Wirkungsanalyse von Routing-Angriffen im Internet

Jan Henke

August 2012

Master Informatik
Department Informatik
Fakultät Technik und Informatik
HAW Hamburg

Inhaltsverzeichnis

1 Einleitung **1**
1.1 Rückblick: BGP + Angriffvektoren 1

2 Analyse **2**
2.1 Topologiemodell von L. Gao 3
2.2 Aktuelle Veränderungen in der Routing-Topologie 6
2.3 Studie von H. Ballani et. al. 9

3 Zusammenfassung + Ausblick **9**

Literatur **11**

Abbildungsverzeichnis

1 Klassische logische Routing-Topologie, Quelle: [1] 5
2 Anzahl ASN vs. Anteil am globalen inter-domain Verkehr, Quelle: [1] . . . 7
3 Aktuelle logische Routing-Topologie, Quelle: [1] 8

1 Einleitung

Diese Arbeit untersucht die Veränderungen die sich aktuell in der Topologie des Internets ergeben und die daraus folgenden Konsequenzen für bestimmter Angriffe auf das Border-Gateway-Protocols (BGP).[2]

Für die so genannte Default-freie Zone wird BGP benutzt, um Informationen über die Routen im Internet zwischen den einzelnen Teilnetzen (im Rahmen des BGP autonome Systeme (AS) genannt) auszutauschen und ist somit von grundlegender Bedeutung für die Funktion des Internets. Default-freie Zone bezeichnet jenen Teil des Internets, der für jede IP-Adresse eine explizite Route kennt. Es ist seit einiger Zeit eine konzeptionelle Schwäche des BGP bekannt, welche es einem Angreifer erlaubt die Pfade von Datenströmen im Internet zu manipulieren. Durch geschickte Wahl dieser Manipulationen kann ein Angreifer die Datenströme entweder dem Empfänger komplett vorenthalten (Blackholing) oder sich in die Kommunikation zwischen mehren Teilnehmern einklinken und sämtliche Daten mitlesen (Redirection). Diese Angriffsszenarien sind bereits seit längerer Zeit bekannt, da diese schon vielfach im Internet aufgetreten sind, allerdings häufig als Folge einer unbeabsichtigten Fehlkonfiguration. Angesicht der Bedeutung, die dem Internet heute beikommt, ist aber von einer Zunahme der bewussten Angriffen auf dieser Ebene in der Zukunft auszugehen.

Es ist daher von großer Bedeutung, die Verbreitung solcher Angriffe im Internet zu verstehen. Dies dient zum Einen dazu, einschätzen zu können, welchen Bedrohungen ein einzelnes AS ausgesetzt sein könnte, zum anderen aber auch um im Falle eines Angriffes auf das eigene AS Rückschlüsse ziehen zu können, an welcher Stelle des Routings der Angreifer vermutlich sitzt. Eine solche Studie der Verbreitungswege hat H. Ballani et. al. [3] bereits erstellt, jedoch entspricht das zu Grund liegende Modell nicht mehr der aktuellen Struktur des Internets. Die in den letzten Jahren auf der Ebene des Routings erfolgten Veränderungen zeigen Labovitz et. al. in [1].

Diese Seminararbeit setzt sich daher kritisch mit diesen beiden Arbeiten auseinander und zeigt auf, welchen Weg meine Masterarbeit in diesem Zusammenhang beschreiten wird.

1.1 Rückblick: BGP + Angriffvektoren

Das BGP ist ein Pfadvektorprotokoll. Jedes AS hat dabei eine lokale Sicht, die zu jeder routbaren IP-Adresse mindestens eine Route enthält. Diese Sicht ist aber spezifisch für die jeweilige Position im Routing-Graphen. Auch sind häufig mehrere alternative Routen für ein bestimmtes Präfix bekannt, so dass Router sich für eine dieser Routen entscheiden müssen.

Diese beiden Punkte sind entscheidend für Angriffe auf der Routing-Ebene. Es sei A der Name des AS, welches ein Angreifer kontrolliert. Dieser möchte nun die Route für den Verkehr von AS X manipulieren. Das prinzipielle Vorgehen besteht nun darin, dass A gegenüber seinen Routing-Nachbarn vorgiebt entweder für alle oder einen Teil der Präfixe von X zuständig zu sein (Invalid Origin/Longest Common Prefix Attack) oder aber die beste Route zu X zu besitzen (Invalid Next Hop Attack).

Zur Abwehr der ersten Klasse von Angriffen basierend auf der Vorgabe fremde IP-Präfixe zu besitzen wurde Anfang des Jahres die Resource Public Key Infrastructre standardisiert, unter anderem in RFC 6480. [4] Diese löst das Problem dadurch, dass für jedes Präfix eine kryptograpische Signatur über das Präfix selber, seine Länge und das dafür gültige Origin-AS, also das AS, welches selbst Routen für das Präfix veröffentlichen darf, erstellt wird. Routen-Updates werden daraufhin nur noch akzeptiert, wenn diese drei Parameter mit der Signatur übereinstimmen. Die Echtheit der Schlüssel wird dabei von einer Chain-of-Trust sichergestellt, welche auch der Vergabe von sonstigen numerischen Ressourcen im Internet entspricht. Das heißt, die Internet Assigned Numbers Authority (IANA) besitzt ein Wurzelzertifikat mit dem die Zertifikate der fünf Regional Internet Registries (RIR) signiert sind. Die RIR stellen wiederum die Infrastruktur bereit, über die alle von ihnen ausgegebenen IP-Präfix und AS-Nummern (ASN) signiert werden.

Ein konsequentes Ausrollen der RPKI in den nächsten Jahren müsste somit die Anfälligkeit für Invaild Origin und Longest Common Prefix Attacks eleminieren. Es ist derzeit aber noch nicht abzusehen, wie schnell dies passieren wird. [5] Die RPKI hilft jedoch nicht gegen die Anfälligkeit für Invalid Next Hop Attacks. Daher beschäftigt sich die weitere Arbeit mit der Analyse dieser Art von Angriffen auf die BGP-Infrastruktur. Dabei werde ich insbesondere der Frage nachgehen, wie sich ein derart gefälschtes BGP-Update verbreitet. Da jeder Knoten der AS-Topologie eine eigene lokale Sicht auf das globale AS-Routing besitzt, ist die Frage nach der Ausbreitung von zentraler Bedeutung für das Verständnis von derartigen Angriffen. Bei Kenntnis der AS-Topologie ermöglicht dies zudem im Vorwege festzustellen, an welcher Stelle sich ein Angreifer platzieren muss, um entweder möglichst vielen oder ganz bestimmten ASes seine gefälschte Route „unterzuschieben“, so dass diese auch genutzt wird.

Dieses Wissen ist offensichtlich geeignet einen möglichen Angriff zu optimieren. Dies ist jedoch nicht das Ziel dieser Arbeit. Vielmehr ist dieses Wissen erforderlich, um sich vor derartigen Angriffen schützten zu können. Zum Einen ist es für jeden Betreiber eines AS unabdingbar, eine Übersicht darüber zu haben, von welchen anderen AS eine Gefahr für einen derartigen Angriff auf das eigene AS ausgeht. Zum Anderen hilft ein solches Verständnis bei der Analyse von aktuell laufenden oder zurückliegenden Angriffen, um den Urheber auszumachen und entsprechende zukünftige Angriffe damit zu verhindern.

Darüber hinaus ergibt sich eine Fragestellung, welche in der Literatur bis jetzt noch nicht tiefgreifend erörter wurde. Welche Möglichkeiten zur Optimierung der Reichweite und Verschleierung bieten sich, wenn ein Angreifer nicht nur ein, sondern mehrere ASes unter seiner Kontrolle hat.

2 Analyse

Dieser Abschnitt befasst sich mit dem Peering-Verhalten der Internet-Provider und mit den Veränderungen, denen dieses Verhalten in den letzten Jahren unterworfen ist. Das Peering-Verhalten, also die Frage zu welchen anderen Providern eine Peering-Beziehung hergestellt wird, folgt stets zwei Grundsätzen. Zunächst benötigt jeder Provider eine vollständige Konnektivität zum restlichen Internet, d.h. er muss über seine Peering-

Verbindungen am globalen Routing teilnehmen können. Des weiteren möchte jeder Provider seine eigenen Kosten minimieren und gleichzeigt maximale Einnahmen generieren. Je nach Art des Providers foglen aus diesen beiden Grundsätzen unterschiedliche Geschäftsmodelle.

In 2.1 wird zunächst das Topologiemodell von Lixin Gao aus dem Jahre 2001 vorgestellt. Dieses Modell wird in vielen Arbeiten als Routing-Modell verwendet, beschreibt aber nur die Topologie zu einem bestimmten Zeitpunkt und einer bestimmten Region. Daher geht es in Abschnitt 2.2 um eine Studie aus dem Jahre 2010. Diese gibt einen Einblick in die Veränderungen, denen die Routing-Topologie aktuell unterworfen ist. In 2.3 geht es um eine Arbeit aus dem Jahre 2007, welches die Verbreitung von BGP-Angriffen bereits analysiert, dabei allerdings auf dem Gao-Modell basiert und daher nicht mehr vollständig für das heutige Internet anwendbar ist.

2.1 Topologiemodell von L. Gao

Die Arbeit "On Inferring Autonomous System Relationships in the Internet" [6] wurde von Lixin Gao im Jahre 2001 veröffentlicht. Zentrales Element bei der Steuerung des Peering-Verhaltens eines AS' sind die so genannten Policies. Die Policies entscheiden darüber, von welchen anderen AS Routen akzeptiert werden und welche Route von mehreren gleichwertigen ausgewählt wird. Da jedes AS nur mit einer begrenzten Anzahl von anderen AS eine direkte Netzwerkverbindung aufweist (im folgenden werden diese AS mit direkter Verbindung auch als „Nachbar-AS" bezeichnet) ist es darauf angewiesen, dass einer oder mehre dieser Nachbarn den Verkehr für Dritte weiterleiten, um mit dem Rest des Internets kommunizieren zu können. Dies wird als Transit bezeichnet. Über die Policies wird für jedes AS festgelegt, welche Nachbar-AS es als Transit benutzten kann und ob es bestimmten anderen AS selbst Transitdienste anbietet. Diese Entscheidungen sind von besonderer Bedeutung, da für die Nutzung eines anderen AS als Transit-Provider in der Regel eine Nutzungsgebühr anfällt. Daher hat jeder Betreiber eines AS' ein wirtschaftliches Interesse, nur bestimmte für ihn günstige AS als Transit zu nutzten.

Aus diesem Sachverhalt folgen zwei Tatsachen. Zum Einen ist die Kenntnis der logischen Konnektivität nicht ausreichend, um einen AS-Graphen zu erstellen, welcher den Weg von Daten im Internet beschreibt. Für jedes AS-Paar, welches eine direkte Verbindung unterhält sind auch die jeweiligen Policies bezüglich des anderen Partners nötig um eine Aussage über Routing-Entscheidungen treffen zu können. Zum Anderen sind die Policies eng mit dem Geschäftsmodell des jeweiligen AS-Betreibers verwoben. Viele AS betrachten ihre Policies daher auch als Geschäftsgeheimnis weshalb diese nicht öffentlich verfügbar sind.

Lixin Gao beschreibt in ihrer Arbeit daher welche Policies aus einer bestimmten wirtschaftlichen Beziehung zu folgern sind, um Routing-Anomalien zu verhindern. Eine Routing-Anomelie bezeichnet dabei den Fall, dass in der Routing-Entscheidung Routen gewählt werden, die auf Grund der wirtschaftlichen Beziehungen eigentlich nicht zur Verfügung stehen. Zum Beispiel ein Kunden-AS, welches als Transit zwischen seinen Upstream-Providern fungiert. Außerdem beschreibt sie einen heuristischen Algorithmus, um aus den Einträgen der Routing-Tabelle auf die jeweiligen Beziehungen schlusszufol-

gern. Auf den Algorithmus werde ich hier nicht weiter eingehen, da er für das beschriebene Modell nicht von Relevanz ist.

Im Folgenden wird die Routing-Topologie als ein AS-Graph beschrieben, wobei die AS jeweils die Knoten sind und die Verbindung von einem AS A zu einem AS B eine gerichtete Kante im Graphen darstellt. Die Darstellung als Graph erlaubt eine genauere mathematische Beschreibung der Routing-Topologie. Nach ihren Erkenntnissen auf der Basis von empirischen Daten gibt es vier verschiedene Typen von Kanten in dem Graphen, jeweils bestimmt von den wirtschaftlichen Beziehungen zwischen den AS.

Kunde-Provider: AS A ist der Kunde von AS B. AS A wird somit seine eigenen Präfixe und die Präfixe, welche von eigenen Kunden gelernt wurden, zum AS B exportieren, damit diese über den Transit von AS B vom restlichen Internet aus erreichbar sind. Nicht zu AS B exportiert werden dürfen die Routen die AS A von einem Peering-Partner oder einem anderen Provider gelernt hat. Würde AS A dies tun würde es ungewollt zu einem Transit-Provider für AS B.

Provider-Kunde: AS A ist der Upstream-Provider von AS B. Da AS A ein Interesse hat, dass sein Transit, den es für AS B anbietet, möglichst viel genutzt wird, exportiert AS A alle ihm bekannten Routen zum AS B unabhängig von der Quelle der jeweiligen Route.

Peering-Partner: Die Peering-Partner möchten diese Verbindung untereinander maximal nutzen, jedoch wieder vermeiden, dass diese Verbindung zum Transit für einen oder mehre der eigenen Provider wird. Daher darf keiner der beiden Partner dem anderen eine Route exportieren, die er von dem eigenen Providern oder anderen Peering-Partnern gelernt hat.

Geschwisternetzwerke: Damit werden Netzwerke bezeichnet, welche eine administrative Einheit sind, jedoch auch Routing-Ebene zwei getrennte AS darstellen. Typische Fälle sind regionales Multihoming, unterschiedliche Policies oder Fusion zweier Firmen. Hier können beide AS sich gegenseitig alle Routen exportieren unabhängig von der jeweiligen Quelle.

Mit dem Wissen über die unterscheidlichen Exportregeln für die verschiedenen Arten von AS-Verbindungen erstellt Lixin Gao aus dem von ihr gesammelten empirischen Datenmaterial ein Modell der BGP-Routing-Topologie. Dieses Modell wird auch Tier-Modell genannt, da man die einzelnen AS hierachisch anordnet und dann als Tier-1, Tier-2 usw. bezeichnet. Tier-1 sind dabei diejenigen AS, welche jedes Präfix des Internets allein über kostenfreies Peering (settlement free peering) erreichen können. Tier-2 sind Kunden von mindestens einem Tier-1 AS, Tier-3 entsprechend Kunde von Tier-2 und so weiter. Abbildung 1 zeigt dieses Modell.

Bei der Untersuchung des so gewonnenen AS-Graphen stellt sie fest, dass beliebige Pfade in diesem AS-Graphen immer einem von sechs Mustern folgten. Diese Eigenschaft nennt sich „valley-free“, da die Pfade im AS-Graphen wie Berge aussehen können. Nach oben meint in diesem Zusammenhang zu einem AS mit einem niedrigeren Tier, nach unten entsprechend zu einem AS mit einem höheren Tier. Gerade meint hier, ein oder mehre gleichartige Kanten hintereinander. Es gibt nun folgende Muster:

1. Der Pfad führt gerade nach oben zum Ziel-AS.

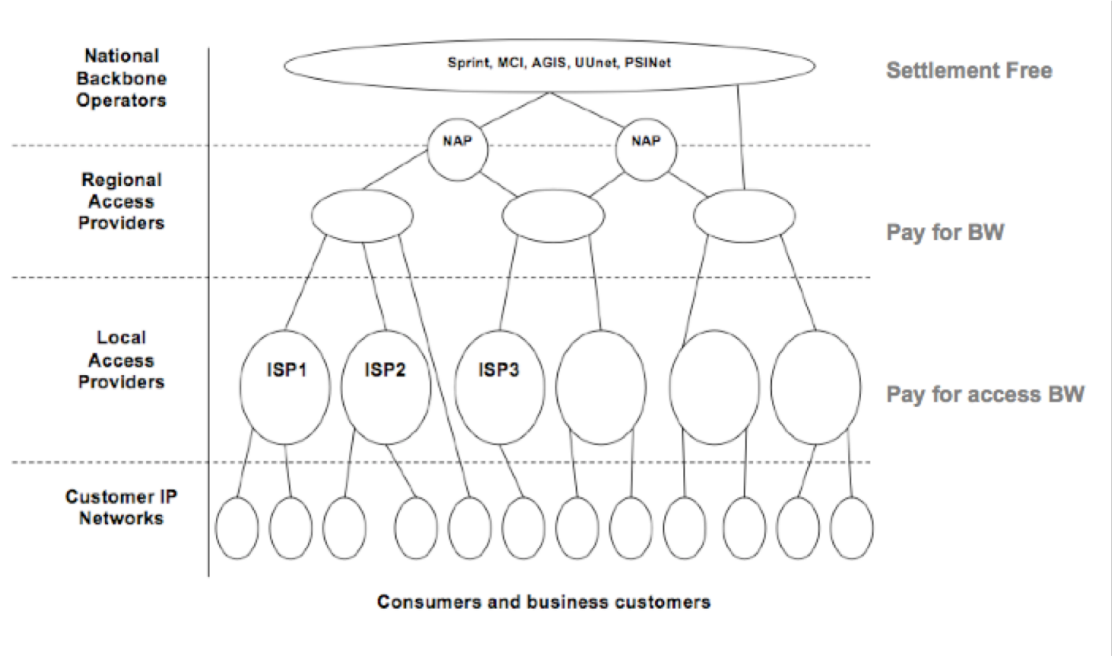

Abbildung 1: Klassische logische Routing-Topologie, Quelle: [1]

2. Der Pfad führt gerade nach unten zum Ziel-AS.
3. Der Pfad führt gerade hoch und von da an gerade nach unten.
4. Der Pfad führt gerade hoch und dann über eine einzelne Peering-Verbindung.
5. Der Pfad führt über eine einzelne Peering-Verbindung und anschließend gerade nach unten.
6. Der Pfad führt gerade nach oben über eine einzelne Peering-Verbingung und dann gerade nach unten.

Somit ist ersichtlich woher der Begriff stammt: Auf eine Peering- oder nach unten gerichtete Kante können nur noch nach unten gerichte Kanten folgen. Ein „Tal“ in der Mitte des Pfades kann nicht vorkommen. Zusätzlich ergibt sich aus der Datenbasis die Erkenntnis, dass in diesem Modell Peering-Kanten relativ selten sind ($\sim 6\%$) und in der Regel relativ weit oben gelegen sind. So findet hier das meiste Peering jeweils zwischen Tier-1 und Tier-2 Providern statt und nimmt bei Tier-3 Providern und abwärts stark ab.

Insgesamt ist es Lixin Gao somit in ihrer Arbeit gelungen, ein in sich konsistentes Modell für die Routing-Topologie zu beschreiben mit dem sich die Wege von Paketen im Internet relativ genau vorhersagen lassen, nachdem man einen entsprechenden AS-Graphen erstellt hat. Jedoch sind einige der beschriebenen Eigenschaften aus den empirischen Daten abgeleitet, die sie für ihre Arbeit genutzt hat. Es ist jedoch auch zu beachten, dass die Arbeit im Jahre 2001 entstanden ist und die Datenbasis vor Allem aus der Sicht der

USA erhoben wurde. Obwohl dieses Modell in einer vielzahl von Arbeiten als Grundlage dient, stellt es damit nur eine Momentaufnahme für den Ort und die Zeit der Entstehung wieder. Die nächste Arbeit beschäftigt sich genauer damit, welche Änderungen sich in den Jahren seit der Erstellung ihrer Arbeit ergeben haben und welche Auswirkungen diese auf das Routing haben.

2.2 Aktuelle Veränderungen in der Routing-Topologie

C. Labovitz et. al. haben für ihre Arbeit[1] mehr als 200 Exabyte an Datenverkehr im Internet analysiert, um Änderungen im Inter-Domain-Verkehrsaufkommen und den Routing-Policies zu untersuchen. Dabei haben sie zwei wesentliche Punkte bestätigt, die für mich im Weiteren von besonderer Bedeutung sind. Zunächst die Tatsache, dass in den letzten Jahren die Bedeutung und Verbreitung der Internet-Exchange-Points (IXPs) stark zugenommen hat und somit zu einer Veränderung der Routing-Topologie führt. Des weiteren sind im zunehmenden Maßen immer weniger AS für einen immer größeren Anteil am weltweiten Internetverkehr verantwortlich, indem der Verkehr entweder aus ihrem AS kommt oder dort endet.

Abbildung 1 zeigt die „klassische“ Routing-Struktur. Diese entspricht dem Gao-Modell, welches in Abschnitt 2.1 beschrieben ist. Das bilaterale Peering ist mit hohen Kosten verbunden (gemietete Leitungen zu einem gemeinsamen Point-of-Presense (PoP), Netzwerk-Hardware für diesen PoP, Wartung), so dass sich diese Peering nur bei entsprechender Nutzung wirtschaftlich gelohnt hat. Peering fand daher überwiegend unter den größten Providern (Tier-1 und Tier-2) statt, da nur diese das nötige Kapital und einen entsprechenden Nutzten davon haben. Auf Grund dieser Nachteile wurde die Idee von Internet-Exchange-Points (IXPs) bereits relativ früh in der Geschichte des Internets gefasst. Deren Bedeutung für die globale Topologie ist jedoch lange Zeit nicht so ausgeprägt gewesen und erst in dem letzten Jahrzehnt deutlich gewachsen.

Die Grundidee von IXPs besteht darin die für das Peering nötigen Kosten zu senken, indem man an einem Ort mit vielen Teilnehmern gleichzeitig Peering-Verbindungen eingegangen werden können. Während klassische Peerings nur direkte Verbindungen zwischen zwei AS herstellten, benötigt man an einem IXP nur einmal die nötigen Hardware um über das lokale Netzwerk des IXPs Peering-Sitzungen mit allen dort angeschlossenen Providern eingehen zu können. Da IXPs nur auf Layer 2 des IP-Stacks operieren, erscheinen diese nicht als Hop im Routing. Der Weg über einen IXP ist daher bei der Routen-Verfolgung nicht sicher zu erkennen. Indizien können dabei IP-Adressen aus dem Pool eines IXPs oder Namen der Router sein.

Insbesondere für kleinere AS bietet der Zugang zu einem IXP entscheidende Vorteile. Es ermöglicht das eingehen von Peering-Verbindungen, die vorher wegen der Kosten nicht realisierbar gewesen wären. Außerdem ist das Eingehen neuer Peering-Beziehungen ohne weitere Investitionen jederzeit möglich. (vorausgesetzt die eigene Netzwerk-Hardware kann den zusätzlichen Verkehr bewältigen) Dadurch, dass das Peering daher auch für kleine Provider erschwinglich wurde, ergeben sich in der heutigen Routing-Topologie wesentlich mehr Peering-Kanten.

Labovitz et. al. zeigen in ihrer Studie, dass ein steigender Anteil am weltweiten Internet-

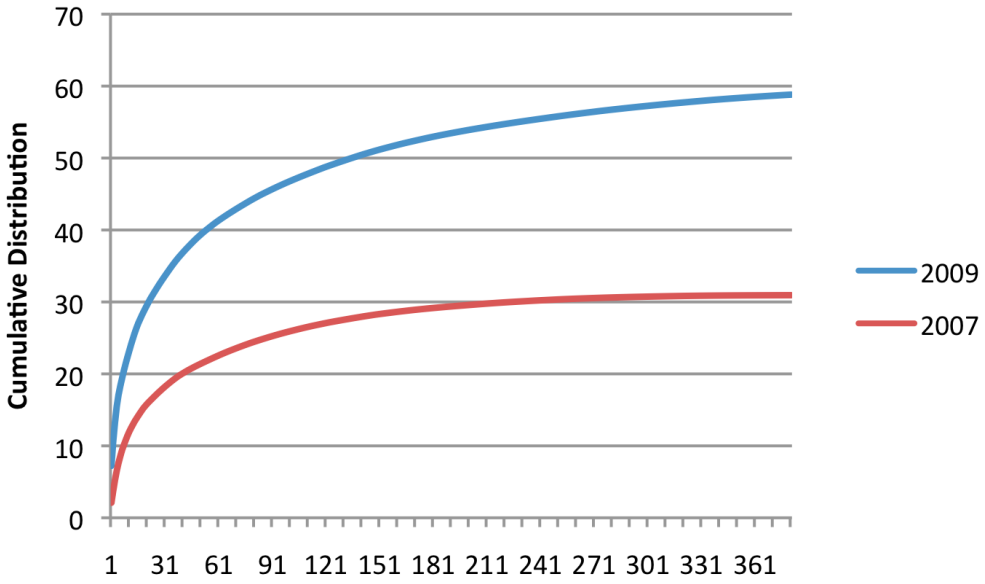

Abbildung 2: Anzahl ASN vs. Anteil am globalen inter-domain Verkehr, Quelle: [1]

Verkehr über die IXPs abgewickelt wird, und der Anteil weiterhin steigen wird. Dabei finden vor allem kleinere AS zunehmend Anschluss an ein IXP. Dies hat natürlich gravierende Auswirkungen auf Routing-Angriffe, da dadurch auch bereits kleine AS stark vernetzt sind und ihre Routen nicht mehr nur an einige wenige Upstream-Provider exportieren.

Es ist somit in der aktuellen Entwicklung ein Trend erkennbar, dass sich die Routing-Topologie von der hierachischen Struktur, wie sie das Tier-Modell beschreibt, immer stärker in Richtung einer vollvermaschten Struktur entwickelt.

Eine weitere wichtige Erkenntnis in dieser Arbeit ist die Konzentration der Verkehrsströme auf wenige große Teilnehmer. Immer weniger AS sind für einen immer größer werdenden Anteil am gesamten Internetverkehr verantwortlich, indem die Pakete entweder aus ihrem AS stammen oder dort enden. Abbildung 2 aus der Arbeit verdeutlicht dies anschaulich. Während im Jahre 2007 nach ihren Erkenntnissen noch ca. 211 der größten AS zusammen für 30% des weltweiten Internetverkehrs verantwortlich waren, verursachten 2009 bereits die 21 größten AS 30% des Verkehrs.

Ausgelöst wurde dieser Wandel durch neue bandbreitenintensive Dienste (z.B. Videodienste), die immer stärker nachgefragt werden. Ein Großteil des zusätzlichen Verkehrs fließt von den Inhalteanbietern, wie Google, Facebook oder den Content-Delivery-Netzwerken (CDNs), zu den klassischen Endkundennetzwerken und letztlich Privatanwendern. Das Geschäftsmodell dieser Inhalteanbieter bedeutet in der Regel, dass deren

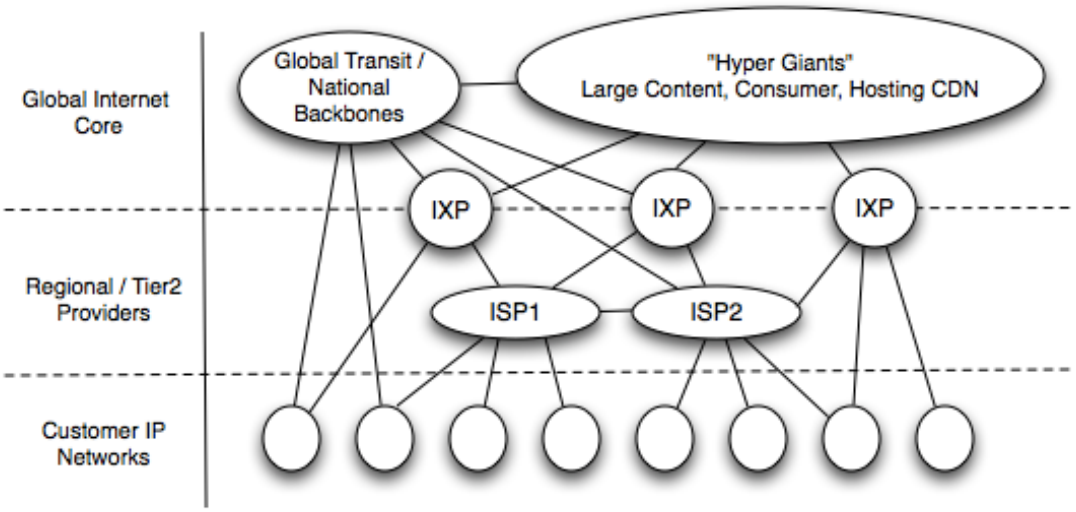

Abbildung 3: Aktuelle logische Routing-Topologie, Quelle: [1]

Einnahmen im direkten Zusammenhang mit der Verbreitung ihrer Inhalte stehen. Diese haben daher ein natürliches Interesse an einer möglichst ungehinderten und breiten Verbreitung ihrer Inhalte. Um dieses Ziel möglichst ungehindert erreichen zu können, verfolgen diese Akteure daher eine neue Strategie, die die alten Strukturen umgeht. Die Anbieter von Inhalten betreiben ein eigenes Backbone-Netz, über das sie in möglichst vielen IXPs den direkten Peering-Kontakt mit den Enkundennetzwerken suchen. Dabei umgehen sie die klassischen Strukturen der Tier-1, Tier-2 usw. -Anbieter.

Auf der anderen Seite stehen die klassischen Endkundenanbieter vor einem Problem durch den stark gesteigen Kosum von Inhalten durch ihre Kunden. Flatrate-Preise ermöglichen es kaum Kosten für den Ausbau der Infrastruktur an die Kunden weiterzureichen, gleichzeitig verlangen diese aber ungestörten Zugriffe auf die Inhalte. Sie sind daher gezwungen die ihre Bandbreite an den IXPs zu vergrößern.

Die Kombination dieser beiden Geschäftsmodelle hat zu einer neuen Art von Peering-Beziehungen geführt, welche umgekeht zu den klassischen Beziehungen funktioniert. Bei dem so genannten „Paid-Peering“ erhalten die Endkundennetzwerke Geld von den „Upstream“-Inhalteanbietern, damit diese die Inhalte ungestört verbreiten. Dies funktioniert nur durch direkten logischen Kontakt dieser ASes in einem oder mehreren IXPs. Dadurch werden die Inhalteanbieter zu so genannten „Hyper Giants“. Obwohl diese nach der Definition keine Tier-1-Provider sind, verhalten sie sich im Routing genauso, wie es die Tier-1-Provider tun.

Diese beiden Effekte zusammen haben in den letzten Jahren zu deutlichen Änderungen in den Strukturen des BGP-Routings geführt. Abbildung 3 zeigt die grundsätzliche neue Struktur die sich so ergeben hat. Insbesondere im Vergleich zu der vorher dargestellten Struktur in Abbildung 1 sind die Veränderungen sehr gut sichtbar. IXPs die wesentliche mehr Peerings auf allen Ebenen erlauben und „Hyper Giants“, die eine extrem

große Anzahl von Peering-Beziehungen aufweisen, sind für die großen Veränderungen verantwortlich. Dies führt zu einer insgesamt wesentlich stärker untereinander verbunden Routing-Topologie. Es ist der Trend zur vollvermaschten Topologie erkennbar.

2.3 Studie von H. Ballani et. al.

H. Ballani et. al. untersuchen in ihrer Arbeit [3] die Verbreitung von BGP-Pfad-Attacken in der Routing-Topologie, um abzuschätzen, welcher Anteil des Internetverkehrs sich auf diesem Wege von einem Angreifer an einer bestimmten Stelle in der AS-Topologie beeinflussen ließe. Dabei ist von besonderem Interesse, dass sie in ihrer Untersuchung zwischen dem *„Hijacking“* und dem *„Intercepting“* differenzieren und die Betrachtungen jeweils getrennt für beide Fälle durchführen.

Hijacking meint hier das Injizieren einer Route, die zur Unerreichbarkeit eines IP-Präfixes führt. Alle Daten, die durch die geschickte Manipulation durch das eigene AS geleitet werden verbleiben hierbei im AS des Angreifers, der sie entweder verwirft oder speichert und auswertet. Dieser Angriff ist technisch wesentlich einfacher durchzuführen, da man sich über die anschließende Weiterleitung der Daten während des Angriffes nicht zu kümmern braucht. Allerdings lässt sich diese Art eines Angriffes auch relativ leicht erkennen, da das Verkehrsvolumen bei dem Opfer zu Beginn des Angriffes relativ scharf abfällt.

Die zweite Art wird mit Intercepting beschrieben. Hierbei will der Angreifer nicht nur erreichen, dass andere die Route durch sein AS wählen, sondern den Verkehr auch anschließend zum Opfer weiterleiten. Dadurch, dass das Opfer weiterhin alle Datenpakete erreichen, ist diese Art eines Routing-basierten Angriffes westenlich schwerer zu entdecken, der übliche Abfall des Verkehrsvolumens entfällt. Ein Angreifer könnte diese Art für Man-In-The-Middle-Angriffe nutzten. Für den Angreifer ist diese Art aber auch technisch aufwendiger, da er sicherstellen muss, dass mindestens eine seiner Routen zu dem Opfer vom eigenen Angriff unbeeinflusst ist, so dass die Pakete ihr ursprüngliches Ziel auch erreichen können.

In dem Versuch, der von den Autoren zur Bestätigung durchgeführt wird, wird auch ein verteilter Angreifer genutzt, jedoch weder theoretisch noch methodisch wird dieser Ansatz in der restlichen Arbeit aufgegriffen und vertieft.

Diese Arbeit stammt aus dem Jahre 2007 und basiert auf dem Routing-Modell wie es Lixin Gao in ihrer Arbeit von 2001 beschreiben hat, welches ich in Abschnitt 2.1 vorgestellt habe. Es werden daher keine der im Abschnitt 2.2 benannten Veränderungen berücksichtigt.

3 Zusammenfassung + Ausblick

Das Internet hat heute eine Status, der es essentiell für die gesamte Gesellschaft macht. Sowohl Privatleute als auch Firmen sind im Alltag auf die korrekte Funktion des Internets angewiesen. Daher wird auf allen Ebenen des Protokollstapels permanent nach sicherheitsrelevanten Schwachstellen gesucht, entweder um sie zu nutzen oder um sie zu beheben. Während die Routing-Ebene dabei lange relativ unerkannt bliebe, wandert

diese langsam ebenfalls in den Blickpunkt. Dabei ist das BGP als einziges Inter-Domain-Routing-Protokoll eine besondere Schwachstelle, da es mehre konzeptionelle Angriffspunkte bietet. Während ein Teil davon durch neue Erweiterungen nun geschlossen werden, bleibt eine der Verwundbarkeiten weiter bestehen. Es ist daher von entscheidender Bedeutung diese Schwachstellen und die Auswirkungen von Angriffen auf ebendiese zu verstehen um sich selbst vor den Auswirkungen bestmöglich zu schützten. Gleichzeitig ist das Internet kein starres Gebilde, sondern im steten Wandel begriffen. Getrieben von neuen Geschäftsmodellen und geänderten Nutzerverhalten ist auch die Struktur des Internets im Laufe der Zeit permanenten Änderungen unterworfen. Wir müssen daher mit unserem Verständnis der Sicherheitsprobleme mit den Veränderungen Schritt halten und diese ebenfalls anpassen. Ebenso ist es nötig neue Angriffsideen zu beleuchten und ihre Implikationen zu verstehen.

In dieser Arbeit wurden drei Arbeiten beschrieben, die sowohl die Evolution des Internets der letzten 10 Jahre als auch den aktuellen Stand der Erkenntnisse von Angriffen auf die BGP-Infrastuktur zeigen.

Es besteht jedoch weiterhin Bedarf an Beschäftigung mit diesem Themengebiet, sowohl um vorhandene Erkenntnise auf die sich wandelden Strukture anzuwenden, als auch die Bereiche zu untersuchen, die bis jetzt noch nicht im Detail betrachtet wurden. So fehlt eine gründliche Analyse der Auswirkungen, wenn ein koordinierter Routing-Angriff von mehre als einem AS begangen wird.

Literatur

[1] C. Labovitz, S. Iekel-Johnson, D. McPherson, J. Oberheide, and F. Jahanian, "Internet Inter-domain Traffic," in *Proc. of the ACM SIGCOMM '10*. New York, NY, USA: ACM, 2010, pp. 75–86.

[2] Y. Rekhter, T. Li, and S. Hares, "A Border Gateway Protocol 4 (BGP-4)," IETF, RFC 4271, January 2006.

[3] H. Ballani, P. Francis, and X. Zhang, "A Study of Prefix Hijacking and Interception in the Internet," in *Proc. of SIGCOMM '07*. New York, NY, USA: ACM, 2007, pp. 265–276.

[4] M. Lepinski and S. Kent, "An Infrastructure to Support Secure Internet Routing," IETF, RFC 6480, February 2012.

[5] M. Wählisch, O. Maennel, and T. C. Schmidt, "Towards Detecting BGP Route Hijacking using the RPKI," in *Proc. of ACM SIGCOMM, Poster Session*. New York: ACM, August 2012, pp. 103–104. [Online]. Available: http://conferences.sigcomm.org/sigcomm/2012/paper/sigcomm/p103.pdf

[6] L. Gao, "On Inferring Autonomous System Relationships in the Internet," *IEEE/ACM Trans. Netw.*, vol. 9, no. 6, pp. 733–745, 2001.