln. Sehr motivierend haben sich die unmittelbare Anwendung der Projektergebnisse in der Praxis und das Feedback für die Studierenden ausgewirkt. Für zukünftige Projekte wird die Verknüpfung des traditionellen Wissenserwerbs mit realen praktischen Erfahrungen als wesentlich angesehen, wobei als praktisches Zielobjekt auch eine Hochschule geeignet ist.

Derartige Projektarbeit macht sowohl Studierenden als auch Lehrenden Spaß. Der Nachteil ist der immense zeitliche Aufwand. Wenn alle Module des Curriculums in dem Maße aktive Lehre einsetzen würden, würde das weit über das verfügbare zeitliche Volumen der Studierenden hinausgehen. Die Argumentation, dass der Lehrende für einen angepassten Umfang die Verantwortung trägt, ist nur bedingt zielführend, da ein solches Projekt gerade von der Aktivität und Initiative der Bearbeiter lebt, so dass eine strikte Begrenzung kontraproduktiv wäre.

Für Lehrende an Fachhochschulen mit 18 SWS ++ wäre eine komplette Umstellung auf aktive Lehr- und Lernformen in dieser Intensität in allen Modulen unter Beibehaltung der gegenwärtigen Studien- und Prüfungsordnungen nicht machbar. Die Durchführung von fächerübergreifenden Projekten stellt einen möglichen Lösungsansatz dar. Im Fallbeispiel konnte gezeigt werden, dass durch einen „dosierten“ Einsatz der aktiven Lehre geforderte Kompetenzen bei den Studierenden besser erreicht werden können als allein durch traditionelle Lehrformen.

Literaturverzeichnis

[AC13] ACM Computer Science Curricula 2013, December 2013, https://www.acm.org/education/CS2013-final-report.pdf, 20.3.2016

[BS14] Bundesamt für Sicherheit in der Informationstechnik (BSI): Die Lage der IT-Sicherheit in Deutschland 2014, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/-Publikationen/Lageberichte/Lagebericht2014.pdf, 20.3.2016

[BS13] Bundesamt für Sicherheit in der Informationstechnik (BSI): ICS Security Kompendium 2013, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security_kompendium_pdf.pdf?__blob=publicationFile&v=2, 20.3.2016

[CS14] Center for Strategic and International Studies: Net Losses: Estimating the Global Cost of Cybercrime, June 2014, http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf, 20.3.2016

[GI05] GI, Gesellschaft für Informatik e.V.: Empfehlungen für Bachelor- und Masterpro-

gramme im Studienfach Informatik an Hochschulen, http://www.gi.de/fileadmin/redaktion/empfehlungen/GI-Empfehlung_BaMa2005.pdf, 20.3.2016

[GI06] GI, Gesellschaft für Informatik e.V.: IT-Sicherheit in der Ausbildung, 2006 verabschiedet, https://www.gi.de/fileadmin/redaktion/empfehlungen/GI-Empfehlung-IT-Sicherheit-in-der-Ausbildung-2006.pdf, 20.3.2016

[EN14] ENISA: Public Private Partnerships in Network and Information Security Education, Case Studies, October 2014, https://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/public-private-partnerships-in-network-and-information-security-education, 20.3.2016

[MK01] Mandl, Heinz; Krause, Ulrike-Marie: Lernkompetenz für die Wissensgesellschaft, Forschungsbericht 145, LMU, 2001, https://epub.ub.uni-muenchen.de/253/1/FB_145.pdf, 20.3.2016

[Mo16] Modulkatalog der Hochschule Zittau/Görlitz, IT-Sicherheitsmanagement, https://web.hszg.de/Modulkatalog/, 20.3.2016

[Rm12] Rummler, Monika: Innovative Lehrformen: Projektarbeit in der Hochschule, Beltz Verlag, Weinheim und Basel, 2012

[Wj05] Wildt, Johannes: From Teaching to Learning, Tagung EWTF, Berlin, 17.11.2005

Shibboleth: Vollständiges Single Logout durch Kopplung von Anwendungs- und Shibboleth-Session am Apache-Webserver

Frank Schreiterer[1]

Abstract: Single SignOn (SSO) im Rahmen einer Authentication and Authorization Infrastructure (AAI) ist sehr verbreitet. Aktuell werden die Entwicklungen für das Single Logout (SLO) wieder vorangetrieben. Beim SSO-Verfahren Shibboleth besteht das Problem, dass beim Terminieren der Shibboleth-Session am Service-Provider nicht zwangsläufig auch die Anwendungs-Session terminiert wird. Dieser Beitrag zeigt eine Möglichkeit auf, vollständiges Single Logout zu erreichen. Dazu werden Shibboleth- und Anwendungs-Session direkt am Apache-Webserver gekoppelt, ohne in die Anwendung selbst einzugreifen.

Keywords: Shibboleth, Single Logout, SLO, Session-Management

1 Ausgangssituation

Durch Single SignOn, kurz **SSO**, lassen sich, basierend auf der Security Assertion Markup Language**,** kurz **SAML**, (vgl. [OA05], S. 1ff.), zahlreiche Webanwendungen grundsätzlich mittels des Shibboleth-Service-Providers, kurz **SP,** (vgl. [SE15]) authentifizieren und autorisieren. Das Abmelden an allen aufgerufenen Anwendungen, das Single Logout, kurz **SLO**, bereitet jedoch einige Probleme, wodurch die Entwicklung nur schleppend vorankommt. Die größte Herausforderung ist, dass sehr viele Anwendungen ein eigenes Session-Management integriert haben. Sie setzen nicht direkt auf die Shibboleth-Session auf. Somit besteht kein direkter Zusammenhang zwischen Anwendungs-Session und Shibboleth-Session (vgl. [SI15], [SL15]). Daneben existieren Anwendungen, welche nativ, d. h. ohne Shibboleth-Service-Provider, SAML unterstützen (vgl. [Ha14], S. 3). Bei diesen Anwendungen treten diese Probleme nicht auf. Sie werden im Folgenden nicht betrachtet.

Der Shibboleth-Identity-Provider, kurz **IdP**, unterstützt ab der Version 3.2 SLO über die Front-Channel-Implementierung, d. h. über den Webbrowser des Nutzers (vgl. [RN15]). Die vollständige Implementierung des SLO auch über Back-Channel, d. h. im Hintergrund via SOAP (Simple Object Access Protocol), wobei IdP und SP direkt miteinander kommunizieren, ist in Umsetzung.

[1] Otto-Friedrich-Universität Bamberg, Rechenzentrum Abteilung Serversysteme & Nutzerverwaltung, Feldkirchenstraße 21, 96052 Bamberg, frank.schreiterer@uni-bamberg.de

Seit IdP-Version 2.1 bis 2.3 existiert eine Implementierung des NIIF Institute (National Information Infrastructure Development Institute aus Ungarn) für SLO (vgl. [AS16]), die sowohl Front-Channel als auch Back-Channel unterstützt (vgl. [SL15]) und für Version 2.4 als Plugin portiert wurde (vgl. [MH16]). Diesen Implementierungen ist gemeinsam, dass beim Logout nur die Shibboleth-Session (SAML-Session), jedoch nicht die Anwendungs-Session (App-Session) terminiert wird (vgl. Abbildung 1).

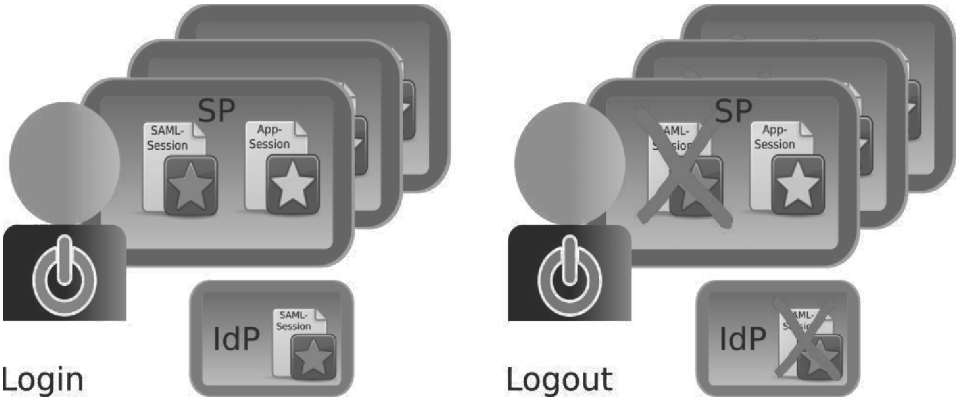


Abbildung 1: Ist-Zustand beim SSO und SLO

Neben diesem Problem resultieren aus der fehlenden Kopplung zwischen Anwendungs- und Shibboleth-Session folgende Probleme:

1. Zugriff ohne Shibboleth-Session
   In diesem Fall besteht die Gefahr eines nicht-autorisierten Zugriffs auf die Anwendung. Dieser erfolgt mit der bestehenden Anwendungs-Session ohne bzw. ungültige Shibboleth-Session, z. B. wenn die Shibboleth-Session am SP beendet wurde und die Existenz einer gültigen Shibboleth-Session nicht Voraussetzung für den Zugriff ist.

2. Manipulation der Anwendungs-Session
   Besitzt ein Angreifer eine gültige Shibboleth-Session, so kann die Anwendungs-Session manipuliert werden und damit ggf. eine nicht mehr bestehende Berechtigung in der Anwendung erreicht werden.

3. Eingriff in bestehende Software unmöglich
   Die Missstände aus 1. und 2. könnten mit Programmieraufwand beseitigt werden. Jedoch setzt dies voraus, dass der Quelltext vorhanden ist und dass die notwendigen Änderungen mit jedem Update wieder geprüft und angepasst werden. Oft ist man nicht in der Lage, diesen erheblichen Wartungsaufwand zu betreiben. Liegt der Quelltext nicht vor, so ist ein Eingriff in die bestehende Software unmöglich.

Ziel ist es daher, die Shibboleth-Session und die Anwendungs-Session direkt am Apache-Webserver ohne Eingriffe in die Anwendung zu koppeln und alle Sessions beim Logout zu terminieren und damit ein vollständiges SLO zu erreichen.

2 Kopplung am Apache-Webserver

Die Abschnitte zeigen Analyse, Entwurf und die Implementierung einer Lösung am Apache-Webserver, mit der eine Kopplung der Anwendungs-Session an die Shibboleth-Session erreicht und damit ein vollständiges SLO ermöglicht wird.

2.1 Analyse

Der Apache-Webserver bietet eine Vielzahl an Kontroll- und Manipulationsmechanismen z. B. bei Umgebungsvariablen und Cookies. Ein sehr mächtiges Werkzeug hierzu ist das Modul **mod_rewrite** (vgl. [AH15], [AM15]). Dieses Modul ermöglicht neben der Manipulation von URIs (Uniform Resource Identifiers) auch das Auslesen von HTTP-Headern und Cookies.

Standardmäßig stellt das Modul des Shibboleth-Service-Providers für den Apache-Webserver neben den Attributwerten die Shibboleth-Session-ID in den Umgebungsvariablen bereit (vgl. [NS15a]). Die Anwendung muss die Session-Information im Cookie oder in der URI speichern, damit diese am Webserver zugänglich ist. Somit ist der Zugriff auf den Identifier der Shibboleth-Session sowie auf den Identifier der Anwendungs-Session mittels mod_rewrite am Apache-Webserver gewährleistet und eine prinzipielle Kopplung von Shibboleth- und Anwendungs-Session möglich.

Die Kopplung muss in einem Datenspeicher abgelegt werden, um Prüfungen durchführen zu können. Prinzipiell kann hier als Datenspeicher memcached, ein einfacher Schlüssel–Wert–Speicher im RAM (vgl. [Mc15]), eingesetzt werden. Allerdings gehen bei einem Reboot oder Neustart des Dienstes die Beziehungen zwischen Shibboleth-Session und der Anwendungs-Session verloren. Gegen die Verwendung einer Datenbank kann der relativ hohe Administrationsaufwand sprechen. Für die Verwendung von memcached spricht, dass dieser zumindest unter Linux sehr einfach über die Paketverwaltung der gängigen Distributionen installiert werden kann.

Anwendungen können die Shibboleth-Session auf drei unterschiedliche Arten anfordern:

1. normal:
   Im Standardfall ist die Anwendung stets durch Shibboleth geschützt (vgl. [NS15b]) und damit ist die Shibboleth-Session immer vorhanden.

2. lazy:
   Die Authentifizierung gegen Shibboleth erfolgt anwendungsgesteuert nach Erfordernis (vgl. [NS15b]). Dadurch ist die Shibboleth-Session nicht stets vorhanden. Shibboleth bleibt aber die einzige Authentifizierungsmöglichkeit.

3. mixedLazy:
   Die Authentifizierung erfolgt anwendungsgesteuert nach Erfordernis. Neben der Authentifizierung gegen Shibboleth kann auch gegen andere Mechanismen authentifiziert werden. Somit kann eine Kopplung zwischen Shibboleth-Session und Anwendungs-Session nur erfolgen, wenn gegen Shibboleth authentifiziert wird.

Nachfolgend wird von den Anwendungsszenarien *normal, lazy und mixedLazy* gesprochen.

2.2 Entwurf

Bevor die Kopplung zwischen Anwendungs-Session und Shibboleth-Session erfolgen kann, muss in den Anwendungsszenarien normal und lazy sichergestellt sein, dass keine Anwendungs-Session vorhanden ist. Ansonsten könnte ungewollt oder vorsätzlich und mutwillig eine nicht mehr zulässige Anwendungs-Session Verwendung finden. Hierfür kann nach erfolgreicher Authentifizierung am IdP und dem Erzeugen der Shibboleth-Session am SP ein **sessionHook** definiert werden, der abgearbeitet wird, bevor das Redirect an die eigentliche Ziel-URI erfolgt (vgl. [NS15c]). Ist eine Anwendungs-Session vorhanden muss die Anfrage abgewiesen werden.

Im Anwendungsszenario mixedLazy kann diese Vorbedingung nicht geprüft werden, da Shibboleth nicht die einzige Authentifizierungsmöglichkeit ist und somit eine vorhandene Anwendungs-Session nicht zum Abweisen der Anfrage führen darf. Erfolgt die Authentifizierung über Shibboleth, so kann jedoch geprüft werden, ob der Identifier der Anwendungs-Session bereits vergeben war. Ist dies der Fall, so muss die Anfrage abgewiesen werden. Der weitere Ablauf erfolgt dann analog zum Anwendungsszenario lazy.

Folgende Parameter müssen somit für Validierung und Kopplung von Shibboleth- und Anwendungs-Session verarbeitet werden:

1. Kontext:
   a) sessionHook, wenn geprüft werden muss, ob eine Anwendungs-Session bereits vorhanden ist; dies ist nur bei den Anwendungsszenarien normal und lazy möglich.
   b) normal, wenn die Anwendung im Szenario normal verwendet wird oder
   c) lazy, wenn die Anwendung in den Szenarien lazy oder mixedLazy verwendet wird.

2. Shibboleth-Session-ID: Der Identifier der Shibboleth-Session, die vom SP-Modul an den Webserver übergeben wird.
3. Name des Cookies der Anwendung-Session, um den Identifier der Session extrahieren zu können.
4. Cookies: Alle Cookies, damit die Kopplung durchführbar ist und Prüfungen vorgenommen werden können. Die Cookies der Shibboleth-Session und der Anwendungs-Session sind in diesen Cookies enthalten.
5. mixedLazy: Ist der Schalter für die Prüfung auf doppelte Identifier der Anwendungs-Session, wobei dieser nur im Anwendungsszenario mixedLazy Verwendung finden darf.

Ausgehend von diesen fünf Parametern findet eine mehrstufige Validierung statt, bis schlussendlich der Identifier der Shibboleth-Session mit dem Identifier der Anwendung-Session assoziiert wird.

2.2.1 Grundsätzliche Validierungen

Cookies aus Parameter 4 (vgl. Abschnitt 2.2) enthalten neben etwaigen anderen Cookies diejenigen mit den Identifiern der Shibboleth-Session sowie der Anwendungs-Session. Der Name des Cookies der Anwendungs-Session bestimmt sich dabei aus Parameter 3. Ebenfalls muss der Identifier der Shibboleth-Session vom SP aus Parameter 2 mit dem Identifier des Shibboleth-Session-Cookies übereinstimmen.

Identifier von Shibboleth- und Anwendungs-Session weisen jeweils ein spezifisches Muster auf. Gegen diese Muster werden beide Sessions geprüft. Weiterhin wird untersucht, dass jeweils nur ein Cookie für die Shibboleth- und Anwendungs-Session übermittelt wurde, d. h. ob nicht versucht wurde, zusätzliche Cookies einzuschleusen.

Im Kontext „sessionHook“ (Parameter 1.a)) wird geprüft, dass keine Anwendungs-Session vorhanden ist. Sind all diese grundsätzlichen Validierungen erfolgreich, so erfolgt anschließend die erweiterte Validierung.

2.2.2 Erweiterte Validierungen

Nach den erfolgreich abgeschlossenen grundsätzlichen Validierungen muss in den Anwendungsszenarien normal und lazy festgestellt werden, ob bereits die Kopplung zwischen Shibboleth-Session und Anwendungs-Session besteht. Wird diese nicht festgestellt, so handelt es sich um eine neue Sitzung. Die Kopplung von Shibboleth-Session und Anwendungs-Session wird im Datenspeicher abgelegt.

Bei einer vorhandenen Kopplung wird zum übergebenen Identifier der Shibboleth-Session der zugehörige Identifier der Anwendungs-Session aus dem Datenspeicher gelesen. Stimmen gelesener und per Cookie übergebener Identifier der Anwendungs-Session

überein, so ist die Anfrage gültig.

Zusätzlich müssen noch zwei Sonderzustände beachtet werden.

1. Im Moment der durchgeführten Authentifizierung mit Shibboleth darf noch keine Anwendungs-Session vorhanden sein, es muss aber eine Shibboleth-Session-ID existieren. Dieser Zustand muss als gültige Anfrage definiert werden.
2. Im Kontext „lazy“ existiert beim ersten Aufruf der Zielressource ein Zustand, bei dem weder die Shibboleth-Session-ID noch die Anwendungs-Session-ID vorhanden sind. Dies muss ebenfalls als gültige Anfrage betrachtet werden.

Das Anwendungsszenario mixedLazy lässt neben Shibboleth die Verwendung von weiteren Authentifizierungsmethoden zu. Damit ist es mit diesem Mechanismus nicht möglich, die Anwendung bei Nicht-Shibboleth-Authentifizierung gegen die Verwendung einer vorhandenen oder manipulierten Anwendungs-Session zu schützen. Hier muss man sich, wie bisher auch, auf die Schutzmechanismen der Anwendung verlassen. Erfolgt die Authentifizierung jedoch über Shibboleth, so ist es zwar nicht möglich, eine Anmeldung mit einer bestehenden Session zu unterbinden. Es kann aber eine Duplikatsprüfung vorgenommen werden.

In der Duplikatsprüfung wird untersucht, ob der Identifier der gelieferten Anwendungs-Session schon einmal an Hand der vorhandenen Daten aus dem Datenspeicher Verwendung fand. Dies bietet bei entsprechender Konfiguration der Verweildauer der Daten im Datenspeicher quasi den gleichen Schutz wie das grundsätzliche Verbot, sich mit einer bestehenden Anwendungs-Session anzumelden. Der Mechanismus zur Vorabprüfung mittels sessionHook auf eine bestehende Anwendungs-Session kann und darf hier nicht durchgeführt werden.

Folgender Abschnitt zeigt die praktische Umsetzung aus Analyse und Entwurf.

2.3 Implementierung

Das Modul mod_rewrite bietet neben den klassischen RewriteRules die Möglichkeit, per *RewriteMap* Skripte zur Bestimmung des Ergebnisses einer RewriteCond (Bedingung) ausführen zu lassen. Auf das Ergebnis der RewriteCond kann dann in einer RewriteRule reagiert werden (vgl. [AM15]). Damit ist es möglich, das zuvor definierte komplexe Regelwerk in einem externen Skript umzusetzen. Versuche, das Regelwerk nur mit RewriteRules umzusetzen, erwiesen sich als nicht zielführend, da Übersicht und Wartungsfreundlichkeit rasch verloren gehen. Als Skriptsprache für die prototypische Implementierung wurde PHP mit memcached als Datenspeicher gewählt[2], da PHP bereits Basis zahlreicher Anwendungen ist. Zur Implementierung der RewriteMap können aber beliebige unterstützte Skriptinterpreter verwendet werden (vgl. [AM15]).

[2] Der Quelltext des Prüfskripts einschließlich Konfiguration und Hilfsskripten für ein vollständiges Logout finden sich unter https://wiki.aai.dfn.de/de:shibslohttpd.

Während der Implementierung trat das Problem auf, dass nicht zu jedem Zeitpunkt der Anfrage die Variablen des Shibboleth-Daemons in den Umgebungsvariablen des Apache-Webservers zur Verfügung stehen. Gelöst konnte dieses nur werden, indem die Shibboleth-Variablen per Direktive *ShibUseHeaders On* auch in den Headern verfügbar gemacht wurden. Dadurch besteht grundsätzlich die Möglichkeit des HeaderSpoofings (vgl. [NS15a]). Jedoch wird vom Shibboleth-Daemon ein HeaderSpoofing mit dem Leeren der Shibboleth-Session quittiert, sodass die Gefahr als eher gering eingestuft werden kann. Es wird jedoch dringend empfohlen, in den Shibboleth nachgelagerten Anwendungen auf Umgebungsvariablen zuzugreifen.

2.3.1 Rückgabewerte Prüfskript

In der RewriteCond wird das Prüfskript mit den Parametern Kontext, Shibboleth-Session-ID, Name des Cookies der Anwendung-Session und den Cookies sowie dem optionalen Parameter 5 „mixedLazy“ aufgerufen (vgl. Abschnitt 2.2). Durch das Prüfskript werden folgende Werte zurückgegeben, auf die mit einer entsprechenden RewriteRule reagiert werden muss:

1. doLogout, d. h. es muss das Logout (vgl. Abschnitt 2.3.3) durchgeführt werden, wenn versucht wurde,
   a) mit einer Anwendungs-Session ohne Shibboleth-Session zuzugreifen,
   b) die Anwendungs-Session während der Sitzung zu verändern,
   c) zusätzlich eine weitere Anwendungs-Session und / oder Shibboleth-Session per Cookie einzuschleusen,
   d) oder die Shibboleth-Session während der Sitzung zu verändern.
2. doAppSession (Sonderzustand 1 aus Abschnitt 2.2.2),
   wenn die Initialisierung der Anwendungs-Session durch einen zusätzlich erzeugten Request sichergestellt werden muss, da ansonsten das Einschleusen einer vorhandenen Anwendungs-Session möglich ist. Der zusätzliche Request lässt sich z. B. durch Hinzufügen eines Refresh-Headers direkt am Webserver erreichen.
3. doLogin (Sonderzustand 2 aus Abschnitt 2.2.2),
   wenn ein Redirect an das Login erfolgen muss, da ansonsten das Einschleusen einer vorhandenen Anwendungs-Session möglich ist. Dieser Rückgabewert kann nur im Kontext lazy erreicht werden.
4. good,
   wenn keine Aktion notwendig ist.

2.3.2 Konfiguration für sessionHook

Wie zuvor ausgeführt, kann durch den sessionHook ein zusätzlicher Request erzeugt werden, der am SP in der shibboleth2.xml mit

```
<ApplicationDefaults
entityID="https://YOURSERVER/shibboleth"
REMOTE_USER="uid"
sessionHook="/checker/checker.php">
```

für die Anwendungsszenarien normal und lazy, jedoch nicht für mixedLazy konfiguriert wird. Das Programm checker.php erzeugt lediglich ein Redirect auf die Anwendung und damit den zusätzlich benötigten Request, um die Prüfung auf die nicht vorhandene Anwendungs-Session durchführen zu können. Am Apache-Webserver wird die Location „checker“ normal mit Shibboleth geschützt und die Gültigkeit der Anfrage per Prüfskript in der RewriteCond validiert, vgl. nachstehender Auszug aus der Konfiguration.

```
<Location /checker>
authType shibboleth
ShibRequestSetting requireSession true
ShibUseHeaders On
RewriteEngine On
#den Wert der Anwendungssession auslesen, um die
#Anwendungssession sauber beim Logout zerstören zu können
RewriteCond %{HTTP:Cookie} APPSESSIONNAME=([^;]+)
RewriteRule .* - [E=appsid:%1]
#Aufruf Prüfskript und Logout bei Rückgabewert doLogout
RewriteCond ${shibchecker:sessionHook,%{HTTP:Shib-
Session-ID},APPSESSIONNAME,%{HTTP:Cookie}} ^doLogout$
RewriteRule .*
https://YOURSERVER/eviluse/SESSIONREMOVER.php?
appsid=%{ENV:appsid
</Location>
```

2.3.3 Entfernen der Sicherungseinträge beim Logout

Im Datenspeicher werden die Sicherungseinträge als Paar der Identifier von Shibboleth-Session und Anwendungs-Session abgelegt. Über diese gespeicherte Kopplung lassen sich diese wieder aus dem Datenspeicher entfernen. Hierzu muss am SP in der Datei shibboleth2.xml das Notify-Element (vgl. [NS15d]) definiert werden:

```
<Notify Channel="back"
Location="https://YOURSERVER/logoutnotify.php"/>
<Notify Channel="front"
Location="https://YOURSERVER/logoutnotify.php" />
```

Das Notify-Element kann jeweils für Front-Channel (Kommunikation über den Browser) und Back-Channel (Kommunikation über SOAP) konfiguriert werden. Dieser Umstand wird genutzt, um per Front-Channel nur die Cookies der Anwendung zu zerstören und um per Back-Channel die Einträge im Datenspeicher zu entfernen und die Anwendungs-Session in der Anwendung selbst zu zerstören.

3 Implikationen für das Single Logout

Mit der vorgestellten Methodik ist es möglich, die Kopplung der Anwendungs-Session an die Shibboleth-Session herzustellen, ohne dass es notwendig ist, Veränderungen an der Anwendung vorzunehmen. Bisherige Implementierungen des NIIF für IdP-Version 2.1 bis 2.3 sowie auch die aktuelle Implementierung im IdP-Version 3.2 lassen das Problem der Kopplung der Anwendungs-Session an die Shibboleth-Session offen. Auch das Shibboleth-Entwicklungsteam zieht sich auf die Aussage zurück, dass die Terminierung der Anwendungs-Session beim Invalidieren der SAML-Session implementiert werden muss (vgl. [SL15], [SI15]).

Mit der vorliegenden Arbeit wird eine Möglichkeit aufgezeigt, die zum breiteren und zuverlässigen Einsatz des vollständigen SLO beitragen kann. Neben dem Problem der fehlenden Session-Kopplung werden von den Shibboleth-Entwicklern weitere technische Probleme diskutiert (vgl. [SI15]), die jedoch als weitestgehend gelöst gelten können. Nicht technische Faktoren wie Nutzerakzeptanz oder auch die organisationsweite Entscheidung, SLO einzusetzen, können hierdurch nicht gelöst, aber entscheidend unterstützt werden.

Damit vollständiges SLO breitere Anwendung findet, wäre allerdings eine Übernahme der Funktionalität direkt in den Shibboleth-Service-Provider notwendig. Mit Unterstützung des DFN-Vereins als Mitglied des Shibboleth-Consortium (vgl. [SC16]) soll auf die Entwickler eingewirkt werden, die Funktionalität direkt in den Shibboleth-Service-Provider aufzunehmen. Damit könnte die Administration einer Anwendung auf die Installation von Zusatzsoftware für den Webserver sowie zusätzliche Speicherstrukturen wie memcached oder Datenbank verzichten und direkt das Session-Management des SPs verwenden. Sollte dies nicht gelingen, so wäre es alternativ denkbar, die Lösung für andere Webserver wie z. B. Internet Information Server oder nginx zu portieren.

Literaturverzeichnis

[AH15] Apache HTTP Server Version 2.4 Documentation, http://httpd.apache.org/docs/2.4/en/, Abruf am 23.11.2015

[AM15] Apache Module mod_rewrite, http://httpd.apache.org/docs/2.4/mod/mod_rewrite.html, Abruf am 23.11.2015

[AS16] AAI Software provided by NIIF Institute, http://software.niif.hu/, Abruf 21.03.2016

[Ha14] Shibboleth-aware Applications, https://www.switch.ch/aai/support/presentations/sp-training-2014/T6-5-Shibboleth-Enabled-Applications.pdf, Abruf am 23.11.2015

[IE16] IdPEnableSLO, https://wiki.shibboleth.net/confluence/display/SHIB2/IdPEnableSLO, Abruf 21.03.2016

[OA05] OASIS (Hrgs.): Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, https://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf, Abruf 23.11.2015

[Mc15] memcached, https://github.com/memcached/memcached/wiki/Overview, Abruf 20.11.2015

[MH16] Manuel Haim, http://www.staff.uni-marburg.de/~haimm/, Abruf 17.03.2016

[NS15a] NativeSPSpoofChecking, https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPSpoofChecking, Abruf 24.11.2015

[NS15b] NativeSPEnableApplication, https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPEnableApplication, Abruf 25.11.2015

[NS15c] NativeSPApplication, https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPApplication, Abruf 25.11.2015

[NS15d] NativeSPNotify, https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPNotify, Abruf 26.11.2015

[PS14] Shibboleth – Single-Log-Out?, https://www.zki.de/fileadmin/zki/Arbeitskreise/VD/Protokolle/2014-03-20/beitrag_vd-ak_2014-03-20_schreiterer_pempe.pdf, Abruf 21.03.2016

[SC16] Shibboleth Consortium – Members, http://shibboleth.net/consortium/, Abruf 21.03.2016

[SE15] Shibboleth® Enabled Applications and Services, https://wiki.shibboleth.net/confluence/display/SHIB2/ShibEnabled, Abruf 23.11.2015

[SI15] SLOIssues, https://wiki.shibboleth.net/confluence/display/CONCEPT/SLOIssues, Abruf 26.11.2015

[SL15] Single Logout in Shibboleth IdP, https://wiki.aai.niif.hu/index.php/ShibIdpSLO; Abruf 26.11.2015

[RN15] ReleaseNotes, https://wiki.shibboleth.net/confluence/display/IDP30/ReleaseNotes, Abruf 24.11.2015

Eingrenzung von Risiken durch Diebstahl von Eduroam-Credentials

Guido Bunsen[1]

Abstract: Die Credentials für WLAN-Zugänge sind in vielen unterschiedlichen Endgeräten abgelegt. Je nach Qualität der Implementierungen der Netzwerktreiber und dem Kenntnisstand der Endnutzer ist es möglich, diese von den Endgeräten oder mit Hilfe von nicht legitimierten Accesspoints zu stehlen. Dieser Beitrag beschäftigt sich mit den daraus entstehenden Risiken und Gegenmaßnahmen, die nicht den verbesserten Schutz wertvoller Passworte zum Ziel haben, sondern die Verwendung von weniger vertraulichen Passworten zu erzwingen, für die der vorhandene Schutz ausreicht. Im Anschluss wird auf die Herausforderungen im Umsetzungsprojekt eingegangen und auf das Potenzial, das entstandene System als Service für andere Hochschulen anzubieten.

Keywords: Eduroam, Passwort, Informationssicherheit,

1 Einleitung

Seit dem Start im Jahr 2002 hat sich Eduroam an den meisten europäischen Hochschulen als ein Standard für den WLAN-Zugang etabliert. Die Roamingfähigkeit von Eduroam hat dabei maßgeblich zum Erfolg beigetragen. Die weite Verbreitung von WLAN in mobilen Endgeräten mit dem Aufkommen der Smartphones hat dazu geführt, dass der durchschnittliche Hochschulangehörige bereits 2 und mehr Endgeräte besitzt, die Eduroam nutzen können.

Damit steigt auch das Risiko, dass Eduroam für Angriffe auf die Hochschulinfrastruktur missbraucht werden kann. Die Ursache liegt weniger im Design der Eduroam-Protokolle, als vielmehr in teilweise unvollständig implementierten Schnittstellen in den Endgeräten sowie mangelnder Sensibilisierung und unzureichenden Kenntnissen bei den Endnutzern.

In diesem Artikel werden diese Risiken dargestellt und im Anschluss daran werden mögliche Maßnahmen diskutiert, um die Risiken zu reduzieren oder die Auswirkungen abzumildern. Anschließend wird ein mittlerweile umgesetztes Projekt zur Realisierung der ausgewählten Maßnahmen vorgestellt und welche Erfahrungen dabei gemacht wurden.

[1]RWTH Aachen, IT Center, Seffenter Weg 23, 52056 Aachen, bunsen@itc.rwth-aachen.de

2 Funktionsweise von Eduroam und Gefährdungen

Eduroam geht auf einen Vorschlag von Klaas Wierenga vom niederländischen SurfNET aus dem Jahr 2002 zurück [Edu16]. Kern dieses Vorschlags ist, den Angehörigen der teilnehmenden Einrichtungen das Roaming zwischen den jeweiligen WLAN Infrastrukturen zu ermöglichen. Vereinfacht kommt dafür auf den Endgeräten des Nutzers ein sogenannter IEEE 802.1X Supplikant zum Einsatz um die Autorisierung am Accesspoint und an den Radiusservern der lokalen Einrichtung und gegebenenfalls der Heimateinrichtung vorzunehmen. Die Radiusserver müssen dazu über eine Softwarekomponente verfügen, um die Autorisierungsanfragen von nicht lokalen Benutzern an deren Heimateinrichtung weiterzuleiten (Proxy-Funktionalität). Da die Autorisierungen gegebenenfalls über mehrere Radiusserver geleitet werden, ist es erforderlich, dass die Anfragen „Ende zu Ende“ verschlüsselt werden um Man-in-the-Middle-Angriffe (MITM Angriffe) auf die Passworte des Benutzers zu verhindern. Eduroam nutzt dazu das TLS-Protokoll, um zwischen dem Supplikanten auf dem Endgerät und dem Radius-Server der Heimateinrichtung einen gesicherten Tunnel zu etablieren. Es ist von entscheidender Bedeutung, dass das Endgerät den Radiusserver korrekt verifiziert, indem das vom Radiusserver präsentierte Zertifikat geprüft wird.

Sofern das Zertifikat des Radius-Servers korrekt verifiziert wird, kann man derzeit von einem ausreichenden Schutz der Benutzerkennung und des Passwortes ausgehen. Eduroam verwendet sichere Protokolle, wenn die Supplikanten diese vollständig und korrekt implementieren, UND wenn die Nutzer die Endgeräte korrekt konfigurieren.

Während man in der Anfangszeit von Eduroam noch davon ausging, dass die meist technikaffinen Nutzer in der Lage waren, die wenigen auf Windows und Linux basierenden Endgeräte korrekt zu konfigurieren, hat sich die Situation bis heute grundlegend geändert. Mittlerweile nutzen die Angehörigen einer Hochschule im Schnitt bereits deutlich mehr als ein Endgerät und die Varianten von Endgeräten (Smartphone, Notebooks, Chromebooks, FireSticks, Chromecast, …) und zugrunde liegenden Betriebssystemen (Windows, Linux, IOS, Androids, …) und deren Versionen sind kaum noch zu überschauen. Für die Hersteller von Geräten ist es wichtiger, dass der Nutzer schnell seine Internetverbindung bekommt, als das diese ausreichend geschützt ist. Im Zweifelsfall unterbleibt die Verifizierung des Zertifikates, wenn sonst die Verbindung nicht zustande kommt. Usability geht vor. Selbst wenn sich ein Endgerät sicher konfigurieren lässt, ist fraglich, ob der Endnutzer die Risiken und die technischen Grundlagen versteht und die Einstellungen korrekt vornimmt. Selbst durch umfangreiche Sensiblisierungsmaßnahmen und Schulungsmaterialien lässt sich keine ausreichende Umsetzung erreichen.

Die beschriebenen Mängel führen dazu, dass Passworte der Benutzer durch sogenannte „Rogue Access Points“ oder „Evil Twins“ mit der SSID „Eduroam“ gestohlen werden können.

Der Vollständigkeit halber sei erwähnt, dass die Passworte auf dem Endgerät im Klartext

verfügbar sein müssen und somit zumindest für Personen mit Administrationsrechten und technischem Know-How zugänglich sind. Ebenso ergibt sich ein Risiko dadurch, dass moderne Smartphones den Inhalt der Geräte in der Cloud „sichern“ oder gar in sozialen Netzwerken mit Freunden teilen [Pcw15].

3 Welche Risiken entstehen für die Hochschule

Seit der Einführung von Eduroam vor mehr als 10 Jahren hat sich die Hochschul-IT-Landschaft dramatisch verändert. Mobile Endgeräte waren noch die Ausnahme und die Prozesse im Student-Life-Cycle wurden erst nach und nach auf Selfservice-Portale im Internet umgestellt. Heute sind die Prozesse im Campusmanagement auf eine zuverlässige Authentifizierung der Nutzer angewiesen. Auch der Betrieb einer E-Mail-Infrastruktur erfordert sichere Authentifizierung der Nutzer. Anderenfalls muss man damit rechnen, das gestohlene Accounts für den Spamversand missbraucht werden und die Reputation der Infrastruktur unter ein akzeptables Maß fällt.

Der im vorherigen Abschnitt skizzierte Diebstahl von Passworten für den WLAN-Zugang alleine ist bereits unerwünscht. Zwar ist die missbräuchliche Nutzung von Bandbreite nicht so problematisch. Aber oft reicht der Zugang zum WLAN einer Hochschule, um kostenpflichtig lizenzierte Dienste zu nutzen.

Das größere Problem aber resultiert aus der Tatsache, dass häufig die Passworte für den WLAN-Zugang auch für den Zugang zu anderen Informationen und Diensten genutzt werden können. Zum Teil war es die Politik zahlreicher Hochschulen unter dem Stichwort Single-Sign-On (SSO) die Usability der Infrastruktur zu verbessern und anderes überhaupt nicht zuzulassen. Zum anderen kamen die Nutzer mangels Sensibilisierung nicht auf die Idee, für unterschiedliche Dienste im Internet verschiedene Passworte zu wählen. So können gestohlene WLAN Credentials auch an anderen Stellen missbraucht werden mit der Konsequenz, dass nicht nur der Eigentümer des Accounts mit unangenehmen Konsequenzen rechnen muss. Auch für die Betreiber des WLANs und anderer Dienste ist mit negativen Konsequenzen zu rechnen wie Reputationsverlust und Aufwänden für forensische Untersuchungen und Aufräumarbeiten.

Aus den obigen Überlegungen lassen sich die folgenden Schlüsse ziehen: Die Angreifbarkeit der WLAN-Zugänge ist von den unmittelbaren Folgen her beherrschbar, weil die Bandbreitennutzung von den Kosten her vernachlässigt werden kann und eine gesetzwidrige Nutzung außerhalb der Verantwortung des Betreibers liegt. Die Verwendung von gestohlenen Credentials für höherwertige Dienste ist deutlich weniger zu akzeptieren.

4 Was können wir tun

Die Frage, die sich natürlicherweise nun stellt, ist die nach geeigneten Maßnahmen um die Risiken für den Diebstahl von WLAN-Passworten zu reduzieren oder zumindest die Folgen eines solchen Diebstahls abzuschwächen.

1. Zunächst zur Betrachtung der Maßnahmen, deren Umsetzung überwiegend in der Verantwortung der Nutzer zu sehen ist. Eine solche Maßnahme wäre die Nutzer so zu schulen, dass sie in der Lage und willens sind, das Endgerät „sicher“ zu konfigurieren. Derartige Sensibilisierungen und Schulungen in Form von Dokumentation sind sinnvoll und sollen auch bereitgestellt werden. Wir sind jedoch davon überzeugt, dass mit dieser Maßnahme allein keine eine ausreichende Wirkung nicht zu erzielen ist.
2. Eine Beschränkung auf Geräte mit einer „guten“ Implementierung würde die Risiken reduzieren. Jedoch ließe sich diese Maßnahme weder erzwingen, noch wäre es möglich, sie zu überwachen. Zusätzlich müsste eine Liste von „guten“ Geräten geführt und hinreichend begründet werden. Auch diese Maßnahme wurde verworfen.
3. Die zwangsweise Verwendung von solchen Passworten für den WLAN-Zugang, die nicht gleichzeitig auch für den Zugang beim Campusmanagement oder für E-Mail-Konten nutzbar sind, lässt sich über geeignete Passwort-Policies realisieren. Dafür hätten jedoch die Passwortregeln für Campusmanagement, den Mailserver und weitere Services angepasst werden müssen.
4. Die zwangsweise Verwendung von solchen Passworten für den WLAN-Zugang, die nicht gleichzeitig auch für den Zugang beim Campusmanagement oder für E-Mail-Konten nutzbar sind, lässt sich auch erreichen, indem die Passworte nicht durch den Benutzer frei wählbar sind, sondern zugewiesen werden. Diese Variante stieß zunächst auf Ablehnung. Weiter unten wird begründet, warum aus unserer Sicht die Nachteile vernachlässigt werden können.
5. Da der Diebstahl von Passworten nur schwer völlig zu verhindern ist, ist es gut, wenn ein solcher Diebstahl möglichst früh entdeckt wird. Das hilft nicht nur bei Diebstahl durch einen bösartigen Accesspoint wie oben beschrieben, sondern auch gegen Diebstahl durch Keylogger oder Phishing. Um einen Diebstahl zu entdecken, soll dem Benutzer die Möglichkeit gegeben werden ein Protokoll seiner Logins einzusehen. Dieses Protokoll könnte neben Datum und Uhrzeit auch eine Geolokation enthalten. Besonders auffällige Muster können benutzt werden, um den Nutzer anzuschreiben oder Accounts zu deaktivieren. Diese Maßnahme muss selbstverständlich datenschutzkonform gestaltet werden.

Wir haben uns entschieden, eine Kombination der beschriebenen Maßnahmen umzusetzen. Die Maßnahmen zur Sensibilisierung und Schulung lassen sich unabhängig von den anderen Maßnahmen durchführen und wurden auch in der Vergangenheit genutzt. Eine Intensivierung ist jedoch sinnvoll und möglich. Auch die Maßnahme zur

schnelleren Entdeckung von gestohlenen Accounts durch mehr Transparenz soll umgesetzt werden, allerdings erst zu einem späteren Zeitpunkt.

Die Maßnahme mit der größten Auswirkung auf den Nutzer und mit größeren Umbauarbeiten in der (Software-) Infrastruktur, nämlich der Zuweisung von Userid und Passwort für WLAN-Zugänge ist bereits im Rahmen eines weiter unten beschriebenen Projektes umgesetzt worden. Dazu vorab noch einige Bemerkungen.

Der Benutzer ist es gewohnt, sein Passwort frei zu wählen. Das ist unter Aspekten der Usability vorteilhaft, weil es so möglich ist, ein Passwort zu verwenden, das man sich leicht merken kann, z. B. weil es bestimmten Bildungsgesetzen folgt oder weil man es an vielen anderen Stellen ebenfalls nutzt. Allerdings geht es hier um WLAN-Passworte, die man typischerweise nur bei der Einrichtung eines Gerätes einmal einträgt und sich dann nicht mehr merken muss. Aus diesem Grund glauben wir, dass dieser Usability-Aspekt eine untergeordnete Rolle spielt. Um diesen gefühlten Nachteil weiter zu kompensieren, kann der Nutzer jederzeit weitere WLAN-Credentials anfordern, wenn er z. B. ein weiteres Gerät anbinden möchte. Er wird sogar dazu ermutigt, für jedes Gerät eigene Credentials zu verwenden. Das hat weitere Konsequenzen. So ist bei korrumpierten Accounts sogar feststellbar, welche Credentials missbraucht werden und damit, von welchem Endgerät sie gestohlen wurden. Alte unbenutzte Accounts werden automatisch nach mehrmonatiger Inaktivität gelöscht. Im Zusammenhang mit einer App wie z.B. der RWTH-App ist es möglich, für Smartphones das Passwort regelmäßig ohne Benutzerinteraktion im Hintergrund zu ändern. Da jedes Gerät eigene Credentials verwendet, sind durch die automatischen Passwortänderungen im Hintergrund keine Auswirkungen auf andere Geräte zu erwarten.

5 Umsetzungsprojekt

Die in den vorherigen Abschnitten beschriebenen Ziele und Ideen wurden etwa von März bis Juni 2014 entwickelt. Im September 2014 fiel die Entscheidung, ein Projekt „Eduroam-Gerätemanagement“ zur Realisierung dieser Ideen aufzusetzen. Zeitgleich wurde ein entsprechender Projektplan mit dem Projektende Dezember 2014 erstellt. Das Projekt hatte die folgenden für den Projektablauf entscheidenden Eigenschaften:

- Die Mehrzahl der Abteilungen im IT Center ist beteiligt (Netze, Services und Betrieb, Servicedesk, IT Prozessunterstützung, Administration und Organisation)
- Zahlreiche IT-Systeme oder Softwareprodukte müssen modifiziert werden (Radius, LDAP, Webanwendung für den Selfservice, Shibboleth)
- Unterstützung der stufenweisen Einführung durch geeignete Öffentlichkeitsarbeit in Zusammenarbeit mit dem Servicedesk für die Erstellung der zielgruppengerechten Dokumentation.

Es zeigte sich im Laufe des Projektes, dass aufgrund dieser Eigenschaften die folgenden

Aspekte in den Planungen berücksichtigt werden müssen:

- Konflikte zwischen Tagesgeschäft und Projektgeschäft
- Die Erfordernis, dass für bestimmte Arbeitspakete Kolleginnen und Kollegen aus verschiedenen Abteilungen gleichzeitig verfügbar sein müssen.
- Konflikte mit anderen Projekten
- Ausfälle durch Urlaub oder Krankheit
- Unklare Priorisierungen

Tatsächlich waren die Kernarbeiten erst Ende 2015 beendet. In der Zukunft werden Projekte, die abteilungsübergreifend durchgeführt werden, eher zunehmen und zur Normalität werden. Daraus resultieren neue Herausforderungen für das Projektmanagement und die abteilungsübergreifende Ressourcenplanung.

6 Erreichte Ziele

Auslöser für das Projekt Eduroam-Gerätemanagement war die Erkenntnis, dass unzureichende Vertraulichkeit der WLAN-Passworte negative Auswirkungen auf die Vertraulichkeit und Integrität anderer Services und Prozesse haben kann. Den damit verbundenen Risiken wurde begegnet, indem die Lösung nicht darin gesucht wurde, durch zahlreiche Maßnahmen einen ausreichenden Schutz der WLAN-Passworte zu erreichen. Ein solcher Schutz wäre nicht in ausreichendem Maße und mit vertretbarem Aufwand zu erreichen gewesen. Viel mehr besteht die Lösung darin, die Abhängigkeiten durch das Ausrollen von unabhängigen Passworten für den WLAN-Zugang aufzulösen.

7 Weitere Entwicklung

Schon in frühen Projektphasen gab es Ideen, das Eduroam Gerätemanagement als Service anzubieten. Der WLAN-Nutzer an der RWTH verwaltet seine WLAN-Accounts nach dem Wechsel auf das neue Verfahren über eine Webanwendung. Dort kann er für jedes seiner Geräte einen neuen Account anlegen. Den Zugang zu dieser Webanwendung erhält er nach Authentifizierung über das Verfahren Shibboleth zur verteilten Authentifizierung und Autorisierung [Sh16]. Zeitgleich mit dem Ergebnis der Authentifizierung erhält die Anwendung die Information, ob der Nutzer berechtigt ist, WLAN-Accounts anzulegen (Autorisierung).

Einer der durch den DFN für seine Mitglieder angebotenen Dienste ist die Authentifizierung- und Autorisierungsinfrastruktur, kurz DFN-AAI. Diese Infrastruktur ermöglicht Nutzern von Einrichtungen aus Wissenschaft und Forschung (Teilnehmer) über das Wissenschaftsnetz einen Zugang zu geschützten Ressourcen von Anbietern.

Nutzer, die auf geschützte Ressourcen zugreifen wollen, können sich an ihrer Heimateinrichtung authentifizieren und nach Übertragung der zur Autorisierung notwendigen Daten (Attribute) Zugang zu den Ressourcen erlangen.

Da die DFN-AAI auch auf Shibboleth basiert, kann die Webanwendung zur Verwaltung von WLAN-Accounts problemlos im Kontext des DFN-AAI als Anbieter eingesetzt werden [Dfna16]. Interessierte Mitglieder im DFN-Verein könnten so mit minimalem Aufwand ihren Angehörigen diesen Service bieten und so die Vertraulichkeit von Passworten für höherwertige Dienste verbessern. Im Rahmen eines Nachfolgeprojektes werden derzeit die Details für Migrations- und Supportkonzepte sowie für entsprechende Serviceangebote erarbeitet.

Eine andere geplante Weiterentwicklung betrifft die Verbindung von Eduroam-Gerätemanagement mit der RWTH-App für IOS oder Android. Durch Erweiterung des Eduroam-Gerätemanagements um einen entsprechenden Webservice kann die bereits authentifizierte App das Eduroam-WLAN automatisch einrichten und später auch periodisch das Eduroam-Passwort für das Endgerät wechseln. Die Vorteile für den Nutzer sind offensichtlich, mit den Details der Konfiguration muss er sich nicht mehr auseinandersetzen und durch die periodische Änderung des Passwortes bestehen eventuelle Risiken durch gestohlene Passworte nur für einen limitierten Zeitraum.

Literaturverzeichnis

[Edu16] eduroam, https://en.wikipedia.org/wiki/Eduroam, Abrufdatum: 5. Januar 2016

[Dfnc15] Google Android / eduroam-Zugangsdaten, https://www.dfn-cert.de/aktuell/Google-Android-Eduroam-Zugangsdaten.html, Abrufdatum 5. Januar 2016

[Pcw15] Windows 10's Wi-Fi Sense password sharing sparks security concerns, http://www.pcworld.com/article/2943752/wifi-passwordsharing-feature-in-windows-10-raises-security-concerns.html, Abrufdatum 5. Januar 2016

[Sh16] Shibboleth (Internet), https://de.wikipedia.org/wiki/Shibboleth_%28Internet%29, Abrufdatum 5. April 2016

[Dfna16] DFN-Verein: DFN-AAI, https://www.dfn.de/dienstleistungen/dfnaai/, Abrufdatum: 5. April 2016

Müller, Neumair, Reiser, Dreo Rodosek (Hrsg.): 9. DFN-Forum Kommunikationstechnologien,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2016 115

Zusammenwachsen von Gebäudeautomation und Computernetzwerken — Eine erste Sicherheitsanalyse

Thomas Mundt[1] und Peter Wickboldt[2]

Abstract: In diesem Papier schildern wir beispielhaft, welche Risiken bei der vernetzten Gebäudeautomation bestehen und wie diese Risiken beschränkt werden können. Dabei legen wir einen besonderen Fokus auf die Integration von Gebäudenetzwerken und allgemein bekannten Computernetzwerken - letztere durchaus auch in den Dimensionen des Internets. Wir betrachten dabei vor allem Büro- und Zweckbauten, in denen die Gebäudeautomation seit Jahren Standard ist, während sie unter dem Stichwort "Smart Home" gerade die Privathaushalte erobert. Klassische Verfahren zur Absicherung, wie Verschlüsselung und Authentisierung, Firewalling, Intrusion Detection / Prevention und Zonenkonzepte sind in der Gebäudeautomation weitgehend unbekannt.

Keywords: Sicherheit, Gebäudeautomation, Konvergenz der Netze.

Danksagung

Vielen Dank an Daniel Horak, Marc Stefan Martens, Claas Fastnacht, Dmitrij Nesterenko, Stephan Saß, Stefan Jastram, Dennis Retsch und Paul Töpper für die Unterstützung im Rahmen ihrer studentischer Abschlussarbeiten. Vielen Dank an Sven Thesenvitz von der Firma "Kieback & Peter - Technologie für Gebäude-Automation" für wertvolle Hinweise und Einblicke. Besonderen Dank an unsere Kollegen Hans-Walter Glock, Till Wollenberg und Andreas Dähn für die Unterstützung bei der forensischen Untersuchung des KNX-Netzwerkes.

1 Einleitung

Gebäudeautomation ist in Zweckbauten allgegenwärtig und wird von unterschiedliche Gewerken genutzt, angefangen von der Zutrittskontrolle über die Heizungs-, Klima- und Beleuchtungssteuerung bis zu Einbruchs- und Brandmeldung. Sie dient der funktionalen Betriebssicherheit, der Einsparung von Energie (z.B. Strom, Fernwärme) und andere Verbräuche (Wasser, Gas etc.), dem Umweltschutz und dem Komfort der Nutzer [As14].

Zur zentralen Steuerung und Überwachung (der Betriebsführung) werden dabei typischerweise mehrere Gebäude mit der Gebäudeleittechnik und auch untereinander vernetzt. Neben den für die Gebäudeautomation typischen Protokollen und Infrastruktur werden dabei

[1] Universität Rostock, Institut für Informatik, thomas.mundt@uni-rostock.de, Telefon +49 381 498 7505
[2] Universität Rostock, Zentrale Verwaltung - Dezernat Technik, Bau und Liegenschaften, peter.wickboldt@uni-rostock.de, Telefon +49 381 498 1397

in der Regel auch auf IP basierende Protokolle eingesetzt. Hierbei ist es natürlich sinnvoll, die ohnehin vorhandene Netzwerk-Infrastruktur gemeinsam zu nutzen. In Zukunft erwarten wir eine immer stärkere Konvergenz der Dienste aus der Gebäudeautomation hin zu IP-Netzwerken. Schon heute werden IP-Netzwerke in Bereichen eingesetzt, die noch vor kurzem eine ausschließliche Domäne von Feldbussen, seriellen Protokollen und Automationsnetzwerken waren.

Dabei wird entweder ein auf IP basierendes Protokoll zum Tunneln von Nachrichten zwischen Komponenten der Gebäudeautomation benutzt oder es wird gleich von Anfang bis Ende auf IP gesetzt. Ein Beispiel aus dem eigenen Universitätsgebäude: Das häufig auf der sogenannten Feldebene zu findende KNX-Protokoll zur Verbindung von Sensoren und Aktoren wird über Twisted-Pair Kupfer-Kabel im Gebäude übertragen, lässt sich aber auch durch IP über weite Entfernungen tunneln. Anbindungen zwischen verschiedenen Etagen und Gebäudeteilen sind so leicht zu erstellen.

In Zukunft dürfte dabei auch immer häufiger das Internet als Medium genutzt werden, insbesondere dann, wenn Aufgaben zusammengefasst werden und z.B. von externen Dienstleistern übernommen werden. Die zunehmende Vernetzung und Komplexität der Systeme zur Gebäudeautomation stellt enorme Anforderungen an die Sicherheit. Gemeint ist dabei nicht ausschließlich die funktionale Sicherheit, sondern auch der Schutz vor Missbrauch und Manipulation. Hier nimmt sogar der private ”Smart Home” Bereich eine Vorreiterrolle ein, zumindest sind private Anwender sensibilisierter und achten auf ”Versprechungen” von Sicherheit.

Die Tatsache, dass die Berichterstattung über erfolgreiche Angriffe von über das Internet ausgeführten Hacker-Angriffen auf traditionelle Computertechnik dominiert wird, sollte nicht über das gegenwärtige Gefährdungspotential in der Gebäudeautomation hinwegtäuschen. In mehreren Fallstudien haben wir Gebäudenetzwerke untersucht. Wir stellen im weiteren Verlauf die Ergebnisse vor und zeigen einige Lösungsmöglichkeiten auf.

2 Typischer Aufbau

Die Abbildung 1 zeigt den typischen Aufbau eines Gebäudeautomationssystems. Auf der untersten Ebene - Feldebene genannt - verbinden sogenannten Feldbusse die vorhandenen Sensoren und Aktoren miteinander. Sensoren können z.B. Schalter, Präsenzsensoren, Temperaturfühler, Schaltkontakte oder ähnliche Geräte sein. Als Aktoren dienen Relais (Jalousiensteuerung, Lampensteuerung etc.), Thermostate, Schlösser und viele andere mehr. Typischerweise werden hier Feldbusse (KNX [Th10], LON, ISOBUS uva.), drahtlose Übertragungsprotokolle (ZigBee, Z-Wave, EnOcean) oder vorhandene Kommunikationsdienste (WLAN, BACnet over IP, KNX over IP, HTTP usw.) eingesetzt.

Daneben werden auch einfachste, oftmals binär / seriell arbeitende, Datenverbindungen eingesetzt (EIA-485, EIA-232 usw.). Einfache Prozesse (auch Rezepte genannt), wie beispielsweise das Einschalten der Beleuchtung bei Aktivierung eines Bewegungssensors werden direkt in der Feldebene automatisiert. Komplexere Prozesse werden durch die Automatisierungsebene ausgeführt.

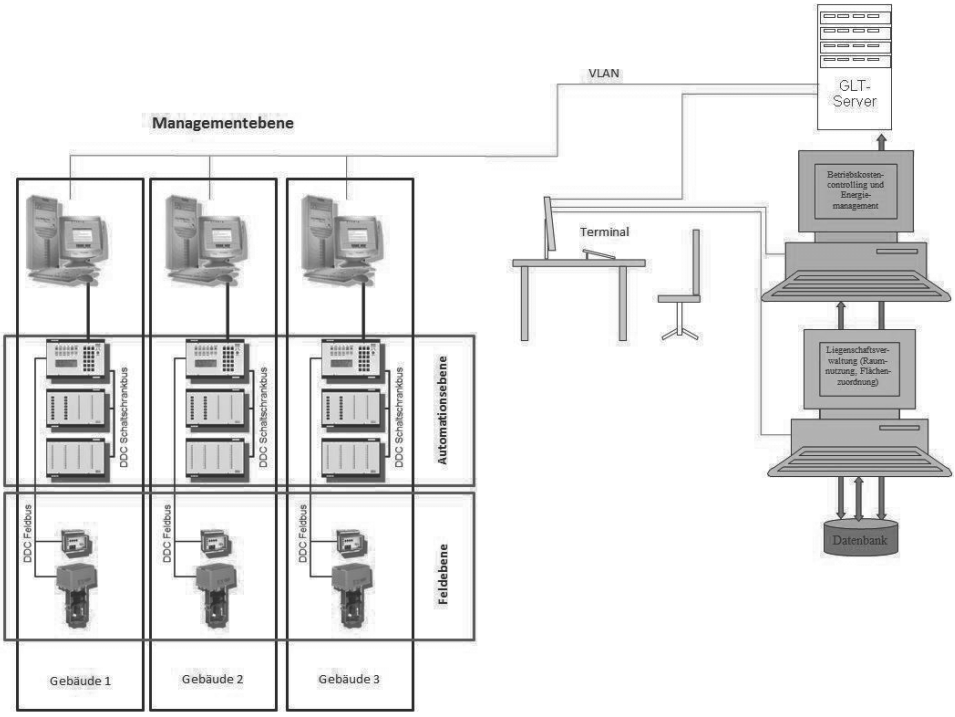


Abb. 1: Typischer Aufbau eines Systems zur Gebäudeautomation.

Auf der eben erwähnten, über der Feldebene liegenden, Automatisierungsebene steuern Controller oder Computer (Direct-Digital-Control-Gebäudeautomation, DDC-GA) die wesentlichen Prozesse im Gebäude. Sie bedienen sich dazu der Sensoren und Aktoren auf der Feldebene und sind mit der Feldebene über Gateways und höhere Protokolle (BACnet [Bu97], IP und darauf basierende Protokolle wie KNX/IP uva.) oder direkt über die zugeführten Feldbusse verbunden. Abhängig von Regelungsvorgaben und den gemessenen Sensorwerten werden Aktoren angesteuert.

Die Gebäudeleittechnik übernimmt die Aufgaben zum Bedienen und Beobachten (Überwachung), zur Messwertarchivierung, zur systemweiten Informationsweitergabe und zur Vorgabe der gewünschten Regelungsprozesse sowie deren Konfiguration.

3 Vernetzung in der Gebäudeautomation

Auf der Feldebene sind aus Kostengründen einfache Protokolle zu finden, häufig auf Twisted Pair Medien [MHH07]. In Europa sind KNX und LON [HBE11] in Zweckbauten besonders beliebt. Gelegentlich findet man auch PowerLine oder Funk als physische Medien. Vor allem im privaten Bereich oder bei der nachträglichen Aufrüstung sind letztere beliebt, da der Installationsaufwand reduziert wird.

Müssen größere Entfernungen überwunden werden, wird das Feldbus-Protokoll oftmals über ein IP-basierendes Protokoll getunnelt (KNX/IP oder LON over IP [DI14]). Bei großen Feldbussen kann das bereits in der Etagen-übergreifenden Installation sinnvoll sein. Zwischen den Geräten auf der Automatisierungsebene und der Gebäudeleittechnik werden regelmäßig IP-basierende Protokolle eingesetzt (weit verbreitet ist dabei BACnet/IP).

Die Zugangsmöglichkeiten zum Netzwerk sind unterschiedlich. Oft reicht es bei einer Zweidraht-Twisted-Pair-Leitung mit freier Topologie und unauthentisiertem und unverschlüsseltem Protokoll, ein Gerät an irgendeiner Stelle im Netzwerk auf der Feldbus-Ebene anzuschließen. Ebenso verbreitet ist der Einsatz von VPNs als Zugangsmöglichkeit auf die Gebäudeleittechnik oder zur Fernwartung der Steuerungssysteme. Über das Internet lassen sich so beispielsweise Updates einspielen oder Konfigurationen ändern. In einigen Ausnahmefällen sind Geräte direkt über offizielle IP-Adressen aus dem Internet erreichbar.

4 Gefährdungspotential

Zunächst stellt sich die Frage, welche Schäden denn überhaupt durch oder an der Gebäudeautomation entstehen können. Ohne übermäßig zu dramatisieren, sind eine ganze Reihe von Angriffen mit hohem Schadenspotential denkbar - siehe auch [PSS00]. Offensichtlich hochgefährlich sind erfolgreiche Angriffe auf Zugangskontrollsysteme sowie kostspielige Angriffe bei denen eine Zerstörung eintritt. Oftmals reicht es dem Angreifer aus, Chaos zu verursachen, ein Gebäude unnutzbar zu machen oder Aufmerksamkeit zu erregen. Unter Umständen kann dabei materieller oder gesundheitlicher Schaden entstehen. Mögliche Szenarios dazu sind:

- Mechanische Überlastung von z.B. Jalousie-Motoren oder Stellmotoren von Lüftungen durch wiederholtes, pausenloses Öffnen und Schließen.
- Elektrische Überlastung von z.B. Transformatoren durch gleichzeitiges Ein- oder Ausschalten von Verbrauchern mit induktiver Last.
- Vorzeitige Alterung von Bauteilen, z.B. Leuchtstoffröhren durch wiederholtes Zünden.
- Manipulation von Schranken oder automatischen Türen, so dass z.B. Autos beschädigt werden.
- Türen werden dauerhaft verschlossen. Mitarbeiter können sich nicht frei im Gebäude bewegen.
- Die Klimatisierung wird mit zu hoher oder zu niedriger Temperatur betrieben. Das wirkt sich auf Mitarbeiter aus, kann aber auch Auswirkungen auf installierte Technik haben. Insbesondere zu kühlenden Computertechnik reagiert sensibel auf deutlich zu hohe Temperaturen.
- Die Beleuchtung wird dauerhaft abgeschaltet oder zum Blinken gebracht. Geräte gehen kaputt oder werden unnötig verschlissen. Mitarbeiter werden am Arbeiten

gehindert. Ein Reputationsschaden kann auch auftreten, wenn mittels der Beleuchtungssteuerung von außen sichtbare Nachrichten auf der Fassade angezeigt werden.

- Die Belüftung wird so gesteuert, dass ein Unterdruck im Raum das Öffnen einer Tür verhindert oder die Tür selbständig öffnet.
- In sensiblen Bereichen (z.B. solche mit chemischen oder biologischen Apparaturen) kann eine Änderung der Belüftung / Ablüftung zur Freisetzung gefährlicher Substanzen führen.

Angriffe gegen die Vertraulichkeit der persönlichen Lebensumstände sind für die Betroffenen äußerst unangenehm. Darüber hinaus lassen sich diese Informationen ebenso als Grundlage für andere Angriffe nutzen. Beispiele sind:

- Überwachung der Anwesenheit von Mitarbeitern in einzelnen Büros.
- Überwachung des Sozialverhaltens. Wir konnten beispielsweise anhand der Daten der Anwesenheitssensoren im Gebäude aufzeigen, wie lange sich eine Person bei der Rückkehr ins Büro im Waschraum aufhielt.
- Nutzung der Gebäudesensoren, um festzustellen, ob gefahrlos in das Gebäude oder in einen bestimmten Bereich eingebrochen werden kann.

Angreifer können dabei ganz unterschiedliche Ziele und Motive haben. Denkbar sind wirtschaftliche Interessen (Störung von Konkurrenten), soziale Motive (beispielsweise Aufmerksamkeit erregen, Lehrveranstaltung oder Prüfung vermeiden) oder auch politische oder gar terroristische Motive bis zu geheimdienstlichen Aktivitäten, beispielsweise zum Zwecke der Destabilisierung.

5 Fallstudien

In mehreren Studien und mit Hilfe studentischer Arbeiten - siehe Danksagung - haben wir die Sicherheit typischer Gebäudeautomatisierungs-Systeme der Universität Rostock untersucht. Die dort verbaute Technik ist recht repräsentativ. Dabei wurde eine Methodik verwendet, die eng an die Sicherheitsanalyse von Computernetzwerken nach dem BSI-Standard 100-3 [BS05] angelegt ist.

Untersuchungsgegenstände waren dabei:

- **Sicherheit der verwendeten Protokolle**. Werden Nachrichten authentisiert und verschlüsselt? Hierbei ist wichtig, ob die Protokolle verlangen, dass Aussendungen nur von definierten Geräten erfolgen können (Authentisierung) oder ob Angreifer beliebige Nachrichten fälschen können. Für die Wahrung der Privatsphären der Nutzer des Gebäudeautomationssystems ist es wichtig, zu überprüfen, ob die Protokolle verschlüsselt oder unverschlüsselt arbeiten. Ebenso spielt es eine Rolle, ob die physikalische Schicht leicht abhörbar ist.

- **Zugriffsmöglichkeiten**. Über welche Wege kann sich ein potentieller Angreifer mit dem System zur Gebäudeautomation verbinden? Muss er vor Ort sein? Benötigt er Zugang zu bestimmten Räumen? Muss er sich physisch mit einem Medium verbinden? Welche Ausrüstung benötigt er für den Zugriff? Benötigt er Kenntnis von kryptografischen Schlüsseln?
- **Mögliche Auswirkungen eines Angriffs**. Welche Gerätschaften sind erreichbar? Welche Schadfunktionen können ausgelöst werden? Wie hoch wäre ein möglicher Schaden?
- **Organisatorische Aspekte**. Wer hat Zugang? Wie werden Zugänge verteilt und weitergegeben? Werden Zugriffe protokolliert?

Beim **ersten untersuchten Gebäude** handelte es sich um das gemeinsam vom IT- und Medienzentrum (ITMZ) und dem Institut für Informatik gemeinsam genutzte **Konrad-Zuse-Haus**. Das Gebäude wurde 2012 fertiggestellt. Auf der Feldebene kommt großflächig KNX über Zweidraht-Twisted-Pair-Kupferleitungen zum Einsatz. Daran angeschlossen sind als Sensoren alle Lichtschalter im Gebäude, sehr engmaschig ausgelegte Infrarot-Bewegungsmelder, Temperatursensoren in den klimatisierten Räumen und einige externe Sensoren für Wind, Regen usw. Als Aktoren sind Relais für Motoren der Jalousien und der innenliegenden Verdunkelungsrollos, Relais und Dimmer für die Beleuchtung und Thermostate über KNX angebunden.

Die elektronische Lautsprecheranlage, die Brandmeldeanlage, elektronische Zugangskontrolle über RFID-Karten, die Computer- und Telefonnetze sowie punktuell vorhandene Multimedia-Funktionen werden hier nicht detailliert betrachtet.

Das KNX-Netzwerk wurde bei der Installation in vier Areas unterteilt, diese wiederum in mehrere Lines. Eine Area bedient dabei eine Etage. Zwischen den Areas wurden Gateways installiert. Diese tunneln KNX-Telegramme über ein VLAN auf der ohnehin vorhandenen strukturierten Ethernet-Verkabelung.

Auf der Automatisierungsebene steuern mehrere DDC-Controller die Heizung und Klimatisierung / Lüftung im gesamten Gebäude. Die Controller sind dazu untereinander und mit dem KNX-Bus unter anderem über Ethernet und IP (VLAN) verbunden. Als Protokoll kommt unter anderem BACnet zum Einsatz. Darüber hinaus verfügen die DDCs über diverse Schnittstellen, beispielsweise HTTP. Das erwähnte VLAN ist von außen über ein VPN angebunden. Als IPv4-Adressen wird augenscheinlich ein privates Netzwerk (10.X.0.0/16) genutzt.

KNX als Protokoll kennt keinerlei Sicherheitsmaßnahmen. Alle Telegramme sind unverschlüsselt und werden nicht vom Absender authentisiert. Einen vermeintlichen, primitiven Schutz bieten lediglich der mechanische Schutz der verbauten Kabel vor Zugriff und die Unterteilung des gesamten Netzwerks in Areas. In einer Area konnten alle Nachrichten mit Quelladresse innerhalb der Area mitgelesen werden. Dazu wurde anfangs die Abdeckung eines öffentlich zugänglichen Lichtschalters entfernt und ein eigenes KNX/IP-Gateway an die vorhandene Zwei-Draht-Leitung angeschlossen. In einem zweiten Expe-

riment [MDG14] konnten die Telegramme berührungslos anhand der elektromagnetisch Abstrahlung des Twisted-Pair-Kabels aufgezeichnet werden. Die Metadaten (Zuordnung der Adressen zu Geräten und damit Standorten) konnten durch Beobachtung oder Provozieren von Aussendungen und Aufzeichnen der Telegramme gewonnen werden. Für Wartungszwecke sind zudem in allen Schaltschränken mit KNX-Bauteilen KNX/USB-Gateways eingebaut worden. Das betrifft auch Schaltschränke in nicht besonders gesicherten Räumen.

Eine Ansteuerung beliebiger Aktoren wäre durch das Aussenden von entsprechenden Telegrammen problemlos möglich gewesen. Sogar die Neukonfiguration der verbauten Lichtschalter etc. hätte von einem Angreifer vorgenommen werden können. So ließen sich zum ”Spaß” die Funktionen zweier Schalter im Gebäude vertauschen. Ebenso hätte zumindest eine Line komplett gestört werden können, durch simplen Kurzschluss oder durch Aussenden von Störimpulsen. Hätte man beispielsweise ein GSM-Modem unauffällig platziert oder eine ohnehin überall im Gebäude mögliche Verbindung zum Internet geschaffen, wäre Abhören und Aussenden eigener Steuerkommandos weltweit möglich. Gateways zu anderen Netzbereichen ermöglichen weitere Angriffe.

Noch gefährlicher sind Angreifer, die direkten, physischen Zugang, zum IP-basierten Backbone-Netz haben. Einige der angeschlossenen Geräte (Computer in der Gebäudeleittechnik, DDC-Controller, Gateways) sind mit Nutzername und Passwort vor dem direkten Zugriff geschützt, andere Geräte ließen unkontrollierten Zugriff auch auf relevante Funktionen zu. Zugang zu diesem übergreifenden Backbone-Netzwerk über ein VPN haben viele Mitarbeiter der Universitätsverwaltung, aber auch mehrere externe Vertragspartner zum Zwecke der Wartung. Eine Überwachung der Zugriffe findet nicht statt. Ob ein Hersteller von technischen Aggregaten darüber hinaus unangemeldete Zugänge über Mobilfunk eingebaut hat, konnte nicht vollständig ausgeschlossen werden. Unüblich wäre ein solches Vorgehen in der Branche nicht.

Mit Hilfe einfacher Netzwerktools (nmap, tcpdump, wireshark, nc, nrep) und einem Webbrowser mit Java konnten wir die Geräte des Backbone-Netzwerkes und deren Funktion ermitteln. Begünstigt durch teilweise vorhandene Hubs (statt Switches) und einer großen Anzahl von Broadcasts konnte die Struktur schnell erkannt werden. Ebenso konnten viele Nachrichten (Statusmeldungen, Steuerkommandos, Abfragen) im Klartext mitgelesen werden. Auf eine weitergehende forensische Untersuchung der Geräte und Netzwerke wurde mit Hinblick auf den laufenden Betrieb verzichtet. Für den Anschluss an das Netzwerk war in diesem Fall Zugang zu nichtöffentlichen Betriebsräumen notwendig.

Eine genauere Untersuchung des IP-basierten Backbone-Netzwerkes (VLAN über die universitätsweit verbreitete Infrastruktur mit inzwischen privaten Adressen), der Zugangsmöglichkeiten und der Maßnahmen zum Schutz dieses Netzwerkes (physische Zugansgbeschränkungen, Vermeidung von Konfigurationsfehlern, Regelungen zum VPN-Zugang etc.) konnte nicht erfolgen, da das ITMZ aus zeitlichen Gründen längere Zeit für eine Befragung nicht zur Verfügung stand. Das öffentlich einsehbare Sicherheitskonzept des ITMZ fokusiert auf die Sicherheit von Computern und traditionellen Computernetzwerken.

In einer **zweiten Analyse** wurden die Gebäude der Bereiche **Chemie und Biologie** untersucht. Hier wurde besonderes Augenmerk auf die Behandlung von giftigen oder gesundheitsgefährdenden Stoffen gelegt. Die Gebäude wurden um 2002 bezogen. Die Gebäudeautomatisierung betrifft im Wesentlichen die Klima- und Lüftungssteuerung. Die übrie Elektroinstallation (Licht, Verdunkelung) ist noch konventionell ausgelegt. Hervorhebenswert sind auf Grund der besonderen Brisanz der Anwendung per LON wiederum über Twisted-Pair-Kabel angebundene Abluftschränke und die Lüftungssteuerung im Laborbereich. Der physische Zugriff auf die Verkabelung ist trivial, zum einen weil die Topologie sehr flexibel ist, man sich also überall "anklemmen" kann, zum anderen, weil an den Lüftungsschränken Anschlussklemmen zu Überwachungs- und Wartungszwecken herausgeführt worden sind.

Für das verwendete LONworks-Protokoll sind zwar rudimentäre Verschlüsselungs- und Authentisierungsmöglichkeiten im Standard vorgesehen, in der Praxis werden diese aber so gut wie nie eingesetzt. Großen Schutz böten diese ohnehin nicht, da die Schlüssel nur 64bit lang sind und in jedem Gerät hinterlegt werden müssen.

Zum Anschluss der DDCs auf der Automatisierungsebene gilt das zuvor beim Konrad-Zuse-Haus gesagte. Auch hier ist das selbe VLAN als Backbone ausgelegt. Schutzmaßnahmen im Netzwerk wurden nicht gefunden, man verlässt sich auf die Abschottung des VLANs gegenüber anderen Netzbereichen. Über den selben, zuvor erwähnten, VPN-Zugang ist auch hier ein universeller Zugriff auf alle Komponenten der Gebäudeautomation möglich. Fremde Rechner können an vielen Stellen unauffällig und dauerhaft in dieses Netzwerk eingeschleust werden. Sobald sich ein Hersteller oder ein Wartungsunternehmen an einem Angriff beteiligen würde, hätte vermutlich selbst der Betreiber keine Chance, die Manipulation zu bemerken.

In einer **dritten Feldstudie** wurde die Anbindung der **Gebäudeleittechnik** betrachtet. Zwischen Leitrechner und DDCs wird überwiegend BACnet über IP eingesetzt. Der Leitstand selbst greift über das Microsoft Remote Desktop Protokoll auf den Leitrechner und auf andere Systeme der Gebäudeautomation zu. Hierbei kommt ebenfalls das schon mehrfach erwähnte VLAN zum Einsatz. Der Leitrechner befindet sich in einem gesicherten Raum. Das VLAN wird vom ITMZ bereitgestellt und lässt sich in nahezu allen Gebäuden der Universität auf freie Ports der dort verbauten Switches schalten. Dort werden dann weitere Steuerungssysteme der Gebäudeleittechnik angeschlossen. Die verwendeten IP-Adressen sind im übrigen überall an den Schaltschränken notiert und können bei der Wartung eingesehen werden. Offensichtlich wurde in den untersuchten Gebäuden der Adressbereich erst nach einiger Zeit von offiziellen IPv4-Adressen auf private Adressen umgestellt, vermutlich um ein einfaches, unbeabsichtigtes Verbinden mit dem Internet zu unterdrücken.

Der mit der Steuerung und Überwachung der Gebäudeautomation betraute Mitarbeiter muss sich individuell am Leitrechner einloggen, hat danach aber umfassende Rechte.

6 Auswertung der Feldstudien

Der "Zoo" von Protokollen, verschiedensten Anwendungen und unterschiedlicher Herstellern aus unterschiedlichen zeitlichen Abschnitten macht eine Absicherung des Systems überaus schwierig. Selbst eine Inventarisierung der verbauten Technik dürfte sich nach mehreren Umbauten und Ergänzungen als problematisch erweisen, erst Recht, wenn die Verantwortlichen wechseln und Drittfirmen ihrer Dokumentationspflicht nicht vollständig nachkommen. Die Ergebnisse der Analysen lassen sich wie folgt zusammenfassen:

- **Sicherheit der verwendeten Protokolle.** Dieser Punkt muss bei den am häufigsten auf der Feldebene eingesetzten Protokollen KNX und LON als verheerend bezeichnet werden. Einfachste Sicherheitsmaßnahmen, wie Verschlüsselung und Authentisierung, sind entweder in den entsprechenden Standards überhaupt nicht vorgesehen oder praktisch nicht von Nutzen. Ein Umstieg auf Protokolle mit besserem Schutz scheidet kurz- und mittelfristig aus, da dazu große Teil der Haustechnik ersetzt werden müssten. Das ist ohne längere Nutzungspause undurchführbar. Auch in den IP-basierten Netzwerken wird das Potential bekannter Schutzmaßnahmen nur selten genutzt. Hier sind ebenfalls ungesicherte Protokolle eher die Regel als die Ausnahme.
- **Zugriffsmöglichkeiten.** Potentiellen Angreifern gelingt es, nach Erlangung des physischen Zugangs, z.B. durch Installation eines Zwischensteckers hinter der Deckenverkleidung oder Öffnen eines Lichtschalters, beliebige Aktionen auf der Feldebene auszulösen. Durch die Strukturierung der Netzwerke und das Übergehen von Nachrichten in andere Netzbereiche wäre ein universeller Zugriff leicht zu bewerkstelligen. In IP-basierten Netzbereichen (VLAN) schützt man sich vor physischem Zugang durch Abschließen der entsprechenden Räume. Die Vielzahl der Räume an sich mit vielen Berechtigten und die Vielzahl der möglichen Netzzugänge und Möglichkeiten zur Fehlkonfiguration lassen das als gültigen Schutz fraglich erscheinen. Generell wurden einige - nicht alle - der untersuchten Zugänge auf Programme, Geräte und Gerätefunktionen mit Passwörtern gesichert. Gerade dann, wenn Zugänge auch an Fremdfirmen gegeben werden (müssen), erscheint auch das überdenkenswert.
- **Mögliche Auswirkungen eines Angriffs.** Wir schätzen das Risiko eines erfolgreichen Angriffs als sehr hoch ein. Einerseits kann der Angriff einfach durchgeführt werden, andererseits sind beträchtliche Schäden möglich. Angriffe mit dem Ziel von Chaos und Aufmerksamkeit sind in den untersuchten Gebäuden besonders leicht durchführbar. Beliebige Aktoren können auf der Feldebene angesteuert werden. Der Datenschutz muss verbessert werden. Sensordaten können zur Zeit einfach aufgezeichnet werden. Das Aufzeichnen von Protokollnachrichten im Backbone-Netz erfordern das Überwinden von Gateways oder das Vordringen in nichtöffentliche Räumen. Mit wenig Fantasie lassen sich Risiken in beträchtlicher Höhe ausmalen, die allesamt einfach und preiswert zu realisieren wären.
- **Organisatorische Aspekte.** Die Zusammenarbeit zwischen Gebäudetechnikern und Verantwortlichen für die Computernetzwerke wird zunehmend wichtiger. Sie soll-

te sich nicht auf das ”Durchschieben” von Nachrichten beschränken. Das Know How aus jahrelanger Erfahrung von Angriffen auf Computernetzwerke ist für die Gebäudeautomation ein wertvoller Wissensschatz, den es zu heben gilt. Hier gibt es Nachholbedarf. Grundsätzlich ist die lange Lebensdauer von Gebäudeautomationssystemen eine Herausforderung. Als unsicher erkannte Technologie kann nicht ohne größere Seiteneffekte problemlos ausgetauscht werden. Hinzu kommt der Wechsel von Verantwortlichkeiten während der Lebensdauer, die Vielzahl der Beteiligten (Planer, Errichter, Betreiber, Nutzer, oftmals jeweils durch Dritte vertreten), die Ergänzung und eventuell der Wechsel von Nutzungsszenarien. Nachträgliche Umbauten wurden und werden oftmals nicht dokumentiert. In vielen Fällen sind die Zuständigkeiten zwischen Gebäudeverwaltern und Netzwerktechnikern getrennt.

Fazit: Um die Sicherheit in der Gebäudeautomation ist es schlecht bestellt. Es muss offensichtlich zunächst etwas passieren, bevor geeigneten Abwehrmaßnahmen ergriffen werden. Gefordert sind hierbei zunehmend auch die Netzwerktechniker.

Literaturverzeichnis

[As14] Aschendorf, Bernd: Energiemanagement durch Gebäudeautomation: Grundlagen-Technologien-Anwendungen. Springer-Verlag, 2014.

[BS05] BSI: BSI-Standard 100-3 - Risikoanalyse auf Basis von IT-Grundschutz. Bundesanzeiger-Verlag. Bonn, 2005.

[Bu97] Bushby, Steven T: BACnet: a standard communication infrastructure for intelligent buildings. Automation in Construction, 6(5):529–540, 1997.

[DI14] DIN: , DIN EN 14908-4:2014 - Firmenneutrale Datenkommunikation für die Gebäudeautomation und Gebäudemanagement – Teil 4: Kommunikation mittels Internet Protokoll (IP) (Ursprüngliche Norm ANSI/CEA-852 – LonMark IP-852 IP-tunneling channel specification), 2014.

[HBE11] Hersent, Olivier; Boswarthick, David; Elloumi, Omar: The Internet of Things: Key Applications and Protocols. John Wiley & Sons, 2011.

[MDG14] Mundt, Thomas; Dähn, Andreas; Glock, Hans-Walter: Forensic analysis of home automation systems. In: The 14th Privacy Enhancing Technologies Symposium. Amsterdam, 2014.

[MHH07] Merz, Hermann; Hansemann, Thomas; Hübner, Christof: Gebäudeautomation: Kommunikationssysteme mit EIB/KNX, LON und BACnet. Hanser Verlag, 2007.

[PSS00] Palensky, Peter; Sauter, Thilo; Schwaiger, Christian: Security und Feldbusse - ein Widerspruch? it-Information Technology, 42(4):31–44, 2000.

[Th10] The KNX Consortium: , KNX Standard - System Specifications - Interworking, 04 2010.

GI-Edition Lecture Notes in Informatics

P-1 Gregor Engels, Andreas Oberweis, Albert Zündorf (Hrsg.): Modellierung 2001.

P-2 Mikhail Godlevsky, Heinrich C. Mayr (Hrsg.): Information Systems Technology and its Applications, ISTA'2001.

P-3 Ana M. Moreno, Reind P. van de Riet (Hrsg.): Applications of Natural Lan-guage to Information Systems, NLDB'2001.

P-4 H. Wörn, J. Mühling, C. Vahl, H.-P. Meinzer (Hrsg.): Rechner- und sensorgestützte Chirurgie; Workshop des SFB 414.

P-5 Andy Schürr (Hg.): OMER – Object-Oriented Modeling of Embedded Real-Time Systems.

P-6 Hans-Jürgen Appelrath, Rolf Beyer, Uwe Marquardt, Heinrich C. Mayr, Claudia Steinberger (Hrsg.): Unternehmen Hochschule, UH'2001.

P-7 Andy Evans, Robert France, Ana Moreira, Bernhard Rumpe (Hrsg.): Practical UML-Based Rigorous Development Methods – Countering or Integrating the extremists, pUML'2001.

P-8 Reinhard Keil-Slawik, Johannes Magenheim (Hrsg.): Informatikunterricht und Medienbildung, INFOS'2001.

P-9 Jan von Knop, Wilhelm Haverkamp (Hrsg.): Innovative Anwendungen in Kommunikationsnetzen, 15. DFN Arbeitstagung.

P-10 Mirjam Minor, Steffen Staab (Hrsg.): 1st German Workshop on Experience Management: Sharing Experiences about the Sharing Experience.

P-11 Michael Weber, Frank Kargl (Hrsg.): Mobile Ad-Hoc Netzwerke, WMAN 2002.

P-12 Martin Glinz, Günther Müller-Luschnat (Hrsg.): Modellierung 2002.

P-13 Jan von Knop, Peter Schirmbacher and Viljan Mahni_ (Hrsg.): The Changing Universities – The Role of Technology.

P-14 Robert Tolksdorf, Rainer Eckstein (Hrsg.): XML-Technologien für das Semantic Web – XSW 2002.

P-15 Hans-Bernd Bludau, Andreas Koop (Hrsg.): Mobile Computing in Medicine.

P-16 J. Felix Hampe, Gerhard Schwabe (Hrsg.): Mobile and Collaborative Business 2002.

P-17 Jan von Knop, Wilhelm Haverkamp (Hrsg.): Zukunft der Netze –Die Verletzbarkeit meistern, 16. DFN Arbeitstagung.

P-18 Elmar J. Sinz, Markus Plaha (Hrsg.): Modellierung betrieblicher Informationssysteme – MobIS 2002.

P-19 Sigrid Schubert, Bernd Reusch, Norbert Jesse (Hrsg.): Informatik bewegt – Informatik 2002 – 32. Jahrestagung der Gesellschaft für Informatik e.V. (GI) 30.Sept.-3. Okt. 2002 in Dortmund.

P-20 Sigrid Schubert, Bernd Reusch, Norbert Jesse (Hrsg.): Informatik bewegt – Informatik 2002 – 32. Jahrestagung der Gesellschaft für Informatik e.V. (GI) 30.Sept.-3. Okt. 2002 in Dortmund (Ergänzungsband).

P-21 Jörg Desel, Mathias Weske (Hrsg.): Promise 2002: Prozessorientierte Methoden und Werkzeuge für die Entwicklung von Informationssystemen.

P-22 Sigrid Schubert, Johannes Magenheim, Peter Hubwieser, Torsten Brinda (Hrsg.): Forschungsbeiträge zur "Didaktik der Informatik" – Theorie, Praxis, Evaluation.

P-23 Thorsten Spitta, Jens Borchers, Harry M. Sneed (Hrsg.): Software Management 2002 – Fortschritt durch Beständigkeit

P-24 Rainer Eckstein, Robert Tolksdorf (Hrsg.): XMIDX 2003 – XML-Technologien für Middleware – Middleware für XML-Anwendungen

P-25 Key Pousttchi, Klaus Turowski (Hrsg.): Mobile Commerce – Anwendungen und Perspektiven – 3. Workshop Mobile Commerce, Universität Augsburg, 04.02.2003

P-26 Gerhard Weikum, Harald Schöning, Erhard Rahm (Hrsg.): BTW 2003: Datenbanksysteme für Business, Technologie und Web

P-27 Michael Kroll, Hans-Gerd Lipinski, Kay Melzer (Hrsg.): Mobiles Computing in der Medizin

P-28 Ulrich Reimer, Andreas Abecker, Steffen Staab, Gerd Stumme (Hrsg.): WM 2003: Professionelles Wissensmanagement – Er-fahrungen und Visionen

P-29 Antje Düsterhöft, Bernhard Thalheim (Eds.): NLDB'2003: Natural Language Processing and Information Systems

P-30 Mikhail Godlevsky, Stephen Liddle, Heinrich C. Mayr (Eds.): Information Systems Technology and its Applications

P-31 Arslan Brömme, Christoph Busch (Eds.): BIOSIG 2003: Biometrics and Electronic Signatures

P-32 Peter Hubwieser (Hrsg.): Informatische Fachkonzepte im Unterricht – INFOS 2003

P-33 Andreas Geyer-Schulz, Alfred Taudes (Hrsg.): Informationswirtschaft: Ein Sektor mit Zukunft

P-34 Klaus Dittrich, Wolfgang König, Andreas Oberweis, Kai Rannenberg, Wolfgang Wahlster (Hrsg.): Informatik 2003 – Innovative Informatikanwendungen (Band 1)

P-35 Klaus Dittrich, Wolfgang König, Andreas Oberweis, Kai Rannenberg, Wolfgang Wahlster (Hrsg.): Informatik 2003 – Innovative Informatikanwendungen (Band 2)

P-36 Rüdiger Grimm, Hubert B. Keller, Kai Rannenberg (Hrsg.): Informatik 2003 – Mit Sicherheit Informatik

P-37 Arndt Bode, Jörg Desel, Sabine Rathmayer, Martin Wessner (Hrsg.): DeLFI 2003: e-Learning Fachtagung Informatik

P-38 E.J. Sinz, M. Plaha, P. Neckel (Hrsg.): Modellierung betrieblicher Informationssysteme – MobIS 2003

P-39 Jens Nedon, Sandra Frings, Oliver Göbel (Hrsg.): IT-Incident Management & IT-Forensics – IMF 2003

P-40 Michael Rebstock (Hrsg.): Modellierung betrieblicher Informationssysteme – MobIS 2004

P-41 Uwe Brinkschulte, Jürgen Becker, Dietmar Fey, Karl-Erwin Großpietsch, Christian Hochberger, Erik Maehle, Thomas Runkler (Edts.): ARCS 2004 – Organic and Pervasive Computing

P-42 Key Pousttchi, Klaus Turowski (Hrsg.): Mobile Economy – Transaktionen und Prozesse, Anwendungen und Dienste

P-43 Birgitta König-Ries, Michael Klein, Philipp Obreiter (Hrsg.): Persistance, Scalability, Transactions – Database Mechanisms for Mobile Applications

P-44 Jan von Knop, Wilhelm Haverkamp, Eike Jessen (Hrsg.): Security, E-Learning. E-Services

P-45 Bernhard Rumpe, Wofgang Hesse (Hrsg.): Modellierung 2004

P-46 Ulrich Flegel, Michael Meier (Hrsg.): Detection of Intrusions of Malware & Vulnerability Assessment

P-47 Alexander Prosser, Robert Krimmer (Hrsg.): Electronic Voting in Europe – Technology, Law, Politics and Society

P-48 Anatoly Doroshenko, Terry Halpin, Stephen W. Liddle, Heinrich C. Mayr (Hrsg.): Information Systems Technology and its Applications

P-49 G. Schiefer, P. Wagner, M. Morgenstern, U. Rickert (Hrsg.): Integration und Datensicherheit – Anforderungen, Konflikte und Perspektiven

P-50 Peter Dadam, Manfred Reichert (Hrsg.): INFORMATIK 2004 – Informatik verbindet (Band 1) Beiträge der 34. Jahrestagung der Gesellschaft für Informatik e.V. (GI), 20.-24. September 2004 in Ulm

P-51 Peter Dadam, Manfred Reichert (Hrsg.): INFORMATIK 2004 – Informatik verbindet (Band 2) Beiträge der 34. Jahrestagung der Gesellschaft für Informatik e.V. (GI), 20.-24. September 2004 in Ulm

P-52 Gregor Engels, Silke Seehusen (Hrsg.): DELFI 2004 – Tagungsband der 2. e-Learning Fachtagung Informatik

P-53 Robert Giegerich, Jens Stoye (Hrsg.): German Conference on Bioinformatics – GCB 2004

P-54 Jens Borchers, Ralf Kneuper (Hrsg.): Softwaremanagement 2004 – Outsourcing und Integration

P-55 Jan von Knop, Wilhelm Haverkamp, Eike Jessen (Hrsg.): E-Science und Grid Adhoc-Netze Medienintegration

P-56 Fernand Feltz, Andreas Oberweis, Benoit Otjacques (Hrsg.): EMISA 2004 – Informationssysteme im E-Business und E-Government

P-57 Klaus Turowski (Hrsg.): Architekturen, Komponenten, Anwendungen

P-58 Sami Beydeda, Volker Gruhn, Johannes Mayer, Ralf Reussner, Franz Schweiggert (Hrsg.): Testing of Component-Based Systems and Software Quality

P-59 J. Felix Hampe, Franz Lehner, Key Pousttchi, Kai Ranneberg, Klaus Turowski (Hrsg.): Mobile Business – Processes, Platforms, Payments

P-60 Steffen Friedrich (Hrsg.): Unterrichtskonzepte für inforrmatische Bildung

P-61 Paul Müller, Reinhard Gotzhein, Jens B. Schmitt (Hrsg.): Kommunikation in verteilten Systemen

P-62 Federrath, Hannes (Hrsg.): „Sicherheit 2005“ – Sicherheit – Schutz und Zuverlässigkeit

P-63 Roland Kaschek, Heinrich C. Mayr, Stephen Liddle (Hrsg.): Information Systems – Technology and ist Applications

P-64 Peter Liggesmeyer, Klaus Pohl, Michael Goedicke (Hrsg.): Software Engineering 2005

P-65 Gottfried Vossen, Frank Leymann, Peter Lockemann, Wolffried Stucky (Hrsg.): Datenbanksysteme in Business, Technologie und Web

P-66 Jörg M. Haake, Ulrike Lucke, Djamshid Tavangarian (Hrsg.): DeLFI 2005: 3. deutsche e-Learning Fachtagung Informatik

P-67 Armin B. Cremers, Rainer Manthey, Peter Martini, Volker Steinhage (Hrsg.): INFORMATIK 2005 – Informatik LIVE (Band 1)

P-68 Armin B. Cremers, Rainer Manthey, Peter Martini, Volker Steinhage (Hrsg.): INFORMATIK 2005 – Informatik LIVE (Band 2)

P-69 Robert Hirschfeld, Ryszard Kowalcyk, Andreas Polze, Matthias Weske (Hrsg.): NODe 2005, GSEM 2005

P-70 Klaus Turowski, Johannes-Maria Zaha (Hrsg.): Component-oriented Enterprise Application (COAE 2005)

P-71 Andrew Torda, Stefan Kurz, Matthias Rarey (Hrsg.): German Conference on Bioinformatics 2005

P-72 Klaus P. Jantke, Klaus-Peter Fähnrich, Wolfgang S. Wittig (Hrsg.): Marktplatz Internet: Von e-Learning bis e-Payment

P-73 Jan von Knop, Wilhelm Haverkamp, Eike Jessen (Hrsg.): "Heute schon das Morgen sehen"

P-74 Christopher Wolf, Stefan Lucks, Po-Wah Yau (Hrsg.): WEWoRC 2005 – Western European Workshop on Research in Cryptology

P-75 Jörg Desel, Ulrich Frank (Hrsg.): Enterprise Modelling and Information Systems Architecture

P-76 Thomas Kirste, Birgitta König-Riess, Key Pousttchi, Klaus Turowski (Hrsg.): Mobile Informationssysteme – Potentiale, Hindernisse, Einsatz

P-77 Jana Dittmann (Hrsg.): SICHERHEIT 2006

P-78 K.-O. Wenkel, P. Wagner, M. Morgenstern, K. Luzi, P. Eisermann (Hrsg.): Land- und Ernährungswirtschaft im Wandel

P-79 Bettina Biel, Matthias Book, Volker Gruhn (Hrsg.): Softwareengineering 2006

P-80 Mareike Schoop, Christian Huemer, Michael Rebstock, Martin Bichler (Hrsg.): Service-Oriented Electronic Commerce

P-81 Wolfgang Karl, Jürgen Becker, Karl-Erwin Großpietsch, Christian Hochberger, Erik Maehle (Hrsg.): ARCS´06

P-82 Heinrich C. Mayr, Ruth Breu (Hrsg.): Modellierung 2006

P-83 Daniel Huson, Oliver Kohlbacher, Andrei Lupas, Kay Nieselt and Andreas Zell (eds.): German Conference on Bioinformatics

P-84 Dimitris Karagiannis, Heinrich C. Mayr, (Hrsg.): Information Systems Technology and its Applications

P-85 Witold Abramowicz, Heinrich C. Mayr, (Hrsg.): Business Information Systems

P-86 Robert Krimmer (Ed.): Electronic Voting 2006

P-87 Max Mühlhäuser, Guido Rößling, Ralf Steinmetz (Hrsg.): DELFI 2006: 4. e-Learning Fachtagung Informatik

P-88 Robert Hirschfeld, Andreas Polze, Ryszard Kowalczyk (Hrsg.): NODe 2006, GSEM 2006

P-90 Joachim Schelp, Robert Winter, Ulrich Frank, Bodo Rieger, Klaus Turowski (Hrsg.): Integration, Informationslogistik und Architektur

P-91 Henrik Stormer, Andreas Meier, Michael Schumacher (Eds.): European Conference on eHealth 2006

P-92 Fernand Feltz, Benoît Otjacques, Andreas Oberweis, Nicolas Poussing (Eds.): AIM 2006

P-93 Christian Hochberger, Rüdiger Liskowsky (Eds.): INFORMATIK 2006 – Informatik für Menschen, Band 1

P-94 Christian Hochberger, Rüdiger Liskowsky (Eds.): INFORMATIK 2006 – Informatik für Menschen, Band 2

P-95 Matthias Weske, Markus Nüttgens (Eds.): EMISA 2005: Methoden, Konzepte und Technologien für die Entwicklung von dienstbasierten Informationssystemen

P-96 Saartje Brockmans, Jürgen Jung, York Sure (Eds.): Meta-Modelling and Ontologies

P-97 Oliver Göbel, Dirk Schadt, Sandra Frings, Hardo Hase, Detlef Günther, Jens Nedon (Eds.): IT-Incident Mangament & IT-Forensics – IMF 2006

P-98 Hans Brandt-Pook, Werner Simonsmeier und Thorsten Spitta (Hrsg.): Beratung in der Softwareentwicklung – Modelle, Methoden, Best Practices

P-99 Andreas Schwill, Carsten Schulte, Marco Thomas (Hrsg.): Didaktik der Informatik

P-100 Peter Forbrig, Günter Siegel, Markus Schneider (Hrsg.): HDI 2006: Hochschuldidaktik der Informatik

P-101 Stefan Böttinger, Ludwig Theuvsen, Susanne Rank, Marlies Morgenstern (Hrsg.): Agrarinformatik im Spannungsfeld zwischen Regionalisierung und globalen Wertschöpfungsketten

P-102 Otto Spaniol (Eds.): Mobile Services and Personalized Environments

P-103 Alfons Kemper, Harald Schöning, Thomas Rose, Matthias Jarke, Thomas Seidl, Christoph Quix, Christoph Brochhaus (Hrsg.): Datenbanksysteme in Business, Technologie und Web (BTW 2007)

P-104 Birgitta König-Ries, Franz Lehner, Rainer Malaka, Can Türker (Hrsg.) MMS 2007: Mobilität und mobile Informationssysteme

P-105 Wolf-Gideon Bleek, Jörg Raasch, Heinz Züllighoven (Hrsg.) Software Engineering 2007

P-106 Wolf-Gideon Bleek, Henning Schwentner, Heinz Züllighoven (Hrsg.) Software Engineering 2007 – Beiträge zu den Workshops

P-107 Heinrich C. Mayr, Dimitris Karagiannis (eds.) Information Systems Technology and its Applications

P-108 Arslan Brömme, Christoph Busch, Detlef Hühnlein (eds.) BIOSIG 2007: Biometrics and Electronic Signatures

P-109 Rainer Koschke, Otthein Herzog, Karl-Heinz Rödiger, Marc Ronthaler (Hrsg.) INFORMATIK 2007 Informatik trifft Logistik Band 1

P-110 Rainer Koschke, Otthein Herzog, Karl-Heinz Rödiger, Marc Ronthaler (Hrsg.) INFORMATIK 2007 Informatik trifft Logistik Band 2

P-111 Christian Eibl, Johannes Magenheim, Sigrid Schubert, Martin Wessner (Hrsg.) DeLFI 2007: 5. e-Learning Fachtagung Informatik

P-112 Sigrid Schubert (Hrsg.) Didaktik der Informatik in Theorie und Praxis

P-113 Sören Auer, Christian Bizer, Claudia Müller, Anna V. Zhdanova (Eds.) The Social Semantic Web 2007 Proceedings of the 1st Conference on Social Semantic Web (CSSW)

P-114 Sandra Frings, Oliver Göbel, Detlef Günther, Hardo G. Hase, Jens Nedon, Dirk Schadt, Arslan Brömme (Eds.) IMF2007 IT-incident management & IT-forensics Proceedings of the 3rd International Conference on IT-Incident Management & IT-Forensics

P-115 Claudia Falter, Alexander Schliep, Joachim Selbig, Martin Vingron and Dirk Walther (Eds.) German conference on bioinformatics GCB 2007

P-116 Witold Abramowicz, Leszek Maciszek (Eds.) Business Process and Services Computing 1st International Working Conference on Business Process and Services Computing BPSC 2007

P-117 Ryszard Kowalczyk (Ed.) Grid service engineering and manegement The 4th International Conference on Grid Service Engineering and Management GSEM 2007

P-118 Andreas Hein, Wilfried Thoben, Hans-Jürgen Appelrath, Peter Jensch (Eds.) European Conference on ehealth 2007

P-119 Manfred Reichert, Stefan Strecker, Klaus Turowski (Eds.) Enterprise Modelling and Information Systems Architectures Concepts and Applications

P-120 Adam Pawlak, Kurt Sandkuhl, Wojciech Cholewa, Leandro Soares Indrusiak (Eds.) Coordination of Collaborative Engineering - State of the Art and Future Challenges

P-121 Korbinian Herrmann, Bernd Bruegge (Hrsg.) Software Engineering 2008 Fachtagung des GI-Fachbereichs Softwaretechnik

P-122 Walid Maalej, Bernd Bruegge (Hrsg.) Software Engineering 2008 - Workshopband Fachtagung des GI-Fachbereichs Softwaretechnik

P-123 Michael H. Breitner, Martin Breunig, Elgar Fleisch, Ley Pousttchi, Klaus Turowski (Hrsg.)
Mobile und Ubiquitäre Informationssysteme – Technologien, Prozesse, Marktfähigkeit
Proceedings zur 3. Konferenz Mobile und Ubiquitäre Informationssysteme (MMS 2008)

P-124 Wolfgang E. Nagel, Rolf Hoffmann, Andreas Koch (Eds.)
9th Workshop on Parallel Systems and Algorithms (PASA)
Workshop of the GI/ITG Speciel Interest Groups PARS and PARVA

P-125 Rolf A.E. Müller, Hans-H. Sundermeier, Ludwig Theuvsen, Stephanie Schütze, Marlies Morgenstern (Hrsg.)
Unternehmens-IT:
Führungsinstrument oder Verwaltungsbürde
Referate der 28. GIL Jahrestagung

P-126 Rainer Gimnich, Uwe Kaiser, Jochen Quante, Andreas Winter (Hrsg.)
10th Workshop Software Reengineering (WSR 2008)

P-127 Thomas Kühne, Wolfgang Reisig, Friedrich Steimann (Hrsg.)
Modellierung 2008

P-128 Ammar Alkassar, Jörg Siekmann (Hrsg.)
Sicherheit 2008
Sicherheit, Schutz und Zuverlässigkeit
Beiträge der 4. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. (GI)
2.-4. April 2008
Saarbrücken, Germany

P-129 Wolfgang Hesse, Andreas Oberweis (Eds.)
Sigsand-Europe 2008
Proceedings of the Third AIS SIGSAND European Symposium on Analysis, Design, Use and Societal Impact of Information Systems

P-130 Paul Müller, Bernhard Neumair, Gabi Dreo Rodosek (Hrsg.)
1. DFN-Forum Kommunikations-technologien Beiträge der Fachtagung

P-131 Robert Krimmer, Rüdiger Grimm (Eds.)
3rd International Conference on Electronic Voting 2008
Co-organized by Council of Europe, Gesellschaft für Informatik and E-Voting. CC

P-132 Silke Seehusen, Ulrike Lucke, Stefan Fischer (Hrsg.)
DeLFI 2008:
Die 6. e-Learning Fachtagung Informatik

P-133 Heinz-Gerd Hegering, Axel Lehmann, Hans Jürgen Ohlbach, Christian Scheideler (Hrsg.)
INFORMATIK 2008
Beherrschbare Systeme – dank Informatik
Band 1

P-134 Heinz-Gerd Hegering, Axel Lehmann, Hans Jürgen Ohlbach, Christian Scheideler (Hrsg.)
INFORMATIK 2008
Beherrschbare Systeme – dank Informatik
Band 2

P-135 Torsten Brinda, Michael Fothe, Peter Hubwieser, Kirsten Schlüter (Hrsg.)
Didaktik der Informatik –
Aktuelle Forschungsergebnisse

P-136 Andreas Beyer, Michael Schroeder (Eds.)
German Conference on Bioinformatics GCB 2008

P-137 Arslan Brömme, Christoph Busch, Detlef Hühnlein (Eds.)
BIOSIG 2008: Biometrics and Electronic Signatures

P-138 Barbara Dinter, Robert Winter, Peter Chamoni, Norbert Gronau, Klaus Turowski (Hrsg.)
Synergien durch Integration und Informationslogistik
Proceedings zur DW2008

P-139 Georg Herzwurm, Martin Mikusz (Hrsg.)
Industrialisierung des Software-Managements
Fachtagung des GI-Fachausschusses Management der Anwendungsentwicklung und -wartung im Fachbereich Wirtschaftsinformatik

P-140 Oliver Göbel, Sandra Frings, Detlef Günther, Jens Nedon, Dirk Schadt (Eds.)
IMF 2008 - IT Incident Management & IT Forensics

P-141 Peter Loos, Markus Nüttgens, Klaus Turowski, Dirk Werth (Hrsg.)
Modellierung betrieblicher Informations-systeme (MobIS 2008)
Modellierung zwischen SOA und Compliance Management

P-142 R. Bill, P. Korduan, L. Theuvsen, M. Morgenstern (Hrsg.)
Anforderungen an die Agrarinformatik durch Globalisierung und Klimaveränderung

P-143 Peter Liggesmeyer, Gregor Engels, Jürgen Münch, Jörg Dörr, Norman Riegel (Hrsg.)
Software Engineering 2009
Fachtagung des GI-Fachbereichs Softwaretechnik

P-144 Johann-Christoph Freytag, Thomas Ruf, Wolfgang Lehner, Gottfried Vossen (Hrsg.)
Datenbanksysteme in Business, Technologie und Web (BTW)

P-145 Knut Hinkelmann, Holger Wache (Eds.)
WM2009: 5th Conference on Professional Knowledge Management

P-146 Markus Bick, Martin Breunig, Hagen Höpfner (Hrsg.)
Mobile und Ubiquitäre Informationssysteme – Entwicklung, Implementierung und Anwendung
4. Konferenz Mobile und Ubiquitäre Informationssysteme (MMS 2009)

P-147 Witold Abramowicz, Leszek Maciaszek, Ryszard Kowalczyk, Andreas Speck (Eds.)
Business Process, Services Computing and Intelligent Service Management
BPSC 2009 · ISM 2009 · YRW-MBP 2009

P-148 Christian Erfurth, Gerald Eichler, Volkmar Schau (Eds.)
9th International Conference on Innovative Internet Community Systems
I²CS 2009

P-149 Paul Müller, Bernhard Neumair, Gabi Dreo Rodosek (Hrsg.)
2. DFN-Forum Kommunikationstechnologien
Beiträge der Fachtagung

P-150 Jürgen Münch, Peter Liggesmeyer (Hrsg.)
Software Engineering
2009 - Workshopband

P-151 Armin Heinzl, Peter Dadam, Stefan Kirn, Peter Lockemann (Eds.)
PRIMIUM
Process Innovation for Enterprise Software

P-152 Jan Mendling, Stefanie Rinderle-Ma, Werner Esswein (Eds.)
Enterprise Modelling and Information Systems Architectures
Proceedings of the 3rd Int'l Workshop EMISA 2009

P-153 Andreas Schwill, Nicolas Apostolopoulos (Hrsg.)
Lernen im Digitalen Zeitalter
DeLFI 2009 – Die 7. E-Learning Fachtagung Informatik

P-154 Stefan Fischer, Erik Maehle Rüdiger Reischuk (Hrsg.)
INFORMATIK 2009
Im Focus das Leben

P-155 Arslan Brömme, Christoph Busch, Detlef Hühnlein (Eds.)
BIOSIG 2009:
Biometrics and Electronic Signatures
Proceedings of the Special Interest Group on Biometrics and Electronic Signatures

P-156 Bernhard Koerber (Hrsg.)
Zukunft braucht Herkunft
25 Jahre »INFOS – Informatik und Schule«

P-157 Ivo Grosse, Steffen Neumann, Stefan Posch, Falk Schreiber, Peter Stadler (Eds.)
German Conference on Bioinformatics 2009

P-158 W. Claupein, L. Theuvsen, A. Kämpf, M. Morgenstern (Hrsg.)
Precision Agriculture Reloaded – Informationsgestützte Landwirtschaft

P-159 Gregor Engels, Markus Luckey, Wilhelm Schäfer (Hrsg.)
Software Engineering 2010

P-160 Gregor Engels, Markus Luckey, Alexander Pretschner, Ralf Reussner (Hrsg.)
Software Engineering 2010 – Workshopband
(inkl. Doktorandensymposium)

P-161 Gregor Engels, Dimitris Karagiannis Heinrich C. Mayr (Hrsg.)
Modellierung 2010

P-162 Maria A. Wimmer, Uwe Brinkhoff, Siegfried Kaiser, Dagmar Lück-Schneider, Erich Schweighofer, Andreas Wiebe (Hrsg.)
Vernetzte IT für einen effektiven Staat
Gemeinsame Fachtagung Verwaltungsinformatik (FTVI) und Fachtagung Rechtsinformatik (FTRI) 2010

P-163 Markus Bick, Stefan Eulgem, Elgar Fleisch, J. Felix Hampe, Birgitta König-Ries, Franz Lehner, Key Pousttchi, Kai Rannenberg (Hrsg.)
Mobile und Ubiquitäre Informationssysteme
Technologien, Anwendungen und Dienste zur Unterstützung von mobiler Kollaboration

P-164 Arslan Brömme, Christoph Busch (Eds.)
BIOSIG 2010: Biometrics and Electronic Signatures Proceedings of the Special Interest Group on Biometrics and Electronic Signatures

P-165 Gerald Eichler, Peter Kropf, Ulrike Lechner, Phayung Meesad, Herwig Unger (Eds.)
10th International Conference on Innovative Internet Community Systems (I^2CS) – Jubilee Edition 2010 –

P-166 Paul Müller, Bernhard Neumair, Gabi Dreo Rodosek (Hrsg.)
3. DFN-Forum Kommunikationstechnologien
Beiträge der Fachtagung

P-167 Robert Krimmer, Rüdiger Grimm (Eds.)
4th International Conference on Electronic Voting 2010
co-organized by the Council of Europe, Gesellschaft für Informatik and E-Voting.CC

P-168 Ira Diethelm, Christina Dörge, Claudia Hildebrandt, Carsten Schulte (Hrsg.)
Didaktik der Informatik
Möglichkeiten empirischer Forschungsmethoden und Perspektiven der Fachdidaktik

P-169 Michael Kerres, Nadine Ojstersek Ulrik Schroeder, Ulrich Hoppe (Hrsg.)
DeLFI 2010 - 8. Tagung der Fachgruppe E-Learning der Gesellschaft für Informatik e.V.

P-170 Felix C. Freiling (Hrsg.)
Sicherheit 2010
Sicherheit, Schutz und Zuverlässigkeit

P-171 Werner Esswein, Klaus Turowski, Martin Juhrisch (Hrsg.)
Modellierung betrieblicher Informationssysteme (MobIS 2010)
Modellgestütztes Management

P-172 Stefan Klink, Agnes Koschmider Marco Mevius, Andreas Oberweis (Hrsg.)
EMISA 2010
Einflussfaktoren auf die Entwicklung flexibler, integrierter Informationssysteme
Beiträge des Workshops der GI-Fachgruppe EMISA (Entwicklungsmethoden für Informationssysteme und deren Anwendung)

P-173 Dietmar Schomburg, Andreas Grote (Eds.)
German Conference on Bioinformatics 2010

P-174 Arslan Brömme, Torsten Eymann, Detlef Hühnlein, Heiko Roßnagel, Paul Schmücker (Hrsg.)
perspeGKtive 2010
Workshop „Innovative und sichere Informationstechnologie für das Gesundheitswesen von morgen“

P-175 Klaus-Peter Fähnrich, Bogdan Franczyk (Hrsg.)
INFORMATIK 2010
Service Science – Neue Perspektiven für die Informatik
Band 1

P-176 Klaus-Peter Fähnrich, Bogdan Franczyk (Hrsg.)
INFORMATIK 2010
Service Science – Neue Perspektiven für die Informatik
Band 2

P-177 Witold Abramowicz, Rainer Alt, Klaus-Peter Fähnrich, Bogdan Franczyk, Leszek A. Maciaszek (Eds.)
INFORMATIK 2010
Business Process and Service Science – Proceedings of ISSS and BPSC

P-178 Wolfram Pietsch, Benedikt Krams (Hrsg.)
Vom Projekt zum Produkt
Fachtagung des GI-Fachausschusses Management der Anwendungsentwicklung und -wartung im Fachbereich Wirtschafts-informatik (WI-MAW), Aachen, 2010

P-179 Stefan Gruner, Bernhard Rumpe (Eds.)
FM+AM`2010
Second International Workshop on Formal Methods and Agile Methods

P-180 Theo Härder, Wolfgang Lehner, Bernhard Mitschang, Harald Schöning, Holger Schwarz (Hrsg.)
Datenbanksysteme für Business, Technologie und Web (BTW)
14. Fachtagung des GI-Fachbereichs „Datenbanken und Informationssysteme“ (DBIS)

P-181 Michael Clasen, Otto Schätzel, Brigitte Theuvsen (Hrsg.)
Qualität und Effizienz durch informationsgestützte Landwirtschaft, Fokus: Moderne Weinwirtschaft

P-182 Ronald Maier (Hrsg.)
6th Conference on Professional Knowledge Management
From Knowledge to Action

P-183 Ralf Reussner, Matthias Grund, Andreas Oberweis, Walter Tichy (Hrsg.)
Software Engineering 2011
Fachtagung des GI-Fachbereichs Softwaretechnik

P-184 Ralf Reussner, Alexander Pretschner, Stefan Jähnichen (Hrsg.)
Software Engineering 2011
Workshopband
(inkl. Doktorandensymposium)

P-185 Hagen Höpfner, Günther Specht, Thomas Ritz, Christian Bunse (Hrsg.)
MMS 2011: Mobile und ubiquitäre Informationssysteme Proceedings zur 6. Konferenz Mobile und Ubiquitäre Informationssysteme (MMS 2011)

P-186 Gerald Eichler, Axel Küpper, Volkmar Schau, Hacène Fouchal, Herwig Unger (Eds.)
11th International Conference on Innovative Internet Community Systems (I^2CS)

P-187 Paul Müller, Bernhard Neumair, Gabi Dreo Rodosek (Hrsg.)
4. DFN-Forum Kommunikations-technologien, Beiträge der Fachtagung 20. Juni bis 21. Juni 2011 Bonn

P-188 Holger Rohland, Andrea Kienle, Steffen Friedrich (Hrsg.)
DeLFI 2011 – Die 9. e-Learning Fachtagung Informatik der Gesellschaft für Informatik e.V. 5.–8. September 2011, Dresden

P-189 Thomas, Marco (Hrsg.)
Informatik in Bildung und Beruf INFOS 2011
14. GI-Fachtagung Informatik und Schule

P-190 Markus Nüttgens, Oliver Thomas, Barbara Weber (Eds.)
Enterprise Modelling and Information Systems Architectures (EMISA 2011)

P-191 Arslan Brömme, Christoph Busch (Eds.)
BIOSIG 2011
International Conference of the Biometrics Special Interest Group

P-192 Hans-Ulrich Heiß, Peter Pepper, Holger Schlingloff, Jörg Schneider (Hrsg.)
INFORMATIK 2011
Informatik schafft Communities

P-193 Wolfgang Lehner, Gunther Piller (Hrsg.)
IMDM 2011

P-194 M. Clasen, G. Fröhlich, H. Bernhardt, K. Hildebrand, B. Theuvsen (Hrsg.)
Informationstechnologie für eine nachhaltige Landbewirtschaftung
Fokus Forstwirtschaft

P-195 Neeraj Suri, Michael Waidner (Hrsg.)
Sicherheit 2012
Sicherheit, Schutz und Zuverlässigkeit
Beiträge der 6. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. (GI)

P-196 Arslan Brömme, Christoph Busch (Eds.)
BIOSIG 2012
Proceedings of the 11th International Conference of the Biometrics Special Interest Group

P-197 Jörn von Lucke, Christian P. Geiger, Siegfried Kaiser, Erich Schweighofer, Maria A. Wimmer (Hrsg.)
Auf dem Weg zu einer offenen, smarten und vernetzten Verwaltungskultur
Gemeinsame Fachtagung Verwaltungsinformatik (FTVI) und Fachtagung Rechtsinformatik (FTRI) 2012

P-198 Stefan Jähnichen, Axel Küpper, Sahin Albayrak (Hrsg.)
Software Engineering 2012
Fachtagung des GI-Fachbereichs Softwaretechnik

P-199 Stefan Jähnichen, Bernhard Rumpe, Holger Schlingloff (Hrsg.)
Software Engineering 2012
Workshopband

P-200 Gero Mühl, Jan Richling, Andreas Herkersdorf (Hrsg.)
ARCS 2012 Workshops

P-201 Elmar J. Sinz Andy Schürr (Hrsg.)
Modellierung 2012

P-202 Andrea Back, Markus Bick, Martin Breunig, Key Pousttchi, Frédéric Thiesse (Hrsg.)
MMS 2012:Mobile und Ubiquitäre Informationssysteme

P-203 Paul Müller, Bernhard Neumair, Helmut Reiser, Gabi Dreo Rodosek (Hrsg.)
5. DFN-Forum Kommunikations-technologien
Beiträge der Fachtagung

P-204 Gerald Eichler, Leendert W. M. Wienhofen, Anders Kofod-Petersen, Herwig Unger (Eds.)
12th International Conference on Innovative Internet Community Systems (I2CS 2012)

P-205 Manuel J. Kripp, Melanie Volkamer, Rüdiger Grimm (Eds.)
5th International Conference on Electronic Voting 2012 (EVOTE2012)
Co-organized by the Council of Europe, Gesellschaft für Informatik and E-Voting.CC

P-206 Stefanie Rinderle-Ma, Mathias Weske (Hrsg.)
EMISA 2012
Der Mensch im Zentrum der Modellierung

P-207 Jörg Desel, Jörg M. Haake, Christian Spannagel (Hrsg.)
DeLFI 2012: Die 10. e-Learning Fachtagung Informatik der Gesellschaft für Informatik e.V.
24.–26. September 2012

P-208 Ursula Goltz, Marcus Magnor, Hans-Jürgen Appelrath, Herbert Matthies, Wolf-Tilo Balke, Lars Wolf (Hrsg.) INFORMATIK 2012

P-209 Hans Brandt-Pook, André Fleer, Thorsten Spitta, Malte Wattenberg (Hrsg.) Nachhaltiges Software Management

P-210 Erhard Plödereder, Peter Dencker, Herbert Klenk, Hubert B. Keller, Silke Spitzer (Hrsg.) Automotive – Safety & Security 2012 Sicherheit und Zuverlässigkeit für automobile Informationstechnik

P-211 M. Clasen, K. C. Kersebaum, A. Meyer-Aurich, B. Theuvsen (Hrsg.) Massendatenmanagement in der Agrar- und Ernährungswirtschaft Erhebung - Verarbeitung - Nutzung Referate der 33. GIL-Jahrestagung 20. – 21. Februar 2013, Potsdam

P-212 Arslan Brömme, Christoph Busch (Eds.) BIOSIG 2013 Proceedings of the 12th International Conference of the Biometrics Special Interest Group 04.–06. September 2013 Darmstadt, Germany

P-213 Stefan Kowalewski, Bernhard Rumpe (Hrsg.) Software Engineering 2013 Fachtagung des GI-Fachbereichs Softwaretechnik

P-214 Volker Markl, Gunter Saake, Kai-Uwe Sattler, Gregor Hackenbroich, Bernhard Mit schang, Theo Härder, Veit Köppen (Hrsg.) Datenbanksysteme für Business, Technologie und Web (BTW) 2013 13. – 15. März 2013, Magdeburg

P-215 Stefan Wagner, Horst Lichter (Hrsg.) Software Engineering 2013 Workshopband (inkl. Doktorandensymposium) 26. Februar – 1. März 2013, Aachen

P-216 Gunter Saake, Andreas Henrich, Wolfgang Lehner, Thomas Neumann, Veit Köppen (Hrsg.) Datenbanksysteme für Business, Technologie und Web (BTW) 2013 – Workshopband 11. – 12. März 2013, Magdeburg

P-217 Paul Müller, Bernhard Neumair, Helmut Reiser, Gabi Dreo Rodosek (Hrsg.) 6. DFN-Forum Kommunikations-technologien Beiträge der Fachtagung 03.–04. Juni 2013, Erlangen

P-218 Andreas Breiter, Christoph Rensing (Hrsg.) DeLFI 2013: Die 11 e-Learning Fachtagung Informatik der Gesellschaft für Informatik e.V. (GI) 8. – 11. September 2013, Bremen

P-219 Norbert Breier, Peer Stechert, Thomas Wilke (Hrsg.) Informatik erweitert Horizonte INFOS 2013 15. GI-Fachtagung Informatik und Schule 26. – 28. September 2013

P-220 Matthias Horbach (Hrsg.) INFORMATIK 2013 Informatik angepasst an Mensch, Organisation und Umwelt 16. – 20. September 2013, Koblenz

P-221 Maria A. Wimmer, Marijn Janssen, Ann Macintosh, Hans Jochen Scholl, Efthimios Tambouris (Eds.) Electronic Government and Electronic Participation Joint Proceedings of Ongoing Research of IFIP EGOV and IFIP ePart 2013 16. – 19. September 2013, Koblenz

P-222 Reinhard Jung, Manfred Reichert (Eds.) Enterprise Modelling and Information Systems Architectures (EMISA 2013) St. Gallen, Switzerland September 5. – 6. 2013

P-223 Detlef Hühnlein, Heiko Roßnagel (Hrsg.) Open Identity Summit 2013 10. – 11. September 2013 Kloster Banz, Germany

P-224 Eckhart Hanser, Martin Mikusz, Masud Fazal-Baqaie (Hrsg.) Vorgehensmodelle 2013 Vorgehensmodelle – Anspruch und Wirklichkeit 20. Tagung der Fachgruppe Vorgehensmodelle im Fachgebiet Wirtschaftsinformatik (WI-VM) der Gesellschaft für Informatik e.V. Lörrach, 2013

P-225 Hans-Georg Fill, Dimitris Karagiannis, Ulrich Reimer (Hrsg.) Modellierung 2014 19. – 21. März 2014, Wien

P-226 M. Clasen, M. Hamer, S. Lehnert, B. Petersen, B. Theuvsen (Hrsg.) IT-Standards in der Agrar- und Ernährungswirtschaft Fokus: Risiko- und Krisenmanagement Referate der 34. GIL-Jahrestagung 24. – 25. Februar 2014, Bonn

P-227 Wilhelm Hasselbring,
Nils Christian Ehmke (Hrsg.)
Software Engineering 2014
Fachtagung des GI-Fachbereichs Softwaretechnik
25. – 28. Februar 2014
Kiel, Deutschland

P-228 Stefan Katzenbeisser, Volkmar Lotz, Edgar Weippl (Hrsg.)
Sicherheit 2014
Sicherheit, Schutz und Zuverlässigkeit
Beiträge der 7. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. (GI)
19. – 21. März 2014, Wien

P-230 Arslan Brömme, Christoph Busch (Eds.)
BIOSIG 2014
Proceedings of the 13th International Conference of the Biometrics Special Interest Group
10. – 12. September 2014 in Darmstadt, Germany

P-231 Paul Müller, Bernhard Neumair, Helmut Reiser, Gabi Dreo Rodosek (Hrsg.)
7. DFN-Forum Kommunikationstechnologien
16. – 17. Juni 2014
Fulda

P-232 E. Plödereder, L. Grunske, E. Schneider, D. Ull (Hrsg.)
INFORMATIK 2014
Big Data – Komplexität meistern
22. – 26. September 2014
Stuttgart

P-233 Stephan Trahasch, Rolf Plötzner, Gerhard Schneider, Claudia Gayer, Daniel Sassiat, Nicole Wöhrle (Hrsg.)
DeLFI 2014 – Die 12. e-Learning Fachtagung Informatik
der Gesellschaft für Informatik e.V.
15. – 17. September 2014
Freiburg

P-234 Fernand Feltz, Bela Mutschler, Benoît Otjacques (Eds.)
Enterprise Modelling and Information Systems Architectures
(EMISA 2014)
Luxembourg, September 25-26, 2014

P-235 Robert Giegerich,
Ralf Hofestädt,
Tim W. Nattkemper (Eds.)
German Conference on Bioinformatics 2014
September 28 – October 1
Bielefeld, Germany

P-236 Martin Engstler, Eckhart Hanser, Martin Mikusz, Georg Herzwurm (Hrsg.)
Projektmanagement und Vorgehensmodelle 2014
Soziale Aspekte und Standardisierung
Gemeinsame Tagung der Fachgruppen Projektmanagement (WI-PM) und Vorgehensmodelle (WI-VM) im Fachgebiet Wirtschaftsinformatik der Gesellschaft für Informatik e.V., Stuttgart 2014

P-237 Detlef Hühnlein, Heiko Roßnagel (Hrsg.)
Open Identity Summit 2014
4.–6. November 2014
Stuttgart, Germany

P-238 Arno Ruckelshausen, Hans-Peter Schwarz, Brigitte Theuvsen (Hrsg.)
Informatik in der Land-, Forst- und Ernährungswirtschaft
Referate der 35. GIL-Jahrestagung
23. – 24. Februar 2015, Geisenheim

P-239 Uwe Aßmann, Birgit Demuth, Thorsten Spitta, Georg Püschel, Ronny Kaiser (Hrsg.)
Software Engineering & Management 2015
17.-20. März 2015, Dresden

P-240 Herbert Klenk, Hubert B. Keller, Erhard Plödereder, Peter Dencker (Hrsg.)
Automotive – Safety & Security 2015
Sicherheit und Zuverlässigkeit für automobile Informationstechnik
21.–22. April 2015, Stuttgart

P-241 Thomas Seidl, Norbert Ritter, Harald Schöning, Kai-Uwe Sattler, Theo Härder, Steffen Friedrich, Wolfram Wingerath (Hrsg.)
Datenbanksysteme für Business, Technologie und Web (BTW 2015)
04. – 06. März 2015, Hamburg

P-242 Norbert Ritter, Andreas Henrich, Wolfgang Lehner, Andreas Thor, Steffen Friedrich, Wolfram Wingerath (Hrsg.)
Datenbanksysteme für Business, Technologie und Web (BTW 2015) – Workshopband
02. – 03. März 2015, Hamburg

P-243 Paul Müller, Bernhard Neumair, Helmut Reiser, Gabi Dreo Rodosek (Hrsg.)
8. DFN-Forum Kommunikationstechnologien
06.–09. Juni 2015, Lübeck

P-244 Alfred Zimmermann, Alexander Rossmann (Eds.) Digital Enterprise Computing (DEC 2015) Böblingen, Germany June 25-26, 2015

P-245 Arslan Brömme, Christoph Busch , Christian Rathgeb, Andreas Uhl (Eds.) BIOSIG 2015 Proceedings of the 14th International Conference of the Biometrics Special Interest Group 09.–11. September 2015 Darmstadt, Germany

P-246 Douglas W. Cunningham, Petra Hofstedt, Klaus Meer, Ingo Schmitt (Hrsg.) INFORMATIK 2015 28.9.-2.10. 2015, Cottbus

P-247 Hans Pongratz, Reinhard Keil (Hrsg.) DeLFI 2015 – Die 13. E-Learning Fachtagung Informatik der Gesellschaft für Informatik e.V. (GI) 1.–4. September 2015 München

P-248 Jens Kolb, Henrik Leopold, Jan Mendling (Eds.) Enterprise Modelling and Information Systems Architectures Proceedings of the 6th Int. Workshop on Enterprise Modelling and Information Systems Architectures, Innsbruck, Austria September 3-4, 2015

P-249 Jens Gallenbacher (Hrsg.) Informatik allgemeinbildend begreifen INFOS 2015 16. GI-Fachtagung Informatik und Schule 20.–23. September 2015

P-250 Martin Engstler, Masud Fazal-Baqaie, Eckhart Hanser, Martin Mikusz, Alexander Volland (Hrsg.) Projektmanagement und Vorgehensmodelle 2015 Hybride Projektstrukturen erfolgreich umsetzen Gemeinsame Tagung der Fachgruppen Projektmanagement (WI-PM) und Vorgehensmodelle (WI-VM) im Fachgebiet Wirtschaftsinformatik der Gesellschaft für Informatik e.V., Elmshorn 2015

P-251 Detlef Hühnlein, Heiko Roßnagel, Raik Kuhlisch, Jan Ziesing (Eds.) Open Identity Summit 2015 10.–11. November 2015 Berlin, Germany

P-252 Jens Knoop, Uwe Zdun (Hrsg.) Software Engineering 2016 Fachtagung des GI-Fachbereichs Softwaretechnik 23.–26. Februar 2016, Wien

P-253 A. Ruckelshausen, A. Meyer-Aurich, T. Rath, G. Recke, B. Theuvsen (Hrsg.) Informatik in der Land-, Forst- und Ernährungswirtschaft Fokus: Intelligente Systeme – Stand der Technik und neue Möglichkeiten Referate der 36. GIL-Jahrestagung 22.-23. Februar 2016, Osnabrück

P-254 Andreas Oberweis, Ralf Reussner (Hrsg.) Modellierung 2016 2.–4. März 2016, Karlsruhe

P-255 Stefanie Betz, Ulrich Reimer (Hrsg.) Modellierung 2016 Workshopband 2.–4. März 2016, Karlsruhe

P-256 Michael Meier, Delphine Reinhardt, Steffen Wendzel (Hrsg.) Sicherheit 2016 Sicherheit, Schutz und Zuverlässigkeit Beiträge der 8. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. (GI) 5.–7. April 2016, Bonn

P-257 Paul Müller, Bernhard Neumair, Helmut Reiser, Gabi Dreo Rodosek (Hrsg.) 9. DFN-Forum Kommunikationstechnologien 31. Mai – 01. Juni 2016, Rostock

The titles can be purchased at:

Köllen Druck + Verlag GmbH
Ernst-Robert-Curtius-Str. 14 · D-53117 Bonn
Fax: +49 (0)228/9898222
E-Mail: druckverlag@koellen.de