Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Ausarbeitung Anwendungen 2

Marco Schneider

Border Gateway Protocoll
Monitoring, Topologie und Sicherheit

Fakultät Technik und Informatik
Department Informatik

Faculty of Engineering and Computer Science
Department of Computer Science

Marco Schneider

Thema

Border Gateway Protocol - Monitoring, Topologie und Sicherheit

Stichworte

Border Gateway Protocol, BGP, Monitoring, Flussmessung, Topologieerkennung, Analyse, Sicherheit

Kurzzusammenfassung

Diese Ausarbeitung ist eine Zusammenfassung der verwandten Arbeiten für das Projekt 1.

Marco Schneider

Title

Border Gateway Protocol - monitoring, topology and security

Keywords

Border Gateway Protocol, BGP, monitoring, flowmeasurement, identification of topology, analysis, security

Abstract

This paper is a summary of the related work for "‘Project 1"’.

Inhaltsverzeichnis

1 Einleitung

Zu den Netzwerkeinstellungen eines gewöhnlichen Arbeitsplatz-PCs gehört neben der eindeutigen IP-Adresse auch ein Gateway. An das Gateway werden alle Pakete geschickt, die der PC nicht direkt in seinem Netzwerk zustellen kann. Diese Hierarchie setzt sich weiter fort: kann der Firmenrouter das Paket auch nicht zustellen, sendet dieser das Paket über seinen Gateway zu seinem Provider.

Bei den Providern funktioniert diese Hierarchie jedoch nicht mehr: es gibt keinen Gateway mehr. Damit die Pakete das Ziel doch erreichen, gibt es eine Instanz, welche die Pakete direkt an den ensprechenden Router weiterleitet. Dies ist die sog. default-free-zone, d.h. es ist die höchste Hierarchieebene im Routingsystem des Internet. Damit dieses System einwandfrei funktioniert, müssen alle Teilnehmer ein gemeinsames Protokoll benutzen: das Border Gateway Protocoll (BGP).

1.1 Motivation

Das Internet ist das Resultat einer Idee, Computer mittels einer universellen Abstraktionsschicht zu verbinden und so eine systemorientierte Rechnerkommunikation zu ermöglichen - unabhängig von dem physischen Übertragungsweg bzw. der Übertragungstechnik. Durch den Erfolg und den Wunsch nach einer Vernetzung aller Computer wurde das Internet immer größer und komplexer. In diesem Gebiet ist viel Bewegung: Forschung und Wissenschaft suchen ständig nach neuen Methoden, die bisherige Technik zu verbessern oder zu erweitern.

Das Border Gateway Protocol (BGP) ist der de-facto Standard des EGP[1] - also des Routings zwischen den verschiedenen IP-Netzen. Der erste Entwurf des heutigen BGP4 wurde bereits 1995 als Neuauflage für das BGP3 eingericht (1). Natürlich gab es viele Veränderungen zur Verbesserung des BGP4, dennoch wird dieses Protokoll nicht in absehbarer Zeit abgelöst werden (2), wie z.B. IPv4 durch IPv6 - ein weiterer Grund, sich mit dem Thema tiefer auseinanderzusetzen.

Das Internet entwickelt sich zu einer Ende-zu-Ende Topologie (3). Techniken wie der Multicast werden immer wichtiger durch den ressourcenschonenden Umgang mit der zur Verfügung

[1] Exterior Gateway Protokoll

stehenden Infrastruktur, deswegen kann ein Einblick in das Rückgrat des Internet sehr hilfreich sein für die Optimierung dieser Multicast-Ströme. Die INET-Gruppe[2] der HAW Hamburg forscht auf diesem Gebiet - jedoch gibt es keine praktischen Experimentiermöglichkeiten am Backbone-Routing.

Durch eine Kooperation mit dem *Berlin Commercial Internet Exchange e.V.*[3] (BCIX) ist es möglich, diese Lücke zu schließen. Dazu wurde ein Hardware-Router der Firma Brocade angeschafft, welcher direkt am BCIX ein eigenes (Test-) Prefix propagieren wird. Die Erkenntnisse können zur Validierung anderer Projekte (z.B. des Routing-Atlas[4]) benutzt werden.

1.2 Problemstellung

Um einen Messplatz am BCIX etablieren zu können, bedarf es nicht nur der vorhandenen Hardware und einer Kooperation: Fehlkonfigurationen können großen Schaden anrichten.

Expertise ist allerdings nicht nur beim Konfigurieren des Routers gefragt, sondern auch beim Messen und Analysieren von BGP-Updates. Zum Validieren eines Routingpfades reicht eine Anfrage an die Routing-Tabelle, doch möchte man potenzielle Angriffe erkennen können, müssen über einen längeren Zeitraum sämtliche Updates ausgewertet werden. Dabei spielt der eigene Standpunkt in der Topologie eine große Rolle, denn je nach Standort ändert sich die Perspektive auf die Topologie. Dies muss man bei aktiven oder passiven Messungen berücksichtigen, da sich die Ergebnisse von den öffentlichen (weiter oben in der Hierarchie angesiedelten) Messplätzen unterscheiden können.

1.3 Aufbau dieser Arbeit

Der Einführungsteil dieser Arbeit endet mit diesem Kapitel. Im folgenden Topologie-Kapitel werden bereits existierende Projekte vorgestellt und verschiedene Messmethoden vorgestellt. Darauf folgt BGP Verwundbarkeit, in dem verschiedene Angriffsmöglichkeiten erklärt werden und wie man diese wirksam verhindert. Den Abschluss bildet die Abgrenzung zu den vorgestellten Arbeiten.

[2] http://inet.cpt.haw-hamburg.de/
[3] http://www.bcix.de/bcix/
[4] http://inet.cpt.haw-hamburg.de/projects/routing-atlas

2 Topologie

Das heutige Internet besteht aus einer ständig steigenden Zahl von Hosts, welche über Netzwerke miteinander verbunden sind. Diese Netzwerke werden vom jeweiligen Inhaber (ISPs, etc.) administriert und sind untereinander mit dem inter-domain Routingprotokoll BGP verbunden. Durch die fehlende, zentrale Administration, ist es jedem Netzbetreiber möglich, eigene Regeln bei z.B. der Pfadauswahl zu treffen (4).

Das Internet ist hierarchisch aufgebaut: es gibt 12 Tier-1 Provider, welche für ihre Kunden die Konnektivität ermöglichen. Dieser Service kostet den Kunden Geld, sodass die kleineren Provider daran interessiert sind, sich direkt untereinander kostenneutral zu vernetzen. Dies findet in der Regel an Internet Exchange Points (IXP) statt, wo sich die physikalischen Leitungen der Provider treffen. Manche Provider peeren nicht öffentlich, sodass man die Links nur an bestimmten Standorte in der Topologie erkennen kann.

Um diese stark vermaschte Topologie und die Abläufe darin überblicken zu können, können die Update-Nachrichten des BGP-Protokolls analysiert werden. Diese kann man sowohl für die Topologieerkennung, als auch für die Anomalieerkennung nutzen.

2.1 Projekte

2.1.1 Route-Views Project

Das Route-Views Projekt[1] ist ein Projekt des Advanced Network Technology Center (ANTC) der University of Oregon. Das ANTC wurde gegründet, um neue Netzwerktechnologien zu erforschen und zu entwickeln.

Das Route-Views Projekt war ursprünglich als ein Tool konzipiert, welches einen Einblick in Echtzeit in die Routing-Informationen des Internets ermöglichen sollte. Diese Informationen sind für (Netzwerk-)Administratoren von entscheidender Bedeutung: mit dem Einblick von einer anderen Sicht des Netzwerkes können die eigene Konfigurationn überprüft, und mögliche Fehler entdeckt werden.

[1] http://www.routeviews.org/

Um eine möglichst umfangreiche Datensammlung zu bekommen, betreibt das Route-Views Projekt insgesamt 16 verschiedene Route-Collectoren. Ein Route-Collector ist ein vollwertiger BGP-Speaker[2], welcher seine aktuelle Forwarding-Information-Base (FIB) extern preisgeben kann.

Jeder Internetteilnehmer hat die Möglichkeit z.B. per Telnet diese Router direkt abzufragen. Für die Analyse ohne Echtzeitanforderung steht ein Datenarchiv bereit. Die Route-Collectoren werden in fest definierten Intervallen mittels eines einfachen Collector-Scriptes abgefragt und archiviert. Diese Archivierung erfolgt seit November 1997 ca. alle zwei Stunden. Es werden in der Regel MRT[3]-Dumps gespeichert, da diese auf den Routern selber erzeugt werden können und eine langwierige Abfrage mittels Telnet überflüssig machen. Jedoch gibt es auch menschenlesbare Ausgaben, sodass man keine speziellen Tools braucht, um an die gewünschten Informationen zu kommen.

Schnell wurde erkannt, dass diese umfangreiche Datenbasis nicht nur für Netzwerk-Experten von Interesse ist: inzwischen gibt es viele Projekte[4], die sich mit der Visualisierung des Internets beschäftigen. Andere Projekte[5] gehen noch einen Schritt weiter und versuchen, die verschiedenen AS-Nummern (ASN) den entsprechenden Ländern zuzuordnen.

2.1.2 RIPE NCC

Das RIPE Network Coordination Center[6] (NCC) ist eine der fünf Regional Internet Registries (RIR's), welche für die Verteilung von IP-Adressen und AS-Nummern (ASN) für den Bereich Europa, naher Osten und Zentralasien zuständig ist.

Da die RIPE für die Verteilung zuständig ist, haben sie eine genaue Übersicht über die IP-Prefixe und die zugehörigen ASN. Den Mitgliedern der RIPE, die sog. Local Internet Registries (LIR's) wird ein Zugang zu dieser Datenbank ermöglicht, sodass diese z.B. für Gültigkeitsprüfungen von BGP-Updates benutzt werden können.

Die RIPE hat selber eine Routing-Working-Group, welche sich u.a. mit dem Route-Flapping beschäftigt (5). Außerdem bietet der Routing-Information-Service (RIS) Möglichkeiten, direkt auf die Rohdaten der BGP-Updates zuzugreifen, sowie auf Routing-Policies[7].

Zur Validierung setzt die RIPE u.a. auf sog. Routing-Beacons. Das sind kleine BGP-Speaker, welche zu geplanten Zeitpunkten bestimmte Routen propagieren. Durch diese Methode hat

[2] Ein BGP-Speaker ist eine Instanz, welche das BGP-Protokoll vollständig implementiert (Control-Plane)
[3] MRT ist ein Exportformat für Routing-Informationen
[4] http://www.psc.edu/networking/nlanr/
[5] http://www.caida.org/home/
[6] http://www.ripe.net/
[7] http://www.ripe.net/data-tools/stats/ris/ris-routing-beacons

man die Möglichkeit, an verschiedenen Standorten diese Updates abzufangen und kann so Informationen über die Topologie und Filterregeln zwischen den AS-Betreibern erhalten.

2.2 Messmethoden

2.2.1 BGP beacons

Passive Monitoringtools wie Oregon's Route-Views oder RIPE geben wichtige Einblicke in die BGP-Updates, jedoch reichen diese Erkenntnisse nicht immer aus. In der University of California in Berkeley[8] wurde in Zusammenarbeit mit der *Internet Initiative Japan*, *Intel Research* und den *AT&T Labs-Research* ein Projekt ins Leben gerufen, wo aktive Messungen durchgeführt werden sollen (6).

Die Grundidee von diesem Ansatz ist, dass Prefixe propagiert und nach definierter Zeit wieder zurückgezogen werden. Dadurch ist es möglich, z.B. die Ausbreitung und die Konvergenzzeit zu messen, da man durch diese Technik genau weiß, wann das Prefix propagiert oder zurückgezogen wurde. Um diesen Mechanismus zu realisieren, wurde die bgpd[9]-Software erweitert um einen externen Trigger, welcher das Propagieren oder Zurückziehen auslöst.

Um die Konvergenzzeit zu messen, wird zeitgesteuert ein Prefix propagiert. Danach werden z.B. im Route-Views Projekt die Update-Nachrichten analysiert vom ersten Auftreten des Prefixes bis zum letzten Update (= der optimale Pfad wurde erreicht).

Dieser aktive Ansatz ermöglicht als Beispiel, das Route-Flap-Damping (RFD - (7)) zu analysieren. RFD ist ein Mechanismus in BGP um eine möglichst gute Routenstabilität zu erreichen. Dabei wird bei ständig wechselnden Routen (*route-flapping*) ein Wert inkrementiert. Wenn ein bestimmter Wert überschritten wird, wird die Route als unstable angesehen und somit nicht mehr propagiert.

2.2.2 Route Monitor Selection

Verschiedene Route-Monitoring-Systeme wie das Route-Views Project wurden etabliert, damit man einen Einblick in die Abläufe erhalten kann. Diese Daten dienen vielen Projekten und Arbeiten als Grundlage, welche alle darauf vertrauen, dass die Daten korrekt sind. Durch die hierarchische Eigenschaft des Internet's und die privaten Policies kann es einen großen Unterschied machen, welchen Monitoring-Standort man für seine Messungen wählt. Da diese Auswirkungen noch nicht untersucht wurden, haben fünf Wissenschaftler der Universitäten

[8] http://www.eecs.berkeley.edu/
[9] http://bgpd.sourceforge.net/

Michigan, Purdue und Carnegie Mellon gemeinschaftlich diese Problemstellung in (8) behandelt.

Es gibt Arbeiten über Algorithmen zur Verteilung von Monitorstandorten wie z.B. (9), jedoch wird in dieser Arbeit die Auswirkung von verschiedenen Szenarien beschrieben. Dazu gibt es drei verschiedene Strategien:

1. nur Tier-1 ISPs[10]
2. Route Views und RIPE
3. viele öffentliche und private Looking-Glasses[11]

In dem Paper wird verdeutlicht, dass die Wahl des Monitor's für die Untersuchung von statischen und dynamischen Netzwerkeigenschaften wichtig ist. Außerdem wird gezeigt, dass eine größere Anzahl von Monitoren eine bessere Genauigkeit erreicht wird, da z.B. Filter für Upstream-Provider verhindern, dass Links bekannt werden.

2.3 Zusammenfassung

Das Route-Views Project ist ein sehr umfassendes Archiv von BGP-Updates, das sehr vielen anderen Projekten als Grundlage dient. Durch die verschiedenen Standorte erhält man einen Einblick in das globale Routing-System. Durch die großen, globalen Kollectoren erhält man keinen Einblick in die logischen Verbindungen innerhalb Deutschlands. Für den Anwendungsbereich der Routenvalidierung (speziell branchenspezifisch) ist der Einblick von einem eigenen, unabhängigen AS unabdingbar.

Die RIPE NCC kann wie das Route-Views Projekt nur eine Verifikation unterstützen oder als Vergleich dienen, jedoch keine Grundlage bilden. Die Daten weichen u.U. erheblich von der realen Topologie ab und es können private Peerings nicht erkannt werden. Somit wäre selbst eine Kombination zwischen Route Views und RIPE nicht ausreichend für die 100 prozentige Routenvalidierung. Dies bestätigt auch das Paper Route Monitor Selection, aus dem hervorgeht, dass eine Menge von öffentlichen und privaten Looking-Glasses sogar genauer sein können, als Tier-1 Provider oder Route Views und die RIPE gemeinsam. Die Details aus Sicht der niedrigeren Hierarchieebene ist sehr wertvoll und kann nur von uns mittels des Routers am BCIX gewonnen werden. Für die generelle Validierung von anderen Standorten aus dem Internet kann auf Route Views zurückgegegriffen werden.

In dem Paper über die BGP beacons wird gezeigt, dass man mit aktiven Ansätzen genauere Informationen über Filter sowie Routen erlangen kann. Dabei kann man einen Teil des eigenen

[10] Internet Service Provider
[11] Ein Looking-Glass ermöglicht einen Einblick in die Routingtabelle eines Routers

Prefix von einem anderen AS propagieren lassen und mittels öffentlicher Looking-Glasses die Ausbreitung beobachten und analysieren. Da dieser Ansatz zum Messen der Konvergenzzeit gedacht war, kann man für die eigenen Arbeiten die Grundidee des Beaconing für andere Messungen benutzen.

3 BGP Verwundbarkeit

3.1 Wirkungsweise bekannter Angriffe

3.1.1 Prefix Hijacking & Interception

Prefix Hijacking ist die unerlaubte Übernahme von einem oder mehreren IP-Blöcken mit dem Ziel, die eigentlichen Inhalte zu stören. Dabei wirkt das störende AS wie ein schwarzes Loch: die Daten werden von dem eigentlichen AS umgeleitet auf das Störende - und werden somit nicht bearbeitet (Denial-of-Service). Diesen Zustand erreicht man, indem man mit einem unter der eigenen Kontrolle stehenden („bösen“) AS seinen Nachbar-AS eine Route propagiert, die einem nicht zusteht. Wenn eines der Nachbar-AS dieses Update akzeptiert und in seine FIB übernimmt, werden alle Anfragen zu diesem Prefix direkt an das eigene AS weitergeleitet. Bei einem Versehen (z.B. einer Fehlkonfiguration) spricht man von Leaking.

Prefix Interception ist die bewusste Übernahme von IP-Blöcken mit der Absicht, die Daten mitschneiden zu können. Dazu wird das eigene AS wie beim Hijacking als beste Route propagiert, jedoch sollen die Daten das ursprüngliche AS erreichen. Dazu wird eine Route zum Prefix propagiert und gleichzeitig wird der Datenverkehr weitergeleitet zum ursprünglichen AS. Dies ist nicht ganz einfach, da man mit der eigenen (falschen) Route möglicherweise die Route zum eigentlichen Ziel überschreibt und somit selber nicht mehr erreichen kann. Das Opfer erlangt in der Regel keine Kenntnis von dem Angriff (man-in-the-middle).

In der Studie (10) von Hitesh Ballani, Paul Francis und Xinyang Zhang (alle Cornell University, Ithaca, New York) wird zuerst auf die Methodik von Prefix-Interception eingegangen. Das Problem dabei ist, dass man nicht zwangsläufig merken muss, dass das eigene Prefix gekapert wurde, denn die Dienste funktionieren wie gewöhnlich. Es ist jedoch schwer bis unmöglich, weltweit ein Prefix zu kapern, da je nach dem topologischen Umfeld des angreifenden AS nur (geographischer) Teil übernommen werden kann (s. Bild 3.1: X ist mit der falschen Route nur bei C3 erfolgreich. Grund könne Policies oder Filter sein). Dies liegt an den Filterregeln und Sicherheitsmechanismen, sofern diese implementiert worden sind. Je größer jedoch der eigene Einfluss im Internet ist, desto größer wird der Schaden, den man anrichten kann.

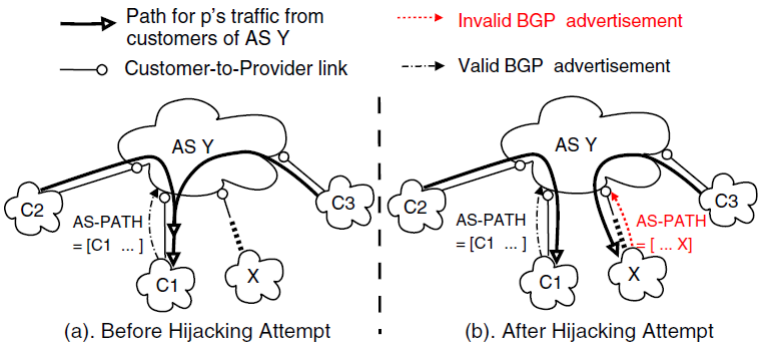

Abbildung 3.1: Hijacking-Angriff aus (10)

So gelang es z.B. der China Telecom (China's größter ISP) im April 2010, ca. 11% des gesamten Internet-Datenverkehrs umzuleiten. Das heißt konkret: ca. 37.000 Prefixe wurden übernommen - u.a. auch die der amerikanischen Behörden und des Militärs. Offiziell war dies eine Fehlkonfiguration, zeigt aber deutlich, dass es möglich ist, brisante Informationen abzufangen[1].

In (10) wird anhand von Routing-Policies errechnet, ob und wie viel Traffic von einem AS gekapert werden kann. Dabei wird unterschieden in Hijacking und Interception, da Interception etwas schwieriger ist, da die eigene (fehlerhafte) Route den Weg zum eigentlichen AS unbrauchbar machen kann. Ein Tier-1 AS kann zwischen 52% und 79% der IP-Prefixe hijacken, während ein Tier-3 AS kann zwischen 13% und 31% erreichen und nur 7% bis 17% des Traffics umleiten.

Um diese Zahlen zu verifizieren, wurde ein Versuch durchgeführt, in dem das eigene Prefix von einem AS regulär propagiert wurde. Vier weitere AS an insgesamt drei ISPs wurden als Angreifer genutzt: Dabei konnte im besten Fall 23,4% des Datenverkehrs umgeleitet werden, im schlimmsten Fall jedoch 78,8%. So wurde bewiesen, dass es auch mit kleinen AS möglich ist, einen signifikanten Teil zu stören oder umzuleiten. Um dies zu verhindern, wurde ein Algorithmus entwickelt, welcher Anomalien im AS_PATH feststellen kann. Dieser basiert auf AS-level traceroutes, welche mit dem next-hop verglichen werden.

[1] http://bgpmon.net/blog/?p=323

3.2 Erkennung & Vermeidung von Angriffen

3.2.1 Erkennung von falschen BGP-Updates

Die „Reliable Software Group[2]“ der University of California, Santa Barbara beschäftigt sich u.a. mit der Erkennung von Anomalien in BGP-Updates (11). Der BGP-Client wird um eine Funktion erweitert, die die Prüfung des AS_PATH erlaubt. Dabei wird die geographische Position des AS mit dem AS_PATH gemeinsam benutzt, um diese Anomalien festzustellen. Zuerst wird über einen Zeitraum passiv die Topologie analysiert. Dieser Schritt ist notwendig, um die AS zu kategorisieren in core- und edge-AS.

Ist dieser Vorgang abgeschlossen, kann der AS_PATH analysiert werden. Dazu gibt es zwei Grundsätze:

1. core-AS (Tier-1) dürfen nur einmal im AS_PATH vorkommen
2. edge-AS (Tier-2/3) sind auf geographisch begrenztem Raum (ca. 300km) direkt verbunden

Nun wird von jedem BGP-Update der AS_PATH analysiert auf diese beiden Eigenschaften. Wenn ein Link zwischen zwei edge-AS die Anforderung 2 erfüllt, ist der Link als legitim anzusehen. Wird die Anforderung nicht erfüllt, muss die Verbindung über ein core-AS erfolgen.

Bei der Verifikation wurden über 6 Millionen BGP-Updates analysiert. Dabei wurden 23 „falsche“ Verstöße gegen den zweiten Grundsatz erkannt, jedoch auch 76 falsche AS-Pfade.

3.2.2 Origin AS Validation

„Neighborhood watch for Internet Routing: Can we improve the robustness of Internet Routing today?“ - Das fragen sich Georgos Siganos und Michalis Faloutsos in (12). Während einer Zeitspanne von 13 Tagen sie fest, dass pro Stunde weniger als 3 verdächtige BGP-Updates vorkommen. Diese Zahl ist zwar nicht groß, doch ein Netzwerkadministrator kann nicht rund um die Uhr diese Updates überwachen.

Aus diesem Grund wurde ein Framework entwickelt zur Überprüfung der Herkunft von BGP-Updates. Die Updates werden kategorisiert in „strong-validated“, „weak-validated“ oder „not validated“. Durch diese Einteilung können die Anzahl der zu überprüfenden Updates stark eingegrenzt werden.

Für die Klassifizierung wird das IP-Prefix sowie die propagierende ASN überprüft. *Strong-validated* ist ein Eintrag, wenn das IP-Prefix und die ASN in der Datenbank der zugehörigen

[2] http://www.cs.ucsb.edu/ seclab/

RIRs wie ARIN (Amerika) oder RIPE (Europa) zu finden ist. Damit ist sichergestellt, dass es sich um ein reguläres und erlaubtes Update handelt. *Weak-validated* ist ein Update, wenn es nicht stark validiert werden kann, aber über eine Internet Routing Registry (IRR) über einen Eintrag zu diesem Prefix verfügt. Eine IRR stellt (gesammelte) Informationen über AS-Links und Policies zur Verfügung. Dies stellt nur eine schwache Validität fest, da jeder Einträge in einer IRR vornehmen kann.

Falls ein Tupel nicht validiert werden kann, wird es als *not-validated* mit einem Flag gekennzeichnet und kann einer weiteren Prüfung z.B. durch den Administrator unterzogen werden.

3.3 Zusammenfassung

Im ersten Paper über Prefix Hijacking & Interception werden die Grundlagen zum Hijacking erklärt. Dabei wird neben einer theoretischen Abhandlung über die Angreifbarkeit auch ein praktischer Versuch durchgeführt. Dieser Versuch zeigt, dass die theoretischen Zahlen stimmen, ist jedoch mit erheblichem Aufwand verbunden. Es wurden insgesamt vier angreifende AS untereinander verbunden, um diesen Angriff möglichst effektiv durchzuführen.

In der Arbeit zur Erkennung von falschen BGP-Updates werden Mechanismen implementiert, welche ein einfaches Hijacking unterbinden sollen mittels zwei einfacher Bedingungen zur Entfernung zwischen den einzelnen AS und der hierarchischen Topologie. Diesem Thema haben sich schon viele Arbeitsgruppen gewidmet (z.B. (13)), von daher wird man die Resultate der Arbeitsgruppen übernehmen können, sofern die eigenen Ergebnisse gegen diese falschen Update-Nachrichten gesichert werden sollen.

Einen weiteren Ansatz zur Validierung stellt das Paper Origin AS Validation dar. Bei diesem werden über verschiedene Datenbanken wie der RIPE die Prefixe zu ASN validiert. Dabei wird unterschieden in stark, schwach und nicht validiert, welches einen Hinweis darauf gibt, ob das Update akzeptiert werden kann oder einen Angriff darstellen kann. Diese Implementierung ist vergleichsweise aufwendig, außerdem wird im Routing-Atlas Projekt bereits eine Validierung vorgenommen, welche als Grundlage verschiedene Anbieter hat, u.a. auch die RIPE.

Kryptographische Ansätze wie RPKI (14) oder sBGP (13) sind wenig verbreitet, bieten aber eine deutlich bessere Sicherheit als die vorgestellten Ansätze. Gerade für den RPKI-Ansatz muss das Protokoll nicht geändert werden, dies wäre ein guter Ansatz für die eigene Arbeit.

4 Abgrenzung

Viele der vorgestellten Arbeiten sind grundlegend wichtig für die eigene Arbeit. Es gibt viele Looking-Glasses, jedoch ist für das eigene Projekt die Sicht aus einem deutschen Rechenzentrum wichtig und intererssant. Aus diesem Grund soll ein privates Looking-Glass zur Validierung etabliert werden und für eigene Erkenntnisse sorgen. Die Informationen der „großen“ Anbieter können für einen Vergleich der Ergebnisse sorgen, um so eine belastbare Information zu bekommen, ob für die Validierung des Routing Atlas das Route Views Projekt reicht, oder ob das eigene Looking-Glass notwendig ist.

Die Implementierung des Routers ermöglicht es neben passiven Messungen wie Routenanalysen oder Anomalieerkennungen auch aktiven Messungen, da das System unter der eigenen Administration steht. Dies umfasst viele Vorteile, die man bei Projekten wie Route-Views nicht hat.

Durch den Router am BCIX eröffnet sich eine Fülle weiterer Fragestellungen, wie die Analyse von Multicast-Strömen oder der Erprobung von einer RPKI-Infrastruktur, welche kürzlich vorgestellt wurde.

Literaturverzeichnis

[1] Y. Rekhter and T. Li, “A Border Gateway Protocol 4 (BGP-4),” IETF, RFC 1771, March 1995.

[2] A. Doria, E. Davies, and F. Kastenholz, “A Set of Possible Requirements for a Future Routing Architecture,” IETF, RFC 5772, February 2010.

[3] C. Lumezanu, “Using internet geometry to improve end-to-end communication performance,” Ph.D. dissertation, University of Maryland, 2009.

[4] L. Gao, “On inferring autonomous system relationships in the internet,” *IEEE/ACM Trans. Netw.*, vol. 9, pp. 733–745, December 2001. [Online]. Available: http://dx.doi.org/10.1109/90.974527

[5] P. Smith and C. Panigl, “Recommendations on route-flap damping.” RIPE, 2006. [Online]. Available: http://www.ripe.net/ripe/docs/ripe-378

[6] Z. M. Mao, R. Bush, T. G. Griffin, and M. Roughan, “Bgp beacons,” in *Proceedings of the 3rd ACM SIGCOMM conference on Internet measurement*, ser. IMC ’03. New York, NY, USA: ACM, 2003, pp. 1–14. [Online]. Available: http://doi.acm.org/10.1145/948205.948207

[7] C. Villamizar, R. Chandra, and R. Govindan, “BGP Route Flap Damping,” IETF, RFC 2439, November 1998.

[8] Y. Zhang, Z. Zhang, Z. Morley, M. Y. Charlie, H. Bruce, and M. Maggs, “On the impact of route monitor selection,” in *Proceedings of the ACM Internet Measurement Conference (IMC)*, 2007.

[9] B. Zhang, R. Liu, D. Massey, and L. Zhang, “Collecting the internet as-level topology,” *SIGCOMM Comput. Commun. Rev.*, vol. 35, pp. 53–61, January 2005. [Online]. Available: http://doi.acm.org/10.1145/1052812.1052825

[10] H. Ballani, P. Francis, and X. Zhang, “A study of prefix hijacking and interception in the internet,” *SIGCOMM Comput. Commun. Rev.*, vol. 37, pp. 265–276, August 2007. [Online]. Available: http://doi.acm.org/10.1145/1282427.1282411

[11] C. Kruegel, D. Mutz, W. Robertson, and F. Valeur, “Topology-based detection of anomalous bgp messages,” in *In Proceedings of the 6th Symposium on Recent Advances in Intrusion Detection (RAID)*, 2003, pp. 17–35.

[12] *Neighborhood Watch for Internet Routing: Can We Improve the Robustness of Internet Routing Today?*, 2007. [Online]. Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4215733

[13] S. Kent, C. Lynn, J. Mikkelson, and K. Seo, “Secure border gateway protocol (s-bgp,” *IEEE Journal on Selected Areas in Communications*, vol. 18, pp. 103–116, 2000. [Online]. Available: http://www.isoc.org/isoc/conferences/ndss/2000/proceedings/045.pdf

[14] R. Bush, “Rpki-based origin validation operations.” IETF, November 2010, internet-Draft. [Online]. Available: http://tools.ietf.org/html/draft-ymbk-rpki-origin-ops-00