Einsatz eines Sicherheitsmusters zur Absicherung einer mobilen Wissensmanagementlösung

Stefan Berger und Jens Ingo Mehlau

Bayerischer Forschungsverbund Wirtschaftsinformatik
Universität Regensburg
berger|mehlau@forwin.de

Zusammenfassung: Der Einsatz mobiler IuK-Technologien führt zu Effektivitäts- und Effizienzsteigerungen im Wissensmanagement. Die vorgestellte mobile Wissensmanagementlösung (U-Know) nutzt diese neuen Möglichkeiten. Jedoch vergrößert der Einsatz der innovativen Technologien auch die Gefahr, dass Unbefugte leichter an sensible Daten gelangen. Eine Bedrohungsanalyse identifizierte potenzielle Schwachstellen von U-Know. Das Auffinden von geeigneten Sicherheitsmaßnahmen wird anhand von Sicherheitsmustern gezeigt. Es wurden mehrere sinnvoll einzusetzende Sicherheitsmuster erkannt. Die Musterbeschreibung ermöglicht die Realisierung von Maßnahmen, die in ihrer Qualität dem Stand der Technik entsprechen, da sie auf erprobten Lösungsansätzen von Experten basieren. Abschließend wird die um Sicherheitsmaßnahmen erweiterte Systemarchitektur von U-Know vorgestellt.

1 Problemstellung

In den vergangenen Jahren haben die Anforderungen an Hochschulen deutlich zugenommen [Küp96]. Die Monopolkommission fordert beispielsweise in ihrem Sondergutachten zur Situation an deutschen Hochschulen mehr Wettbewerb als neues Leitbild für die Hochschulpolitik [o.V00]. Verstärkt besteht daher auch für Universitäten, die aufgrund einer weitgehend vorherrschenden inputorientierten Kameralistik [Rei96] eigentlich nicht auf Gewinnerzielung angewiesen sind [Küp02], der Bedarf, ihre Abläufe möglichst effizient zu gestalten. Angesichts der These, dass in Organisationen nur 20 bis 30 Prozent der eigentlich verfügbaren Wissensbasis wirklich genutzt werden, lässt zielgerichtetes Wissensmanagement noch große Produktivitätspotenziale vermuten [Sch96b]. War die technische Unterstützung des Wissensmanagements bis vor Kurzem noch überwiegend auf stationäre Systeme beschränkt, so werden mithilfe mobiler Technologien weitere Effektivitäts- und Effizienzsteigerungen realisierbar [BL02]. Über mobile Endgeräte können Mitarbeiter auf dem Universitätsgelände oder auf Reisen ohne stationären Rechner auf benötigtes Wissen zugreifen bzw. sind in ihrer Eigenschaft als Wissensträger für Kollegen erreichbar.

Durch die Nutzung von mobilen Endgeräten und Funknetzen vergrößert sich jedoch auch die Gefahr, dass Unbefugte leichter an unternehmensinternes Wissen gelangen als dies bei stationären Lösungen der Fall wäre [MB02]. Über gestohlene oder verlorene Mobilgeräte kann beispielsweise ein unauthorisierter Zugriff auf unternehmensinterne Daten erfolgen. Die Kommunikation zwischen Endgeräten und Diensterbringern, bei der unterschiedliche Netze involviert sind, kann ebenfalls Gegenstand von Angriffen (z. B. Lauschangriffen)

werden. Hinsichtlich der Verteilung und Verwaltung sensibler Daten stellt der Einsatz mobiler IuK-Technologien somit neue Sicherheitsanforderungen an Wissensmanagementlösungen.

Nachfolgend wird die mobile Wissensmanagementlösung U-Know (Ubiquitous Knowledge Management) der Universität Regensburg vorgestellt. Sie stellt eine geeignete technische Plattform für einen ortsunabhängigen Zugriff auf benötigtes Wissen dar. Da mit Nutzung dieses Systems sensible Daten leichter zugänglich werden, wird anschließend gezeigt, wie ein Musteransatz die Absicherung der beschriebenen Architektur methodisch unterstützen kann.

2 U-Know: Mobile Wissensplattform an der Universität Regensburg

2.1 Ausgangssituation und Zielsetzung

Aufgrund der vermuteten Produktivitätspotenziale des Wissensmanagements wird an der Wirtschaftswissenschaftlichen Fakultät der Universität Regensburg ein effektiver und effizienter Umgang mit dem vorhandenen Wissen über Verordnungen, Zuständigkeiten, Ansprechpartner sowie Verwaltungsabläufe angestrebt. Folgende Rahmenbedingungen sind dabei zu berücksichtigen:

- Umfangreicher Aufgabenbestand der Fakultät
  Die Aufgaben einer Fakultät umfassen die Durchführung des Unterrichts, die Heranbildung des wissenschaftlichen und künstlerischen Nachwuchses, die Verantwortung für eine wirksame Studienberatung sowie die Sorge für die wissenschaftliche Forschung und die Anwendung hochschuldidaktischer Erkenntnisse [Rei99]. Aus diesen vielfältigen Aufgaben lassen sich verschiedene Haupt- und Serviceprozesse der Hochschulen ableiten [SBU99]. Der Hauptprozess Studium und Lehre erzeugt Ausbildungs- und Prüfungsleistungen und übergibt diese an Studierende. Die im Hauptprozess Forschung erzeugten Leistungen werden von Forschungspartnern sowie der interessierten Öffentlichkeit in Anspruch genommen. Daneben existieren Serviceprozesse in der Administration, wie etwa die Mittelbewirtschaftung und Personalwirtschaft, die ihre Leistungen an beteiligte Haupt- und Serviceprozesse abgeben. Da die Geschäftsprozesse letztendlich die relevanten Wissensinhalte bestimmen [Hei01], ist demnach aufgrund des umfangreichen Aufgabenbestandes in der öffentlichen Verwaltung auch das benötigte Wissen sehr vielgestaltig [WTL01]; [LTW01].
- Wissensintensität der Prozesse
  Viele Typen der Verwaltungsprozesse sind in hohem Ausmaß auf Information und Wissen angewiesen [WTL01]. Wissensintensive Geschäftsprozesse besitzen einen großen Anteil informationsverarbeitender Tätigkeiten und zeichnen sich durch unbestimmten Abläufe, Sonderfälle, schlecht definierte Aufgaben und große Entscheidungsspielräume der Mitarbeiter aus [Leh00]; [GH00]. Wissensintensive Geschäftsprozesse können durch Wissensmanagementaktivitäten flankiert werden [Leh00].
- Bürokratische Strukturen und hoher Autonomiegrad der Organisationseinheiten
  Forschung und Lehre werden weitgehend dezentral von den Lehrstühlen und die Verwaltung von der Fakultätsleitung (Dekanat) verantwortet. Die Organisation der Universitäten ist durch staatliche Gesetze und Verordnungen geregelt, was ihnen einen

weitgehend bürokratischen Charakter verleiht [Küp96, 152]. Diese Normen setzen oft nur einen Rahmen, der im weiteren Verlauf durch Ermessen und Konsensbildung ausgefüllt wird [Ros99]. Zur Durchführung der oben genannten Aufgaben und zur Sicherstellung der Innovations- und Wettbewerbsfähigkeit besteht daher umfangreicher Koordinations- und Kommunikationsbedarf zwischen den beteiligten Stellen [Rei96], der in Abbildung 1 in Form verschiedener Steuer- und Leistungsflüsse angedeutet ist. [1]

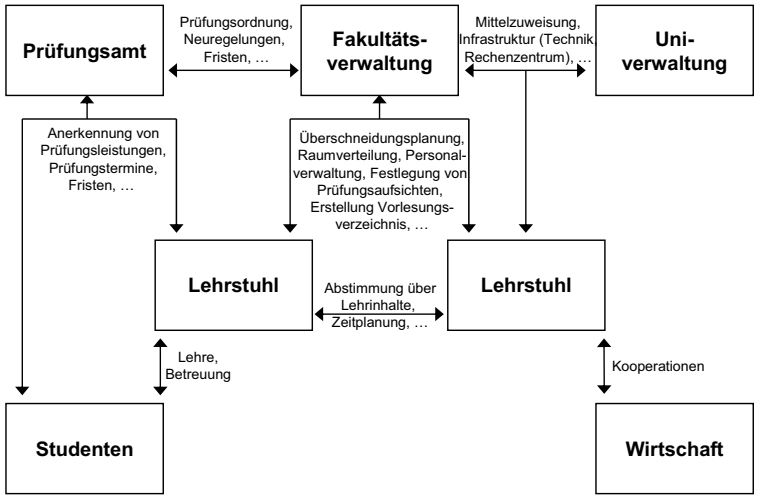

Abbildung 1: Koordinationsbedarf an der Universität

Informationen, wie etwa Bekanntmachungen, Ansprechpartner oder Telefonnummern lassen sich vielfach nur über den jeweiligen Internetauftritt der einzelnen Organisationseinheiten herausfinden.

- Häufige Personalwechsel
  Der Großteil des Fakultätspersonals besteht aus wissenschaftlichen Mitarbeitern, die auf Basis von befristeten Arbeitsverträgen angestellt sind (üblicherweise zwischen 2-5 Jahre), in dieser Zeit an ihrer Dissertation oder Habilitation arbeiten und nach ihrem Abschluss überwiegend die Universität verlassen. Gleichzeitig müssen neue Mitarbeiter möglichst schnell in den Lehr- und Forschungsbetrieb integriert werden. Damit steht die Fakultät vor ähnlichen Problemen wie Unternehmensberatungen, bei denen ebenfalls durch hohe Personalfluktuation nicht unerhebliche Teile der organisationalen Wissensbasis verloren gehen.

Vor diesem Hintergrund sind für eine verbesserten Wissensnutzung an der Fakultät folgende zwei Ziele relevant:

[1] Zum Begriff der Steuer- und Leistungsflüsse vgl. [FS01].

- Bereitstellung von häufig benötigten Informationen in leicht zugänglicher Form
  Die Wissensverteilung ist einer der Kernprozesse im Wissensmanagement [PRR98]. Diese Aufgabe kann durch geeignete Informations- und Kommunikationsstrukturen unterstützt werden [Wil02].
- Förderung der Kommunikation zwischen Mitarbeitern
  Häufig sind Informationen in Organisationen nicht explizit dokumentiert, sondern lediglich in Form von Erfahrungswissen („tacit knowledge“) vorhanden [NT95]. Die Förderung der Kommunikation ist daher für das Wissensmanagement im universitären Bereich von zentraler Bedeutung [Wil02]. „Anders ausgedrückt: Ohne Kommunikation kein common knowledge!“ [Leh00].

Eine wesentliche Maßnahme zur Erreichung dieser Ziele bildet der Einsatz von elektronischen Hilfsmitteln zur Unterstützung der Information und Kommunikation an der Fakultät.

2.2 Umsetzung

Vor diesem Hintergrund entsteht zur Zeit an der Universität Regensburg der Prototyp einer internetbasierten[2] Wissensplattform, die speziell auf die Nutzung mittels mobiler Endgeräte, also Handys und PDAs, abgestimmt ist. Die Bezeichnung „Plattform“ steht für eine Sammlung von Technologien, die Informationen an zentraler Stelle aggregieren und die Teilnehmer untereinander vernetzen.

Besonderes Augenmerk wird auf den Einsatz mobiler Technologien gelegt. Diese geben dem Wissensmanagement mit seinen Kernaktivitäten wie die Wissensidentifikation oder -verteilung keine neue Bedeutung, jedoch ist der Aspekt der Mobilität eine neue Dimension bei der Konzeption von Informationssystemen [LB01].

Die Verwendung mobiler Geräte erlaubt die leichte Verfügbarkeit benötigter Informationen (Ziel 1) und die Unterstützung der Mitarbeiterkommunikation (Ziel 2). Sie sind handlich und ortsunabhängig nutzbar, wenn situativ Informationen benötigt oder Ansprechpartner gesucht werden. Diese Technologien unterstützen deshalb sinnvoll die Wissensverteilung und Kommunikation in Organisationen.

Seit September 2002 findet die inkrementelle Umsetzung eines Prototypen statt. Bei diesem Vorgehen wird das Produkt als Folge von Versionen betrachtet, die aufeinander aufbauen [LHM00]. Dies stellt sicher, dass die Plattform relativ zügig genutzt werden kann und neue, aus der Nutzung resultierende Anforderungen sukzessive implementiert werden können. Die Zielgruppe von U-Know besteht aus den Mitarbeitern der Wirtschaftswissenschaftlichen Fakultät der Universität Regensburg, also Professoren, wissenschaftlichen Mitarbeitern und Verwaltungsangestellten. Auch sie sind im Rahmen ihrer täglichen Aufgaben mobil. Professoren und wissenschaftliche Mitarbeiter besuchen beispielsweise Fachkonferenzen, sind auf dem Campus unterwegs oder nehmen an Besprechungen außerhalb ihres Büros teil. Folgende Funktionen sind bisher realisiert und für mobile Endgeräte verfügbar:

Abbildung 2 zeigt zur Veranschaulichung das U-Know-Hauptmenü ① , das Ergebnis einer Expertensuche ② sowie Projektinformationen ③ auf einem PDA.

[2] Gemäß einer Untersuchung von [SA97] besteht eine hohe Affinität zwischen Internettechnologie und Wissensmanagement.

Bereitstellung von Informationen	Aktuelle Mitteilungen der Fakultät
	Gelbe Seiten • Mitarbeiterverzeichnis (alphabetisch) • Mitarbeiterverzeichnis (thematisch nach Arbeitsschwerpunkt) • Einrichtungen • Projekte
	Checklisten
	FAQ - Liste
	Gebäudeplan
Unterstützung der Kommunikation	Newsgroups
	SMS - Versand

Tabelle 1: Bisher realisierte Funktionen von U-Know

Abbildung 2: Screenshots von U-Know

Der Aufbau der Plattform soll mithilfe der nachfolgenden Systemarchitektur, welche die einzelnen Systemkomponenten und ihre Beziehung untereinander beschreibt, verdeutlicht werden.

Die Nutzung von U-Know ist sowohl über stationäre als auch mobile Clients unter Einbeziehung heterogener Netze (stationäre Netze, WLAN, GSM-Netze) möglich. Der Benutzer kann z. B. mit seinem Browser über das Internet per HTTP-Anfrage auf U-Know zugreifen ① . Soll eine Informationsbereitstellung über Mobiltelefone durch eine Sprachverarbeitung erfolgen, so wird zusätzlich ein Voice-Server benötigt, der die Spracherkennung, Sprachausgabe und Dialogsteuerung übernimmt [Mat02] ② . Für einen SMS-Versand an einen oder mehrere Nutzer wird die Nachricht samt Zielrufnummer(n) an den Webserver übertragen und von dort an ein SMS-Gateway weitergeleitet ③ . Die Verteilung von E-Mails übernimmt ein SMTP-Server ④ . Im Bereich des Wireless LAN (WLAN) kann der ortsunabhängige Zugriff auf U-Know auch durch Notebooks oder PDAs, die mit ei-

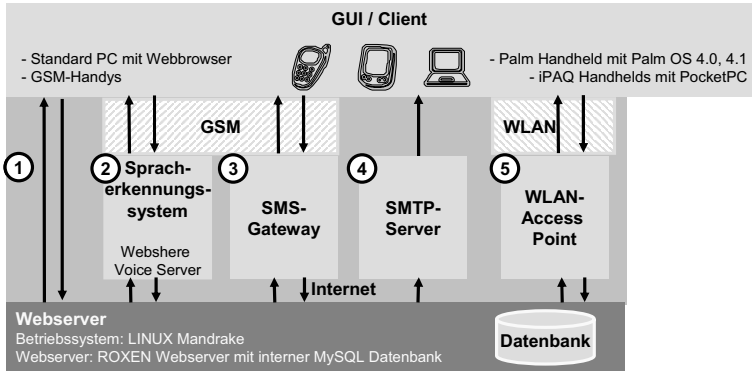

Abbildung 3: Systemarchitektur von U-Know

ner Funkkarte ausgestattet sind, erfolgen ⑤ . Da die Universität Regensburg bereits jetzt über eine vollständige WLAN-Abdeckung verfügt, wird dieses Medium mit zunehmender Verbreitung mobiler Endgeräte eine maßgebliche Bedeutung erlangen. Im folgenden wird daher exemplarisch die Absicherung dieses Zugangskanals unter Anwendung von Sicherheitsmustern betrachtet.

3 Bedrohungsanalyse

Eine drahtlose Kommunikation, die bei Nutzung mobiler Endgeräte häufig eingesetzt wird, unterliegt prinzipiell einer stärkeren Bedrohung als eine Festnetzkommunikation. Sensible Dienste und vertraulicher Nachrichtenaustausch sind daher in besonderer Weise gegen Missbrauch zu schützen.

Die folgenden Bedrohungen gelten nicht ausschließlich für mobile Dienste, aber aufgrund der spezifischen Eigenschaften mobiler Endgeräte, wie eine häufig eingesetzte drahtlose Kommunikation und Portabilität, ergeben sich z. T. neue Aspekte, die bei einer Absicherung beachtet werden müssen [WEG+02, 97].

- *Unbefugter Zugriff:* Aufgrund der Portabilität sind mobile Endgeräte in besonderem Maße der Gefahr eines unbefugten Zugriffs ausgesetzt. Dieser kann durch Diebstahl, unbeaufsichtigtes Stehenlassen, Verlust oder einer unberechtigten Weitergabe des Gerätes erfolgen [Eck01, 206]. Ein Verlust ermöglicht einen unauthorisierten Zugriff auf Ressourcen des mobilen Endgerätes. Darüber hinaus kann man sich u. U. die Identität des Besitzers aneignen und Zugriff auf weitere Ressourcen, z. B. ein Intranet, erlangen. [JKGK03]
- *Lauschangriff:* Dieser kann durch Vorspielen eines berechtigten Nutzers oder durch Mitschneiden der Datenkommunikation erfolgen. Diese Bedrohung gewinnt an Bedeutung, da kaum Möglichkeiten bestehen, den Netzzugang innerhalb der spezifizierten Reichweite von 30-150 Metern ausschließlich für eine gesicherte Umgebung zu ermöglichen. Darüber hinaus besteht je nach Umgebungsbedingungen und verwendeten

Empfangsgeräten auch über die spezifizierte Nutzreichweite hinaus eine Abhörgefahr. [BSI02, 9]

- *Manipulation:* Während einer Datenübertragung oder im System selbst können Daten modifiziert werden. Beispiele stellen Trojanischen Pferde[3] oder Viren[4] dar.
- *Blockade der Verfügbarkeit:* Die limitierten Ressourcen mobiler Endgeräte führen zu einer erhöhten Bedrohung durch Angriffe auf die Verfügbarkeit. Bei Einsatz von Funk-LANs werden Informationen anhand von elektromagnetischen Wellen übertragen. Andere elektromagnetische Quellen im gleichen Frequenzband können eine Kommunikation stören und im Extremfall den Betrieb des Funknetzes unterbinden. Neben unbeabsichtigten Verfügbarkeitseinschränkungen (z. B. durch andere technische Systeme, wie Bluetooth-Netze, andere Funk-LANs und Mikrowellengeräte) ist auch ein Angriff auf die Verfügbarkeit durch den gezielten Einsatz von Störquellen (Jammer) zu berücksichtigen [BSI02, 9]. Herrschende Meinung ist, dass gegen diese Bedrohung wohl auch zukünftig keine Gegenmaßnahmen existieren werden. Eine vollkommen neue Form der Verfügbarkeitseinschränkung stellen Angriffe auf die Energieversorgung dar. Da die betriebenen Endgeräte im mobilen Einsatz häufig über keinen Stromanschluss verfügen, kann ein provozierter Einsatz von energieaufwendigen Operationen, z. B. dem ständigen Betrieb einer Festplatte, die Akkulaufzeit drastisch verkürzen und somit die Verfügbarkeit stark einschränken.
- *Bedrohung durch Nutzung heterogener Netze:* Bei einer Kommunikation mit mobilen Endgeräten werden mit hoher Wahrscheinlichkeit unterschiedliche Zellen und/oder Netze mit unterschiedlichen Sicherheitsniveaus und Sicherheitsgrundsätzen (security policies) involviert sein. Interaktionen mit nicht vertrauenswürdigen Gastnetzen stellen prinzipiell eine Bedrohung bezüglich der Vertraulichkeit und Integrität der Kommunikation dar.

Die aktuelle Generation mobiler Endgeräte zeichnet sich nach wie vor durch geringe Rechenleistung und beschränkte Speicherkapazität aus, sodass eine Umsetzung etablierter Sicherheitsmaßnahmen zur Absicherung erschwert oder nicht möglich ist [MB02, 66].

4 Analyse der Sicherheitsmaßnahmen des IEEE 802.11 Standards

Das WLAN wird durch den Standard 802.11 des „Institute of Electrical and Electronics Engineers“ (IEEE) spezifiziert. IEEE 802.11b ist der verbreitetste Standard der Protokollfamilie mit einer Übertragungsrate von 11 MBit/s im 2,4 GHz Bereich und nutzt zur Übertragung das Direct Sequence Spread Spectrum (DSSS)-Funkübertragungsverfahren.[5] Der

[3] Digitale Trojanische Pferde (abgekürzt auch „Trojaner“) sind Programme, die in erster Linie einen nützlichen Zweck zu erfüllen versprechen und harmlos erscheinen, aber Zusatzfunktionen enthalten, die nur unter ganz bestimmten Umständen ausgelöst werden.[Pfl96, 179]

[4] Ein Virus ist ein Computercode, der sich an ein anderes Computerprogramm anhängt. Neben einer Fortpflanzungsfunktion können sie auch Schadensfunktionen beinhalten. Man unterscheidet Dateiviren, Boot-Sektor-Viren und interpretierte Makroviren. [Sch01, 145]

[5] Das DSSS-Funkübertragungsverfahren spreizt das Signal über mehrere Frequenzbereiche durch die Modulation des Trägersignals mit einer pseudostatistischen Codesequenz (Spreizbandtechnik), sodass ein Abhören der Kommunikation erschwert wird [Lip01, 155 f.].

Standard 802.11 definiert mit dem Wired Equivalent Privacy (WEP) Protokoll bereits Sicherheitsmaßnahmen gegen oben geschilderte Bedrohungen. Die WEP-Spezifikation umfasst eine optionale Punkt-zu-Punkt Sicherheit indem die Vertraulichkeit und die Integrität durch Verschlüsselung und Nutzung einer Prüfsumme gewährleistet wird. Eine unautho-risierte Nutzung der Funkinfrastruktur wird durch eine Zugriffskontrolle unterbunden. Allerdings bietet keine der Maßnahmen nach 802.11 ein zufriedenstellendes Sicherheitsniveau.

Zur Verschlüsselung wird das symmetrische Verschlüsselungsverfahren RC4, das ein Vertreter der Stromchiffrierer[6] ist, eingesetzt. Anhand eines geheimen Schlüssels K wird ein Strom von Pseudozufallszahlen erzeugt, der über ein exklusives ODER ($\oplus$) mit dem zu verschlüsselnden Klartext verknüpft wird. Der Standard spezifiziert zwei Schlüssellängen: 40 Bit und 104 Bit[7]. Unter der Annahme, dass Sender und Empfänger über einen geheimen Schlüssel K verfügen, verläuft der Algorithmus wie folgt:

- Prüfsummenberechnung: Um die Integrität zu gewährleisten wird zunächst auf Basis des CRC-32-Algorithmus[8] für die Nachricht M eine Prüfsumme $CRC(M)$ berechnet. Die Verkettung $M \mid CRC(M)$ wird anschließenden verschlüsselt.
- Verschlüsselung: Der Sender wählt einen 24-Bit langen Initialisierungsvektor IV und erzeugt in Kombination mit dem geheimen Schlüssel K den Schlüsselstrom $RC4(IV, K)$. Zur Berechnung des Geheimtextes C wird der Schlüsselstrom anhand exklusivem ODER mit Nachricht und Prüfsumme verknüpft: $C = RC4(IV, K) \oplus (M \mid CRC(M))$.
- Versand: Danach werden Geheimtext C und Initialisierungsvektor IV übertragen.
- Entschlüsselung: Der Empfänger berechnet ebenfalls den gleichen Schlüsselstrom $RC4(IV, K)$. Eine erneute Verknüpfung ergibt die ursprüngliche Nachricht: $M = C \oplus RC4(IV, K) = M \oplus RC4(IV, K) \oplus RC4(IV, K)$.
- Integritätsprüfung: Der Empfänger prüft schließlich die Korrektheit anhand der erhaltenen Prüfsumme durch einen Vergleich mit der selbst errechneten $CRC(M)$.

4.1 Angriffe auf die Vertraulichkeit

Neben einer grundsätzlichen Kritik bezüglich des Einsatzes eines Verschlüsselungsverfahrens, dessen Algorithmus geheim gehalten wurde [Sch96a, 455 f.], weist das Protokoll folgende Defizite auf:

[6] Symmetrische Verschlüsselungsalgorithmen werden üblicherweise in Stromchiffrierung und Blockchiffrierung unterteilt. Die Stromalgorithmen behandeln den zu verschlüsselnden Klartext bit- bzw. byteweise, während die Blockalgorithmen Bitgruppen fester Größe (Blöcke) bearbeiten [Sch96a, 4].

[7] Nach herrschender Meinung bieten Schlüssellängen von 40 Bit keine ausreichende Vertraulichkeit [Eck03, 228 f.]; [Sch96a, 268 f.].

[8] CRC (Cyclic Redundancy Checksum) ist ursprünglich ein Fehlersicherungsverfahren, bei dem Prüfzeichen durch die Summenbildung von Datengruppen gebildet werden [Lip01, 102 f.]. Dieser Algorithmus gilt nicht als starke kryptographische Hashfunktion [Eck03, 665].

4.1.1 Known-Plaintext-Angriff

Stromchiffrierverfahren sind anfällig gegenüber Known-Plaintext-Angriffen[9]. Stellt C eine mit K verschlüsselte Chiffre der Nachricht M dar, also:

$$C = M \oplus RC4(K) \quad (1)$$

Mit der Kenntnis eines Kryptotextes C' und dem dazugehörigen Klartext M' gilt bei festem Schlüssel K:

$$M \oplus M' = C \oplus C' \Leftrightarrow M = (C \oplus C') \oplus M' \quad (2)$$

Mit einem bekannten Paar C' und M' kann man ohne Kenntnis von K den Klartext M erhalten. Daraus folgt unmittelbar, dass bei Einsatz von Stromchiffrierverfahren niemals der gleiche Schlüssel verwendet werden sollte.

Wegen dieser Eigenschaft wird der statische Schlüssel für jedes Datenpaket um einen 24 Bit langen Initialisierungsvektor (IV) erweitert. Schlüssel und IV bilden zusammen den RC4 Initialisierungswert (Schlüssel) für das Datenpaket. Um den Empfänger ebenfalls in Kenntnis des IV zu setzen, wird er in Klartextform im Header des Datenpakets mit übertragen. Aufgrund seiner kurzen Länge von 24 Bit, wiederholt sich der IV bei einem genügend ausgelasteten Access Point innerhalb von einigen Stunden. Spätestens zu diesem Zeitpunkt wäre ein neuer Schlüssel zwischen Client und Access Point auszuhandeln[10]. Da 802.11 nicht die Erzeugung von IV spezifiziert, wird bei vielen WLAN-Karten der Initialisierungsvektor standardmäßig bei jedem Neustart mit 0 initialisiert, sodass eine Zufälligkeit des RC4-generierten Datenstroms nicht mehr gewährleistet ist.

4.1.2 Initialisierungsvektor-Angriff

Dieser Angriff nutzt eine Schwäche der WEP-Spezifikation aus und hat die Ermittlung des WEP-Schlüssels zum Ziel. Die Unsicherheit des WEP Protokolls wurden erstmals von [FMS01] beschrieben und von [SIR03] implementiert. Die Kenntnis des IV und der ersten Ausgabebytes von RC4 geben die Möglichkeit, bei so genannten „resolved conditions“[11] Rückschlüsse auf Schlüsselbits zu ziehen. Bereits die Analyse von ca. 256 resolved conditions reichen für eine Rekonstruktion des WEP-Schlüssels aus. Für diesen Angriff ist das Abfangen und die Analyse von ca. 5-6 Millionen Datenpaketen notwendig. Eine aktuelle Implementierung dieses Angriffs stellt das Tool Airsnort[12] da.

4.2 Angriffe auf die Integrität

Anhand des CRC-32-Algorithmus wird eine Prüfsumme für die zu versendenden Datenpakete gebildet. Der CRC-Algorithmus ist unabhängig vom WEP-Schlüssel und ist eine

[9] Bei einem Known-Plaintext-Angriff verfügt der Angreifer neben dem Chiffretext auch über dazugehörige Klartextsegmente [Opp97, 50 f.].

[10] Dies ist allerdings in der Praxis aufgrund des Administrationsaufwandes unüblich (vgl. Abschnitt 4.3).

[11] [FMS01] konnten in ihrer Arbeit zeigen, dass bei ausgewählten IV dieser Rückschluss möglich ist. Die Verwendung eines derartigen IV stellt für sie eine „resolved condition“ (gelöste Bedingung) dar.

[12] http://airsnort.shmoo.com/

lineare Funktion, sodass gilt:

$$CRC(M \oplus M') = CRC(M) \oplus CRC(M') \tag{3}$$

4.2.1 Modifikation von Nachrichten

Die nach WEP-Spezifikation eingesetzten Verfahren RC4 und CRC-32 weisen beide Linearitätseigenschaften auf. Dies erlaubt eine unentdeckte Manipulation von Daten durch Dritte [BGW01, 185].

Stellt C ein Kryptotext des Klartextes M dar, so gilt:

$$C = RC4(IV, K) \oplus (M \mid CRC(M)) \tag{4}$$

Es ist allerdings möglich ein neues C', den Kryptotext von $M' = M \oplus \Delta$, zu erzeugen. Δ stellt eine beliebige Manipulation des Angreifers dar. Für eine erfolgreiche Manipulation ist die Ableitung von C' aus C notwendig, sodass C' den korrekten Kryptotext von M' repräsentiert. Aufgrund der Linearitätseigenschaften von RC4 und CRC-32 lässt sich C' wie folgt herleiten [BGW01, 185]:

$$\begin{aligned} C' &= C \oplus (\Delta \mid CRC(\Delta)) \\ &= RC4(IV, K) \oplus (M \mid CRC(M)) \oplus (\Delta \mid CRC(\Delta)) \\ &= RC4(IV, K) \oplus (M \oplus \Delta) \mid (CRC(M) \oplus CRC(\Delta)) \\ &= RC4(IV, K) \oplus (M') \mid (CRC(M) \oplus CRC(\Delta)) \\ &= RC4(IV, K) \oplus (M') \mid (CRC(M')) \end{aligned}$$

Daraus folgt, dass beliebige Änderungen an den Nachrichten M vorgenommen werden können, ohne dass sie vom Empfänger erkannt werden. Eine gezielte Manipulation, z. B. die Veränderung einer Prüfungsnote, setzt allerdings Kenntnis von M voraus, damit ein geeignetes Δ gewählt werden kann.

4.2.2 Einspeisen neuer Nachrichten

Das Einspeisen neuer Nachrichten gestaltet sich einfacher als die Manipulation. Unterstellt man, dass dem Angreifer ein Klar-/Geheimtext Paar (M, C) vorliegt,[13] kann er anhand des Paares den $RC4(IV, K) = C \oplus (M \mid CRC(M))$ berechnen. Für eine neue Nachricht N wird nun $C' = RC4(IV, K) \oplus (N \mid CRC(N))$ berechnet. Man beachte, dass der Angreifer keinerlei Kenntnis des geheimen Schlüssels K haben muss, er verwendet nur den erzeugten Schlüsselstrom. Der Empfänger wird N als korrekte Nachricht akzeptieren.

4.3 Angriffe auf die Authentifizierung

Der WEP-Standard definiert zwei unterschiedliche Authentifizierungsmöglichkeiten. Die Open System Authentication erlaubt jedem kommunikationswilligen Benutzer den Zugang zum Funknetz. Bei der Shared Key Authentication wird ein gemeinsamer Schlüssel

[13] Eine Möglichkeit diese Paare zu erhalten liefert der WEP-Authentifizierungsvorgang: Der Access Point sendet einen Klartext als Challenge, die der Empfänger verschlüsselt beantwortet. Selbstverständlich können interne Angreifer ihre eigene Kommunikation verfolgen und somit eine beliebige Anzahl von Klar-/Geheimtext Paaren sammeln.

zur Authentifizierung anhand eines Challenge-Response-Protokolls genutzt. Der Client verschlüsselt eine vom Access Point erhaltene 1024 Bit lange Zufallszahl und sendet das Ergebnis der Berechnung zurück. Bei Kenntnis des korrekten Schlüssels erhält der Nutzer Zugang zum Funknetz. Die Schlüsselverteilung ist nicht Gegenstand des Standards. In der Praxis wird der Schlüssel manuell auf die jeweiligen Rechner verteilt. Zum einen haben bei dieser Vorgehensweise die Administratoren Kenntnis von dem Schlüssel, zum anderen liegt der Schlüssel auf mehreren Clients dezentral vor. Es sind bereits Angriffe bekannt, die es erlauben, den Schlüssel am Client zu extrahieren [BGW01, 183]. Durch Kompromittierung eines einzelnen Clients kann somit ein kompletter Netzzugang gewonnen werden.

5 Lösungsansatz über Sicherheitsmuster

5.1 Muster als methodischer Ansatz

Mit Mustern wird (Entwurfs-)wissen erfahrener Entwickler beschrieben und bewährte Lösungen für immer wieder auftretende Probleme angeboten. Mit ihrem Einsatz besteht die Möglichkeit, Erfahrungswissen zu sammeln, zu systematisieren und zu katalogisieren [Str99, 38]. Muster dienen damit der Wiederverwendung und Dokumentation von bekannten und erprobten Lösungen und erleichtern darüber hinaus den Kommunikations- und Lernprozess [BMR+98, 5 ff.].

Musterbeschreibungen umfassen üblicherweise eine Problembeschreibung in einem Kontext und einer aufgezeigten Lösung: „A Pattern is an idea that has been useful in one practical context and will probably be useful in others“ [Fow97].

In der Praxis finden neben den bekanntesten GoF-Mustern[14] eine Vielzahl von unterschiedlichen Mustern Berücksichtigung. So lassen sich u. a. Analysemuster, die durch einen stärkeren fachlichen Bezug den Bereich der konzeptionellen Modellierung unterstützen und sogar Organisationsmuster für das Projektmanagement identifizieren [Fow97]; [BMT99]. [BMR+98] beschreiben explizit Architekturmuster, in denen das grundsätzliche Strukturierungsprinzip von Softwaresystemen anhand einer Menge vordefinierter Subsysteme und Regeln zur Gestaltung der Beziehungen erfolgt. Der Musteransatz begleitet also nicht ausschließlich eine Phase des Softwareentwicklungsprozesses, sondern kann eine methodische Unterstützung über sämtliche Phasen der Softwareentwicklung bieten.[15]

Muster werden natürlich-sprachlich beschrieben und ggf. mit semi-formalen Diagrammen, die üblicherweise aus dem Bereich der objektorientierten Modellierung stammen, angereichert. Die eingesetzten Notationen unterscheiden sich vor allem im Grade ihrer Strukturierung. Man findet Beschreibungsformen von reiner Prosa (belletristischer Stil) bis hin zu einer stärker strukturierten Beschreibung (schematisierte Prosa) [Str99, 41 f.]. Die zwei bekanntesten Beschreibungsschemata (Pattern Templates) sind die von Gamma

[14] GoF (Gang of Four) Musterkatalog, der von Gamma, Helm, Johnson und Vlissides entwickelt wurde. Die Muster beziehen sich ausschließlich auf den objektorientierten Entwurf [GHJV96].

[15] Vergleiche hierzu auch die Arbeit von [MM97], die eine Einteilung von Musterabstraktionsstufen vom object level, microarchitecture level, framework level, application level, system level, enterprise level bis zum global level vornehmen.

et al. (GoF-Schema) und von Buschmann et al., wobei das Schema von Buschmann einen höheren Strukturierungsgrad aufweist [GHJV96]; [BMR+98].

Bei der Gestaltung eines Systems wird eine Vielzahl unterschiedlicher Muster eingesetzt. Daher ist es notwendig, dem Entwickler eine aggregierte Form der einzelnen Musterbeschreibungen anzubieten, bei der insbesondere auch die Interdependenzen der Muster untereinander beschrieben werden. Es lassen sich hierbei folgende Musterzusammenstellungen unterscheiden [Str99, 42 f.]; [BMR+98, 359 ff.]:

- Mustersammlung (pattern set): Beinhaltet Muster ohne Beschränkung auf eine Domäne und Beschreibung der Interdependenzen untereinander. Sie sind schwach kategorisiert und stammen oft von mehreren Autoren, sodass u. U. innerhalb der Mustersammlung Redundanzen auftreten können.
- Musterkatalog (pattern catalog): Enthält nach bestimmten Kriterien klassifizierte Muster. Während die Muster von einer Vielzahl von Autoren stammen können, wird der Katalog selber von wenigen Personen verfasst.
- Mustersystem (pattern system): Muster werden aufeinander abgestimmt und in Beziehung gesetzt. Dabei werden die Abhängigkeiten inklusive Kombinationsregeln zwischen anderen Mustern beschrieben.
- Mustersprache (pattern language): Beschreibung erfolgt weitgehend analog zum Mustersystem, wobei einige Autoren eine noch größere Verzahnung fordern. Wesentlicher Unterschied ist aber der Vollständigkeitsanspruch, dem die Mustersprache gerecht wird. Dies ist der Grund, weswegen Mustersprachen meist domänenspezifisch sind.

Nachfolgend wird für Konzepte der IT-Sicherheit ein Beschreibungsschema entwickelt, das die Basis für ein zukünftiges Sicherheitsmustersystem sein kann.

5.2 Sicherheitsmuster

Die Sicherheit eines Informationssystems hängt sowohl von der Qualität als auch vom ergänzenden Zusammenwirken der einzeln eingesetzten Sicherheitsmaßnahmen ab. Die Qualität ist eine Aussage über den Grad der Aufgabenerfüllung einer Maßnahme. Durch das Zusammenwirken unterschiedlicher Maßnahmen soll ein erhöhtes Sicherheitsniveau erreicht werden. Zum einen werden unterschiedliche Sicherheitsprobleme abgedeckt, zum anderen existieren mehrere Maßnahmen mit redundanten Sicherheitszielen, sodass beim Versagen einer Maßnahme das Erreichen eines Schutzzieles durch andere Sicherheitsmechanismen gewährleistet ist. Der Musteransatz ermöglicht eine geeignete Darstellung von erprobten Lösungen einschließlich ihrer interdependenten Beziehungen untereinander. Es bietet sich daher an, diesen Ansatz auf den Problembereich der Sicherheit zu übertragen. Unter einem Sicherheitsmuster wird die Beschreibung eines Sicherheitsproblems in einem spezifischen Kontext, verbunden mit einer Lösungsbeschreibung, verstanden [Meh02, 207]. Sie sollen bei ihrer Anwendung bestehende Konzepte sinnvoll ergänzen.

Analog des klassischen Musteransatzes müssen Sicherheitsmuster in einer strukturierten Form dargestellt werden, sodass durch eine einheitliche Beschreibung Anwendern ein leichter Vergleich und eine systematische Suche ermöglicht wird. Das im Folgenden definierte Beschreibungsschemata erfüllt diese Anforderungen und berücksichtigt in seinem

Aufbau die fünf grundlegenden Elemente: Name, Kontext, Problem-, Lösungs- und Konsequenzabschnitt [GHJV96, 3 f.].

Mustername: Durch Benennung wird das Entwurfsvokabular erweitert. Es wird eine leichtere Diskussion mit Beteiligten und eine vereinfachte Dokumentation ermöglicht [GHJV96, 3 f.].

Kontext: Beschreibung der Situationen in denen das Muster anwendbar ist [BMR+98, 21].

Problemabschnitt: Beschreibt, für welche Probleme ein Muster Verwendung finden kann und welche Voraussetzungen für den Einsatz des Musters erfüllt sein müssen. Insbesondere sollten Anmerkungen zu folgenden Unterpunkten erfolgen:

- *Bedrohungen:* Bedrohungen lassen sich aufgrund des Sicherheitsfokus als ein elementarer Bestandteil des Problemabschnitts identifizieren. Da mit einer starken Redundanz zu rechnen ist (Sicherheitsmuster wehren üblicherweise nicht exklusiv einzelne Bedrohungen ab), bietet sich u. U. auch die Beschreibung der Bedrohungen selbst als Muster an, sodass lediglich auf ein oder mehrere Bedrohungsmuster verwiesen werden kann.
- *Abstraktionsniveau:* Die Benennung des Abstraktionsniveaus erfolgt in Anlehnung eines Kategorisierungsschemata von [MM97], die folgende Niveaus unterscheiden: Objektebene, Mikroarchitekturebene, Frameworkebene, Applikationsebene, Systemebene, Unternehmensebene und eine Globale Ebene.

Lösungsabschnitt: Beschreibt die Lösungselemente mit ihren Beziehungen, Zuständigkeiten und Interaktionen. Die Lösung beschreibt dabei nicht einen expliziten Entwurf. Die Lösung muss auf einer geeigneten abstrakten Ebene beschrieben werden, sodass eine leichte Adaption an konkrete Problemstellungen erfolgen kann.

- *Generelle Form:* Beschreibung des Musters, sinnvoll durch Diagramme ergänzt.
- *Lösungstyp:* Da IT-Sicherheit nicht ausschließlich durch technische Maßnahmen gewährleistet wird, ist eine Differenzierung der Muster in mehrere Lösungstypen sinnvoll. In Anlehnung an [BMT99, 7 ff.] werden die Lösungstypen „Technologie“, „Prozess“ und „Rolle“ unterschieden. Der Lösungstyp Technologie zeigt, dass mit dem Muster eine neue Software oder ein gesamtes System erzeugt wird. Der Prozess beschreibt das Verhalten eines Systems, das sowohl technische als auch organisatorische Bestandteile enthalten kann, während der Typ Rolle Personen oder Gruppen bestimmte Verantwortlichkeiten zuweist.
- *Variationen:* Liste von Variationen dieses Musters. Erfolgt entweder durch einen Verweis auf ein anderes Muster des Musterkatalogs oder durch explizite Beschreibung.

Konsequenzabschnitt: Beschreibt die Auswirkung der Musterverwendung. Aufgrund der Domäneneinschränkung kann eine genaue Aussage über die verfolgten Sicherheitsziele erfolgen. Die Zielerreichung wird anhand eines Netzgraphen vorgenommen, sodass der Leser schnell einen Überblick gewinnen kann, welches Sicherheitsniveau sich mit dem Muster realisieren lässt. Die betrachteten Schutzziele spiegeln nicht sämtliche Sicherheitsziele, wie z. B. die Forderung nach Anonymität, wider. Folgende Auswahl an Schutzzielen wird betrachtet:

- „*Vertraulichkeit* beschreibt den Zustand, in dem Daten vor unbefugter Kenntnisnahme geschützt sind.“ [RKN00, 500] Für einen Kommunikationsvorgang bedeutet dies, dass niemand außer den Kommunikationspartnern den Inhalt der Kommunikation erkennen soll [WP00, 175].
- „*Verfügbarkeit* sichert die Nutzbarkeit von Ressourcen und Diensten, wenn ein Teilnehmer sie benutzen will“ [WP00, 175], wohingegen die „Erreichbarkeit sichert, dass zu einer Ressource (Nutzer oder Maschine) Kontakt aufgenommen werden kann, wenn gewünscht.“ [PSWW00, 16] Beide Ziele laufen auf Schutz gegen unautorisierte Beeinträchtigung der Nutzbarkeit hinaus. Verfügbarkeit beschreibt dieses Schutzziel unter dem Gesichtspunkt der Kommunikationsinhalte, Erreichbarkeit unter dem Aspekt der Kommunikationsumstände.
- *Integrität* fordert, dass Modifikationen der kommunizierten Inhalte durch den Empfänger erkannt oder verhindert werden [PSWW00, 15]. In [FP00, 706] werden drei Stufen unterschieden:
  - „schwache“ Integrität, d. h. das Erkennen, ob etwas gefälscht wurde,
  - „starke“ Integrität, d. h. zusätzlich mit der Möglichkeit zu erkennen, wer bzw. was den Verlust der Integrität herbeigeführt hat,
  - „stärkste“ Integrität, d. h. ein stets korrektes und integres Arbeiten eines Systems, bei dem es gar nicht erst zu einem Integritätsverlust kommt. Eine solche Forderung bedeutet eigentlich, Integrität und Verfügbarkeit in einem zu erreichen.
- „*Verbindlichkeit* heißt, dass kein Partner im System eine Kommunikationshandlung im Nachhinein bestreiten kann.“ [GK00, 500] Verbindlichkeit, auch Zurechenbarkeit genannt, ist besonders relevant bei der Abwicklung von Geschäftstransaktionen. Ist keine Verbindlichkeit gegeben, kann dies zu verantwortungslosem Handeln führen und Geschädigte können ihre Ansprüche auf Schadensersatz nicht durchsetzen [Ran00, 490].

5.3 VPN Muster

Anhand des in Abschnitt 5.2 vorgestellten Beschreibungsrahmens für Sicherheitsmuster wird im Folgenden ein VPN-Sicherheitsmuster beispielhaft beschrieben. Dieses Muster wird neben anderen zur Absicherung der Systemarchitektur von U-Know eingesetzt (vgl. Abschnitt 6).

Mustername: Ende-zu-Ende VPN

Kontext: Kommunikationspartner sollen über externe Kommunikationsnetze einen einfachen gegenseitigen Zugriff auf ausgewählte Dienste erhalten. Dies ermöglicht z. B. die Abfrage von E-Mails oder den Zugriff auf einen WWW-Server, der ansonsten nur innerhalb des eigenen Intranet zugänglich ist. Zur Kommunikation sollen öffentliche Netze genutzt werden, da sie gegenüber Mietleitungen erhebliche Kostenvorteile aufweisen. Eine Folge ist, dass die beteiligten Kommunikationspartner nicht kontrollieren können, ob Dritte Zugriff auf die transportierten Daten hatten.

Problemabschnitt:

- *Bedrohungen:* Öffentliche Netzwerke entziehen sich weitgehend Kontrollmöglichkeiten der beteiligten Kommunikationspartner. Kommunikationsdaten unterliegen daher folgenden Bedrohungen:
  - Modifikation: Eine Kommunikation kann verfälscht oder komplett unterschlagen werden.
  - Abhören: Nach außen gerichtete Kommunikation kann auf Transfersystemen mitgeschnitten werden, ohne dass dies für Absender oder Empfänger in irgendeiner Weise feststellbar wäre.
  - Beobachtung von Kommunikationsaktivitäten: Durch Mitverfolgen der Kommunikation über öffentliche oder interne Netze lassen sich Informationen darüber gewinnen, wann bestimmte Dienste und Stapelläufe stattfinden. Gelingt es, Aktivitäten einzelner Mitarbeiter zu identifizieren, so kann man daraus günstige Zeitpunkte für einen Angriff ableiten, zum Beispiel während der Mittagspause, nach dem Verlassen des Büros oder während der Urlaubstage eines Mitarbeiters.
- *Abstraktionsniveau:* Systemebene

Lösungsabschnitt:

- *Generelle Form:*

  Zur Unterbindung einer unberechtigten Einspeisung von Daten ist der Einsatz einer Zugriffskontrolle erforderlich. Der Einsatz von kryptographischen Funktionen muss die Integrität und Verschlüsselung der Daten sicher stellen, sodass Modifikation und Abhören von Datenpaketen verhindert werden.

  Das VPN-Konzept stellt diese Funktionalität bereit, indem Verbindungen mehrerer Kommunikationsteilnehmer mithilfe von virtuellen Standleitungen über öffentliche Netze realisiert werden. Um eine Absicherung der virtuellen Verbindung zu ermöglichen, werden die zu übertragenden Pakete um zusätzliche Angaben (Krypto Kopf) erweitert. Dadurch wird der Einsatz einer Verschlüsselung und einer kryptographischen Prüfsumme zur Wahrung der Integrität ermöglicht. Die Authentifizierung der Datenquelle eines Datenpakets wird anhand von Schlüsseln vorgenommen, über die beide Kommunikationspartner verfügen.

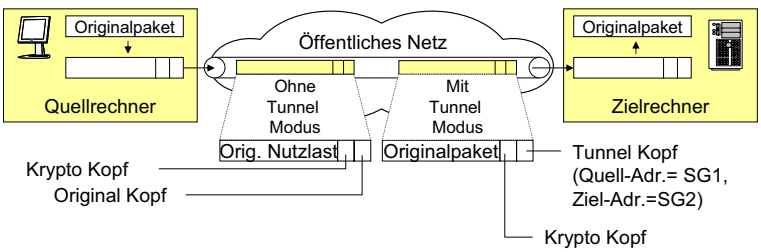

Abbildung 4: Ende-zu-Ende VPN

Zum Aufbau eines virtuellen Kommunikationskanals kann das Tunneling Konzept angewendet werden, bei dem die Kommunikationsquelle das ursprünglich zu übertragende Datenpaket als Nutzlast (Payload) in ein neues Datenpaket überträgt. Das neu erzeugte Datenpaket kann im Vergleich zum ursprünglichen einem anderem Kommunikationsprotokoll angehören, sodass z. B. Protokollunterschiede zwischen einem LAN und einen WAN überwunden werden können. Bei der erneuten Verpackung (Encapsulation) wird dem Original-Datenpaket ein zusätzlicher Rahmenkopf (Header) vorangestellt, der im Ziel-Rechner zur Rekonstruktion des ursprünglichen Pakets wieder entfernt wird (Decapsulation). Allerdings bringt die Nutzung eines Tunnels neben der Möglichkeit zur Berücksichtigung von Protokollheterogenitäten auch einen beträchtlichen Kommunikations-Overhead, da zusätzliche Rahmenköpfe mit zu übertragen sind (s. Abb. 4).

- *Lösungstyp:* Technologie
- *Variationen:* Standort-zu-Standort VPN, Remote-Access VPN

Konsequenzabschnitt: Das vorgestellte Konzept bietet für eine Kommunikation über offene Netze einen Schutz gegen aktive und passive Angriffe. Dabei werden folgende Schutzziele erreicht:

- *Vertraulichkeit:* Eine Verschlüsselung der Daten gewährleistet die Vertraulichkeit. Eine Entschlüsselung der Daten ist nur mit einem geheimen Schlüssel möglich.
- *Integrität:* Datenpakete werden vor unberechtigten Änderungen während der Übertragung geschützt, indem jedem Paket eine kryptographische Prüfsumme hinzugefügt wird. Anhand eines gemeinsamen Schlüssels kann der Empfänger die erstellte Signatur überprüfen.
- *Verfügbarkeit:* Das Konzept hat geringen Einfluss auf die Verfügbarkeit. Es ist zu beachten, dass beim Einsatz von öffentlichen Netzen, wie z. B. dem Internet, Nachteile gegenüber der Nutzung von Mietleitungen oder eigenen Leitungen entstehen können.
- *Verschleierung der Kommunikationsaktivität:* Im beschriebenen Muster wird eine Ende-zu-Ende Sicherheit realisiert. Dies impliziert, dass die beteiligten Kommunikationspartner direkt miteinander kommunizieren müssen. Selbst der Einsatz von Tunneln kann nicht die beteiligten Kommunikationspartner gegenüber Dritten verbergen, sodass die Kommunikationsaktivität nach wie vor auszuspähen ist.

6 Absicherung ausgewählter Bereiche von U-Know

Basis für die Konzeption der Sicherheitsmaßnahmen ist die in Abschnitt 2 dargestellte Architektur von U-Know. Betrachtungsgegenstand der nachfolgenden Sicherheitskonzeption ist die sichere Gestaltung der WLAN Umgebung wie sie unter ⑤ der Abbildung 3 beschrieben wurde. Die eingesetzten Maßnahmen können darüber hinaus einen Beitrag zur Absicherung der restlichen Kommunikationskanäle leisten. Aufgrund des gewählten Betrachtungsfokus werden diese Auswirkungen nicht weitergehend thematisiert.

Da die vorgesehenen Sicherheitsmaßnahmen des IEEE 802.11 Standards keinen ausreichenden Schutz gegen die in Abschnitt 3 identifizierten Bedrohungen bieten, sind weitere Sicherheitsmaßnahmen zu implementieren. Abbildung 5 zeigt die erweiterte Architektur

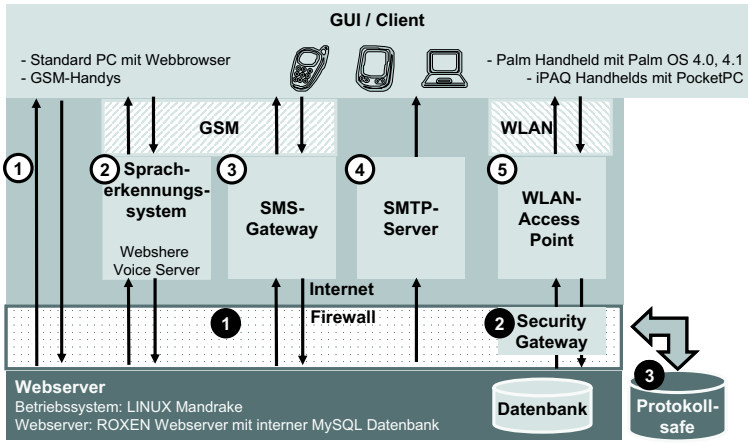

Abbildung 5: Abgesicherte Systemarchitektur von U-Know

von U-Know. Anhand eines Kataloges mit Sicherheitsmustern wurden geeigneten Maßnahmen identifiziert. Geeignete Sicherheitsmuster sind in diesem Beispiel das 1-stufige Firewallmuster ❶ [Meh02, 210], das Protokollsafemuster ❸ und das im vorherigen Abschnitt vorgestellte Ende-zu-Ende VPN-Muster ❷ .

Für eine Umsetzung des VPN Konzepts ist zunächst eine Entscheidung zugunsten eines konkreten Protokolls zu treffen. Zur Zeit finden das Layer 2 Tunneling Protocol (L2TP), das Point-to-Point Tunneling Protocol (PPTP) und das Protokoll von IP Security (IPsec) die größte Verbreitung. Sie unterscheiden sich bezüglich ihrer Protokollebene und der Nutzung des Remote Access Services (RAS). Die Wahl fiel zugunsten eines IPsec basierten VPNs aus, da es zum einen auf IP-Pakete aufsetzt und zum anderen ein offener Standard ist. Diese Entscheidung impliziert sowohl Client- als auch Server-seitig eine Modifikation des IP-Stacks.

Eine Testumgebung wurde unter Verwendung von Palm Handhelds mit Palm OS 4.1 und iPAQ Handhelds mit PocketPC realisiert. Das VPN wird auf Basis des Softwareprodukts movianVPN betrieben, da es eine Unterstützung für beide benötigten Betriebssysteme anbietet. Das Security Gateway basiert auf einer FireWall-1/VPN-1 von CheckPoint. IPsec wurde in der Transport-Mode Betriebsart implementiert. Eine Nutzung des Tunnel-Mode kann aufgrund der Ende-zu-Ende Kommunikation nicht die beteiligten Kommunikationspartner verdecken, sodass die Kommunikation durch Vermeidung des Protokoll-Overheads des Tunnel-Mode deutlich beschleunigt wird.

Tests zeigten allerdings Performanceeinbußen, die auf die beschränkte Rechenkapazität der mobilen Endgeräte zurückzuführen sind. Zur Optimierung bietet sich eine Klassifikation der Daten von U-Know an. Dies würde eine bedarfsgerechte Nutzung der rechenaufwändigen Verschlüsselung erlauben. Nicht sicherheitsrelevante Transaktionen, wie die Abfrage einer öffentlichen Telefonnummer, könnten somit deutlich beschleunigt werden.

7 Bewertung und Ausblick

Der Preisverfall und die zunehmende Leistungsfähigkeit mobiler Endgeräte lässt vermuten, dass sie in Zukunft von immer mehr Hochschulangehörigen zur Unterstützung ihrer täglichen Aufgaben genutzt werden. Die beschriebenen Funktionen eines mobilen Wissensmanagements können daher zu einer gesteigerten Verfügbarkeit von benötigten Informationen und einer verbesserten Erreichbarkeit von Mitarbeitern beitragen.

Die aus fachlichen Gesichtspunkten erstellte Architektur des Wissensmanagement Systems behandelte aufgrund ihrer Zielsetzung Sicherheitsaspekte in einem ungenügenden Maß. Eine Bedrohungsanalyse identifizierte potenzielle Schwachstellen, sodass für das angestrebte Sicherheitsniveau ein Einsatz von mehreren Sicherheitsmaßnahmen notwendig wurde. Das Auffinden der geeigneten Sicherheitsmaßnahmen erfolgte über Sicherheitsmuster und wurde beispielhaft anhand eines VPN-Musters gezeigt. Einerseits wurden mit diesem Ansatz leicht mehrere sinnvoll einzusetzende Sicherheitsmuster erkannt, sodass notwendige und optionale Maßnahmen schnell gefunden wurden. Andererseits begünstigte die Musterbeschreibung die Realisierung von Maßnahmen, die in ihrer Qualität dem Stand der Technik entsprechen, da sie auf erprobten Lösungsansätzen von Experten basieren.

Im nächsten Schritt muss nun die vorgestellte Architektur und deren Nutzerakzeptanz im praktischen Einsatz analysiert werden. Da der Bedarf nach Kommunikation und Vernetzung von Mitarbeitern nicht nur im universitären Umfeld, sondern gerade auch in der Wirtschaft weiter zunehmen wird, können die gewonnenen Erkenntnisse einen Beitrag bei der Realisierung derartiger Lösungen in anderen Bereichen leisten.

Literatur

[BGW01] N. Borisov, I. Goldberg, and D. Wagner. Intercepting Mobile Communications: The Insecurity of 802.11. In *MOBICOM 2001, Proceedings of the seventh annual international conference on Mobile computing and networking, July 16-21, 2001, Rome, Italy*, pages 180–189, New York, 2001. ACM Press.

[BL02] S. Berger and F. Lehner. Intra- und Interorganisationale Kooperationen - Unterstützung der Prozesskopplung durch mobile Technologien. In D. Bartmann, editor, *Kopplung von Anwendungssystemen: FORWIN - Tagung 2002*, pages 281–297, Aachen, 2002. Shaker.

[BMR+98] F. Buschmann, R. Menier, H. Rohnert, P. Sommerlad, and M. Stal. *Pattern-orientierte Software-Architektur: ein Pattern-System*. Addison-Wesley-Longman, Bonn, Paris, 1998.

[BMT99] W.J. Brown, H.W. McCormmick III, and S.W. Thomas. *AntiPatterns and Patterns in Software Configuration Management*. Wiley Computer Publishing, New York, 1999.

[BSI02] BSI Bundesamt für Sicherheit in der Informationstechnik. *Sicherheit im Funk-LAN (WLAN, IEEE 802.11)*. BSI, http://www.bsi.de/fachthem/funk_lan/wlaninfo.pdf, 2002. Abruf am 25.03.2003.

[Eck01] C. Eckert. Zur Sicherheit mobiler persönlicher Endgeräte - eine Bestandsaufnahme. In P. Horster, editor, *Kommunikationssicherheit im Zeichen des Internet*, pages 204–217, Braunschweig, Wiesbaden, 2001. Vieweg.

[Eck03] C. Eckert. *IT-Sicherheit: Konzepte - Verfahren - Protokolle*. Oldenbourg, München, Wien, 2., überarbeitete und erweiterte auflage edition, 2003.

[FMS01] S. Fluhrer, I. Mantin, and A. Shamir. Weaknesses in the Key Scheduling Algorithm of RC4. In S. Vaudenay and A. M. Youssef, editors, *Selected areas in cryptography : 8th annual international workshop, SAC 2001, Toronto, Ontario, Canada, August 16 - 17, 2001*, pages 111–124, Berlin, Heidelberg, 2001. Springer.

[Fow97] Martin Fowler. *Analysis Patterns: Reusable Object Models*. Addison-Wesley-Longman, Reading, Massachusetts, 1997.

[FP00] H. Federrath and A. Pfitzmann. Gliederung und Systematisierung von Schutzzielen in IT-Systemen. *DuD - Datenschutz und Datensicherheit*, 24(12):704–710, 2000.

[FS01] O.K. Ferstl and E.S. Sinz. *Grundlagen der Wirtschaftsinformatik*. Oldenbourg, München, Wien, 4., überarb. und erw. aufl. edition, 2001.

[GH00] T. Goesmann and M. Hoffmann. Unterstützung wissensintensiver Prozesse durch Workflow-Management-Systeme. In R. Reichwald and J. Schlichter, editors, *Verteiltes Arbeiten - Arbeit der Zukunft. Tagungsband der DCSCW 2000*, pages 139–152, Stuttgart, 2000. Teubner.

[GHJV96] E. Gamma, R. Helm, R. Johnson, and J. Vlissides. *Entwurfsmuster: Elemente wiederverwendbarer objektorientierter Software*. Addison-Wesley-Longman, Bonn, 1996.

[GK00] D. Gerd tom Markotten and J. Kaiser. Benutzbare Sicherheit - Herausforderungen und Modell für E-Commerce-Systeme. *Wirtschaftsinformatik*, 42(6):531–538, 2000.

[Hei01] P. Heisig. Business Process Oriented Knowledge Management - Methode zur Verknüpfung von Wissensmanagement und Geschäftsprozessgestaltung. In H. Müller, A. Abecker, K. Hinkelmann, and H. Maus, editors, *Geschäftsprozessorientiertes Wissensmanagement, Workshop im Rahmen der 1. Konferenz Professionelles Wissensmanagement - Erfahrungen und Visionen*, 2001.

[JKGK03] W.A. Jansen, T. Krygiannis, S. Gavrilla, and V. Korolev. *Assigning and Enforcing Security Policies on Handheld Devices*. Proceedings of the Canadian Information Technology Security Symposium 2002, http://csrc.nist.gov/mobilesecurity/Publications/MobileDeviceSecurity.%pdf, 2003. Abruf am 25.03.2003.

[Küp96] H. Küpper. *Struktur, Aufgaben und Systeme des Hochschul-Controlling. In: Bayerisches Staatsinstitut für Hochschulforschung und Hochschulplanung: Beiträge zur Hochschulforschung*. München, 1996.

[Küp02] H. Küpper. Konzeption einer Perioden-Erfolgsrechnung für Hochschulen. *Zeitschrift für Betriebswirtschaft*, 72(9):929–951, 2002.

[LB01] F. Lehner and S. Berger. Mobile Knowledge Management. Schriftenreihe des lehrstuhls für wirtschaftsinformatik iii, Universität Regensburg, 2001.

[Leh00] F. Lehner. *Organisational Memory. Konzepte und Systeme für das organisatorische Lernen und das Wissensmanagement*. Carl Hanser, München, 2000.

[LHM00] F. Lehner, K. Hildebrand, and R. Maier. *Wirtschaftsinformatik: Theoretische Grundlagen*. Carl Hanser, München, 2000.

[Lip01] K. Lipinski. *Lexikon der Datenkommunikation*. mitp-Verlag, Bonn, 6., aktualisierte und erweiterte auflage edition, 2001.

[LTW01] K. Lenk, R. Traunmüller, and M. Wimmer. The Significance of Law and Knowledge for Electronic Government. In Grönlund, editor, *Electronic Government - Design, Applications and Management*, New York, 2001. Idea Group Publishing.

[Mat02] V. Matousek. *Implementierung eines Dialogmanagers in VoiceXML. Vortrag am Informationstag Mobile Computing am 7. Juni 2002*. Lehrstuhl für Wirtschaftsinformatik III der Universität Regensburg, http://www-mobil.uni-r.de/infotag2002.html, 2002. Abruf am 20.11.2002.

[MB02] J. Merkle and A. Bertsch. Geheimhilfe: Geschützte Datenkommunikation mit mobilen Endgeräten. *iX*, (6):66–71, 2002.

[Meh02] J. I. Mehlau. Sicherheitsmuster und ihre Rolle bei der Kopplung von Anwendungssystemen. In D. Bartmann, editor, *Kopplung von Anwendungssystemen: FORWIN - Tagung 2002*, pages 203–218, Aachen, 2002. Shaker Verlag.

[MM97] T.J. Mowbray and R.C. Malveau. *CORBA Design Patterns*. John Wiley & Sons, New York, 1997.

[NT95] I. Nonaka and H. Takeuchi. *The Knowledge-Creating Company. How Japanese Companies Create the Dynamics of Innovation*. Oxford University Press, New York, 1995.

[Opp97] R. Oppliger. *IT-Sicherheit - Grundlagen und Umsetzung in der Praxis*. Vieweg, Braunschweig, Wiesbaden, 1997.

[o.V00] o.V. Wettbewerb als Leitbild für die Hochschulpolitik.Sondergutachten der Monopolkommission gem. § 44 Abs. 1 Satz 4 GWB. Technical report, Monopolkommission, 2000.

[Pfl96] C.P. Pfleeger. *Security in Computing*. Prentice Hall, New York, 1996.

[PRR98] G. Probst, S. Raub, and K. Romhardt. *Wissen managen: Wie Unternehmen ihre wertvollste Ressource optimal nutzen*. Gabler, Frankfurt, 2. auflage edition, 1998.

[PSWW00] A. Pfitzmann, A. Schill, A. Westfeld, and G. Wolf. *Mehrseitige Sicherheit in offenen Netzen*. Vieweg, Braunschweig, Wiesbaden, 2000.

[Ran00] K. Rannenberg. Mehrseitige Sicherheit - Schutz für Unternehmen und ihre Partner im Internet. *Wirtschaftsinformatik*, 42(6):489–497, 2000.

[Rei96] R. Reichwald. Universitätsstrukturen und Führungsmechanismen für die Universität der Zukunft. Master's thesis, Arbeitsberichte des Lehrstuhls für Allgemeine und Industrielle Betriebswirtschaftslehre an der Technischen Universität München, 1996.

[Rei99] A. Reich. *Bayerisches Hochschulgesetz - Kommentar*. Karl Heinrich, Bock, 4., vollst. neubearb. aufl. edition, 1999.

[RKN00] S. Röhrig, K. Knorr, and H. Noser. Sicherheit von E-Business-Anwendungen - Struktur und Quantifizierung. *Wirtschaftsinformatik*, 42(6):499–507, 2000.

[Ros99] H. Rossen. *Vollzug und Verhandlung*. Mohr Siebeck, Tübingen, 1999.

[SA97] D. Skyrme and D. Amidon. The Knowledge Agenda. *Journal of Knowledge Management*, 1(1):27–37, 1997.

[SBU99] E.J. Sinz, M. Böhnlein, and A. Ulbrich-vom Ende. Konzeption eines Data Warehouse-Systems für Hochschulen. In H. Mayr, C. Steinberger, H. Appelrath, and U. Marquardt, editors, *Tagungsband zum Workshop Unternehmen Hochschule '99 im Rahmen der Informatik '99*, pages 111–124, Paderborn, 1999.

[Sch96a] B. Schneier. *Angewandte Kryptographie: Protokolle, Algorithmen und Sourcecode in C*. Addison-Wesley, Bonn, 1996.

[Sch96b] J. Schüppel. *Wissensmanagement. Organisatorisches Lernen im Spannungsfeld von Wissens- und Lernbarrieren*. DUV, Wiesbaden, 1996.

[Sch01] B. Schneier. *Secrets & Lies : IT-Sicherheit in einer vernetzten Welt*. dpunkt Verlag, Heidelberg, 2001.

[SIR03] A. Stubblefield, J. Ioannidis, and A. D. Rubin. *AT&T Labs Technical Report TD-4ZCPZZ: Using the Fluhrer, Mantin, and Shamir Attack to Break WEP*. AT&T, http://www.cs.rice.edu/~astubble/wep_attack.pdf, 2003. Abruf am 17.04.2003.

[Str99] Susanne Strahringer. Objektorientierte Muster - ein Statusbericht. *HMD - Praxis der Wirtschaftsinformatik*, 36(210):37–53, 1999.

[WEG+02] E. Weippl, W. Essmayr, F. Gruber, W. Stockner, and T. Trenker. Towards Authentication using Mobile Devices. In B. Jerman-Blažic and T. Klobucar, editors, *Advanced Communications and Multimedia Security*, pages 91–105, Dordrecht, 2002. Kluwer Academic Publishers.

[Wil02] R. Wille. Wissensmanagement im universitären Bereich. Ausarbeitung des Vortrages auf der Tagung Wissensmanagement der Technischen Universität Darmstadt am 19.02.2002. Technical report, Universität Darmstadt, 2002.

[WP00] G. Wolf and A. Pfitzmann. Charakteristika von Schutzzielen und Konsequenzen für Benutzungsschnittstellen. *Informatik Spektrum*, 23(3):173–191, 2000.

[WTL01] M. Wimmer, R. Traunmüller, and K. Lenk. Prozesse der öffentlichen Verwaltung: Besonderheiten in der Gestaltung von e-Government. In P. Horster, editor, *Elektronische Geschäftsprozesse: Grundlagen, Sicherheitsaspekte, Realisierungen, Anwendungen. Tagungsband zur gemeinsamen Arbeitskonferenz GI/VOI/BITKOM/OCG/TeleTrusT*, pages 436–445, Höhenkirchen, 2001. it.