Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Grundseminar

Möglichkeiten zur Sicherung des Internet-Routing

Colin Sames

bei
Prof. Dr. rer. nat. Thomas Lehmann
und
Prof. Dr. Axel Schmolitzky

19. März 2017

Inhaltsverzeichnis

1 Einleitung

Während das Browsen im Internet wenig Gefahr für Leib und Leben darstellt, so sind es die persönlichen Daten, die für Politik und Wirtschaft von Interesse geworden sind. Versuchen zu schützen kann sich der Einzelne, indem er darauf achtet, welche Informationen er online öffentlich darstellt. Neben den persönlichen Daten gibt es Daten, die vom Internetnutzer häufig übersehen werden, Metadaten. Für bestimmte Gruppen oder Organisationen kann es von großem Interesse sein, wer, wann eine Website besucht hat. In Ländern, in denen das Internet stark zensiert und überwacht ist, mag es vielleicht schon reichen zu wissen, *ob* eine Person eine Website besucht hat, unabhängig davon, *was* sie dort gemacht hat. Daher ist es wichtig Internet-Routing für Dritte so unangreifbar wie möglich zu machen.

2 Internetverkehr und Sicherheit

2.1 Was ist Internetverkehr?

Auf tiefer Ebene betrachtet ist das Internet das Versenden und Empfangen von Daten zwischen Clients und Server. Diese Daten werden als Pakete bezeichnet und sie enthalten, je nachdem von welcher Anwendung aus sie gesendet wurden, unterschiedliche Inhalte. Beim Aufrufen einer Website in einem Browser werden Pakete mit dem Inhalt der Website vom Webserver an den Client geschickt, der diese Seite angefragt hat. Diese Pakete werden an die entsprechende lokale Anwendung weitergeleitet.

Der Verkehr zwischen Client und Server, wird über Router geregelt. Router enthalten interne Listen, die ihnen sagen, an welchen nächsten Router die Pakete geschickt werden sollen, damit sie letztlich ihr Ziel erreichen.

2.2 Was ist Internetsicherheit?

Sicherheit im Internet bedeutet, Clients und Server gegen Angriffe von Dritten zu sichern, seien es Spionage oder manipulative Angriffe. Im Zusammenhang mit dem Internetverkehr müssen Sicherheitsvorkehrungen existieren, die einen gesicherten Ablauf der oben beschriebenen Prozesse gewährleisten. Dabei soll der Blick nicht auf die Sicherheit lokal beim Client oder Server gerichtet werden, sondern auf die Übertragungswege. Router zum Beispiel, die für Weiterleitung des traffics zuständig sind, sind anfällig gegen Fehlkonfigurationen. Dabei ist es unabhängig davon, ob diese Konfiguration absichtlich fehlerhaft ist, oder nicht. Nameserver könnten von Dritten übernommen und manipuliert werden. Es gibt Möglichkeiten gegen solche Angriffe auf Router oder Nameserver vorzugehen.

3 Domain Name System

3.1 Navigation im Internet

Bevor ein Client eine Website aufrufen kann, muss die IP-Adresse des Servers herausgefunden werden. Der Name einer Internetadresse, z.B. www.inet.haw-hamburg.de, ist lediglich eine lesbare Übersetzung von dem für Menschen weniger leicht zu merkenden IP-Adressen, in diesem Fall 141.22.28.254.

Um dem Umwandlungsprozess anzustoßen, wird vom Client der Resolver angestoßen. Der Resolver fragt an entsprechende Nameserver die einzelnen Komponenten der URL an, beginnend von hinten mit de.

Um den Traffic von Nameservern zu reduzieren werden Anfragen gecached, damit der Auflösungsprozess des Resolvers bei häufig besuchten Webseiten wie www.google.de nicht jedes Mal erneut angestoßen werden muss. Ein Nameserver kann einen anderen Server nach einer Adresse anfragen und eine Antwort bekommen, z.B.

Nameserver A: *"Wie lautet die IP-Adresse von www.inet.haw-hamburg.de"*
als Antwort kommt

Nameserver B: *"Die IP-Adresse von www.inet.haw-hamburg.de lautet 141.22.28.254"*
Nameserver A kann den Eintrag nun cachen, um bei einer Anfrage durch einen Resolver gleich eine Antwort liefern zu können. Caching ist jedoch mit Risiken verbunden, da es Angriffe gibt, die es erlauben gefälschte Einträge in den Cache zu injizieren.

3.2 Risiken durch Caching

Das Fälschen von Cache-Einträgen wird Cache-Poisoning oder DNS-Spoofing genannt. Hierbei muss ein Angreifer einen Nameserver unter seine Kontrolle bringen. Gelingt ihm dies, kann er von dem gehackten Nameserver aus andere Nameserver angreifen. Um den Cache zu manipulierenn muss der Angreifer nun lediglich eine Antwort auf eine nicht gestellte Frage an einen Anderen Nameserver senden, etwa

Gehackter Nameserver: *"Die IP-Adresse von www.inet.haw-hamburg.de lautet XYZ"*

wobei XYZ die IP-Adresse des Angreifers ist. Der Nameserver, der nun diese Antwort auf eine nicht gestellte Frage bekommt, cached diese. Ein Resolver, der jetzt eine Anfrage an den Nameserver sendet, bekommt die gefälschte IP-Adresse des Angreifers zurück. Somit gelingt es einem Angreifer beispielsweise, Anfragen auf bestimmte Seiten auf seine eigene umzuleiten (Steinhoff u. a., 2006).

Um gegen derartige Angriffe sicher zu sein, gibt es einige Verbesserungen von DNS. Eine von diesen ist DNSSEC (siehe 4.2). Zunächst muss in diesem Zusammenhang jedoch auf Public Key Infrastructures eingegangen werden.

4 Public Key Infrastructure

Eine Public Key Infrastructure (PKI) ist eine Struktur, in der kryptografische Zertifikate ausgestellt und verwaltet werden. Ein typisches Beispiel hierfür findet sich innerhalb einer Zertifizierungsstelle (engl. Certification Authority, CA). Eine CA stellt digigale Zertifikate für die Mitarbeiter eines Unternehmens aus. Diese Zertifikate werden für E-Mail-Verschlüsselung verwendet. Nachrichten können mit Hilfe einer CA zudem auf Authentizität geprüft werden. Zertifikate erlauben es digitale Unterschriften an eine Mail anzuheften. Der Empfänger kann diese Unterschift durch die CA prüfen lassen (Schmeh, 2013).

Es ergibt sich eine Hierarchie zwischen CA und Unternehmen. Die CA steht hierbei über dem Unternehmen. Untersteht der CA dabei einer weiteren, übergeordneten CA, wird das Vertrauen weitergegeben. Das bedeutet für das Unternehmen folgendes: vertraut es der CA die in Anspruch genommen wird, so vertraut es allen CA die hierarchisch über diese CA stehen. Eine Vertrauenskette wird aufgebaut, die für PKIs typisch sind.

4.1 Hierarchie im Internet

Im Internet findet sich in einigen Bereichen eine hierarchische Struktur wieder. Diese ist unabhängig vom Routing des Verkehrs und bezieht sich mehr auf die Verwaltung von Adressbereichen.

Ein Internet Service Provider (ISP) verfügt über einen zugeteilten Raum an IP-Adressen, die er an seine Kunden vergeben kann, z.B. alle Adressen im Bereich 46.59.128.0/17[1]. Dieser Bereich wird dem ISP von einer Regional Internet Registry (RIR) zugewiesen. Insgesamt existieren fünf RIRs, jede ist für einen Kontinent zuständig. Für Europa ist es die Réseaux IP Européens Network Coordination Centre (RIPE NCC). RIPE NCC wiederum bekommt die Adressbereiche, die sie vergeben darf, von der Internet Assigned Numbers Authority (IANA), der höchsten Instanz, zugewiesen. So wird eine Hierarchie von der IANA aus bis hin zum ISP/zur Hochschule/Universität/zum Unternehmen aufgebaut.

[1] Adressbereich von Willy Tel, Stand Juli 2016

4.2 DNSSEC

Die beschriebene PKI lässt sich auf die Hierarchie im Internet anwenden, ähnlich wie bei einer Zertifizierungsstelle. Die IANA bildet hierbei die Root-Stelle und vergibt Zertifikate an Nameserver in bestimmten Gebieten. Diese fungieren wieder als übergeordnete Instanzen über weiteren Nameservern. So baut sich eine Vertrauenskette auf. Angeforderte Routen können mittels Prüfsummen dieser Zertifikate überprüft werden.

Leider bringt DNSSEC einen erheblichen Mehraufwand mit sich. Server müssen aufwendig konfiguriert werden, was sehr fehleranfällig ist. Zudem müssen die Zertifikate häufig erneuert und verteilt werden. Aufgrund dessen findet DNSSEC noch eher verhalten Anwendung.

5 Border Gateway Protocol

5.1 Funktionsweise

BGP-Router enthalten Listen nach denen sie entscheiden, an welches AS sie ein Paket als nächstes schicken müssen. In diesen Listen sind Einträge, welche Adressbereiche (Prefix) zu welchem AS gehören. Diese Listen ändern sich laufend, daher senden BGP-Router Updates an andere BGP-Router. Diese Updates enthalten neue Prefixes, sollte sich z.B. der Adressbereich geändert haben. Empfangene Updates werden von den Routern bedingungslos angenommen.

5.2 Prefix-Hijacking

Dieses bedingungslose Verhalten lässt Fehler und Angriffe zu. Annonciert ein BGP-Router fälschlicherweise einen zu großen Adressbereich, so verbreitet sich der Fehler schnell im Internet. Die Folge davon ist, dass viele Verbindungen über das AS, welches den Fehler begangen hat, geroutet werden.

Im Falle eines gewollten Angriffes könnte ein AS nun gefälschte BGP-Updates in den Umlauf bringen und somit erhebliche Teile des Traffics auf sich umleiten. Die empfangenen Pakete können beispielsweise gedropped werden (Black Hole Attack) oder schlicht abgehört und weitergeleitet werden (Karlin u. a., 2008; Zhao u. a., 2002).

6 BGPSEC

6.1 Resource Public Key Infrastructure

Wie bei DNSSEC werden auch bei BGPSEC Zertifikate durch die IANA erzeugt und nach unten an die RIRs und die weiter unten liegenden Autonomen Systeme verteilt. Der Unterschied hier liegt in den Informationen, welche die Zertifikate zusätzlich enthalten. Neben dem kryptografischen Inhalt werden dem Zertifikat die Prefixes des AS angehängt, für das es erstellt wird. Das erzeugte Zertifikat wird anschließend in der Resource Public Key Infrastructure (RPKI) hinterlegt. Bekommt ein BGP-Router ein BGP-Update, in dem steht, das eine AS ein neues Prefix annoncieren möchte, so kann der Router eine Anfrage an die RPKI stellen und überprüfen, ob das AS autorisiert ist, das bekannt gegebene Prefix für sich zu beanspruchen. Ist es in dem Zertifikat enthalten, wird das Update übernommen, andernfalls nicht.

6.2 Probleme

BGPSEC hat Schwierigkeiten sich zu verbreiten. Der Grund dafür ist ein Ähnlicher wie bei E-Mail-Verschlüsselung. Wenn es niemand nutzt, bietet es dem Einzelnen keine Vorteile. Die Motivation es einzusetzen ist demnach sehr gering (Goldberg, 2014). Weitere Gründe, warum etwa Content Delivery Networks gehemmt sind, auf Standards wie BGPSEC umzusteigen, müssen in den kommenden Jahren analysiert werden (Wählisch u. a., 2015).

7 Ausblick

Die vorgestellten Möglichkeiten zu Sicherung des Routingverkehrs unterlaufen einem stetigen Verbesserungsprozess. Sie müssen auf Fehler und Anwendbarkeit hin geprüft werden, damit eine breitere Anwendungsbereitschaft sichergestellt werden kann. Die Internet Engineering Task Force (IETF) tagt regelmäßig an verschiedenen Orten auf der Welt, um gemeinsam Technologien wie DNSSEC und BGPSEC in Papern zu standardisieren. Es lässt sich somit vermuten, dass die Ausweitung stetig stattfindet. Jedoch müssen noch Problemfelder analysiert werden, damit eine kontinuierliche Optimierung sichergestellt werden kann.

8 Fazit

Internetsicherheit ist heutzutage unabdingbar, wenn es um die Privatsphäre der Anwender geht. Gerade die Bereiche, auf die der Anwender keinen oder nur sehr wenig Einfluss hat, müssen besondern beachtet werden, da er sich sonst nicht vor Angriffen von Dritten schützen kann.

Im Rahmen des Grundseminars habe ich mich das Thema Internetsicherheit angenommen, da ich ein persönliches Interesse für diese Thematik hege. Dieses eher unscheinbare Gebiet der Internetsicherheit bietet viele Facetten. Die Forschungseinrichtung der HAW *inet* ist aktiv und nah an der Entwicklung beteiligt, ich konnte und kann noch viel von den Mitarbeitern dort lernen.

Literaturverzeichnis

[Goldberg 2014] Goldberg, Sharon: Why Is It Taking So Long to Secure Internet Routing? In: *Queue* 12 (2014), August, Nr. 8, S. 20:20–20:33. – URL http://doi.acm.org/10.1145/2668152.2668966. – ISSN 1542-7730

[Karlin u. a. 2008] Karlin, Josh ; Forrest, Stephanie ; Rexford, Jennifer: Autonomous security for autonomous systems. In: *Computer Networks* 52 (2008), 10, Nr. 15, S. 2908–2923. – URL http://www.sciencedirect.com/science/article/pii/S138912860800203X. – Zugriffsdatum: 2016-07-01

[Schmeh 2013] Schmeh, Klaus: *Kryptografie*. 5. dpunkt.verlag, 2013

[Steinhoff u. a. 2006] Steinhoff, U. ; Wiesmaier, Alexander ; Araújo, Roberto ; Lippert, Marcus: The State of the Art in DNS Spoofing. In: Zhou, Jianying (Hrsg.) ; Yung, Moti (Hrsg.) ; Bao, Feng (Hrsg.): *4th International Conference on Applied Cryptography and Network Security (ACNS'06)*, 2006, S. 174–189

[Wählisch u. a. 2015] Wählisch, Matthias ; Schmidt, Robert ; Schmidt, Thomas C. ; Maennel, Olaf ; Uhlig, Steve ; Tyson, Gareth: RiPKI: The Tragic Story of RPKI Deployment in the Web Ecosystem. In: *Proc. of Fourteenth ACM Workshop on Hot Topics in Networks* (2015), 11. – URL https://inet.haw-hamburg.de/papers/wssmu-rtsrd-15.pdf. – Zugriffsdatum: 2016-06-23

[Zhao u. a. 2002] Zhao, Xiaoliang ; Pei, Dan ; Wang, Lan ; Massey, D. ; Mankin, A. ; Wu, S. F. ; Zhang, Lixia: Detection of invalid routing announcement in the Internet. In: *Dependable Systems and Networks, 2002. DSN 2002. Proceedings. International Conference on*, 2002, S. 59–68