

Prefix Hijacking-Angriffe und Gegenmaßnahmen

Rafael Fedler

Betreuer: Johann Schlamp, Dipl.-Inf.

Seminar Future Internet SS 2012

Lehrstuhl Netzarchitekturen und Netzdienste

Fakultät für Informatik, Technische Universität München

Email: fedler@in.tum.de

KURZFASSUNG

Das Border Gateway Protocol BGP, der de facto-Standard für Routing im Internet, wurde ohne Berücksichtigung von Sicherheitsaspekten entwickelt. Daher kann beim sogenannten Prefix Hijacking ein Angreifer sehr einfach ganze Adressbereiche Dritter übernehmen. Er ist dadurch in der Lage, große Teile des weltweiten Datenverkehrs für diese Adressbereiche zu sich umzuleiten. Als Folge hiervon leidet das Netz des Angegriffenen unter einem Verlust der Konnektivität, aber auch unerkannte Man-in-the-Middle-Angriffe gegen ganze Netze („Interception“) können durchgeführt werden. Diese Schwachstellen sind schon lange in der Theorie bekannt und wurden in der Praxis bereits viele Male ausgenutzt. Gegenmaßnahmen sind jedoch sehr schwer umzusetzen, weshalb bis heute keine Änderungen am BGP vorgenommen worden sind. Die vorliegende Arbeit gibt einen Einblick in die Schwachstellen des Border Gateway Protocol und stellt größere Vorfälle und Angriffe auf die weltweiten Routing-Systeme vor. Außerdem werden Ansätze zur Absicherung der globalen Routing-Infrastruktur vorgestellt. Hierbei wird sowohl auf Erkennungssysteme wie auch auf in Entwicklung befindliche Änderungen und Erweiterungen des BGP zur Beseitigung seiner Schwachstellen eingegangen.

Schlüsselworte

BGP, IP Prefix, Hijacking, Interception, MOAS, PHAS, iSPY, BGPsec, RPKI, S-BGP, soBGP, psBGP

1. EINLEITUNG

Das Internet besteht aus einer Vielzahl von eigenständigen Netzen, welche als Autonome Systeme (AS) bezeichnet werden. Bei der Datenübertragung zwischen Hosts in verschiedenen Netzen werden die Daten durch mehrere auf dem Weg liegende Netze geleitet, bevor sie ihr Ziel erreichen. Die Bestimmung der bevorzugten Route für die Datenpakete wird durch Routing-Protokolle wie das Border Gateway Protocol (BGP) vorgenommen. Dieses Protokoll ist der de facto-Standard für das Routing zwischen Autonomen Systemen (Exterior Gateway Protocol) [1]; für das Routing innerhalb von Autonomen Systemen werden Interior Gateway-Protokolle verwendet. Allerdings wurden bei der Entwicklung des BGP, ähnlich wie bei vielen frühen Netzwerkprotokollen, Sicherheitsaspekte unberücksichtigt gelassen. Das BGP bietet keinerlei Möglichkeiten, die Authentizität und Korrektheit übertragener Routing-Informationen zu überprüfen oder die Berechtigung für Urheberschaft von Adressbereichen festzustellen. Dies ermöglicht es Angreifern, die globale Routing-Tabelle zu manipulieren und fremde Adress-

bereiche zu kapern („Hijacking“). Dadurch sind sie in der Lage, den für ein angegriffenes AS bestimmten Verkehr ganz oder teilweise zum eigenen Netz umzuleiten. Die Konsequenzen können, abhängig von den Zielen des Angreifers, vielfältig sein, wie bspw. Verlust der Verfügbarkeit aus Zensurgründen oder Verlust der Vertraulichkeit der übermittelten Daten [2]. Als Reaktion auf solche Fälle, die in den vergangenen Jahren mehrfach aufgetreten sind und verstärkt als Problem wahrgenommen werden, wurden verschiedene Gegenmaßnahmen vorgeschlagen. Diese Verfahren bieten Möglichkeiten, Hijacking-Vorfälle zu erkennen oder zu verhindern.

Die vorliegende Arbeit gibt eine Einführung in die Hintergründe von IP Prefix Hijacking, die Schwachstellen von BGP sowie den Ablauf und die Folgen von größeren bekannten Angriffen. Darauf folgend werden Systeme zur Erkennung und Verhinderung vorgestellt und verglichen. Abschnitt 2 erläutert die technischen Grundlagen von Internet-Routing, Autonomen Systemen sowie dem Border Gateway Protocol. Auch werden die Voraussetzungen für IP Prefix Hijacking dargestellt und eine Klassifikation vorgenommen. Abschnitt 3 gibt einen Einblick in ausgewählte, größere Hijacking-Vorfälle. Danach werden in Abschnitt 4 Präventiv- und Gegenmaßnahmen vorgestellt und evaluiert. Abschnitt 5 gibt einen Überblick über verwandte Arbeiten. Abschließend folgen Zusammenfassung und Fazit der Arbeit.

2. GRUNDLAGEN

Das Internet wird durch aktuell mehr als 40.000 eigenständige, miteinander verbundene Netze gebildet [3]. Diese werden als Autonome Systeme (AS) bezeichnet. Sie befinden sich unter der Kontrolle jeweils genau einer Organisation und werden durch eine eindeutige Nummer identifiziert. Jedes AS veröffentlicht außerdem die ihm zugewiesenen IP-Adressbereiche, die sogenannten Präfixe, und teilt sie seinen benachbarten Routern mit.

Bei der Übertragung eines Datenpakets von einem Quell-Host in einem AS zu einem Ziel-Host in einem anderen AS passiert dieses mehrere Zwischenstationen („Hops“), im Durchschnitt 16 [4]. Um sicherzustellen, dass ein Paket sein Ziel erreicht, kommen Routing-Protokolle zum Einsatz. Hierbei sind Interior Gateway-Protokolle für das Routing innerhalb eines AS („Intra-Domain Routing“) und Exterior Gateway-Protokolle für das Routing zwischen den AS zuständig („Inter-Domain Routing“). Auch wird versucht, die Anzahl an Hops zu minimieren, um das Routing schnell und effizient durchzuführen.

Das Border Gateway Protocol (BGP) hat sich als Stan-

dard für das Inter-Domain Routing etabliert. Es dient dem Austausch von Routen-Informationen zwischen Routern verschiedener Netze. Als Pfad-Vektor-Protokoll speichert es den gesamten Pfad von einem Router zu jedem Ziel-AS. Hierfür teilt jedes AS die ihm zugewiesenen Präfixe seinen Nachbar-routern in BGP-Update-Nachrichten mit. Da die Nachbar-router sowohl die ihrem AS zugewiesenen Präfixe wie auch die ihnen bekannten AS und zugehörige Präfixe wiederum ihren Nachbarn mitteilen, konvergieren die BGP-Tabellen in allen Routern gegen den selben Informationsstand. Vor der Weitergabe der eigenen bekannten Routen hängt sich das jeweilige AS vorne an jeden Eintrag an. Somit wird sichergestellt, dass jeder Router die Pfade zu allen Zielen kennt. Dies soll an dem in Abbildung 1 dargestellten Beispielnetz verdeutlicht werden:

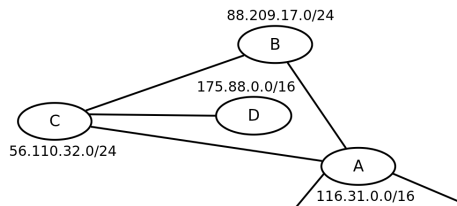


Abbildung 1: Beispiel-Netz

Die Routing-Tabelle für Router A gestaltet sich hierbei wie in Tabelle 1:

Tabelle 1: Routing-Tabelle von Router A

Präfix	Pfad
116.31.0.0/16	A
88.209.17.0/24	A → B
56.110.32.0/24	A → C
175.88.0.0/16	A → C → D
...	...

Die Tabelle wird in dieser Form an alle Nachbar-Router von A weitergegeben, die sich an alle Pfade vorne anfügen und die Tabelle danach ebenfalls weiterverbreiten. Auf diese Weise werden weltweit jedem BGP-Router die Pfade zu den Autonomen Systemen hinter den Routern B, C und D bekannt. Die Metrik, welche die Effizienz des Routings sicherstellt, wählt den Weg der geringsten Hop-Anzahl. Aus diesem Grund ist die Route von A nach D nicht A → B → C → D, selbst wenn diese Pfadinformation A früher erreicht hat als die von Router C.

Treffen mehrere Präfixe auf eine Ziel-Adresse zu, gilt die Longest Prefix Match-Regel. Diese besagt, dass das spezifischste Präfix als korrektes Ziel-System angenommen werden soll [5].

2.1 Schwachstellen des BGP

Viele ältere Netzwerkprotokolle wurden ohne Berücksichtigung von Sicherheitsaspekten entwickelt, wie z.B. DNS, SMTP oder auch IPv4. Mechanismen, die die Authentizität, Integrität und Vertraulichkeit von übermittelten Informationen sicherstellen, sind nicht integriert. Aus diesem Grund wurden die Protokolle weiterentwickelt oder erweitert. Für das Domain Name System wurde DNSSEC entwickelt, welches eine hierarchische Public Key-Infrastruktur (PKI) für

DNS-Einträge etabliert. IPv6 wurde um IPsec, Internet Protocol Security, erweitert. S/MIME und PGP sind Verfahren, die die Nutzdaten von SMTP verschlüsseln. Anwendungsprotokolle, die selber keine Verschlüsselung bieten, können auf TLS aufsetzen und damit Integrität und Vertraulichkeit, optional auch Authentizität, gewährleisten.

Die genannten Defizite im Protokolldesign treffen auf das Border Gateway Protocol ebenfalls zu. Insbesondere kann ein AS ohne Weiteres jedes Präfix als zu sich gehörend proklamieren und sich somit als „Origin AS“, also als das für das Präfix autoritative AS, ausgeben. Eine Authentizitätsüberprüfung findet nicht statt. Beanspruchen mehrere AS, das Origin AS eines Präfixes zu sein, spricht man von einem Multiple Origin AS-Konflikt, abgekürzt MOAS-Konflikt.

Weitere Probleme entstehen durch die mangelnde Sicherheit auf Transportebene. BGP setzt auf TCP auf und ist somit anfällig für übliche Angriffe auf TCP. Insbesondere können mit RST-Paketen gezielt Verbindungen zwischen BGP-Routern abgebrochen und permanent gestört werden. Somit kann ein Angreifer Einfluss auf die Verbreitung von Routen-Informationen und wahrgenommene Erreichbarkeit von Autonomen Systemen nehmen [1].

2.2 IP Prefix Hijacking und Interception

Da weder eine Überprüfung der Validität, noch des Ursprungs der Routen-Informationen vorgenommen wird, kann jeder BGP-Router beliebige Routen-Informationen veröffentlichen. Diese werden von seinen Nachbarn als Route gewählt, wenn die gelernten Pfade bevorzugbar erscheinen, und wiederum an ihre Nachbarn weiterverbreitet. Auf diese Weise kann ein Angreifer große Teile der globalen Routing-Tabelle manipulieren. Insbesondere ist er dazu in der Lage, beliebige IP-Adress-Präfixe selber zu annoncieren. Abbildung 2 verdeutlicht dies.

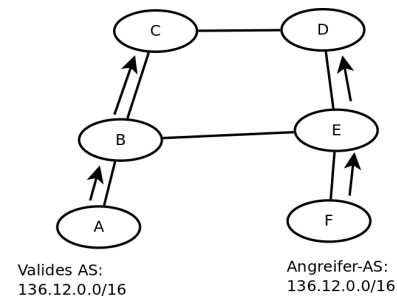


Abbildung 2: IP Prefix Hijacking

Im vorliegenden Beispiel übernehmen die Router der Autonomen Systeme D und E die falschen BGP-Updates des Angreifers F, da die Anzahl an Hops für sie minimal ist. Für B und C ist die Route nach A, dem legitimen Besitzer des Präfix 136.12.0.0/16, kürzer als nach F. Sie übernehmen daher die falschen Pfad-Informationen, die sie über D und E erhalten, nicht. Als Konsequenz werden alle Router, die die gefälschten Routen-Informationen übernehmen, sämtlichen an das annoncierte Präfix adressierten Verkehr zum Netz F des Angreifers leiten. An das Präfix 136.12.0.0/16 adressierte Pakete aus den Netzen D und E erreichen somit nicht den legitimen Empfänger in Netz A, sondern werden zu Netz F geschickt.

2.2.1 Typologie von Hijacking-Angriffen

Hijacking-Angriffe können auf verschiedene Weisen durchgeführt werden. Es ergeben sich hauptsächlich drei Vorgehensweisen [6]:

Um **vollständiges Prefix-Hijacking** handelt es sich, wenn wie im Beispiel in Sektion 2.2 ein Angreifer sich als legitimer Besitzer des gesamten angegriffenen Präfix ausgibt. Die Verbreitung der falschen Routen-Information wird durch die Metrik der kürzesten Pfade limitiert. Es wird nur ein begrenzter Teil des Internets durch die falschen Pfad-Informationen manipuliert.

Subprefix-Hijacking nutzt die Longest Prefix Match-Regel aus. Gibt sich ein Angreifer als Besitzer kleinerer Teilnetze des anzugreifenden Adressraumes aus und annonciert diese über das BGP, werden andere Router diese bevorzugen. Ein Großteil aller BGP-Router wird somit diese Route wählen und weitergeben.

Bei **Interception** verwendet ein Angreifer einzelne andere Autonome Systeme, deren Routen-Informationen nicht manipuliert wurden. Sie dienen ihm dazu, den abgefangenen Verkehr zurück an das Hijacking-Opfer zu leiten. Sie sind somit der Rückkanal eines BGP-basierten Man-in-the-Middle-Angriffs.

Dass BGP auf TCP aufsetzt, kann ein Angreifer zu seinem Vorteil nutzen. Beispielsweise kann er die Verbreitung seiner falschen BGP-Announcements beschleunigen, indem er BGP-Verbindungen, über die legitime Pfad-Informationen übertragen werden, via RST-Nachrichten kappt. Ferner kann er den Datenverkehr über bestimmte Routen zwingen, indem er die BGP-Verbindungen zu vermeidender AS auf die selbe Weise stört.

2.2.2 Folgen

Abhängig von der Methodik und den Motiven eines Angreifers haben Hijacking-Angriffe verschiedene Konsequenzen. Folgende Schutzziele können durch Hijacking-Angriffe betroffen sein:

- **Verfügbarkeit:** Werden nur die Routing-Tabellen illegitim ohne weitergehendes Wirken des Angreifers manipuliert, ist die Konnektivität des Opfer-AS beeinträchtigt. Da Antworten auf Pakete, die aus dem Opfer-Netz verschickt wurden, nicht wieder zurück in das betroffene AS geleitet werden, ist das Netz nicht mehr erreichbar. Dies gilt zumindest für Kommunikation mit allen Netzen, die die falschen Pfad-Informationen des Angreifers übernommen haben, oder auf deren Pfad sich manipulierte Netze befinden. Erreicht der Verkehr sein Ziel nicht und wird vom angreifenden System verworfen, spricht man von *Blackholing*. Wird solch ein Angriff bewusst durchgeführt, kann die Motivation bspw. ein Denial of Service-Angriff oder Zensur sein.
- **Authentizität:** Übernimmt ein Angreifer die Adressbereiche fremder Organisationen, nehmen dritte Parteien und Systeme an, er sei die angegriffene Organisation. Versendet er beispielsweise aus dem Adressbereich einer Firma Spam, kann dies den Ruf der Firma schädigen. Sie wird ggfs. auch noch nach Ende des Angriffs länger auf Spam-Blacklists enthalten sein. Ferner können fremde Dienste vorgetäuscht werden. Dies geschieht unerkennbar für Nutzer. Sie erhalten bei Auflö-

sung von Domain-Namen durch das DNS zwar die korrekte IP-Adresse zurück, ihre Anfrage wird aber zum System des Angreifers geleitet.

- **Vertraulichkeit und Integrität:** Bei allen genannten Angriffsformen ist ein Angreifer in der Lage, den an das angegriffene Netz adressierten Verkehr abzufangen und zu lesen. Somit kann ein Angreifer potentiell vertrauliche oder geschäftskritische Daten erhalten. Auch kann er Systeme in seinem Netz als legitime Systeme im angegriffenen Netz ausgeben, um bidirektionale Kommunikation zu ermöglichen. Authentifikationsdaten, wie bspw. bei Challenge-Response-Verfahren preisgegeben, können auf diese Weise abgefangen werden. Ebenso können Spoofing- und Phishing-Angriffe durchgeführt werden. Alternativ kann er als Man in the Middle bei Interception-Angriffen die Integrität übertragener Daten verletzen, indem er Pakete manipuliert.

3. BEKANNTE VORFÄLLE

Die Sicherheitsdefizite des BGP und ihre Implikationen sind in der Theorie bereits sehr lange bekannt [7]. Auch in der Praxis wurden sie bereits mehrfach ausgenutzt. Vorfälle unterschiedlichen Ausmaßes und unterschiedlicher Motivation wurden von diversen Parteien verursacht. Im Folgenden werden die bedeutendsten vorgestellt. Eine umfassendere Liste ist in [2] zu finden.

3.1 AT&T WorldNet

Dezember 1999. Ein anderer Internet Service Provider (ISP) veröffentlicht versehentlich falsche Routen-Informationen zu Einwahlservern des ISP AT&T WorldNet. Es kommt zu Blackholing, wodurch 1,8 Millionen Kunden einen Tag lang keinerlei Internetzugriff haben. [2]

3.2 Spammer – Northrop Grumman

14. Mai, 2003. Ein großer Teil des ungenutzten Adressbereichs der Rüstungsfirma Northrop Grumman wird von Spammern via falscher BGP-Updates übernommen. Im Vorfeld hatten die Spammer im DNS die Domain, die als Kontaktadresse für diesen Adressbereich angegeben war, unbemerkt auf sich neu registriert. Von dieser Domain aus schickten sie nun eMails an ihren Provider und gaben sich als legitime Besitzer des Adressbereichs aus. Der Provider versendete in der Folge BGP-Announcements, die den entsprechenden Adressbereich von Northrop Grumman dem Netz der Spammer zuwies. Es dauerte zwei Monate, bis Northrop Grumman den Adressbereich zurückerlangen konnte. In der selben Zeit wurden enorme Mengen an Spam versendet, sodass der Adressbereich auf nahezu allen Spam-Blacklists landete. [8]

3.3 Malaysia – Yahoo

Mai 2004. Der malaysische ISP DataOne annonciert die verwendeten Präfixe eines Rechenzentrums von Yahoo, woraufhin dieses aus weiten Teilen des Internets nicht erreichbar ist. [8]

3.4 Türkei – Internet

24. Dezember, 2004. Der türkische ISP TTNNet veröffentlicht via BGP Routen für das gesamte Internet zu seinem Netz, höchstwahrscheinlich wegen einem Konfigurationsfehler. Telecom Italia hatte eine BGP-Session mit einem BGP-Router

von TTNNet, aber kein Limit für die Anzahl zu übernehmender Routen (**MAXIMUM_PREFIX**-Attribut). Die Telecom Italia übernahm somit sämtliche falschen Routen-Informationen, die TTNNet veröffentlichte. Weitere Provider sowohl in Europa wie auch in den USA, die wiederum BGP-Sessions mit Telecom Italia hatten, verbreiteten die falschen Routen-Informationen weiter. Die großen nordamerikanischen ISPs Verizon, Sprint und Hurricane hatten hieran einen sehr hohen Anteil. In der Konsequenz waren ihre Kunden für die Dauer des Falls nicht erreichbar. Betroffen waren sowohl Privat- wie auch Firmenkunden, die über die genannten Provider angebunden sind. Hierzu gehören u.a. Microsoft, Amazon und Yahoo. Der Vorfall dauerte insgesamt einen ganzen Tag, währenddessen der Großteil des Internets nicht oder nur teilweise erreichbar war. [9, 10]

3.5 DNS Root-Server L

November 2007 bis Mai 2008. Bis November 2007 befand sich der Root-Server L des DNS in einem Präfix, welches nicht zum Adressraum der ICANN gehörte. Am 1. November 2007 zog die ICANN die Adresse des Root-Servers in ihren eigenen Adressbereich um. In den darauf folgenden Monaten erschienen mehrere falsche L-Root-Server. Die Betreiber dieser Server veröffentlichten inkorrekte Routen-Informationen, die die alte Adresse des DNS-Root-Servers L ihren Netzen zuwiesen. Mangelnde Filterung ihrer Provider hatte zur Folge, dass sich diese falschen Routen-Informationen weiterverbreiteten. Da diese falschen Server nach außen hin keine erkennbare bössartige oder fehlerhafte Funktionalität aufwiesen, ist die Motivation der Betreiber unklar. [11, 12] Kontrolle über DNS-Server ermöglicht es Angreifern, die Auflösung von beliebigen Adressen zu steuern und so Nutzer auf falsche Server umzuleiten, um bspw. Authentifikationsdaten abzufangen. Auch können DNS-Anfragen mitgeschnitten werden, um das Verhalten der anfragenden Clients zu überwachen. Außerdem bedienen sich bereits im Einsatz befindliche Zensursysteme manipulierter DNS-Einträge [13].

3.6 Pakistan – YouTube

24. Februar 2008. Pakistan Telecom blockiert auf Basis von BGP YouTube, um die Webseite auf nationaler Ebene zu zensieren. Allerdings werden die falschen Routen unbeabsichtigt weltweit weiterverbreitet, weshalb YouTube nahezu global für zwei Stunden nicht erreichbar ist. Bei diesem Vorfall handelte es sich um Subprefix-Hijacking, da YouTube 208.65.152.0/22 annouciert, während das angreifende System 208.65.153.0/24 proklamiert. Wegen der Longest Prefix Match-Regel wird die Route nach Pakistan global bevorzugt. Als Gegenmaßnahme bewirbt YouTube nun erst 208.65.153.0/24 und darauf folgend 208.65.153.128/25 sowie 208.65.153.0/25. Auf Grund der Longest Prefix-Regel werden nun wieder die korrekten Routen global bevorzugt. [14]

3.7 DEFCON Proof of Concept

Auf der DEFCON 16 wurde 2008 ein Proof of Concept für BGP-basierte Interception geführt. Dies ist zwar kein reell aufgetretener Vorfall, es handelt sich allerdings um eine praktische Demonstration von Prefix Hijacking zum Durchführen einer BGP-basierten Man-in-the-Middle-Attacke. Hierbei kann ein Angreifer möglichst viele BGP-Router dazu bringen, das Netz des Angreifers für das Netz des Angegriffenen zu halten – mit Ausnahme genau einer Route. Diese

Route hält sich der Angreifer gezielt als Rückkanal offen. Somit leiten alle betroffenen Systeme ihren Verkehr für das angegriffene System zum Angreifer, und dieser den Verkehr transparent über den Rückkanal zum Opfer des Angriffs.

Um dies zu ermöglichen, nutzt der Angreifer eine Eigenschaft des BGP zur Schleifenverhinderung. Findet ein AS im Pfad, der in einem BGP-Update angegeben ist, seine eigene AS-Nummer, verwirft es dieses Update. Zur Ermittlung des Rückkanals führt der Angreifer ein Traceroute in Richtung seines Ziels durch. Er übernimmt alle AS auf der Route nun in sein gefälschtes BGP-Update, welches den Pfad zum zu kapern den Adressbereich angibt. Zur Schleifenverhinderung werden die angegebenen AS dieses BGP-Update ignorieren. Somit besteht für die AS entlang des Pfades vom Angreifer zum Angegriffenen weiterhin die legitime Route. Die BGP-Router aller anderen AS schicken den an das Opfer-Netz adressierten Verkehr nun zum Angreifer. Dieser Angriff wurde auf der DEFCON auch praktisch demonstriert. [15]

3.8 China – USA

Am 8. April 2010 annouciert ein kleiner chinesischer ISP, IDC China Telecommunication, Routen zu mehr als 8.000 US-amerikanischen Präfixen, 1.100 australischen und 230 von France Telecom, sowie weitere. Diese Routen werden ungefiltert von der staatlichen China Telecom übernommen und propagiert. Die Deutsche Telekom, AT&T, Level3 und andere Provider übernehmen diese Routen ebenfalls und verbreiten sie wiederum weiter. Als Folge dessen enden für 20 Minuten 15% aller Routen weltweit in China. Betroffen sind hiervon sowohl privatwirtschaftliche Unternehmen wie auch viele militärische und Regierungs-Institutionen der USA. Jedoch tritt, im Gegensatz zu bisherigen Vorfällen, kein Blackholing auf, da der Verkehr auf nicht beeinträchtigten Routen zurück in die USA geleitet wird. Der Vorfall wird durch die U.S.-China Economic and Security Review Commission des Kongresses der USA als Hijacking bezeichnet [16].

4. GEGENMAßNAHMEN

Obwohl die Sicherheitsdefizite des BGP bereits seit 1998 bekannt sind und seitdem mehrere Vorfälle und Angriffe auf die globale Routing-Infrastruktur auftraten, sind die Schwachstellen bis heute nicht korrigiert worden. Dies liegt hauptsächlich darin begründet, dass eine Transition auf eine kryptographisch abgesicherte Version des BGP, ähnlich DNSSEC, kompliziert und im Betrieb außerordentlich ressourcenintensiv ist. Aus diesem Grund wurden behelfsmäßig Systeme entwickelt, die dazu dienen, Angriffe frühzeitig zu erkennen und manuell Gegenmaßnahmen ergreifen zu können. Im Folgenden werden mit PHAS und iSPY solche reaktiven Erkennungssysteme vorgestellt, wie auch Ansätze zur präventiven Korrektur der Sicherheitsdefizite des BGP.

4.1 Erkennungssysteme

4.1.1 PHAS

Um Hijacking-Vorgänge global und in Echtzeit zu erkennen, bezieht das Prefix Hijacking Alert System PHAS BGP-Datenströme von mehreren Dutzend bis Hundert BGP-Routern. Diese Datenströme werden durch BGP-Monitoring-Systeme wie Route Views, BGPmon oder die Routing Information Services von RIPE aggregiert. PHAS nimmt also eine möglichst globale Perspektive ein. Es wird stellvertretend für verschiedene vorherige Erkennungssysteme behandelt, da

seine Funktionsweise weitestgehend ähnlich ist. PHAS unterhält für jedes Präfix, welches via BGP propagiert wird, eine Menge an Autonomen Systemen. Diese Menge beinhaltet genau solche Autonome Systeme, welche dieses Präfix initial annonciieren, also die Origin AS. Die Menge wird als Vereinigung aller gemeldeter Origin AS von allen Routern gebildet, die Daten an den Monitoring-Dienst wie Route Views, BGPmon oder RIPEs RIS liefern. Diese Vereinigungsmenge aller weltweit observierten Origin AS wird *Origin Set*, formell O_{SET} , genannt. Für jedes annoncierte Präfix überwacht PHAS dieses Origin Set auf Änderungen. Dies soll durch folgendes Beispiel verdeutlicht werden.

Das Präfix 123.98.76.0/24 gehöre dem AS 5678. Zu einem beliebigen Zeitpunkt t sei dieses AS 5678 das einzige AS, welches das Präfix 123.98.76.0/24 annonciert. Somit beobachten alle BGP-Router, die als Datenquellen für BGP-Beobachtungsdienste dienen, einzig das AS 5678 als Origin AS für das genannte Präfix. Also gilt zum Zeitpunkt t : $O_{SET} = \{5678\}$. Führe nun zu einem beliebigen späteren Zeitpunkt $t' > t$ das AS 6666 einen Hijacking-Angriff durch, indem es das selbe Präfix annonciert. Sobald der erste BGP-Router des Monitoring-Systems Kenntnis dieser neuen Route erhält und sie übernimmt, da sie vorteilhaft erscheint, ändert sich O_{SET} . Das neue O'_{SET} beinhaltet nun auch das AS 6666: $O'_{SET}(123.98.76.0/24) = \{5678, 6666\}$. Unter der Annahme, dass die Route überall als günstiger betrachtet wird, wird nach der Konvergenz der globalen Routing-Tabelle zum Zeitpunkt t'' das legitime Origin AS 5678 aus dem O'_{SET} entfernt, da kein BGP-Router es mehr in seiner Routing-Tabelle hält. Somit ist zum Zeitpunkt t'' das Origin Set $O''_{SET}(123.98.76.0/24) = \{6666\}$. Wird der Angriff bemerkt und Gegenmaßnahmen ergriffen, ändert sich das Origin Set über $\{6666, 5678\}$ wieder zurück zu $\{5678\}$.

All diese Änderungen werden im von PHAS vorgehaltenen Origin Set für das Präfix 123.98.76.0/24 verfolgt. Es kann somit Konflikte feststellen, bei denen mehrere Origin AS für ein Präfix auftauchen. Damit Besitzer von Präfixen bei Vorfällen benachrichtigt werden, können sie sich bei PHAS für ihr Präfix registrieren. PHAS versendet bei Änderungen des Origin Set Mitteilungen per eMail an für das betroffene Präfix registrierte Nutzer. Da bei Hijacking-Vorfällen die Verfügbarkeit des betroffenen Netzes schnell sinkt, wird empfohlen, möglichst viele verschiedene eMail-Adressen bei verschiedenen Anbietern anzugeben. Dies soll sicherstellen, dass zumindest über eine Route noch eMails empfangen werden können. Nachteilhaft an PHAS ist, dass es trotz seiner möglichst globalen Sicht keine MOAS-Konflikte erkennen kann, die in ihrer Verbreitung begrenzt sind. Dies kann durch einen Angreifer gezielt herbeigeführt werden. [17]

4.1.2 iSPY

Statt wie PHAS eine möglichst allumfassende, externe Sicht zu erhalten, verwendet iSPY die interne Perspektive eines AS nach außen. Hijacking-Angriffe führen meist in kürzester Zeit zu Unerreichbarkeit einer signifikanten Anzahl von Zielen. iSPY nutzt diesen bei MOAS-Konflikten auftretenden Effekt des Konnektivitätsverlusts aus, um Vorfälle schnell zu erkennen. Hierfür verwendet iSPY eine Heuristik, die die individuelle Unerreichbarkeitssignatur eines AS überwacht und von Konnektivitätsverlust aus anderen Ursachen unterscheidet. Die Erreichbarkeit des eigenen Netzes wird durch periodisch durchgeführte Tests wie z.B. Pings – ICMP-basierte wie auch andere – ermittelt.

Um die Erreichbarkeit eines AS von innen heraus zu erfassen, führt iSPY für jedes Transit-AS eine Datenstruktur, die den Pfad zum jeweiligen Transit-AS darstellt. Transit-AS sind solche AS, welche für die Weiterleitung von Netzwerkverkehr zuständig sind. Außerdem haben Transit-AS nur einen kleinen Anteil an der Gesamtheit aller AS, weshalb die zu testende Anzahl an AS stark reduziert wird. Als Knotenpunkte des Routings werden Transit-AS jedoch notwendigerweise von BGP-Änderungen betroffen. Daher haben Hijacking-Angriffe auch zwingend auf Transit-AS Auswirkungen.

Der Pfad zu jedem Transit-AS wird via Traceroute ermittelt und als Datenstruktur T festgehalten. Ausgehend von einer Momentaufnahme T_{old} , welche vollständige Konnektivität abbildet, überprüft iSPY für jedes AS, ob der neu ermittelte Pfad zu jedem AS T_{new} teilweise oder vollständig nicht ermittelbar ist. Unermittelbarkeit eines oder mehrerer Hops im Pfad ist ein Indikator für Unerreichbarkeit des durch iSPY überwachten AS. Alle unerreichbaren Hops in allen T_{new} werden in einer Vereinigungsmenge Ω gespeichert. Diese ist die aktuelle Unerreichbarkeitssignatur. Da BGP-Updates immer eine größere Verbreitung erreichen, ist Ω bei Hijacking-Vorgängen notwendigerweise immer groß. Bei anderen Ursachen, die nicht per BGP weiterverbreitet werden, wie z.B. der Ausfall eines Links oder einzelner Router, ist Ω wesentlich kleiner. Die Unerreichbarkeitssignatur ist bei MOAS-Konflikten um mehrere Ordnungen größer als bei anderen Ursachen. Dies wurde auch durch Simulationen verifiziert, sodass durch iSPY eine Kardinalität von 10 für Ω als Schwellwert für Alarm verwendet wird.

Bei Datenbeständen vergangener Vorfälle und Simulationen erreicht iSPY laut seinen Entwicklern eine Fehlerrate erster Art kleiner als 0,45%. Fehler zweiter Art, also fälschliche Erkennung inexisterter Angriffe, treten mit einer Wahrscheinlichkeit von unter 0,17% auf. iSPYs Verlässlichkeit hängt weder von der Sicht einer beschränkten Anzahl an Kontroll-Routern eines einzigen, potentiell ausfallgefährdeten Systems ab, noch ist die Benachrichtigung des Angegriffenen bei Vorfällen beeinträchtigt. Vollständiges Prefix-Hijacking sowie Subprefix-Hijacking werden verlässlich erkannt. Allerdings wird ein korrekt durchgeführter Interception-Angriff nicht notwendigerweise festgestellt. [4]

4.2 Kryptographische Erweiterungen

4.2.1 S-BGP

S-BGP (Secure BGP) ist einer von vielen Vorschlägen, das Border Gateway Protocol kryptographisch abzusichern und Authentizität, Autorisierung und Integrität zu gewährleisten. Ähnlich DNSSEC etabliert es eine Public Key-Infrastruktur entlang der Adressvergebearchie. Die IANA ist die Wurzel der Vertrauenshierarchie und stellt die Zertifikate der regionalen Registries aus, welche wiederum den großen ISPs Zertifikate ausstellen. Diese zertifizieren ihre Kundenetze usw. Die gesamte PKI besteht aus zwei Teil-PKIs. Eine der beiden ist für die Absicherung der Vergabe von Adressbereichen zuständig, die andere für die Vergabe von AS-Nummern. Durch Attestierungen erlaubt eine Partei einer anderen, Adressen zu proklamieren oder Routen zu veröffentlichen. Die Attestierungen werden von der autoritativen Partei signiert und beinhalten die berechnete Partei sowie die Gegenstände der Berechtigung. Auf diese Weise wird sichergestellt, dass ein Router, der einen Adressbereich bewirbt, auch zum Origin AS gehört. Äquivalent gilt dies auch für BGP-Updates, diese müssen ebenfalls attestiert werden.

Da jeder Router die BGP-Nachrichten signiert, findet eine Verschlüsselung mit Signaturen statt, die alle Einträge einzeln verifiziert. Durch diese PKI werden Adressbereiche und AS-Nummern an Organisationen gebunden, und Organisationen an Router [1, 18]. Im trivialen Fall berechtigt sich also ein AS dafür, den ihm zugewiesenen Adressbereich zu proklamieren. Sicherheit auf Netzwerk- und Transportebene wird durch IPsec geleistet, welches von S-BGP vorgeschrieben wird. Es schützt die Vertraulichkeit und Integrität der BGP-Daten während der Übertragung. Die Schlüsseldistribution für IPsec wird durch die PKI von S-BGP übernommen. Die wichtigsten Schwachstellen des BGP, also Validität von Routen-Informationen sowie Berechtigungen für Annoncierung, werden durch S-BGP behoben.

Der Nachteil des Systems liegt in den Hürden der Inbetriebnahme und dem ressourcenintensiven Einsatz. Beim Aufbau einer BGP-Sitzung zwischen zwei Routern muss die gesamte Routing-Tabelle ausgetauscht werden. Für diese gesamte Routing-Tabelle müssen alle Einträge kryptographisch auf Legitimität geprüft werden. Im Jahr 2000 war das Netz, gemessen an der Anzahl Autonomer Systeme, um den Faktor 8 kleiner als zum jetzigen Zeitpunkt. Dabei waren pro Router, mit dem eine Sitzung etabliert wurde, 220.000 Überprüfungen notwendig. Aus diesem Grund wird von den Protokollentwicklern das Nachrüsten von nichtflüchtigem Massenspeicher für jeden Router vorgeschlagen, um verifizierte Daten zu cachen. [18]

4.2.2 *Secure Origin BGP*

Secure Origin BGP (soBGP) [1] basiert ebenfalls auf einer PKI. Diese ist allerdings nicht hierarchisch organisiert, sondern dezentral als Web of Trust. Jedem BGP-Router werden drei Zertifikate übergeben: (1) Ein Zertifikat bindet einen öffentlichen Schlüssel an den zertifikatsinhabenden Router. (2) Ein weiteres Zertifikat beinhaltet die Netzwerkconfiguration und Topologie-Information über Netzwerkknachbarn. (3) Ein drittes Zertifikat dient der Attestierung von Origin AS für ihre Adressbereiche und Erlaubnis für Routen-Propagation. Das Topologie-Zertifikat wird außerdem weiterverbreitet, sodass alle Router die Topologie kennen. Wie S-BGP setzt auch soBGP auf IPsec auf.

soBGP ist weniger vollständig als S-BGP, dafür aber mit insgesamt geringeren Einsatzhürden verbunden. Die größte Gefahr, das Annoncieren von Präfixen durch AS, die nicht das legitime Origin AS sind, wird unterbunden. Dennoch bestehen einige Mängel: Gefälschte Pfad-Informationen, die Topologie-konform sind, können nicht erkannt werden. Sie sind ggfs. ineffizient, aber werden nicht als bösartig erkannt. Außerdem sind die verwendeten Zertifikate nicht konform zu bereits existierenden Standards. Ferner konvergiert die Topologie-Information weltweit nicht schnell, und ist ohne Neuausstellung von Zertifikaten nicht änderbar, bspw. wenn Präfixe anderen Organisationen zugeordnet werden. Dies sorgt für eine geringere Flexibilität. Besonders wegen der Knappheit an IPv4-Adressen scheint es wahrscheinlich, dass in Zukunft mehr Adressen die Organisation wechseln.

4.2.3 *Pretty Secure BGP*

Pretty Secure BGP (psBGP) bildet den Mittelweg zwischen soBGP und S-BGP. Für die Authentisierung von AS wird eine zentralisierte PKI der Tiefe 1 verwendet. Sie bindet AS-Nummern an öffentliche Schlüssel, sodass Angreifer sich nicht für andere AS ausgeben können. Der Unterschied zu

S-BGP besteht darin, dass alle ASN direkt von der IANA zertifiziert werden, um den enormen Aufwand der PKI von S-BGP zu minimieren. Um IP-Adressen an AS zu binden, kommt eine dezentrale PKI als Web of Trust zum Einsatz. Hierbei gibt jedes AS Listen von Präfixen an, die es als zu ebenfalls angegebenen AS-Nummern zugeordnet erklärt. Eine solche Liste legt jedes AS für sich an wie auch für seine Peers, also Nachbar-AS mit beidseitigem kostenlosem Transit. So bestätigen sich mehrere AS gegenseitig, dass sie die korrekten Origin AS für ihre Präfixe sind. Integrität wird ebenfalls durch IPsec sichergestellt. Validität der Pfad-Informationen wird identisch zu S-BGP implementiert, indem eine verschachtelte Signierung aller Einträge einer BGP-Route vorgenommen wird. [19]

4.2.4 *RPKI*

Den Ansätzen S-BGP, soBGP und psBGP ist gemein, dass sie Attestierungen verwenden, um die Berechtigung zur Annoncierung von Adressbereichen und Weiterverbreitung von Routen zu gewähren. RPKI, die Resource Public Key-Infrastruktur, verwendet hingegen Zertifikate. Hierbei handelt es sich um X.509-Zertifikate, die auch in vielen anderen Gebieten Anwendung finden. Im Fall von RPKI beinhalten diese Zertifikate ein Feld, in welchem Netzwerkressourcen wie IP-Adressen und AS-Nummern angegeben sind. Identisch zu S-BGP verläuft die Hierarchie der RPKI entlang der Adressvergabekette. In dieser Kette stellen hierarchisch höher angesiedelte Institutionen die Certificate Authorities der ihnen untergeordneten Institutionen dar und stellen ihnen Zertifikate aus. Eine weitere Form von Objekten, sogenannte Route Origin Authorizations, werden von autoritativen Organisationen signiert. Sie bestätigen dem Besitzer der ROA, dass er berechtigt ist, bestimmte Präfixe zu annoncieren. Ein solches ROA beinhaltet ein oder mehrere Präfixe und genau eine AS-Nummer, die berechtigt ist, diese Präfixe via BGP zu bewerben. Die ROAs werden in der RPKI veröffentlicht. Ebenfalls enthalten sie ein Maximum Prefix Length-Feld, welches die maximale Länge eines annoncierbaren Präfix angibt. Es verhindert Subprefix-Hijacking durch Ausnutzen der Longest Prefix Match-Regel. [20]

Auf diese Weise wird sichergestellt, dass kein AS Präfixe für sich beansprucht, die ihm nicht gehören, und diese Informationen in die globale Routing-Tabelle gibt. Dies verhindert die gefährlichsten Angriffe auf das BGP und garantiert die Validität von Origin AS. Allerdings wird nicht die Validität der gesamten Route sichergestellt. So kann ein Angreifer zwar nicht sein AS als das Ziel-AS für ein bestimmtes Präfix ausgeben, aber immerhin Verkehr über sich leiten. RPKI bietet hiergegen keine Sicherheit. Allerdings ist die RPKI, auch wenn sie eigenständig operieren kann, nur ein Teil von BGPsec. Bei BGPsec handelt es sich um eine Überarbeitung des BGP, welche alle in Sektion 3 genannten Probleme adressiert. BGPsec wird von der IETF-Arbeitsgruppe für Secure Inter-Domain Routing (SIDR) entwickelt. Auch schreibt BGPsec gesicherten Transport über Protokolle wie TLS oder TCP/MD5 vor, um den Problemen von TCP zu begegnen. Es kann auch über SSH getunnelt werden [21]. RPKI ist das erste für den Einsatz fertige Ergebnis der SIDR-Arbeitsgruppe. Auf lange Sicht soll BGPsec möglichst weitgehend umgesetzt werden, um so die bekannten Angriffsvektoren des BGP zu schließen. [20]

Der größte Vorteil von BGPsec bzw. RPKI liegt dort, wo bisherige Vorschläge scheitern. Der RPKI-Standard sieht Ca-

ches vor, welche Zertifikate und ROAs vorhalten und die kryptographische Validierung vornehmen [21]. Somit werden Speicher- und rechenintensive Operationen, welche signifikanten Overhead produzieren und eine Erweiterung der Hardware von BGP-Routern fordern würden, an dedizierte Instanzen ausgelagert. Auch wird redundanter Verkehr und Datenhaltung reduziert, da ein Cache Dienste für mehrere BGP-Router erbringen kann. Dies macht den Einsatz von RPKI weitaus einfacher und weniger ressourcenintensiv als bisherige Ansätze zur kryptographischen Absicherung des BGP. RIPE hat sich für eine Weiterentwicklung und Förderung von RPKI ausgesprochen [22]. Die American Registry for Internet Numbers (ARIN) hat in Koordination mit anderen Registries den Testbetrieb der RPKI begonnen [23]. Der aktuelle Entwicklungsstand von RPKI ist in den RFCs mit Draft-Status 6480 bis 6493 festgehalten [24].

5. VERWANDTE ARBEITEN

Die vorliegende Arbeit gibt einen Einblick in die technischen Hintergründe von BGP Hijacking und Interception. Hierfür werden die Schwachstellen des BGP aufgezeigt. Die praktische Vorgehensweise bei BGP-basierten Angriffen wird durch Vorfälle aus der Praxis beleuchtet. Reaktive Erkennungssysteme zur frühen Identifikation von Vorfällen aus verschiedenen Perspektiven wurden ebenso vorgestellt wie präventive Erweiterungen des BGP zur Beseitigung der Ursachen. Als weiterführende Arbeiten seien folgende empfohlen:

- [1] ist eine umfassende Sicherheitsanalyse des BGP. Es beleuchtet detailliert sowohl die Schwachstellen des BGP wie auch die in dieser Arbeit behandelten Lösungsansätze S-BGP, psBGP und soBGP. Da RPKI zum Zeitpunkt der Veröffentlichung der Arbeit noch nicht weit entwickelt war, erhält es keine eingehende Behandlung. Diese Arbeit ist sehr umfassend und erörtert nahezu alle relevanten Aspekte der BGP-Sicherheit.
- Bei [25] handelt es sich um eine Bachelorarbeit zur Entwicklung einer RPKI-Validierungs-Bibliothek. Insbesondere geht sie detailliert auf BGPsec und RPKI ein.
- [2] setzt einen starken Fokus auf BGP-Angriffe. Die Theorie von Angriffen auf die globale Routing-Infrastruktur wird sehr ausführlich erläutert. Auch wird ein Überblick über eine Vielzahl vergangener BGP-Vorfälle gegeben.
- In [26], einer Präsentation für die North American Network Operators Group, wird der in Abschnitt 3.4 vorgestellte Vorfall ausführlich beleuchtet. Vor allem findet eine graphische Analyse der Propagierung der falschen Routen und eine zeitliche Aufbereitung des Verlaufs des Vorfalls statt. Diese Aufbereitung vermittelt einen guten Eindruck des Ablaufs von Hijacking-Angriffen.

6. ZUSAMMENFASSUNG

Trotz langjähriger Bekanntheit der Schwachstellen im einzigen eingesetzten Protokoll für Inter-Domain Routing, dem BGP, ist dieses noch in fast ursprünglicher Form im Einsatz. Das BGP sieht keine Mechanismen vor, die Angaben über Routen oder Präfix-Ursprünge validieren können. Daher kann jedes Netz beliebige Präfixe für sich beanspruchen.

Vorfälle durch Fehlkonfiguration und -verhalten von BGP-Routern traten in der Vergangenheit mit großem Effekt auf. Große Teile des Internets waren zeitweise, von mehreren Stunden bis hin zu mehr als einem Tag, vollkommen un erreichbar. Hiervon waren große Firmen wie Microsoft oder Amazon ebenso wie viele Millionen bis hin zu Milliarden Nutzer betroffen. Auch gezielte Angriffe können bis dato sehr einfach und erfolgreich durchgeführt werden. Zum Versand von Spam-Mails, zur Zensur oder auch zu vielen anderen Zwecken können Adressbereiche anderer Organisationen übernommen werden, sodass in großen Teilen der Welt Blackholing auftritt. Bei korrekter Umsetzung können sogar Man-in-the-Middle-Angriffe gegen ganze Netze durchgeführt werden.

Mit PHAS und iSPY wurden zwei Systeme zur Erkennung von Hijacking-Vorfällen vorgeschlagen. Sie unterscheiden sich insbesondere in der Perspektive, die zur Erkennung eingenommen wird. Wird ein Vorfall beobachtet, benachrichtigen PHAS und iSPY den Präfix-Besitzer, der manuell Gegenmaßnahmen ergreifen kann. Nachteilig an PHAS ist, dass u.U. die Benachrichtigungen das angegriffene Präfix nicht erreichen. Wegen der Redundanz durch die weitverbreitete Nutzung mobiler Datennetze ist dies heutzutage jedoch nicht mehr von großer Relevanz. Beiden Systemen ist gemein, dass sie nur die Symptome eines unsicher entwickelten Protokolls bekämpfen.

Validität von Routen und Präfix-AS-Zuordnungen kann nur durch kryptographische Absicherung des BGP erreicht werden. Mit S-BGP existiert bereits lange ein Ansatz, der alle Schwachstellen des BGP adressiert. Allerdings ist S-BGP sehr ressourcenintensiv. Insbesondere fordert es Hardware-Erweiterungen mit nichtflüchtigem Speicher an allen BGP-Routern, um PKI-Objekte vorzuhalten. Auch der Overhead durch kryptographische Operationen ist signifikant. Aus diesen Gründen ist S-BGP sowohl in der Inbetriebnahme wie auch im laufenden Einsatz nicht praktikabel und mit sehr großen Hürden verbunden. psBGP und soBGP haben zwar geringere Einsatzhürden, bieten aber keinen vollständigen Schutz gegen die in Sektion 2 genannten Schwachstellen. Aus diesen Gründen konnte sich bis heute keines dieser drei Systeme durchsetzen.

RPKI, als eigenständig einsetzbarer Teil von BGPsec, behebt die Nachteile von S-BGP. Insbesondere wird die Datenhaltung der PKI-Objekte auf externe Caches ausgelagert, die mehrere BGP-Router bedienen können. Gleichzeitig ist der durch BGPsec gebotene Schutz ebenso vollständig wie der von S-BGP und schließt alle bekannten Schwachstellen. RPKI eliminiert im eigenständigen Betrieb immerhin den größten Angriffsvektor, indem es die Validität von Origin AS forciert. Hijacking von fremden Adressbereichen ist somit nicht mehr möglich. RIPE hat seine Unterstützung von RPKI erklärt und ARIN unterhält eine öffentliche RPKI-Testumgebung. Ferner haben alle relevanten Netzausrüstungshersteller das RPKI-Protokoll bereits zu großen Teilen implementiert [27].

7. FAZIT

Mit BGPsec und insbesondere RPKI scheint eine Lösung gefunden zu sein, die breite Unterstützung durch Standardisierungskomitees, Registries wie auch durch Hersteller erfährt. Die Einsatzhürden sind wesentlich geringer als bei vorherigen Lösungen, der Schutz jedoch bei Fertigstellung von BGPsec vollständig. Die von RPKI gebotene Sicherheit ge-

gen Fälschung von Präfix-Besitz und somit Hijacking beseitigt das größte Problem des BGP. RPKI wird daher bereits als eigenständige Lösung Einsatz finden.

Komplementär zu RPKI kann, um Manipulation der via BGP verbreiteten Pfade zu erkennen, auf PHAS und iSPY gesetzt werden. Diese können auch parallel betrieben werden. Sie sind mit keinen nennenswerten Einsatzhürden verbunden, weshalb ihre Inanspruchnahme keine Nachteile mit sich bringt. In der Übergangsphase bis zum Einsatz von RPKI sind sie eine gute Möglichkeit, auf Hijacking-Vorfälle reagieren zu können. Aber auch darüber hinaus können sie Vorfälle erkennen, die nicht durch RPKI abgedeckt werden, z.B. solche, die durch Entwendung von Zertifikaten herbeigeführt werden.

8. LITERATUR

- [1] K. Butler, T. R. Farley, P. McDaniel, and J. Rexford, „A Survey of BGP Security Issues and Solutions”, in *Proceedings of the IEEE*, vol. 98, pp. 100–122, Januar 2010.
- [2] K. T. Latt, Y. Ohara, S. Uda, and Y. Shinoda, „Analysis of IP Prefix Hijacking and Traffic Interception”, *International Journal of Computer Science and Network Security*, vol. 10, pp. 22–31, Juli 2010.
- [3] T. Bates, P. Smith, and G. Huston, „CIDR Report”, März 2012. <http://www.cidr-report.org/as2.0/>.
- [4] Z. Zhang, Y. Zhang, Y. C. Hu, Z. M. Mao, and R. Bush, „iSPY: Detecting IP Prefix Hijacking on My Own”, in *ACM SIGCOMM*, 2008.
- [5] S. M. Günther, *Skript: Grundlagen Rechnernetze und Verteilte Systeme*. Lehrstuhl für Netzarchitekturen und Netzdienste, Fakultät für Informatik, Technische Universität München. 2011.
- [6] X. Hu and Z. M. Mao, „Accurate Real-time Identification of IP Prefix Hijacking”, 2006.
- [7] S. Murphy, „BGP Security Analysis”, August 1998.
- [8] L. Benkis, „Practical BGP Security: Architecture, Techniques and Tools”, September 2005.
- [9] T. Underwood, „Internet-wide catastrophe – last year”, 24. Dezember 2005. <http://www.renesys.com/blog/2005/12/internetwide-nearcatastrophela.shtml>.
- [10] A. C. Popescu, B. J. Premore, and T. Underwood, „The Anatomy of a Leak: AS9121”, 15. Mai 2005.
- [11] M. A. Brown, A. Popescu, and E. Zmijewski, „Who’s Manning the L root?”, in *NANOG Meeting 43*, renesys, Juni 2008.
- [12] E. Zmijewski, „Identity Theft Hits the Root Name Servers”, 19. Mai 2008. http://www.renesys.com/blog/2008/05/identity_theft_hits_the_root_n_1.shtml.
- [13] G. Lowe, P. Winters, and M. L. Marcus, „The Great DNS Wall of China”, 21. Dezember 2007.
- [14] RIPE Network Coordination Centre, „YouTube Hijacking: A RIPE NCC RIS case study”, März 2008.
- [15] A. Pilosov and T. Kapela, „Stealing The Internet – An Internet-Scale Man In The Middle Attack”, DEFCON 16, 10. August 2008. www.defcon.org/images/defcon-16/dc16-presentations/defcon-16-pilosov-kapela.pdf.
- [16] U.S.-China Economic and Security Review Commission, „Report to Congress”, U.S. Congress, November 2010.
- [17] M. Lad, D. Massey, D. Pei, Y. Wu, B. Zhang, and L. Zhang, „PHAS: A Prefix Hijack Alert System”, 2006.
- [18] S. Kent, C. Lynn, and K. Seo, „Secure Border Gateway Protocol (S-BGP)”, *IEEE Journal on Selected Areas in Communications*, vol. 18, April 2000.
- [19] T. Wan, E. Kranakis, and P. C. van Oorschot, „Pretty Secure BGP (psBGP)”, 5. November 2004.
- [20] G. Huston and R. Bush, „Securing BGP and SIDR”, *IETF Journal*, vol. 7, Juli 2011. <http://isoc.org/wp/ietfjournal/?p=2438>.
- [21] R. Bush and R. Austein, „The RPKI/Router Protocol (Draft)”, 3. Februar 2012. <https://datatracker.ietf.org/doc/draft-ietf-sidr-rpki-rtr/>.
- [22] M. Neylon, „RIPE Members Vote To Continue RPKI Work”, 3. November 2011. http://www.circleid.com/posts/20111103_ripe_members_vote_to_continue_rpki_work/.
- [23] ARIN, „RPKI Pilot”, 2011. <https://rpki-pilot.arin.net/>.
- [24] SIDR Work Group, „Secure Inter-Domain Routing (sidr) Work Group Documents.” <https://datatracker.ietf.org/wg/sidr/>.
- [25] F. Holler, „Konzeption und Entwicklung einer Client-seitigen RPKI-RTR Library zur Validierung der Präfix-Zugehörigkeit von autonomen Systemen in BGP-Routen”, Bachelorarbeit, Hochschule für Angewandte Wissenschaften Hamburg, 9. November 2011.
- [26] A. C. Popescu, B. J. Premore and T. Underwood (Renesys Corporation), „The Anatomy of a Leak: AS9121”, 15. Mai 2005. <http://www.renesys.com/tech/presentations/pdf/renesys-nanog34.pdf>.
- [27] R. Bush, R. Austein, K. Patel, H. Gredler, and M. Waehlich, „RPKI Router Implementation Report”, 8. Januar 2012.