Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Anwendungen 1 Ausarbeitung

Jan Henke

Sicherheit im Internet Backbone

Fakultät Technik und Informatik
Studiendepartment Informatik

Jan Henke

Thema der Anwendungen 1 Ausarbeitung
Sicherheit im Internet Backbone
Stichworte
Routing Internet Backbone Sicherheit BGP RPKI
Kurzzusammenfassung

Jan Henke

Title of the paper
Internet backbone security
Keywords
routing internet backbone security BGP RPKI
Abstract

Inhaltsverzeichnis

Kapitel 1

Einleitung

Das Internet ist in den vergangenen Jahren ein immer wichtigerer Faktor im alltäglichen Leben geworden. Unternehmen, Privatpersonen, aber auch Staaten vertrauen auf die ständige Verfügbarkeit eines Zugangs zum Internet. Gleichzeitig werden aber auch immer wichtigere und vertrauchlichere Daten über das Internet ausgetauscht.[1] Um eine hohe Verfügbarkeit des Internets sicherzustellen, ist neben der Hardware vor allem auch das Routing entscheidend, die Information, welche Zieladresse auf welchem Wege zu erreichen ist.

Da das Routingprotokoll den Weg der Datenpakete durch das Internet bestimmt, ist es daher auch verstärkt das Ziel von Angriffen, mit dem Ziel, den IP-Verkehr so umzuleiten, dass dieser durch ein vom Angreifer kontrolliertes Netzwerk geleitet wird. Auf diese Weise kann ein Angreifer Einblick in die Daten nehmen, sich als das angegriffene Netzwerk ausgeben oder aber konsequent jedes für den Angegriffenen bestimmte Paket verwerfen und so wie ein schwarzes Loch für IP-Pakete wirken. Die Motivation kann dabei von (Wirtschafts-)Spionage bis hin zu kriegerischen Absichten zwischen zwei oder mehreren Staaten reichen, meistens ist auch nur eine bloße Fehlkonfiguration die Ursache.

Routingprotokolle werden nach Art ihrer Verwendung in eine von zwei Kategorien eingeordnet. So genannte interior gateway protocols (IGP), welche innerhalb eines Autonomen Systems (AS)[2] zum Einsatz kommen, und den so genannten exterior gateway protocols (EGP), welche zwischen verschiedenen AS gesprochen werden. Als einziges EGP wird heute im Internet das Border Gateway Protocol (BGP) in der Version 4 verwendet, um das es in dieser Arbeit gehen soll. Das Border Gateway Protocol (BGP)-4 ist in der aktuellen Fassung in RFC4271 spezifiziert[7].

Ziel dieser Arbeit ist es, zunächst die Sicherheitsprobleme des BGP genauer darzustellen, in dem verschiedene Angriffsmöglichkeiten auf dieses Protokoll beschrieben werden. Auf der Grundlage des dadurch erworbenen Verständnisses des Problems sollen weitere Arbeiten zu diesem Themenbereich folgen.

---

[1] Zitat des BSI-Präsidenten auf der BMBF-Konferenz „zukünftiges Internet" am 06.07.2011: „Das Internet ist eine kritische Infrastrktur"[3]

[2] Der Begriff des Autonomen Systems wird in Abschnitt 2.1 definiert.

Kapitel 2

Routing im Internet Backbone

Dieses Kapitel soll eine Einführung in das Routing geben, wie es mit dem BGP im Internet realisiert ist. Dazu werden in Abschnitt 2.1 zunächst einige Begriffe definiert, wie sie im Rahmen dieser Arbeit verwendet werden und zu verstehen sind.

Abschnitt 2.2 zeigt anschließend, wie das Routing abläuft, wenn keine Angriffe stattfinden.

Der Abschnitt 2.3 stellt danach dar, wie man auf das BGP-Routing Einfluss nehmen kann, um den Weg von Verkehr fremder Autonomer Systeme durch das Internet zu verändern.

2.1 Begrifflichkeiten

In der Einleitung ist bereits der Begriff des *Autonomen Systems* (AS) gefallen. Ein AS ist definiert als eines oder mehrerer Netzwerke, welche unter einer administrativen Domain stehen. In der Praxis bedeutet dies, dass ein AS in der Regel als das Netzwerk einer Organisation zu sehen ist, z.B. einer Hochschule oder eines Unternehmens. Das BGP beschreibt das Routing nur auf der Basis dieser Autonomen Systeme, da für das Interdomain-Routing der innere Aufbau der jeweiligen Netzwerke nicht relevant ist. AS sind daher eine Hierarchisierung, um die Komplexität des Routings zu reduzieren. Jedes AS wird über eine 16 Bit lange positive Ganzzahl identifiziert, der *Autonomous System Number* (ASN), die analog zu den IP-Adressen zentral von der IANA verwaltet und ausgegeben werden. Dadurch lässt sich jedes AS eindeutig durch seine ASN identifizieren, außer wenn eine der ASN verwendet wird, die zur privaten Verwendung analog zu den 192.168.0.0/16 Adressen bestimmt sind. Dies sind die ASN 64512 bis 65535, welche nach RFC1930[4] nicht im öffentlichen Internet annonciert werden dürfen.

AS lassen sich danach unterscheiden, ob diese über eine Standardroute (engl. *default route*) verfügen oder nicht. Kleinere AS, welche nur über einen bezahlten Zugang zum Internet über einen oder mehre Internet Service Provider (ISP) verfügen, können einen der ISP als Standardroute verwenden und müssten so nicht am BGP-Routing teilnehmen. Dem gegenüber stehen die AS, bei denen die Übergangsrouter (engl. *edge* oder *border router*)

über keine Standardroute verfügen, sondern in ihrer Routingtabelle explizite Einträge für jedes im Internet erreichbare benötigen, um dieses erreichen zu können. Die Gesamtheit aller dieser AS, welche über keine Standardroute verfügen, wird auch als *default free zone* (DFZ) bezeichnet.

Während der Entwicklung des Internets gab es lange Zeit speziell als Backbone konzipierte Netzwerke, um die einzelnen Teile miteinander zu verbinden und so die globale Erreichbarkeit sicherzustellen. Mit der Kommerzialisierung des Internets, ab den 1990er Jahren, wurde diese Funktion aber immer mehr von großen kommerziellen Anbietern übernommen, ein Vorgang, der mit der Abschaltung des NSFNet, im Jahre 2005, seinen Abschluss fand. Seit dem gibt es keine feste Definition des Begriffs „Internet Backbone" mehr. In dieser Arbeit wird daher der Begriff „Internet Backbone" also Synonym für die DFZ angesehen, da die DFZ aus der Sicht des Routings den Kern des Internets bildet. Um die Bedeutung der einzelnen Netzwerke im Internet kompakt zu beschreiben, werden diese häufig nach Kategorien von Tier-1 bis Tier-3-Provider bezeichnet. Die Geschäftsbeziehungen zwischen den Providern bilden eine Hierarchie, denen diese Bezeichnung zu Grunde liegt. Ein Tier-3-Provider ist Kunde bei mindestens einem Tier-2-Provider und ein Tier-2-Provider ist Kunde bei mindestens einem Tier-1-Provider. Tier-1-Provider wiederum sind groß genug um das gesamte Internet nur über Peering- und Kundenverbindungen erreichen zu können. Tier-1-Provider sind zum Beispiel AT&T, Sprint und Level 3.

2.2 BGP-Routing

Dieser Abschnitt erläutert die Funktionsweise von BGP unter normalen Bedingungen, d.h. wenn keiner der in Abschnitt 2.3 beschriebenen Angriffe durchgeführt wird.

BGP ist ein Pfadvektorprotokoll, welches Routing-Informationen nur über direkte TCP-Verbindungen auf Port 179 mit anderen BGP-Sprechern austauscht. BGP benutzt kein Broadcast und verfügt auch über keine Discovery-Funktion, d.h. BGP-Sessions müssen manuell in den Routern konfiguriert werden.

BGP arbeitet intern mit drei routing information bases (RIB). Diese werden Adj-RIBs-In, Loc-RIB und Adj-RIBs-Out genannt.

Für jede aktive BGP-Sitzung gibt es eine Adj-RIB-In, welche alle über diese Sitzung empfangen Routen enthält. Aus allen bestehenden Adj-RIBs-In wird dann die Loc-RIB gefüllt. Die Loc-RIB enthält für jedes bekannte Präfix nur eine Route, wobei Longest-Common-Prefix-Match gilt und jeweils das spezifischste Präfix gilt. Sind für ein Präfix mehrere Routen bekannt wird eine Kombination von so genannten „Tie-Breaker" und lokalen Policies angewendet (siehe unten), bis nur noch eine Route übrig ist. Aus der Loc-RIB füllt der Router seine forward information base (FIB), diese wird im Cache der Line-Cards gehalten und für das eigentliche Routing benutzt. Für jede aktive BGP-Sitzung gibt es wiederum eine Adj-RIB-Out. Eine lokale Policy bestimmt, welche Routen aus der Loc-RIB in die jeweiligen Adj-RIBs-Out übernommen werden, deren Inhalt dann über die jeweilige BGP-Sitzung exportiert wird.

Routing-Informationen werden im BGP über UPDATE Nachrichten ausgetauscht, diese

enthalten eine Vielzahl von Informationen von denen im Folgenden nur die für das Verständnis der späteren Abschnitte wichtigen Attribute erläutert werden.

Neben der Information, welches Netzwerk (Präfix) über welche Schnittstelle zu erreichen ist (NLRI), ist besonders der AS-Pfad (im RFC als AS_PATH bezeichnet) wichtig. Wenn ein Paket von einem AS in das nächste weitergereicht wird, muss der Router, dessen AS das Paket verlässt, seine eigene ASN am Anfang des AS Pfades einfügen. Daraus kann ein Router mehrere Informationen ableiten:

- Das letzte AS im AS-Pfad ist somit per Definition immer das Ursprungs-AS (engl. *Origin-AS*), also das AS, welches den IP-Adressbereich (Präfix) besitzt und im restlichen Internet bekannt macht.
- Die Anzahl der ASN im AS-Pfad ist ein Indikator für die Länge der Route und eine der wichtigsten Entscheidungsgrundlagen, welche Route aus der Loc-RIB in die FIB übernommen wird, wenn es für ein Ziel mehrere Routen gibt. [3]

Wie oben bereits beschrieben kommen im BGP mehrere so genannte Policies und „Tie-Breaker" zum Einsatz. Eine Import-Policy dient dazu Routen von bestimmten Adj-RIBs-In zu bevorzugen. Existieren danach für ein Präfix noch mehr als eine mögliche Route, ist im RFC4271[7] eine Reihenfolge von „Tie-Breakern" definiert. Die erste und wichtigste dieser Regeln ist dabei die Länge des AS-Pfades, welche häufig bereits ausreicht. So enthält die Loc-RIB (und die FIB) für jede Zieladresse nach Longest-Common-Prefix-Match nur noch eine einzige Route.

Zuletzt bestimmt die Export-Policy, welche Route aus der Loc-RIB in die jeweiligen Adj-RIBs-Out übertragen werden und somit über welche BGP-Sessions diese Route exportiert werden. Diese Export-Policy ist dabei von der wirtschaftlichen Beziehung der beiden AS abhängig, je nach dem ob das andere AS ein Kunde, Provider oder Peering-Partner des eigenen AS ist.

In dem Paper "On inferring autonomous system relationships in the Internet"[2] beschäftigt sich Lixin Gao eingehend mit der Klassifizierung von Verbindungen zwischen zwei AS. Basierend auf empirischen Daten über die Struktur des Internets, lassen sich drei Arten von AS-AS-Beziehungen beschreiben, Kunde-Provider, Peering und so genannte „Geschwister"-Netzwerke, wobei letztere eher selten auftreten und daher im Weiteren nicht betrachtet werden. Da ein Kunde seinen Provider für die verwendete Bandbreite bezahlen muss, Peering-Verbindungen jedoch keine nutzungsabhängigen Kosten aufweisen, hat ein AS ein Interesse möglichst viel Verkehr über seine Peering-Verbindungen zu leiten, während die Verbindung zum Provider möglichst wenig genutzt werden soll. Umgekehrt haben Provider ein Interesse, möglichst viel Verkehr an ihre Kunden weiterzureichen, da sie ja dafür bezahlt werden. Aus diesem Zusammenhang folgen ein paar Grundsätze für die Export-Policy. Routen, die ein AS von seinen Providern oder Peering-Partnern erhält, sollten nur an die eigenen Kunden, sofern vorhanden, weitergereicht werden, damit das AS als Transit für diese Kunden dienen

[3] Es ist dabei auch üblich seine eigene ASN mehrfach einzufügen, um den gesamten Pfad dadurch zu verlängern. Dies reduziert absichtlich die Attraktivität dieser Route für nachfolgende AS.

kann. Routen, welche von einem Kunden stammen, sollten jedoch an alle Nachbar-AS exportiert werden. Es sollte daher auf jeden Fall vermieden werden, Routen, welche von einem Provider oder Peering-Partner stammen, an einen anderen Provider oder Peering-Partner zu exportieren. Tut dies ein AS dennoch, wird dieses AS ein *„policy violator"* genannt und kann schwere Netzwerkprobleme für alle Beteiligten verursachen.

Auf Grund der oben erwähnten Bevorzugung von Kunden-Routen, würden z.B. zwei Provider den Verkehr zwischen ihren AS dann durch das AS des *„policy violator"* routen, wenn dieser Kunde der beiden Provider ist und zudem die neue Route wiederum an ihre Provider weiterreichen. Womit der *„policy violator"* zu den bevorzugten Routen für eine große Datenmenge würde, die sein Netzwerk nicht verkraften kann. Dies kann zur Folge haben, dass sich mehrere große AS untereinander nicht mehr erreichen können.

2.3 Angriffe auf das BGP-Routing

Allen Angriffen gemein ist, dass sie den IP-Verkehr auf einen anderen Weg leiten, sodass das eigentliche Ziel nicht direkt oder gar nicht erreicht wird. Begrifflich unterscheidet man dabei zwei Arten, das *„prefix leaking"* resultiert aus der Fehlkonfiguration eines Routers, während das *„prefix hijacking"* absichtlich herbeigeführt wird. Im Folgenden werden verschiedene Angriffsmöglichkeiten beschrieben, dabei wird in den Beispielen die in Abbildung 2.1 gezeigte Netzwerkkonfiguration zur Erläuterung verwendet, wobei das AS A den IP-Verkehr von AS D erhalten möchte. Die Pfeile zeigen dabei jeweils vom Provider in Richtung Kunden, während die Verbindungen ohne Pfeil eine Peering-Beziehung darstellen. Die Informationen dieses Abschnitts stammen dabei größtenteils aus [5, 1].

2.3.1 Origin AS Attack

Diese Klasse der Angriffe besteht darin, dass ein Router sich selbst als Besitzer für einen IP-Adressbereich ausgibt, der gar nicht im eigenen AS existiert. Dies ist möglich, weil im BGP keine Verifikation des Ursprungs-AS vorgesehen ist, so kann jeder Router von sich behaupten jeden beliebigen Adressbereich zu besitzen. Noch effektiver wird dieser Angriff, wenn nicht das gesamte Subnetz eines anderen AS annonciert wird, sondern nur ein Teil dessen. Da bei der Routenfindung immer die speziellste Route zum Ziel (Longest-Common-Prefix-Match) ausgewählt wird, wird die neue Route für den gesamten Verkehr für den speziellen Teil dieses Subnetzes gelten.

Diese Art des Angriffs ist in der Geschichte des Internets bereits häufiger vorgekommen, wobei angenommen wird, dass ein Großteil versehentlich passiert. Außerdem lassen sich diese Art der Angriffe bereits mit den heutigen Mitteln des BGP verhindern, in dem Provider nicht alle Routen von ihren Kunden akzeptieren, sondern vorher einen Abgleich durchführen, da in der Regel bekannt ist, welche Präfixe ein Kunde besitzt. Es führen jedoch nicht alle AS diese Art der Filterung durch oder teilweise enthalten die Filter Fehler.

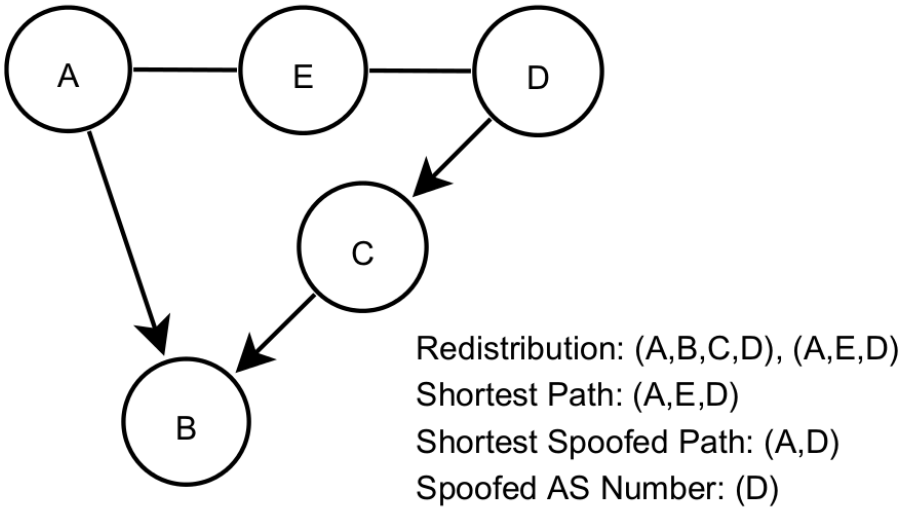

Abbildung 2.1: In den Beispielen verwendetes Netzwerk, Quelle: [5]

2.3.2 Invalid Path Attack

Diese Klasse der Angriffe basiert darauf, dass ein Router den AS-Pfad ausgehender Routen manipuliert, um so IP-Verkehrsströme nach eigenem Willen umzuleiten. Auch der AS-Pfad wird im BGP nicht verifiziert und per Definition als korrekt angenommen.

Shortest spoofed path

Beim *„shortest spoofed path*"-Angriff (kürzester gefälschter Pfad-Angriff) entfernt ein Router vor dem Weiterleiten einer Route den gesamten AS-Pfad zwischen seinem AS und dem Ursprungs-AS, gibt also vor, eine direkte Verbindung zum Ursprungs-AS zu besitzen. So soll der Anschein eines gültigen AS-Pfades für andere AS erweckt werden, gleichzeitig stellt dieser AS-Pfad den kürzest möglichen Pfad zum angegriffenen AS dar, sodass diese Route eine höhere Wahrscheinlichkeit hat, von anderen AS ausgewählt zu werden.

Ein Beispiel (siehe Abbildung 2.1): AS A möchte den Verkehr, der für AS D bestimmt, ist durch sich selbst hindurch leiten. Dazu exportiert AS A an seine Nachbarn eine Route mit dem gefälschten AS-Pfad (A,D). In diesem Beispiel würde AS B so den Eindruck gewinnen, es hätte zwei gleichlange Routen zu AS D und würde eventuell die Route über AS A wählen, obwohl diese in Wirklichkeit länger ist.

Shortest valid path

Ein Problem des *„shortest spoofed path*"-Angriffs besteht darin, dass eine gefälschte Kante in den AS-Pfad eingefügt wird. Hat ein anderes AS Kenntnis von der Netzwerkstruktur könnte die Fälschung als solche erkannt werden. Daher gibt es diese Variation des Angriffs, welche *„shortest valid path*"-Angriff (kürzester gültiger Pfad-Angriff) genannt wird. Ein Angreifer löscht hierbei den gesamten AS-Pfad und fügt stattdessen den kürzest möglichen Pfad zwischen sich und dem angegriffenen AS ein, der tatsächlich existiert. Dies erhöht wiederum die Wahrscheinlichkeit, dass andere AS ihren IP-Verkehr für das angegriffene AS durch das eigene AS routen.

Das gleiche Beispiel, wie beim letzten Angriff: AS A möchte sich den IP-Verkehr für AS D zu eigen machen. AS A exportiert dazu eine Route an seine Nachbarn, welche für die IP-Präfixe von AS D den AS-Pfad (A,E,D) enthält. Dabei ist zu beachten, dass dieser Pfad per Definition eine Policy Violation darstellt, denn AS A kann diese Route nicht von AS E gelernt haben. Dieses darf nämlich seine über Peering von AS D erhaltenen Routen nicht an seinen anderen Peering-Partner AS A exportieren. AS A verletzt so die allgemeine Export-Policy, erhält aber eine kürzere Route nach AS D, die auch existiert, womit es als Route zu AS D attraktiver erscheint.

Redistribution

Ein *„redistribution"*-Angriff (Weiterverteilungsangriff) ist allgemein die Verletzung der Export-Policy, indem Routen, die von einem Provider oder Peer gelernt wurden, an andere Provider oder Peers exportiert wurden. Wie bereits vorher erwähnt besteht hier die Gefahr vor allem darin, dass potentiell der Verkehr zwischen zwei großen AS durch ein kleines AS geleitet wird, welches nicht die Ressourcen hat, so viel IP-Verkehr zu verarbeiten. So wird das kleine AS, welches nun ungewollt als Transit zwischen den beiden großen AS dienen muss, zum schwarzen Loch für einen guten Teil des so umgeleiteten und auch für den normalen Verkehr auf dieser Route.

In dem bereits bekannten Beispiel bestünde ein derartiger Angriff darin, dass AS A für das Ziel AS D seine Routen über seine Peering-Verbindung (A,E,D) oder seine Kunden-Verbindung (A,B,C,D) an andere exportieren würde. Dies setzt natürlich voraus, dass die entsprechenden Verbindungen AS A auch bekannt sind.

ASN spoofing

Der *„ASN spoofing"*-Angriff (ASN-Fälschungsangriff) ist der am schwierigsten durchzuführende dieser Angriffe. Die Idee besteht darin, gegenüber anderen AS als der eigentliche Besitzer eines Präfixes zu erscheinen. Möchte ein AS Z den IP-Verkehr für das Präfix P von AS X erhalten, würde das AS Z an seine Nachbarn ein Route exportieren, in der das AS X als Ursprungs-AS für P enthalten ist, in der Hoffnung, dass andere AS die Verbindung zu AS Z stattdessen für eine Verbindung zum AS X halten.

Die Schwierigkeit dabei besteht darin, dass jedes AS in der Regel genau weiß, zu welchem AS seine Verbindungen führen und daher die Route verwerfen würde. Damit dieser

Angriff erfolgreich sein kann, muss AS Z daher noch weitere Maßnahmen ergreifen, damit diese gefälschte Route auch akzeptiert wird, z.B. durch eine heimliche Zusammenarbeit zweier AS.

Ein Beispiel anhand der Abbildung 2.1: AS A möchte von AS E den für AS D bestimmten IP-Verkehr erhalten. Dazu exportiert AS A an AS E eine Route, in der es behauptet AS D zu sein. Wenn AS E diese Route akzeptiert und in seine Routingtabelle übernimmt, hätte es nun zwei Routen für das gleiche Präfix und das gleiche Ursprungs-AS, die aber auf unterschiedliche Verbindungen führen. Dadurch könnte ein Teil des für AS D bestimmten Verkehrs über die Verbindung geleitet werden, die eigentlich nach AS A führt.

Das derzeit in der Standardisierung befindliche RPKI-Verfahren dient dazu, diese Art der Angriffe zu unterbinden. Dazu wird kryptographisch die Kombination von Origin-AS und Präfix signiert.

2.4 Zusammenfassung

Dieses Kapitel hat eine Einführung in die grundlegende Funktionsweise von BGP gegeben. Es wurde gezeigt, dass BGP über die Verwendung von Poilicies gut an die Bedürfnisse der einzelnen Netzwerke angepasst werden kann und muss, um Probleme zu verhindern. Gleichzeitig besteht ein grundsätzliches Problem, dass BGP Routing-Entscheidungen auf Basis von Informationen trifft, deren Richtigkeit nicht festgestellt werden kann. Was dazu benutzt werden kann, dass sowohl absichtlich wie auch unabsichtlich, den Weg, den die Daten im Internet vom Sender zum Empfänger nehmen, zu beeinflussen.

Allerdings sind diese Angriffe darauf angewiesen, dass die präparierten Routen-Updates auch von den relevanten AS genutzt und nicht wegen eines zu langen AS-Pfads oder anderer Kriterien ignoriert werden.

Kapitel 3

Ausblick

Die Sicherheitsprobleme von BGP, wie sie hier dargelegt wurden, sind hinreichend bekannt, sodass die Internet Engineering Task Force (IETF) eine Arbeitsgruppe gebildet hat, die Secure Inter-Domain Routing Working Group (sidr).

Dieses hat das Ziel, die bekannten Verwundbarkeiten im Inter-Domain-Routing zu reduzieren. Dazu wird derzeit das Resource Public Key Infrastructure (RPKI) System standardisiert, ein Teil der Spezifikation wurde im Februar 2012 im RFC6480 verabschiedet. Dies benutzt ein Public-Key-Verfahren um die Kombination von Präfix und ASN bei Routing-Updates zu signieren, sodass BGP-Router in die Lage versetzt werden, die Echtheit von diesen Updates zu überprüfen. Dabei entwickelt die Forschungsgruppe Internet Technologies an der HAW Hamburg derzeit die erste Open-Source-Implementierung. Da es sich hierbei um eine Sicherheitssoftware handelt, steht hierbei vor allem die Prüfung auf angreifbare Schwächen in der Implementierung im Vordergrund, zusätzlich zu der Anpassung an Veränderungen, die sich im Laufe des weiteren Standardisierungsverfahrens noch ergeben sollten. Zusätzlich werden noch alternative Angriffstechniken auf der Routing-Ebene untersucht, welche in der Fachliteratur bis jetzt kaum behandelt wurden. Für das Seminar Anwendungen 2 ist zudem ein Vergleich mit anderen Vorschlägen die zur Lösung des Problems an die sidr eingereicht wurden, vorgesehen.[8, 6]

Literaturverzeichnis

[1] Iljitsch van Beijnum. *BGP*. O'Reilly, Beijing [u.a.], 1.ed. edition, 2002.

[2] Lixin Gao. On inferring autonomous system relationships in the internet. In *Global Telecommunications Conference, 2000. GLOBECOM '00. IEEE*, volume 1, pages 387 –396 vol.1, 2000.

[3] Michael Hange. Risiken und perspektiven einer sicheren infrastruktur internet. online: `http://www.future-internet-konferenz.de/programm/Michael_Hange_Folien.pdf` (Zugriff 24.02.2012), 06. Juli 2011.

[4] J. Hawkinson and T. Bates. Guidelines for creation, selection, and registration of an autonomous system (as). RFC 1930 (Best Current Practice), March 1996.

[5] Josh Karlin, Stephanie Forrest, and Jennifer Rexford. Autonomous security for autonomous systems. *Computer Networks*, 52(15):2908 – 2923, 2008. <ce:title>Complex Computer and Communication Networks</ce:title>.

[6] M. Lepinski and S. Kent. An Infrastructure to Support Secure Internet Routing. RFC 6480 (Informational), February 2012.

[7] Y. Rekhter, T. Li, and S. Hares. A border gateway protocol 4 (bgp-4). RFC 4271 (Draft Standard), January 2006. Updated by RFC 6286.

[8] Matthias Waehlisch, Fabian Holler, Thomas C. Schmidt, and Jochen Schiller. Updates from the internet backbone: An rpki/rtr router implementation, measurements, and analysis. February 2012.