Messung und Implementierung von Internet-Backbone-Sicherheit: Aktuelle Herausforderungen, aufkommender Einsatz und zukünftige Entwicklungen [1]

Matthias Wählisch[2]

Abstract: Diese Arbeit geht von der Beobachtung aus, dass das Internet eine kritische Infrastruktur ist, die besonderen Schutz bedarf. Die Arbeit orientiert sich dabei an einer praktischen Sicht auf das Internet. Es wird das gesamte Ökosystem bestehend aus Netzwerk, Endgeräten und Diensten betrachtet, welche sowohl von aktuellen als auch zukünftigen Internet-Protokollen bedroht werden. Wir fassen Werkzeuge, Methoden und Messungen zur Verbesserung des aktuellen Standes von Wissenschaft und Technik und der operativen Praxis auf Basis der Dissertation [Wä16] zusammen.

1 Einleitung

Das Internet ist ein global verteiltes Netzwerk, welches aus aus mehr als 60.000 autonomen Systemen besteht. Das primäre Ziel eines jeden autonomen Systems ist die Erreichbarkeit zwischen Internet-Teilnehmern sicherzustellen. Das Internet ermöglicht dabei die Kommunikation zwischen unterschiedlichen Anwendungen über die Grenzen eines jeden autonomen Systems hinweg. Dieses Ökosystem, bestehend aus Netzen, Endgeräten und Diensten, unterliegt einem kontinuierlichen Wandel.

Für den Erfolg der heutigen digitalen Kommunikation ist die Offenheit des Internets maßgeblich verantwortlich, da sie den permanenten Technologiewandel unterstützt. Die Offenheit spiegelt sich sowohl in technischen als auch ökonomischen Aspekten wider. Einerseits ist es jedem autonomen System (AS) freigestellt, mit welchem anderen AS es Daten direkt austauscht, solange es ein gegenseitiges Einverständnis in der Etablierung sogenannter *Peering*-Beziehungen gibt. Andererseits kann jeder Betreiber eines autonomen Systems innerhalb seines Netzes beliebige Technologien einsetzen, so lange ein gemeinsames Protokoll zwischen den Netzen gesprochen wird. Ein derartiges offenes und dezentrales System fordert die Zuverlässigkeit und die Sicherheit heraus.

Der Bedarf nach Sicherheit

Heutige Informations- und Kommunikationssysteme sind fast alle über das Internet miteinander verbunden. Das Internet bildet für nahezu alle öffentlichen und industriellen

[1] Englischer Titel der Dissertation [Wä16]: "Measuring and Implementing Internet Backbone Security: Current Challenges, Upcoming Deployment, and Future Trends".

[2] Freie Universität Berlin, Institut für Informatik m.waehlisch@fu-berlin.de

Organisationen unseres Landes, aber auch für wesentliche Teile des gesellschaftlichen Lebens eine kritische Kommunikationsinfrastruktur. Es gibt eine Vielzahl von Ansätzen auf den unterschiedlichen Schichten, um die Sicherheit und Verfügbarkeit der Internet-Kommunikation zu erhöhen. Dabei ist zu beachten, dass ein Schutz auf den oberen Schicht nur eingeschränkt Wirkung entfalten kann, wenn die untere Schicht verwundbar bleibt. Als Beispiel sei ein Schutz zur Erhöhung der Verfügbareit auf der Transportschicht genannt, welcher unwirksam wird, wenn auf der darunterliegenden Netzwerkschicht eine Verkehrsumleitung zu einem anderen Endpunkt erreicht wird. Viele Sicherheitslösungen wurden in den letzten Jahren vorgeschlagen, aber überraschend wenige erfahren einen praktischen Einsatz.

1.1 Hintergrund: Heutige und zukünftige Internet-Kommunikation

Internet Core: Angriffe auf das Border Gateway Protocol

Die Bekanntmachung der Erreichbarkeit von Internet-Adresspräfixen (z.B. `10.20.0.0/16` für den Adressbereich `10.20.0.0-10.20.255.255`) erfolgt durch das *Border Gateway Protocol* (BGP) [RLH06]. Jeder BGP-Router informiert seine Nachbarn über seine eigenen IP-Präfixe und die ihm anderweitig bekannten Adressbereiche. Die Auswahlregeln, welche Präfixe bzw. Wege zu einem Präfix verteilt werden, sind komplex und nach außen weitgehend unsichtbar. Sie hängen vom jeweiligen Internet Service Provider (ISP) ab. Die Richtigkeit der verteilten BGP-Informationen ist aber für die korrekte Datenverteilung im Internet elementar. Durch Falschinformationen kann es zu einer ungewollten Datenumleitung kommen, wodurch sich Datenverkehr mitlesen lässt oder unzustellbar wird.

In der ursprünglichen Entwicklung von BGP gab es keine Schutzmechanismen gegen Falschinformationen. Das Protokoll [RLH06] basiert auf Vertrauen. Folglich kann jeder BGP-Router z.B. behaupten, der Besitzer eines IP-Präfixes zu sein, wodurch der Router Datenverkehr für dieses Präfix illegitim anzieht. Solche Fehler [Bu10] (auch *Prefix Hijack* genannt) passieren überraschend oft – ob unfreiwillig oder mutwillig ist dabei häufig unklar. Anfang 2012 wurden Internet-Standards verabschiedet und zum Einsatz gebracht, um sich vor einen Teil der Bedrohungen zu schützen. Internet-Betreiber haben nun die Möglichkeit, kryptographisch zu attestieren, welches autonome System welches IP-Präfix initial annoncieren darf. Die Arbeit [Wä16] analysiert erstmalig den Verbreitungsgrad und Gründe für die Nichtverbreitung dieses neuen Schutzverfahrens.

Internet Edge: Entfernte Angriffe auf Endgeräte

Neben Angriffen auf das Internet-Backbone sind Angriffe auf Internet-Endgeräte üblich und stellen eine ernstzunehmende Bedrohung dar. Das heutige Internet folgt weiterhin dem Ende-zu-Ende-Prinzip, auch wenn Middleboxes wie z.B. *Network Address Translation* die reine Lehre brechen. Endgeräte kommunizieren direkt miteinander. Das Internet sollte die Daten auf Basis der Endpunkt-IP-Adressen weiterleiten. Dies vereinfacht den Betrieb des

Internet-Cores erheblich, macht aber die Endgeräte angreifbarer. Wenn es keine separaten Filtermechanismen gibt, kann erst einmal jedes Endgerät Daten an jedes andere Endgerät schicken. Sogenannte *Denial of Service* Angriffe sehen vor, dass der Angreifer mehr Daten schickt, als das Netzwerk oder das Endgerät verarbeiten kann. Diese Angriffe sind für einen Großteil heutiger bösartig herbeigeführter Netzausfälle verantwortlich. Internet Service Provider und Endnutzer haben nur sehr eingeschränkte Möglichkeiten sich davor zu schützen, ohne dabei gleichzeitig die Offenheit des Internets aufzugeben. Es wurde untersucht, wieweit Angriffe auf Endgeräte abhängig vom Netzzugang sind.

Vom Edge zum Core: Informationszentrische Netze als zukünftige Netzarchitektur

Informationszentrische Netze (ICN) [Ah12] wurden entworfen, um sowohl die Verteilung von Inhalten als auch die Sicherheit im Netz zu verbessern. Die Kernidee besteht darin, dass das Netz die Daten inhaltsorientiert verteilt, statt ausschließlich basierend auf einer Endpunktadresse. ICN gibt das klassische Ende-zu-Ende-Pardigma des jetzigen Internets auf, um asynchrones, globales Caching im Netz nativ zu ermöglichen. Für Endgeräte ist es damit nicht mehr wichtig, woher der Inhalt kommt, sondern nur dass der richtige Inhalt zu einer passenden Anfrage ausgeliefert wird.

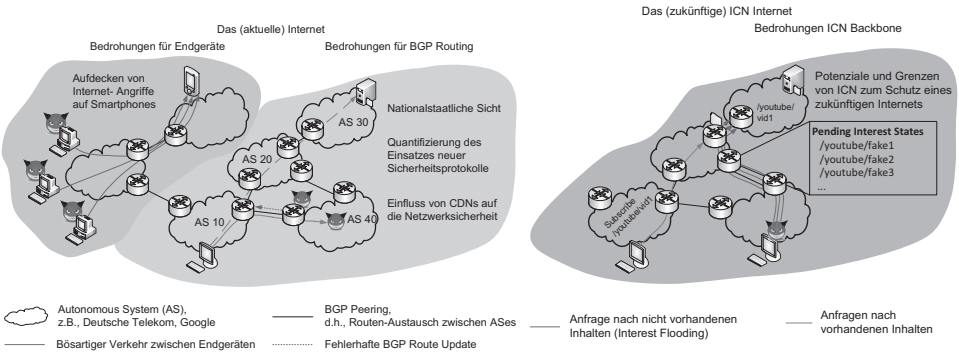
In ICN folgt die Kommunikation somit nur noch der Nachfrage nach Netzinhalten. Folglich sind Denial of Service Angriffe zwischen Endgeräten inhärent nicht mehr möglich – so lange ein Endgerät kein Interesse an Inhalten signalisiert hat, werden auch keine Daten an dieses Endgerät ausgeliefert. Insbesondere kann ein Angreifer nicht unaufgefordert Daten an ein anderes Endgerät schicken.

Named Data Networking (NDN) ist eine prominente Ausgestaltung von ICN. NDN implementiert dabei namensbasiertes Routing direkt auf der Netzwerkschicht. Entsprechend der Anfrage eines Endgeräts werden für die (delokalisierte) Datenverteilung dynamisch Zustände auf den Routern implementiert. Andere ICN-Ansätze funktionieren im Detail anders, verlangen aber ebenfalls eine dynamische Zustandsetablierung auf Core-Netzkomponenten. Es wurden die Auswirkungen der Entwurfsentscheidung in ICN auf die Sicherheit eines zukünftigen Internet-Backbones untersucht.

Nachfolgend geben wir einen genaueren Überblick über die einzelnen Beiträge der Arbeit [Wä16].

2 Beitrag: Eine nationalstaatliche Sicht auf das Internet-Backbone

Empirische Untersuchungen der globalen Internet-Infrastruktur werden seit mehr als zehn Jahren mit stetig steigender Beachtung durchgeführt. Analysen einer nationalen Sicht auf das Internet existieren bisher nur vereinzelt [KFR09]. Doch nicht allein aus gesellschaftlichen Aspekten ist eine landeszentrische Untersuchung der Internet-Infrastruktur von Interesse. Vielmehr begründen die nachfolgenden Fragestellungen einen eigenständigen Forschungsgegenstand.



(a) Angriffe auf die aktuelle Internet-Infrastruktur (b) Gefahren für informationszentrische Netze

Abb. 1: Aktuelle und zukünftige Bedrohungen im Internet

- Ist eine nationale Klassiffizierung auf IP- bzw. AS-Ebene im Internet sinnvoll möglich?
- Inwieweit lässt sich das IP-Routing national abgrenzen?
- Wie sind die strukturellen Abhängigkeiten des nationalen Netzes und dessen Robustheit beschaffen?
- Wie abhängig ist die Landesnetzinfrastruktur von dem internationalen (länderspezifischen) Transport?
- Wie kann das nationale Backbone gegen internationale Angriffe und 'Routen-Entführung' geschützt werden?
- Wie hängen Regionalität und Routen-Proximität voneinander ab?

Um diese Fragen zu beantworten, müssen nationale Teilnehmer und die Routing-Strukturen, welche innerstaatliche Verkehrsflüsse lenken, identifiziert, analysiert und bewertet werden. Das Interesse an einer kontinuierlichen, zeitnahen Beobachtung erfordert dabei eine fast vollständige Automatisierung dieser Analyseschritte. Die Arbeit [Wä16] hat sowohl Methoden als auch Software-Werkzeuge hierfür entwickelt. Dieser Lösungsvorschlag zur Gewinnung einer 'nationalen' Perspektive auf das Internet wurde für Deutschland qualitativ und quantitativ analysiert.

Der Untersuchungsschritt widmet sich zunächst den Möglichkeiten und Grenzen, IP-Adressbereiche und ihre zugehörigen Autonomen Systeme (ASe) länderspezifisch zuzuordnen und die deutschen Teilnehmer herauszufiltern. Obgleich alle vorhandenen administrativen Datenbestände stark verrauscht sind, gelingt es durch eine Verkettung von Prüf- und Korrekturwerkzeugen, die verbleibende Fehlermenge auf weniger als 3 % zu minimieren. Eine schlüsselwortbasierte Suche ermöglicht es hiernach, die wichtigsten autonomen Systeme Kernbranchen zuzuordnen, so dass im Ergebnis eine Liste klassifizierter autonomer Systeme vorliegt, welche deutschen Einrichtungen zuzuordnen sind oder welche IP-Blöcke deutsche Inhaber umfassen.

Unter Nutzung einschlägiger Monitordaten des Internets einschließlich gängiger Peering-Modelle werden in einem weiteren Schritt die minimalen Routing-Graphen zwischen den 'deutschen ASen' ermittelt. Hierbei werden auch alle landesfremden Transit-ASe und -

Pfade bestimmt, so dass eine Visualisierung und quantitative Bewertung des Routing-Teilgraphen möglich wird, der die landesinterne Infrastruktur vollständig funktionsfähig macht. Als Ergebnis umfangreicher Analysen und Datenaufbereitungen konnte eine Sammlung von Topologievisualisierungen erstellt werden, welche Strukturen, Schichten, Branchen und Anwendungsflüsse der deutschen Internet-Infrastruktur veranschaulichen.

Die Analyse der Branchengraphen hat gezeigt, dass ein Peering selten direkt zwischen Autonomen Systemen gleicher Industriebereiche stattfindet, sondern häufig einige wenige ASe – teilweise internationalen Ursprungs – verbindend wirken. Die Entscheidung für ein unmittelbares Peering ist dabei sehr kontextspezifisch. Finanzinstitute beispielsweise sind mit ihren ersten AS-Nachbarn weitgehend unabhängig von einem konkreten Ziel verbunden. Demgegenüber unterhalten Firmenprovider in 80% der Fälle Peering-Beziehungen dediziert abhängig von der Zielbranche. Interessanterweise dienen die Peering-Beziehungen nicht primär der Verkürzung der Inter-AS-Wege, denn die Distanzverteilungen der einzelnen Branchen sowie des gesamten DE-Graphen sind bis auf wenige Ausnahmen gleichmäßig verteilt mit einer mittleren Pfadlänge zwischen 3.0 und 3.4 AS-Knoten.

3 Beitrag: Protokolle zum Schutz des Internet-Backbone-Routings

3.1 Analyse des Einsatzes von RPKI auf Routern

Die Resource Public Key Infrastructure (RPKI) stellt kryptographische Datensätze bereit, mit denen sich der Besitz von Internet-Ressourcen (IP-Präfixe, AS-Nummern) nachweisen lässt [Hu09]. Diese Informationen sollen für die Erkennung von klassischen Präfix-Hijacking benutzt und zukünftig für die Aufdeckung von BGP-Pfadmanipulationen Einsatz finden. Der Erfolg dieser Technologie hängt von zwei Faktoren ab: (1) Wie zuverlässig lassen sich tatsächliche Hijacks erkennen? (2) Welche systemischen Auswirkungen hat der Einsatz von RPKI auf BGP-Routern?

Die Arbeit [Wä16] präsentiert erste Einsichten bezüglich der zusätzlichen Systemlast durch RPKI auf Standard-Routern nund diskutiert neue Angriffsvektoren, die sich hieraus ergeben. Die Ergebnisse basieren auf Experimenten. Hierfür wurden die notwendigen Protokolle und Funktionen in einer C-Bibliothek implementiert, welche auf BGP-Routern zum Einsatz kommt [Wä13a]. Diese Referenzbibliothek ist das erste Werkzeug zur echtzeitfähigen RPKI-Validierung von Internet-Routen. Auf Basis echter BGP-Ströme konnte nachgewiesen werden, dass auf sogenannter *Commodity Hardware* eine ausgesprochen geringe Zusatzlast durch RPKI hervorgerufen wird, welche einen Einsatz nicht verhindert.

Weiterhin wurden die invaliden Präfixen im Detail untersucht: Welche IP-Präfixe sind auf Basis aktueller RPKI-Daten richtig und welche falsch [WMS12]? Hierbei zeigte sich, dass ein überraschend großer Anteil an aktuell im Internet verbreiteten BGP-Announcement inkorrekt sind. Genauere Untersuchungen haben dann gezeigt, dass diese invaliden Präfixe primär Fehlkonfigurationen der RPKI durch die Besitzer der IP-Präfixe zuzuordnen sind. Die Arbeit [Wä16] schlägt eine Heuristik vor, um solche Fehler automatisch zu erkennen. Diese Heuristik hat schließlich dazu beigetragen, die Datenqualität innerhalb der RPKI zu erhöhen.

3.2 Analyse des Schutzes der Webserver-Infrastruktur durch RPKI

Das Web stellt einen der wichtigsten Dienste oberhalb des Internets dar. Durch das Umlenken des Internet-Verkehrs lässt sich die Kommunikation nicht nur mitlesen, sondern auch stören, so dass Webserver nicht mehr erreichbar sind. Folglich ist es von besonderem Interesse, die Webserver-Infrastruktur im Routing abzusichern. In der Arbeit [Wä15, Wä16] wurde untersucht, welche Web-Domains durch die RPKI geschützt sind, d.h. für welche IP-Präfixe von Webservern kryptographisch gesicherte RPKI-Objekte existieren.

Eine solche Analyse ist primär von der Herausforderung begleitet, die hinter einem Domain-Namen verborgene Webserver-Infrastruktur zu ermitteln. Hinter einem Namen (z.B. `www.google.com`) können sich mehrere IP-Adressen (z.B. `216.58.213.228` und `216.58.213.229`) verbergen. Sogenannte *Content Delivery Networks* erschweren diesen Auflösungsprozess insofern, als dass DNS-Antworten vom topologischen und geographischen Ort des Anfragenden (also des Web-Clients) abhängen.

In der Arbeit [Wä16] wurden 1 Millionen Domain Namen untersucht. Im Gegensatz zu bisherigen Verfahren zur Namensauflösung von Webadressen wurden sämtliche Namen mit und ohne `www`-Präfix aufgelöst. Es wurde gezeigt, dass dieser Schritt für die Abbildung auf IP-Präfixe abhängig vom konkreten Domain-Namen wichtig ist. Weiterhin wurde gezeigt, dass populäre Webseiten deutlich schwächer geschützt sind als unpopuläre, entgegen gängiger Vermutungen. Dies ist insbesondere dadurch begründet, dass populäre Webseiten durch Content Delivery Networks (CDN) ausgeliefert werden. Die Betreiber von CDNs haben die Präfixe ihrer eigenen Netze aber nicht durch die RPKI abgesichert, wie gezeigt werden konnte. CDN-Inhalte werden – wenn überhaupt – ausschließlich durch Dritt-Betreiber geschützt.

Die Arbeit [Wä16] hat weiterhin technologiespezifische Gründe identifiziert, die den Einsatz von RPKI verhindern. Hierbei wurden ökonomische und politische Aspekte analysiert. Insbesondere die Einsicht, dass die RPKI mit bestimmten Geschäftsmodellen von Internet Service Providern im Konflikt steht, stellt eine bis dahin wenig beachtete Erkenntnis dar.

4 Beitrag: Sind Angriffe auf Endgeräte abhängig vom Netzzugang?

Mobilgeräte wie z.B. Smartphones sind deutlich leistungsschwächer als herkömmliche PCs. Klassische Schutzverfahren wie Virenscanner oder Firewall können nur bedingt oder überhaupt nicht eingesetzt werden, da die vorhandenen Hardware-Ressourcen auf den Geräten den Leistungsanforderungen der Software nicht genügen. Insbesondere steht eine kontinuierliche Überwachung im Konflikt mit batteriebetriebenen Geräten. Demnach ist zu vermuten, dass Mobilgeräte eine besonderes Angriffsziel darstellen. Die Identifizierung von Netzbereichen, die diese Geräte beherbergen, kann einerseits durch Scans andererseits durch Meta-Informationen in den Datenbanken der Internet Registries erfolgen.

In dieser Arbeit [Wä16] wurde ein *Mobile Honeypot* [Wä13b] entworfen und erprobt, um zu untersuchen, inwieweit sich Angriffe auf Mobilgeräte im Vergleich zu sonstigen PCs

unterscheiden. Die Auswertungen basieren auf Daten von drei unterschiedlich angebundenen Honeypots (Darknet, UMTS, vollständig offenes Netz) über einen Messzeitraum von mehr als 1,5 Jahren.

5 Beitrag: Inhärente Bedrohungen in zukünftigen Netzarchitekturen

Informationszentrische Netze geben die Ende-zu-Ende-Kommunikation auf, um Endgeräte vor ungewollter Kommunikation zu schützen. Somit lassen sich *Denial of Service* Angriffe auf Endgeräte verhindern. In dieser Arbeit [Wä16] wurde erstmalig analysiert, welche Auswirkungen dieser fundamentale Entwurfsschritt der ICN-Netzarchitektur auf die Gefährdung eines zukünftigen Internet-Backbones hat [WSV13a, WSV13b]. Die Arbeit hat inhärente Kernprobleme herausgearbeitet. Die Aufgabe des Ende-zu-Ende-Paradigmas verlangt, dass dynamisch Zustände auf Routern in einem ICN-Backbone erzeugt werden. Diese Zustände sind getrieben durch (a) Endnutzer und (b) Daten. Folglich hat das Abrufen von Inhalten innerhalb eines ICN-Netzes direkten Einfluss auf die Kerninfrastruktur. Dies steht im fundamentalen Gegensatz zum jetzigen Internet, in dem Forwarding-Zustände unabhängig von Endgeräten oder Daten etabliert bzw. aktualisiert werden. Durch die Verhinderung von *Denial of Service* Angriffen auf Endgeräte wird das Internet-Backbone selber angreifbar. Das Problem wird von den Endgeräten auf das Backbone verlagert.

In der Arbeit wurden neue Angriffsvektoren und konkrete Angriffe definiert und diskutiert. Die Angriffe und deren Auswirkungen wurden simuliert und in praktischen Experimenten bestätigt. Weiterhin wurde ein analytisches Modell entwickelt, mit dem sich die Gefahrenlage abhängig von den Eigenschaften der Netztopologie quantifizieren lässt.

6 Zusammenfassung und Ausblick

Die Dissertation [Wä16] betrachtet das Internet als kritische Infrastruktur. Dabei sollte der Schutz der selbigen nicht die offene Kommunikation einschränken, denn die Offenheit des Internets ist maßgeblich für den Erfolg digitaler Kommunikation verantwortlich. Es wurde eine praktische Sicht auf das Thema Internet-Sicherheit eingenommen, wobei wir das Internet-Core, Endgeräte und Dienste berücksichtigten. Wir stellten das gesamte Internet-Ökosystem in den Kontext aktueller und zukünftiger Netzarchitekturen und -protokolle. Neben neuen Methoden, Konzepten und Messungen trägt die Arbeit Werkzeuge zur Analyse und Verbesserung der Sicherheitslage im Internet bei. Die adressierten Fragestellungen der Dissertation [Wä16] sind in den Tabellen 1 und 2 zusammengefasst.

Unsere zukünftige Forschungsagenda wird auf den gewonnenen Erkenntnissen aufsetzen. Wir werden inbesondere zwei Fragestellungen weiter nachgehen: (1) Warum werden vorhandene Schutzmechanismen nur bedingt eingesetzt, obgleich es einen Bedarf nach einer sicheren Internet-Infrastruktur gibt; sind diese Gründe primär technisch oder ökonomisch motiviert? (2) Lassen sich Endgeräte und Backbone in einem zukünftigen, informationszentrischen Internet inhärent schützen, ohne die Offenheit des Internets zu gefährden?

	Forschungsfragen	Methodik				Kernergebnisse
		S	E	M	Data	
Internet Core	***Aufdecken einer nationalstaatlichen Sicht auf das verteilte Internet, um die für ein Land wichtige Kommuninkationsinfrastruktur zu schützen.***					
	Welche Internet-Ressourcen ermöglichen eine nationalstaatliche Sicht auf die Internet-Infrastruktur?	✘	✘	✓	RIR DB, Maxmind	Durch die Nutzung von IP-Blöcken statt IP-Präfixen konnten 25% mehr ASes identifiziert werden. Verglichen mit gängigen Datenbanken (Maxmind) führt eine Abbildung von IP-Blöcken auf Ländern nur zu 0,2% an False Positives und False Negatives.
	Wie robust ist das Internet-Routing aus Sicht kritscher Geschäftsbranchen?	✘	✘	✓	RIR DB, BGP Dumps	Mitglieder der gleichen Branchen tendieren nicht dazu, miteinander direkt Daten auszutauschen, sondern sind über einige ausgewählte nationale aber auch internationale ASes verbunden. Wieweit sich der erste Hop unterscheidet, hängt von der jeweiligen Branche ab.
	Quantifizierung der Herausforderungen beim Einsatz neuer Sicherheitsvefahren im Internet-Backbone.					
	Wieweit verringert RPKI die Leistungsfähigkeit von Backbone-Routern?	✘	✓	✓	BGP Dumps, RPKI Daten	Eine vollständige RPKI-Tabelle würde 5% mehr RAM auf herkömmlichen Routern benötigen. 10 Millionen ROA-Einträge können in weniger als einer Minute initial verarbeitet werden, wodurch ein Router unmittelbar nach dem Start einsatzfähig wäre. Die Validierung von echten BGP-Daten (max. $\approx$ 92.000 Einträge pro Minute) benötigt weniger als 0,5% der CPU-Ressourcen.
←	Wieweit verändert ein voranschreitener Einsatz von RPKI die Router-Leistung?	✘	✓	✘	künstliche BGP, RPKI Daten	Der Anteil von validen, invaliden und ungeschützten Präfixen kann die CPU-Last um eine Größenordnung verändern.
	Sind invalid BGP-Präfixe Hijacks?	✘	✘	✓	BGP Dumps, RPKI Daten	Zu Beginn des RPKI-Deployments waren 90% der invaliden Updates in der Miskonfiguration der RPKI begründet. In 90% der Fälle war das legitime AS nur einen AS-Hop entfernt.
	Können wir die Zahl der falsch konfigurierten RPKI-Objekte verbessern, indem wir eine geringe Menge an Änderungen vornehmen?	✘	✘	✓	BGP Dumps, RPKI Daten	30%-40% der invaliden Updates werden durch die fünf RPKI-Einträge bestimmt.
Core / Edge Dienste	***Analyse des Einflusses von CDNs auf die Netzwerksicherheit.***					
	Wieweit beeinflussen Namenspräfixe (`www.google.com` vs. `google.com`) den Ort der Webinhalte?	✘	✘	✓	Aktive DNS Daten	Für die ersten 100.000 Alexa-Domains stimmen 76% der IP-Präfixe für www und nicht-www überein. Für die verblebleibenden Domain-Namen weisen 94% das gleiche IP-Präfix auf.
	Für welche IP-Präfixe der Webserver-Infrastruktur gibt es eine Absicherung mittels RPKI?	✘	✘	✓	BGP Dumps, aktive DNS Daten	6% der 1 Millionen Alexa-Domains werden durch RPKI geschützt, wobei $\approx$ 0,09% der zugehörigen BGP Updates invalide sind.
←	Korreliert die Popularität von Webseiten mit einem erhöhten Schutz im Internet-Routing?	✘	✘	✓	BGP Dumps, RPKI, DNS	Populäre Webseiten sind schlechter geschützt. Nur 4% der 100.000 populärsten Webseiten sind überhaupt geschützt.
	Warum sind populäre Webseiten schlechter geschützt?	✘	✘	✓	BGP Dumps, RPKI, DNS	Populäre Webseiten werden in der Regel durch CDNs verteilt, welche RPKI bisher nicht einsetzen.

Tab. 1: Übersicht: Forschungsfragen, Experimente und Kernergebnisse der Dissertation [Wä16] (S=Simulation, E=Emulation, M=Messungen)

	Forschungsfragen	Methodik				Kernergebnisse
		S	E	M	Data	
	Aufdecken von Internet-Angriffen auf Mobilgeräte.					
Internet Edge	Wieweit hängen Angriffe vom Netzzugang ab?	✘	✘	✓	Honeypot-Daten	DSL-, UMTS- und Darknet-Knoten sind durch Angriffe in der gleichen Grösenordnung bedroht.
	Zielen Remote-Angriffe speziell auf mobile Endgeräte?	✘	✘	✓	Honeypot Daten	Angreifer führen selten mobil-spezifische Angriffe durch, sondern eher eher allg. Linux-spezifische Antriffe, indem sie z.B. das generische Linux-Dateisystem durchsuchen.
⟵	Ist der Angreiferort abhängig vom Ziel (mobile vs. stationäre Ziele)?	✘	✘	✓	BGP, Maxmind, honeypot Daten	Ein Grosteil der Angriffe wird von der selben Menge an autonomen Systemen durchgeführt. Die Top-5 ASes sind in China und Russland lokalisiert.
	Potentiale und Grenzen von ICN zum Schutz eines zukünftigen Internets.					
Internet Edge / Core	Welche Angriffe sind auf die ICN-Infrastruktur möglich?	✘	✓	✘	CCNx	Die Verwaltung von Zuständen kann zur Überlast auf den Routern und damit zum Datenverlust führen.
	Wieweit beeinflussen im Internet gängige Laufzeiten die Leistungsfähigkeit von ICN?	✘	✓	✘	analytisches Modell, PingER Daten, CCNx	Laufzeiten sind im Internet sehr heterogen und damit nur sehr schwer vorhersagbar. Laufzeiten, die gängie *Expiration Timer* überschreiten, führen zu einem erhöhten Aufwanf für die Verwaltung der Zusta”nde. Dies wiederum verlangt eine Überversorgung der Router-Hardware.
	Wie beeinflusst die Router-Hardware den Entwurf von ICN-Netzen?	✘	✓	✘	CCNx	Der Upstream Router des schwächsten Routers benötigt 50$-500% mehr Speicher als jeder andere Router im Netz. Für eine zuverlässige Datenzustellung müssten die Router gleichmäßig ausgestattet sein.
	Ist eine geringe Leistungsfähigkeit des Netzes ausschließlich eine Randeffekt von lokalen, insuffizienten Systemressourcen?	✓	✘	✘	ndnSim, Sprintlink-Topologie (Rocketfuel)	Nein. Unsere Simulationen haben geseizgt, dass ICN-Routing die zur Verfügung stehenden Übertragungsressourcen in realistischen Topologien häufig nicht ausnutzen kann, da es pro Zustand unkoordiniertes Hop-by-Hop Forwarding nutzt.

Tab. 2: Übersicht: Forschungsfragen, Experimente und Kernergebnisse der Dissertation [Wä16] (S=Simulation, E=Emulation, M=Messungen)

Matthias Wählisch Herr Wählisch studierte Informatik und Neue deutsche Literatur an der Freien Universität Berlin. In seiner Diplomarbeit erforschte er einen neuartigen Ansatz für die skalierbare, adaptive Gruppenkommunikation mittels bidirektionaler Präfix-Bäume. Von 2009 bis 2016 war Herr Wählisch wissenschaftlicher Mitarbeiter, Dozent und Projektleiter am Lehrstuhl Computer Systems & Telematics. Seit 2016 ist Matthias Wählisch Juniorprofessor an der Freien Universität Berlin und leitet den Bereich Internet-Technologien. Herr Wählisch verantwortet mehrere von ihm eingeworbene Drittmittelprojekte und ist Mitglied zahlreicher Programm- und Organisationskomitees wissenschaftlicher Veranstaltungen (u.a. IEEE ICNP 2013, ACM ICN 2017, ACM SIGCOMM 2017). Seine Forschungsleistungen wurden mehrfach ausgezeichnet, u.a. mit dem Nachwuchspreis 2011 des Leibniz-Kolleg Potsdam und dem Nachwuchspreis 2015 der Stiftung für Industrieforschung.