Wirkungsanalyse von Routing-Angriffen im Internet

Seminarausarbeitung drittes Mastersemester

Jan Henke

Februar 2013

Master Informatik
Department Informatik
Fakultät Technik und Informatik
HAW Hamburg

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Einleitung

Das Internet ist heute eine kritische Infrastruktur[1]. Sowohl Unternehmen als auch Privatpersonen vertrauen mittlerweile in vielen Bereichen auf seine ständige Verfügbarkeit. Mit der steigenden Nutzung des Internets in allen Lebensbereichen hat auch die Bedeutung der über dieses Medium transportierten Daten enorm zugenommen. Beispiele sind Privatpersonen, die Einkäufe und Bankgeschäfte über das Internet abwickeln, oder Unternehmen, die zum Beispiel Firmengeheimnisse über das Internet zwischen ihren Standorten austauschen.

Die Sicherheit vor unberechtigten Ausspähen der übertragenen Daten war lange Zeit nicht wichtig, dies hat sich jedoch durch die Verbreitung in alle Lebenslagen des Menschen geändert. Die Sicherung der Datenströme im Internet vor unbefugten Zugriff stellt derzeit eines der größten Probleme des Internets dar. Während sich die Angriffe vielfach auf die verwendeten Anwendungen selbst konzentrieren, steigt die Anzahl der Angriffe auf die Infrastruktur des Internets. So ist die derzeit stattfindende Einführung von DNSSEC [2], um DNS Anfragen vor Manipulation zu schützen, ein deutliches Indiz für gestiegenes Interesse an der Sicherung der Kerninfrastruktur.

Besondere Bedeutung kommt im aktuellen Internet dem *Border Gateway Protocol* (BGP) [3] zu. Das BGP ist das derzeit einzige im Internet verwendete Interdomainrouting-Protokoll. Somit hängt die globale Erreichbarkeit im Internet direkt mit dem funktionieren des BGP ab. Gleichzeitig hat ein erfolgreicher Angriff auf BGP auch weitreichende Folgen, da alle darüberliegenden Schichten davon direkt betroffen sind. Teilnehmer, wie Privatleute oder Firmen ohne eigenes AS, können selbst keine Vorbeugung treffen können, da ihnen der Zugang zu dieser Ebene des Internets fehlt.

BGP wurde 1994 spezifiziert, als die Struktur des Internets noch bedeutend anders war. Es bestand kein Bedarf dafür kryptographisch sicher die Echtheit von empfangen Routen-Updates verifizieren zu können. Diese Design-Schwäche ist in der Fachliteratur bekannt und auch ausgiebig diskutiert worden. Das Internet jedoch ist kein statisches Gebilde. Insbesondere in den letzten Jahren gibt es einen deutlichen Topologiewandel zu einer immer stärker vermaschten Struktur zwischen den Teilnetzen [1]. Die Arbeiten auf diesem Gebiet stützten sich jedoch auf ein Strukturmodell, welches 2001 entwickelt wurde und nicht mehr zeitgemäß ist. Gleichzeitig gibt es mit dem *Resource Public Key Infrastructure*(RPKI)-Verfahren [4] einen Standard der versucht einen Teil der prinzipiellen Sicherheitsschwäche von BGP zu beseitigen. Damit ist zawr die Herkunft gesichert, jedoch bleibt der Pfad weiterhin ungeschützt.

Die Zielsetzung der anstehenden Masterarbeit ist es daher, die Auswirkungen der Strukturänderungen und von RPKI auf die bereits bekannten Angriffsarten zu untersuchen. Dabei liegt der Schwerpunkt besonders auf jenen Angriffen, welche von außen nur schwer zu detektieren sind und somit großen Schaden anrichten können.

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

2 Rückblick: Das Border Gateway Protocol

Zum Verständnis des weiteren Textes sind grundlegende Kenntnisse über die Funktionsweise des BGP und dem generellen Aufbau der Angriffe auf dieses erforderlich.

2.1 Protokollbeschreibung

BGP ist ein Pfadvektorprotokoll für IP-Präfixe. Es transportiert nicht nur Informationen über welche topologische Verbindung ein IP-Präfix jeweils zu erreichen ist, sondern zusätzlich auch den gesamten Pfad zu diesem IP-Präfix. Um die Beschreibung des Pfades möglichst kompakt zu halten bedient sich BGP einer Hierarchisierung durch die Einführung der so genannten Autonomen Systeme (AS). Ein AS ist dabei definiert als eine verbundene Gruppe von einem oder mehreren IP-Präfixen, welche von einem oder mehren Netzwerk-Operatoren betrieben wird und über eine einzelne und klar definierte Routing-Policy verfügt [5]. Jedes AS verfügt dabei über eine global eindeutige Nummer, die Autonomous System Number (ASN). Der Pfad in einer BGP-Update-Nachricht besteht aus einer Liste von ASNs die diese Route bis jetzt weitergeleitet haben. Die erste Nummer in dieser Liste kennzeichnet zwangsläufig jenes AS, welches das IP-Präfix besitzt und die Route zuerst bekanntgegeben hat. Dieses AS wird als das Origin-AS für dieses IP-Präfix bezeichnet.

Die Routing-Policy ist ein zentrales Element im Zusammenhang mit BGP. Über die Policy wird das Verhalten von BGP in vielen Bereichen bestimmt. Dadurch ist es möglich BGP so wohl in großen als auch in kleinen Netzwerken zuverlässig zu benutzten. Gleichzeitig muss das Erstellen und Bearbeiten der Policy von Hand erfolgen, so dass das Verhalten einzelner AS sich abhängig von der Erfahrung der Betreiber unterscheiden kann. Darüber hinaus lässt die Policy vielfältige Rückschlüsse auf das Geschäftsmodell des AS-Betreibers zu, daher sind diese in der Regel nicht öffentlich verfügbar.

Im BGP-Routing gibt es keine globale Sicht. Zum Einen ist von jedem AS aus ein anderer Pfad sichtbar, um ein bestimmtes Präfix zu erreichen. Zum Anderen ist es Routern erlaubt, mehrere Routen vor dem weiterleiten zu aggregieren oder zu deaggregieren. Durch das Zusammenfassen mehrerer zusammenhängender IP-Präfix zu einem einzigen Präfix kann die Anzahl der Einträge in den Routing-Tabellen gesenkt werden, was von allen Beteiligten bevorzugt wird. Jedoch ist es für nachfolgende AS dadurch nicht mehr möglich die genauen Strukturen vor der Aggregierung zu sehen. Deaggregierung ist allgemein nicht gewünscht, jedoch wird es teilweise genutzt, um Verkehrsströme über mehrere Verbindungen zu verteilen (Load-Balacing).

BGP Router arbeiten insgesamt mit vier Routen-Tabellen. Drei so genannte Routing-Information-Bases (RIBs), Adj-RIB-In enthält alle von Außen kommenden Routen, Loc-RIB alle für den Routing-Process in Frage kommenden Routen und Adj-RIB-Out alle Routen, die an andere Router exportiert werden. Welche Routen in die jeweils nächste Tabelle (Adj-RIB-In $\rightarrow$ Loc-RIB $\rightarrow$ Adj-RIB-Out) übernommen werden, ist durch die Policy des ASes definiert. Die vierte Tabelle ist die sogenannte Forward-Information-Base, welche für das eigentliche Routing genutzt wird. Sie enthält für jedes Prefix genau eine Route. Gibt es zu einem Präfix in der Loc-RIB mehr als eine Route definiert der

Standard eine Abfolge von Regeln (Tie-Breaking-Rules), mit denen schrittweise Routen ausscheiden werden, bis nur noch eine übrig bleibt um von der Loc-RIB in die FIB übernommen zu werden. Die erste dieser Regeln ist die Wichtigste und arbeitet mit der Länge des AS-Pfades, was vielfach schon reicht um eine einzelne (kürzeste) Route zu finden.

Erhält ein BGP Router ein Packet zum routen, so wird die Zieladresse mit den Präfixen in der FIB verglichen. Es wird dabei das spezifischte Prefäx aus der FIB ausgewählt, welches mit der Zieladresse übereinstimmt (Longest-Common-Prefix-Match). So können ASes Präfixe bekanntgeben und gleichzeitig Teilbereiche an andere AS delegieren, ohne das immer über das delegierende AS geroutet werden muss. Im Internet begrenzen die meisten ASes in ihrer Policy die maximal akzeptierte Präfix-Länge auf ein /24-Präfix, um die Größe der FIB zu begrenzen.

2.2 Angriffsvektoren auf BGP

Ziel eines jeden Angriffes auf Routing-Ebene besteht immer darin, den übrigen Teilnehmern des Routings gefälschte Informationen unterzuschieben, damit diese eine vom Angreifer gewünschte Routing-Entscheidung treffen. In der Regel wird ein Angreifer versuchen das Routing so zu beeinflussen, dass der Verkehr, welcher für ein bestimmtes IP-Präfix bestimmt ist, durch das AS des Angreifers gerouted wird. Der Angreifer kann daraufhin das angegriffene IP-Präfix unerreichbar machen, indem er alle Pakte für dieses Präfix einfach verwirft (*Blackholing*) eine Denial-of-Service-Attacke oder die Kommunikation zu diesem IP-Präfix belauschen indem er alle Packte, die durch sein AS fließen, mitschneidet(*Redirection*), Grundlage für Man-in-the-Middle-Attacken. Auf Basis des BGP gibt es dabei mehrere prinzipielle Vorgehensweisen.

1. Die Bindung zwischen Origin-AS und IP-Präfix wird aufgebrochen.
2. Der AS-Pfad wird manipuliert.
3. Die Verbreitung von Routen oder die Nutzung einzelner Links der Router wird durch die Verwendung von DoS-Attacken verhindert.
4. Verteilte koordinierte Angriffe

Ein Angreifer kann sich jedoch fremdes IP-Präfix aneignen, indem er Präfix und/oder Origin-AS in Routen-Updates fälscht. Um zum Beispiel das Präfix 198.51.100/24[2] zu kapern kann ein Angreifer sämtlichen BGP-Updates vor dem Weiterleiten den AS-Pfad entfernen und seine eigene ASN als einzige ASN und somit Origin-ASN eintragen. Alternative kann sich ein Angreifer die Longest-Common-Prefix-Match-Regel zu nutzte machen, indem er das Präfix deaggregiert in zwei Routen mit 198.51.100.0/25 und 198.51.100.128/25

[2]Sämtliche Beispiele in dieser Arbeit nutzen das für Dokumentationszwecke reservierte IP-Präfix 198.51.100.0/24[6]. Da es sich dabei um ein /24-Subnetz handelt enthalten die Beispiele auch Routen für kleine Subnetze, obwohl diese im Internet von vielen Anbietern nicht geroutet werden.

veröffentlicht. Da diese spezifischer als das /24 Subnetz sind, werden alle Router die neuen Routen bevorzugen. So geschehen zum Beispiel als Pakistan Telecom versehentlich das Präfix von YouTube weltweit kaperte und unerreichbar machte [7].

Die zweite Art einen Angriff auf BGP-Ebene durchzuführen besteht darin den AS-Pfad der Update-Nachrichten zu modifizieren, bevor „der Angreifer“ das Update an seine eigenen Peers weiterleitet. Laut dem Protokollstandard soll jeder Router vor der Weiterleitung in ein anderes AS seine eigene ASN an das Ende des AS-Pfades anhängen und kann gegebenenfalls noch mehrere Updates zu einem Update für ein kürzeres IP-Präfix aggregieren. Ein Angreifer jedoch kann noch weitere Änderungen durchführen. Zum Beispiel kann versucht werden, den Verkehr für das IP-Präfix durch das eigene AS routen zu lassen, indem man aus dem bisherigen AS-Pfad alle ASes zwischen dem eigenen und dem Origin-AS entfernt. Dadurch erscheint es für nachfolgende ASes, als ob der Angreifer eine direkte Verbindung zum Origin-AS hätte. Dies steigert die Wahrscheinlichkeit, dass andere AS die gefälschte Route wählen, da sie diese Verbindung für kürzer als andere Routen halten.

2.3 Die Resource Public Key Infratructure

Die Resource Public Key Infratructure(RPKI)[4] wurde im Februar 2012 standardisiert. Sie stellt einen Ansatz dar um einen Teil der möglichen Angriffe, die in Abschnitt 2.2 beschrieben sind, zu verhindern. RPKI definert so genannte *Route Origination Authorization* (ROA). Ein ROA enthält die Verbindung eines IP-Präfixes zu einer ASN, dieses wird anschließend mit einem Public-Key-Verfahren signiert. Der dafür notwendige Schlüssel wird dabei durch einen Baum von Signaturen authentifiziert. Diese startet Internet Assigned Numbers Authority (IANA) mit einem Wurzelzertifikat, dem alle uneingeschränkt vertrauen müssen. Damit sind die Zertifikate der Regional Internet Registries (RIRs) signiert. Die RIRs signieren schließlich die einzelnen ROAs. Die Validierung der ROA wird dabei aus Lastgründen häufig außerhalb der Router durchgeführt, so dass die Router auf eine Liste aller gültigen und validen ROAs zugreifen können.

Wird RPKI verwendet, so wird für jedes BGP-Update überprüft, ob es ein gültiges ROA für dieses Präfix gibt. Ist das der Fall, so wird das Update nur akzeptiert, wenn Präfixlänge und Origin-AS mit den Angaben aus dem ROA übereinstimmen, ansonsten wird es verworfen. Dies hat zur Folge, dass auch Fehlkonfiguration zu einem Ausfall eines IP-Präfixes führen kann [8]. Gleichzeitig macht es die Infrastruktur anfällig für externe Kontrolle. Das derzeitige Internet ist sehr dezentral aufgebaut. Bewusst einzelne ASes auszuschalten ist nur schwer zu erreichen. Das einfache in-validieren der Signatur aller ROAs, die zu einem bestimmten AS gehören, würde dieses AS effektiv ausschalten. Daher ist es derzeit nicht absehbar, ob RPKI in Zukunft global genutzt werden wird oder nicht.

RPKI bietet keine Möglichkeit AS-Pfad basierte Angriffe zu verhindern. RPKI verändert BGP nicht, es ist lediglich Teil der Routing-Policy ungültige Updates zu verwerfen. Eine Validierung des AS-Pfades jedoch würde eine Änderung von BGP erfordern und zusätzlich müsste jedes Element des AS-Pfades einzeln signiert werden, was viel zusätzliche Rechenleistung auf den Routern benötigen würde und daher auf breiten Widerstand trifft.

3 Rückblick: Die Routing-Struktur des Internets

Für die Betrachtung von Angriffen auf der Routing-Ebene kommt der Struktur des Internets aus Sicht des Routings eine besondere Bedeutung zu. Diese Struktur definiert sich dabei darüber, ob zwei AS eine Verbindung zueinander aufweisen und über diese Routen-Information austauschen (Peering). Ohne Wissen über diese Struktur kann nur eingeschränkt Aussage über die Auswirkungen von Routing-Angriffen getroffen werden.

Die Struktur ist dabei die Folge der Policy der jeweiligen ASes. Diese Policy wiederum resultiert aus den technischen Möglichkeiten und dem Geschäftsmodell des AS-Betreibers. Änderungen oder Neuerungen auf einem dieser beiden Gebiete ziehen daher auch Veränderungen in der Struktur des Internets nach sich.

Diese Struktur wird dabei häufig als gerichteter Graph beschreiben. Dabei sind die ASes die Knoten und die Verbindungen zwischen diesen die Kanten.

3.1 Das Tier-Modell

Die Grundlage zur Beschreibung der Routing-Struktur des Internet hat Lixin Gao 2001 gelegt [9]. Sie nutzte dafür empirische Daten aus Nordamerika aus dem selben Jahr. In der Arbeit wird gezeigt, dass die Beziehung auf der Routing-Ebene, das heißt, welche Routen ein AS zu einem anderen AS exportiert, direkt aus der wirtschaftlichen Beziehung zwischen den ASes folgt. Wenn der Routen-Export von der wirtschaftlichen Beziehung abweicht kommt es zu einer so genannten Routing-Anomalie.

Die Kernaussage dieser Arbeit besteht darin, dass die AS im Internet eine hierarchische Struktur bilden. Die Spitze bilden die so genannten Tier-1-Provider. Diese können jede IP-Adresse im Internet erreichen, ohne dafür zahlen zu müssen. Unterhalb der Tier-1-Provider gibt es die Tier-2-Provider, welche einen Tier-1-Provider für den Upstream-Zugang bezahlen und darüber das gesamte Internet erreichen können. Dies setzt sich über die weiteren Ebenen fort. Dabei werden jene AS, die primär Privatkundenanschlüsse bereitstellen häufig auch als Eyeball-Provider bezeichnet. Abbildung 1 stellt dieses Topologie-Modell dar.

Dieses Modell dient als Grundlage weiterer Arbeiten (z.B. [10]), jedoch haben sich seit dem Erscheinen der Arbeit von Gao neue Geschäftsmodelle im Internet gebildet, welche dort nicht berücksichtigt sind. Im Internet heute finden sich daher auch vermehrt Strukturen, welche von Gao nicht beschrieben wurden. Außerdem wurde das Modell ins besondere in der Betrachtung der US-amerikanischen Strukturen erstellt. In anderen Teilen der Welt haben sich durchaus andere Strukturen herausgebildet, so sind zum Beispiel in Europa Internet-Exchange-Points traditionell stärker verbreitet, als es in den USA der Fall war.

3.2 Einfluss der Content-Netzwerke und IXPs

Die Arbeit von Labovitz et.al. [1] aus dem Jahre 2010 ist eine neuere Untersuchung der Routing-Struktur des Internets. Es werden im Besonderen die Strukturen beschrieben, die sich durch neue Geschäftsmodelle gebildet haben.

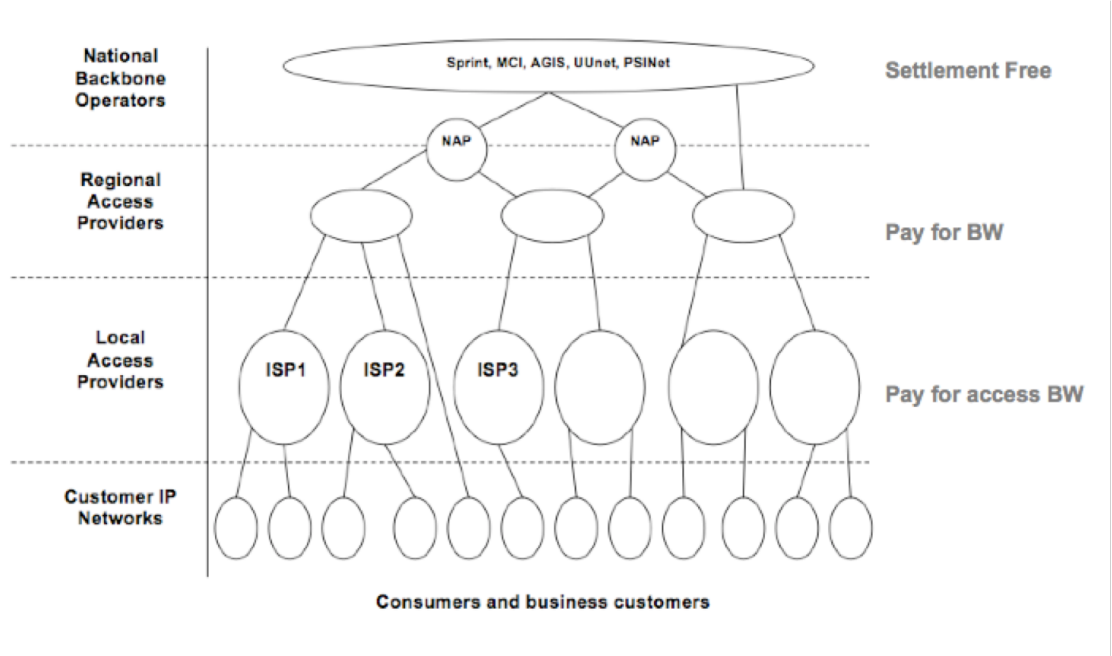

Abbildung 1: Klassische Routing-Topologie [1]

Eine der großen Veränderungen besteht darin, dass eine immer kleiner werdende Gruppe von ASes für einen immer größer werdenden Anteil am globalen Verkehr verantwortlich ist. Verantwortlichkeit meint damit, dass die entsprechenden Packte entweder an einer Adresse in diesem AS adressiert sind oder von diesem AS losgeschickt werden. Dieser Sachverhalt ist in Abbildung 2 an Hand von zwei Zahlenreihen dargestellt. Im Jahre 2007 wurden 30% des weltweiten inter-domain Verkehrs von etwa 230 der größten ASes verursacht. Im Jahre 2009 verursachten die 30 größten ASes bereits allein 30% des weltweiten Verkehrs.

Ursache dieser Entwicklung ist das Aufkommen und das schnelle Wachstum einer neuen Gruppe von ASes, den so genannten Content-Netzwerken. In diese Gruppe zählen zum Einen die Content-Delivery-Netzwerke (CDNs), zum Anderen Anbieter, wie Facebook und Google. Allen diesen Anbietern ist gemein, dass ihr Geschäftsmodell darauf basiert möglichst große Mengen von Inhalten an die Konsumenten auszuliefern. Entweder, weil dies als Dienstleistung verkauft wird (CDNs), oder, weil die Werbeeinnahmen mit der Anzahl der Seitenaufrufe skalieren.

Um das Ziel einer möglichst großen Verbreitung der eigenen Inhalte zu erzielen unterhalten diese Netzwerke meist etliche global verteilte Points-of-Presence mit eigenen Backbone-Kommunikation zwischen diesen Standorten. Dies ermöglicht ihnen somit an weltweit „vor Ort“ zu sein und niedrige Latenzen zu anderen Netzwerken aufrecht zu erhalten. Da die Konsumenten in der Regel zum größten Teil in den Eyeball-Netzwerken sitzen, ist für diese Gruppe natürlich die Verbindung zu den Eyeball-Netzwerken besonders wichtig. Daher gehen die Content-Netzwerke häufig auch direktes Routing mit den

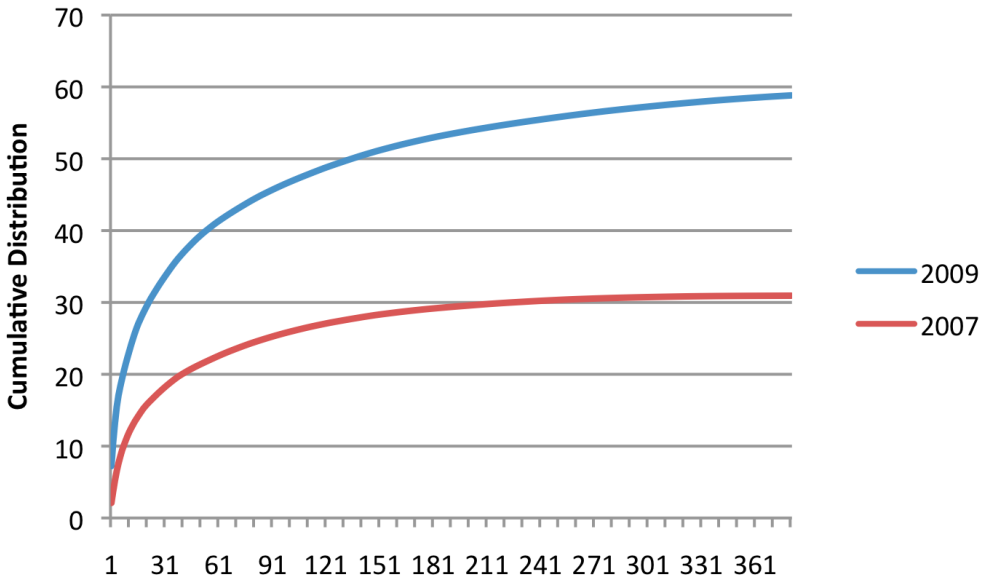

Abbildung 2: Anzahl ASN im Vergleich zu ihrem Anteil am globalen inter-domain Verkehr [1]

Eyeball-Providern ein, das sogenannte Paid-Peering. Insbesondere die Eyeball-Provider haben dies als Geschäftsmodell entdeckt, um an beiden Enden ihres Netzwerkes Geld zu verdienen.

Alle diese Faktoren führen dazu, dass die Gruppe der Content-Netzwerke von außen wie Tier-1-Provider erscheint. Sie verhalten sich jedoch anders und suchen direkte Verbindungen zu ASes, welche im Tier-Modell auf der untersten Stufe liegen. Aus Sicht der BGP-Sicherheit sind sie interessant, da diese Content-Netzwerke große Teile des Internets ziemlich direkt mit nur wenigen Routing-Hops erreichen können.

Die andere große Veränderung besteht darin, dass die Rolle der Internet-Exchange-Points (IXPs) stark zugenommen hat. Die IXPs kommen in dem Gao-Modell nicht vor. Peering ist mit deutlichen Kosten verbunden. Das AS benötigt eine direkte Anbindung an den Peering-Punkt, dort die nötige Routing-Hardware und entsprechende Wartung. Ohne die Nutzung von IXPs, wie es im Gao-Modell beschrieben ist, fallen diese Kosten für jede Peering-Verbindung einzeln an, so dass sich diese wirtschaftlich nur zwischen großen ASes lohnen und daher meist auf die Ebene der Tier-1 und Tier-2 Netzwerke beschränkt sind. Die technischen Vorteile von Peering-Verbindungen, redundante Verbindungen, Verteilung der benötigen Bandbreite auf mehrere Verbindungen, kürze Pfade, sind jedoch für ASes jeder Größe gegeben. Es wurde daher nach Wegen gesucht den Nachteil der hohen Kosten per-Verbindung zu reduzieren, das Ergebnis sind die IXPs.

IXPs bieten einen (mitunter über die Stadt verteilten) verteilte Standorte sowie eine Layer-2-Infrastruktur an. Jeder Interessierte Netzwerkbetreiber kann sich an diese Infrastruktur anschließen und darüber alle anderen Teilnehmer des IXPs erreichen. Über diese Infrastruktur ist es einfach möglich Peering-Verbindungen mit den anderen dort anwesenden ASes einzugehen, da bereits entsprechende Router und topologische Verbindungen bestehen. Dabei gibt es das „public Peering“, bei dem über einen zentralen Route-Reflektor alle ASes ihrer eigenen Präfixe und die ihrer Kunden miteinander austauschen, sowie das „private Peering“, bei dem eine Peering-Verbindung nur nach direkter expliziter Vereinbarung hergestellt wird. Auf diese Weise ist es auch kleinen und mittleren ASes möglich mit einmaligen Kosten leicht eine zweistellige Anzahl von Peering-Verbindungen einzugehen. Es wird daher zunehmend mehr des globalen Internetverkehrs über Infrastruktur von IXPs zwischen ASes ausgetauscht, wobei der IXP selbst im Routing nicht sichtbar ist.

Dies ist für die Betrachtung von Routing-Angriffen interessant. Es gibt im Routing sehr viel mehr Querverbindungen zwischen ASes auf der gleichen Tier-Ebene, besonders unterhalb der Tier-2-Provider, vergleichen mit dem Modell von Lixin Gao. Zusätzlich bietet die Verbreitung von IXPs Angreifern die Möglichkeit leichter Zugriff auf BGP-Ebene zu ihren Opfern zu erhalten. Es bedarf nur eines IXPs an dem das Opfer ein öffentliches Peering betreibt. In der Tat sind viele ASes bereit, im Prinzip mit jedem Interessenten am IXP ein Peering einzugehen, über welches ein Angreifer Transit-Routen bekannt geben kann.

Abbildung 3 zeigt die Struktur des Rotuing im Internet, wie man sie sich auf Grund der aktuellen Daten vorstellt. Vergleichen mit den traditionellem Tier-Modell (Abbildung 1) sind vor allem die von den Autoren „Hyper-Giants“ genannten Content-Netzwerke sowie die zusätzlichen Querverbindungen durch die IXPs hinzugekommen.

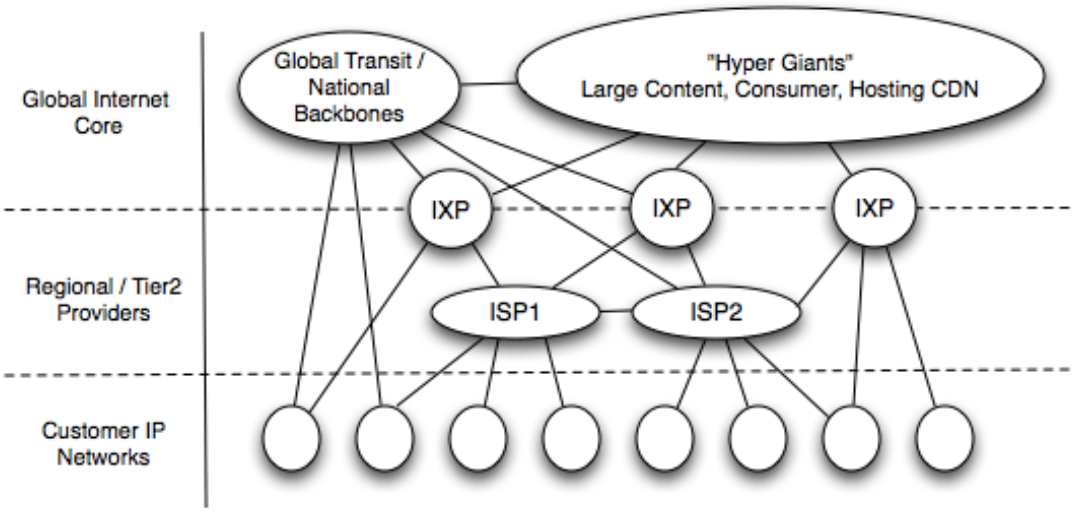

Abbildung 3: Aktuelle Routing-Topologie [1]

Es zeigt sich daher, dass bisherige Untersuchungen über die Reichweite von Routing-Angriffen ([10]), welche auf dem Gao-Modell basieren, auf das heutige Internet nur noch eingeschränkt angewandt werden können.

4 Masterarbeit

4.1 Ziele der Masterarbeit

In den vorherigen Abschnitten wurde dargelegt, dass sich auf der Ebene des Internet-Routings in den letzten Jahren starke Veränderungen ergeben haben. Es gibt neue Strukturen, die in den bekannten Modellen zu Angriffen auf der Routing-Ebene nicht ausreichend beachtet wurden, speziell RPKI, Content-Netzwerke, IXPs und koordinierte Angriffe zweier ASes. Ebenso wurde in des meisten bisherigen Modellen unterstellt, dass der Angreifer eine möglichst große Reichweite seines Angriffes erzielen möchte.

In Bezug auf RPKI ist die Frage zu klären, wie stark dieses wirklich die Möglichkeiten eines Angreifers einschränkt. Da RPKI wie erwähnt nur einen Teil der Sicherheitsprobleme abdeckt besteht die Vermutung, dass viele bekannte Angriffstechniken trotz Nutzung von RPKI weiterhin möglich sind.

Ein weiterer Punkt sind die Content-Netzwerke. Ihr Routing- und Peering-Verhalten unterscheidet sich von dem klassischer ASes gleicher Größe (Tier-1-Provider). Dies hat natürlich auch Auswirkungen auf die Abschätzung der Reichweite eines Routing-Angriffes. Insbesondere ist hier interessant, welche Auswirkungen eine Fehlkonfiguration hier haben könnte.

Des weiteren sind die IXPs in Zusammenhang mit den Routing-Angriffen ein interessantes Untersuchungsobjekt. Durch die wesentlich erhöhte Interkonnektivität, die sie

ermöglichen, bieten sie neue Verbreitungsmöglichkeiten und leichteren Zugang zu den Routing-Tabellen vieler Netzwerke. Auch dies hat deutliche Auswirkungen, die bis jetzt nicht untersucht wurden.

Während in den bisherigen Untersuchungen davon ausgegangen wurde, dass der Angreifer nur ein einzelnes AS unter Kontrolle hat um seinen Angriff durchzuführen, besteht eine weitere Interessante Frage darin, welche Möglichkeiten sich dadurch ergeben, wenn zwei ASes zusammenarbeiten um einen Angriff durchzuführen.

Neben diesen Erweiterungen bekannter Angriffs-Szenarios soll sich die Arbeit auch mit einem neuen Angriffsszenario beschäftigen, das in der Form bislang noch gar nicht untersucht wurde. Das Szenario wird in seinen Grundzügen in Abschnitt 4.2 erläutert.

Die Arbeit hat somit das Ziel Bedrohungsszenarien aufzuzeigen, so dass entsprechende Vorkehrungen dagegen getroffen werden können und ein Bewusstsein für die mögliche Bedrohung geschaffen wird.

4.2 Verborgenes Prefix-Hijacking

Eine wesentliche Grundannahme bei bisherigen Arbeiten zu diesem Themenkomplex besteht darin, dass als das Ziel eines Angriffes die möglichst komplette Übernahme der Kontrolle über ein bestimmtes IP-Präfix angenommen wird. Das heißt, alle Packte für IP-Adressen innerhalb dieses Präfixes sollen das AS des Angreifers passieren. In diesem Fall ist das Opfer in der Regel jenes AS, welches das gekaperte IP-Präfix besitzt. Als Clients kann man in diesem Zusammenhang jene ASes bezeichnen, die eine IP-Adresse aus dem Präfix erreichen möchten. Die Annahme besteht darin, möglichst vielen Clients eine gefälschte Route zu einem IP-Präfix eines Opfers glaubhaft zu machen.

Je nach Intention des Angreifers kann es jedoch auch von Vorteil sein, nur einem einzelnen Client andere Routen zu vielen verschiedenen IP-Präfixen glaubhaft zu machen. Vorteil besteht dabei in der wesentlich schwereren Nachvollziehbarkeit dieses Angriffes von außen. Außerdem lassen sich so wesentlich komplexe Manipulationen durchführen. Der Angreifer kann in seinem eigenen AS eine Schatteninfrastruktur aufbauen, die vom Rest des Internets nicht gesehen wird, dem einen Client gegenüber jedoch als Teil des normalen Internets vorkommt. Zum Beispiel kann der Angreifer neben der Phishing-Seite für Bankdaten auch Server bereithalten, die die Gültigkeit eines gefälschten TLS-Zertifikats bestätigen. Dies kann erreicht werden, indem die Anfrage nach einer Certificate-Revocation-List ebenfalls vom Angreifer beantwortet wird. Im dem genannten Beispiel eines Phishing-Angriffes könnten vor allem die privaten Internetanschlüsse das Ziel sein. Da viele ISPs die verschiedenen Privatkunden in eigene regionale ASes organisiert haben, ist diese Art von Angriff noch schwerer zu entdecken.

4.3 Vorgehensweise und Risiken

Die weitere Vorgehensweise zur Erstellung der Arbeit sieht wie folgt aus. Zunächst werden im Rahmen der Projektarbeiten vollständige Angriffsszenarios entwickelt. Der Schwerpunkt liegt dabei eindeutig auf den speziellen Punkten, die als Ziele der Arbeit genannt wurden. Diese Szenarios enthalten dabei die beteiligten Akteure, ihre Routing-

Beziehungen zueinander und eine theoretische Vorsage des erwarteten Ergebnisses in Bezug auf die Auswirkungen und die Reichweite des Angriffes.

Danach ist es das Ziel, die Vorhersage durch das Sammeln von Daten zu bestätigen. Dadurch erhält man eine belastbares Vorhersagemodell für zukünftige ähnliche Angriffe. Zum Sammeln von Messdaten gibt es dabei zwei mögliche Datenquellen, die für die Arbeit kombiniert verwendet werden sollen. Zum Einen sind das die Daten, welche von dem Forschungsprojekt „Peeroskop“ gesammelt werden. Zum Anderen werden aktiv Messungen durchgeführt, indem die entsprechenden Angriffsszenarios in einer kontrollierten Art und Weise durchgeführt werden. Dazu wird zunächst die prinzipielle Funktionsweise an einem Testaufbau im Labor verifiziert und anschließend die Daten mit Hilfe der für Testzwecke im Internet betriebenen ASes gesammelt.

Risiken bestehen dabei in der Abschätzung des Zeitbedarfs, der Komplexität der Messungen bzw. der Datensammlung und schließlich in der Frage, ob die betrachteten Modelle und gesammelten Daten sich so auch auch Situationen außerhalb der Laborbedingungen übertragen lassen. Insbesondere können sich im Internet einzelne ASes anders verhalten, als man es erwartet, da die Routing-Policies normalerweise nicht öffentlich bekannt sind.

5 Fazit

Das Internet ist ein komplexes Gebilde, dessen Funktionsweise von den verwendeten Routing-Protokollen abhängt. Im heutigen Internet wird für das inter-domain-Routing nur das Border-Gateway-Protocol verwendet. Dieses weist bekannte Sicherheitsschwachstellen auf, die Konsequenz des Protokoll-Designs sind und sich daher nicht so einfach beheben lassen. Es existieren bekannte Beispiele, dass diese Sicherheitslücken auch ausgenutzt werden, um den Weg von Verkehrsströmen im Internet zu beeinflussen. Das Internet ist jedoch kein statisches Gebilde, sondern permanentem Wandel unterworfen, getrieben von neuen technischen Möglichkeiten und Geschäftsmodellen. Dieser Wandel in der Struktur hat auch Auswirkungen auf die Funktionsweise von Angriffen auf BGP. Um daher Angriffe in Zukunft besser verstehen zu können ist es nötig in der Master-Arbeit die Auswirkungen zu Untersuchen und neue Vorhersagemodelle für diese zu entwickeln. Damit ist dann auch ein besserer Schutz in der Zukunft möglich.

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] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose, "DNS Security Introduction and Requirements," IETF, RFC 4033, March 2005.

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

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

[5] J. Hawkinson and T. Bates, "Guidelines for creation, selection, and registration of an Autonomous System (AS)," IETF, RFC 1930, March 1996.

[6] J. Arkko, M. Cotton, and L. Vegoda, "IPv4 Address Blocks Reserved for Documentation," IETF, RFC 5737, January 2010.

[7] M. A. Brown, "Pakistan hijacks YouTube – Renesys Blog," February 2008. [Online]. Available: http://www.renesys.com/blog/2008/02/pakistan-hijacks-youtube-1.shtml

[8] 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

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

[10] 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.