BGP Hijacking

Mark Klement*[1]

*Chair for Cybersecurity, Goethe-University Frankfurt
[1]s6840520@stud.uni-frankfurt.de

Abstract

Ziel dieses Papers ist es die systematischen Schwächen des Border Gateway Protokolls (BGP) zu beleuchten. Es soll die Frage geklärt werden, welche Ursachen den Schwächen des Protokolls zugrunde liegen und welche Ansätze es zur Lösung dieser gibt. Zunächst soll die Herkunft und der Stellenwert des Protokolls für moderne, verteilte Informationssysteme erklärt werden. Anschließend wird anhand eines realen Vorfalls verdeutlicht, wie die beschriebenen Schwächen des Protokolls zum Problem werden können. Schlussendlich folgt eine Beschreibung von Methoden und Mechanismen, die dabei helfen sollen, das Protokoll und dessen Verwendung sicherer zu gestalten.

1 Introduction

Das Border Gateway Protokoll (kurz BGP) ist eines der wichtigsten Protokolle für das moderne internet. Es dient der Erstellung von routing Tabellen, die verwendet werden, um Pakete und Daten auch in beliebig großen Netzwerken möglichst effizient zwischen Absendern und Empfängern zu vermitteln. Im Wesentlichen besitzen Gateway Protokolle zwei verschiedene Ausprägungen, die sich darin unterscheiden, ob es sich um das Routing innerhalb eines Autonomen Systems oder zwischen verschiedenen Autonomen Systemen handelt. Innerhalb eines Autonomen Systems (kurz AS) werden sogenannte Internal Gateway Protokolle (kurz IGPs) verwendet, während für den Aufbau der Routing Tabellen zwischen den Autonomen Systemen Exterior Gateway Protokolle (kurz EGPs) verwendet werden.

Vorsicht: EGP kann sowohl eine Klasse von Protokollen als auch ein bestimmtes Protokoll bezeichnen. Das Protokoll EGP ist quasi der Vorgänger des BGP.

2 Das Border Gateway Protokoll

Mit der fortschreitenden Verbreitung des Internets und der damit einhergehenden Zunahme an Größe und Komplexität stieg die Notwendigkeit einen Nachfolger für das ursprüngliche EGP zu finden. Das Hauptziel bei der Entwicklung des BGP war es ein Protokoll zu erschaffen, das zuverlässig in besonders großen und komplexen Netzwerken funktioniert. Das bedeutet, dass das Protokoll in Bezug auf seinen (kommunikativen) Overhead möglichst effizient funktionieren soll und dabei gleichzeitig eine hohe Flexibilität bei der Erstellung der Routingtabellen und Nutzung des Netzwerkes ermöglicht.
Tatsächlich ist genau diese Effizienz- und Flexibilitätsanforderung die Hauptursache der Schwächen des Protokolls. Diverse Sicherheitsmaßnahmen wie kryptografische Verschlüsselungen, ausstellung von Zertifikaten oder ähnliches kosten wertvolle Systemressourcen. Je nach Verfahren kann es sich bei diesen Ressourcen um Speicherplatz oder Rechenleistung handeln. Was in kleinen Netzwerken möglicherweise noch vertretbare Aufwände sind, kann in einem sehr großen Netzwerk oder gar dem globalen Internet sehr schnell zu einem unüberwindbaren Hindernis werden. Sicherheit und Effizienz/ Geschwindigkeit sind in der Praxis oft zwei Anforderungen, die nur schwer gleichzeitig erfüllbar sind. Entsprechend waren in der "Basisversion" des BGP so gut wie keine nennenswerten Sicherheitsmechanismen integriert, da diese der Geschwindigkeitsanforderung an das Protokoll im Wege stehen würden.

3 Austausch von BGP Informationen

In seiner ursprünglichen Form funktioniert der Austausch von BGP Daten quasi auf Vertrauensbasis, da das Unterlassen einer stringenten Prüfung der versendeten/ erhaltenen Daten beträchtliche men-

gen an Systemleistung einspart. Die dedizierten BGP Router, die die ASes miteinander verbinden, informieren sich also gegenseitig darüber, mit welchen ASes sie jeweils verbunden sind. In einer Kette von 3 ASes (Bspw. AS 1, AS 2 und AS 3 mit AS 2 in der Mitte) würde AS 2 die jeweils Anderen darüber informieren, dass AS 1 und AS 3 via AS 2 miteinander kommunizieren können. So lange es keine Bad-Actors in diesem System gibt funktioniert dies sowohl zuverlässig als auch effizient.

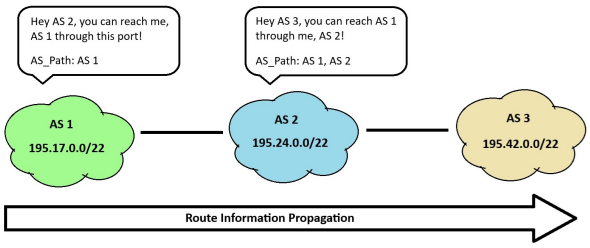

Figure 1: ASes exchanging Routing information

Problematisch wird ein Verfahren auf Vertrauensbasis aber logischerweise immer dann, wenn sich Akteure mit bösen Absichten in das System einschleichen. Die Einfachheit diese Vertrauensbasis auszunutzen gepaart mit der Tatsache, dass die BGP-Router wie Weichen für große Mengen an Traffic funktionieren, machen dieses Protokoll extrem interessant für Hacker. Durch das Verbreiten falscher BGP Informationen können auf einen Schlag riesige Mengen an Traffic umgeleitet werden. Traffic kann entweder manipuliert und/oder über unnötig lange Schleifen ans Ziel geführt, oder sogar gänzlich ins Nichts geroutet werden. Die Motive dafür sind vielfältig und reichen von der Absicht der Sabotage von Services oder Netzwerken (DOS Angriffe) bis hin zu staatlich organisierter Spionage.

4 Typen und Ablauf eines Angriffs

4.1 Spezifischeren Adressraum announcen

Generell bevorzugen Router bei der Erstellung ihrer Routingtabellen möglichst präzise Announcements. Ein Announcement wird immer dann präziser, wenn der Prefix in der CIDR Notation länger , also die Zahl nach dem "/" größer wird.

Beispiel:

`192.232.0.0/22` → less precise

`192.232.0.0/24` → more precise

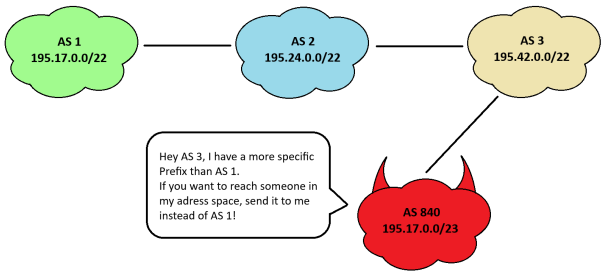

Figure 2: Prefix hijack

Je präziser die Prefixes in den Announcements sind, desto kleiner ist automatisch der Adressraum, der in dem Prefix enthalten ist. Das kann für einen Angreifer einen Nachteil darstellen, wenn er einen möglichst großen Adressraum angreifen will aber die Empfänger seiner Announcements alle zu unspezifischen Announcements verwerfen. Um sein Ziel dann zu erreichen muss er eine auffällig hohe Menge an sehr spezifischen Announcements versenden, was schnell dazu führen kann, dass der Angriff als solcher erkannt wird.
Wie wir in dem im folgenden Kapitel beschriebenen Fallbeispiel erkennen werden, kann diese Methode aber auch von legitimen ASes verwendet werden, um den gekaperten Adressraum zurückzuerobern.

4.2 Kürzeren AS_Path announcen

Ein weiteres extrem relevantes Attribut bei der erstellung der Routingtabellen ist der sogenannte "AS_Path" und seine Länge. Das BGP soll möglichst effizient, aber auch flexibel und dynamisch sein. Aus diesem Grund werden Routen mit kurzem AS_Path gegenüber denen mit langem Pfad bevorzugt. Die Grundidee ist, dass ein kürzerer Pfad weniger Hops bedeutet, was die Anzahl der potenziellen points of failure auf der Route, den kommunikativen Overhead und auch (wahrscheinlich) die Latenz reduziert.
Nicht nur Angreifer, sondern auch legitime ASes können dieses Attribut "manipulieren". Legitime ASes können den Pfad beispielsweise künstlich verlängern, indem sie ihre eigene AS_Number mehrfach hintereinander in den Pfad schreiben, um

anderen mitzuteilen, dass zwar ein Pfad durch ihr Netzwerk existiert, dieser in der Praxis aber nicht genutzt werden soll. Dieses Vorgehen dient oftmals der Umsetzung von routing Policies und wird “ Path prepending” genannt.

Angreifer können dieses Prinzip ausnutzen, indem sie behaupten, dass sie einen Weg zu einem bestimmten AS kennen, der viel kürzer ist als alle anderen bisher bekannten Wege. Um der Effizienzanforderung nachzukommen liegt es dann im Interesse der anderen ASes diesen kurzen Pfad zu übernehmen und ihren Traffic dem Angreifer zu schicken, in der Hoffnung, dass dieser sämtliche Pakete auf der kürzesten Route weiterleitet.

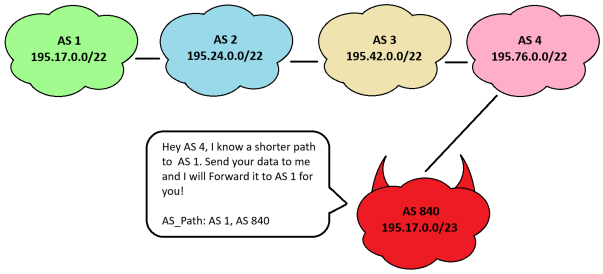

Figure 3: BGP Path Hijack

Sobald der Angreifer erstmal im Besitz des Traffics ist, hat er viele Möglichkeiten großen Schaden anzurichten. Er kann diesen beispielsweise verwerfen und dadurch die Verfügbarkeit eines Netzwerkes oder Dienstes stören (real world incident: Pakistan Telecom taking down YouTube). Ist das Ziel großangelegte Spionage, hat der Angreifer aber auch die Möglichkeit die Pakete zu inspizieren/ manipulieren und dann an den eigentlichen Empfänger weiterzuleiten, um noch mehr Informationen zu erhalten und dabei unbemerkt zu bleiben.

5 Real world Incidents

In diesem Kapitel werden wir den genauen zeitlichen Ablauf eines echten Vorfalls beschreiben.

Es handelt sich um einen Versuch der Zensur des Internets durch die pakistanische Regierung. Ziel war die Blockade von YouTube innerhalb von Pakistan, die allerdings unbeabsichtigt eskalierte und dabei über die Landesgrenzen von Pakistan hinaus Einfluss auf die Verfügbarkeit der Webseite hatte.

Pakistan Telecom taking down YouTube [1]

Event Timeline:

- Before, during and after Sunday, 24 February 2008: AS36561 (YouTube) announces 208.65.152.0/22
- Sunday, 24 February 2008, 18:47 (UTC): AS17557 (Pakistan Telecom) starts announcing the more specific address space of 208.65.153.0/24. Routers around the world receive the announcement, and YouTube traffic is redirected to Pakistan.
- Sunday, 24 February 2008, 20:07 (UTC): AS36561 (YouTube) starts announcing 208.65.153.0/24. With two identical prefixes in the routing system, BGP policy rules, such as preferring the shortest AS path, determine which route is chosen. This means that AS17557 (Pakistan Telecom) continues to attract some of YouTube’s traffic.
- Sunday, 24 February 2008, 20:18 (UTC): AS36561 (YouTube) starts announcing 208.65.153.128/25 and 208.65.153.0/25. Because of the longest prefix match rule, every router that receives these announcements will send the traffic to YouTube.
  Here we can see how Youtube uses/ needs two more specific announcements with Prefixes of Length 25 to cover the full address space with a prefix of length 24.
- Sunday, 24 February 2008, 20:51 (UTC): All prefix announcements, including the hijacked /24 which was originated by AS17557 (Pakistan Telecom) via AS3491 (PCCW Global), are seen prepended by another 17557. The longer AS path means that more routers prefer the announcement originated by YouTube.
- Sunday, 24 February 2008, 21:01 (UTC): AS3491 (PCCW Global) withdraws all prefixes originated by AS17557 (Pakistan Telecom), thus stopping the hijack of 208.65.153.0/24.

6 Sicherheitsmaßnahmen

RPKI (Resource Public Key Infrastructure)

RPKI ist ein kryptografisches Verfahren, das der Authentifizierung von Routing Informationen dient. Dabei werden Kombinationen von AS Nummern und Präfixen signiert und validiert. Auf diese Weise wird verhindert, dass Autonome Systeme Prefixes announcen, die sie nicht kontrollieren. Der

[1] https://www.ripe.net/about-us/news/youtube-hijacking-a-ripe-ncc-ris-case-study/

entstandene Datensatz wird auch als Route Origin Authorization (ROA) bezeichnet. Die Verwendung dieses VErfahrens liegt in der Verantwortung der Internet Service Provider (ISPs).

BGPsec
Ähnlich wie RPKI ist auch BGPsec ein kryptografisches Verfahren. Im Unterschied zu RPKI werden hier aber nicht die kombinationen aus AS_Number und Prefix signiert, sondern die Pfade innerhalb der Announcements. Dass BGPsec aktiv ist, erkennt man daran, dass das Attribut "AS_Path" in den Announcements durch das Attribut "BGPsec_Path" ersetzt wurde.

Route Filtering
Route Filtering kann sowohl für eingehende, als auch ausgehende Announcements angewendet werden. Hierzu verwalten die BGP Router Listen von Routen oder Präfixen, die sie auf bestimmten Ports erwarten und entsprechend akzeptieren. Diese Informationen können von der Internet Routing Registry (IRR) bezogen werden.
Logischerweise ist es im Interesse der ISPs die eingehenden Announcements zu filtern, um sich selbst vor Angriffen zu schützen. Seriöse ISPs filtern aber auch ihre ausgehenden Announcements, um beispielsweise fehlerhafte Announcements durch (versehentliche) Miskonfigurationen zu vermeiden. Im Idealfall filtern alle ISPs beziehungsweise deren BGP Router sowohl die ein- als auch die ausgehenden Announcements.

Monitoring und Anomalieerkennung
Beim Monitoring geht es primär um die Beobachtung von Veränderungen im gewöhnlichen Betriebsablauf.

Ein Beispiel hierfür wäre die plötzliche Veränderung einer Route. Wird eine Veränderung beobachtet, gilt es den Grund dafür herauszufinden. Möglicherweise handelt es sich nur um den Ausfall der gewöhnlichen Route aus Gründen wie einem Hardwaredefekt an einem Router oder Stromausfall. Da sich in einem solchen Fall die Route dynamisch an die gegebenheiten anpassen soll, um Ausfallsicherheit zu garantieren, gäbe es hier vermutlich nichts zu befürchten und das BGP erfüllt wie gewollt seinen Job. Wenn aber keinerlei Probleme mit der ursprünglichen Route bekannt sind, kann das schon ein Anlass sein die Veränderung der Route genauer zu untersuchen.

Ein Weiteres Beispiel einer Anomalie, die es zu untersuchen gilt, kann eine ungewöhnliche Menge an Traffic, insbesondere in Form von BGP-Announcements sein. Werden plötzlich ungewohnt hohe Mengen an Traffic durch das eigene Netzwerk geleitet, kann dies ein Hinweis darauf sein, dass sich eine Route geändert hat und es gilt wie zuvor beschrieben herauszufinden, warum dies der Fall ist. Erhält der eigene Router plötzlich eine auffällig hohe Menge an BGP-Announcements, ist dies möglicherweise ein Indiz dafür, dass ein anderes AS versucht das Routing gezielt zu manipulieren. Das passiert zum Beispiel dann, wenn ein AS einen großen Adressraum mit vielen, sehr spezifischen Announcements mit langen Präfixen übernehmen möchte.

7 References

Wikipedia Eintrag zum BGP:
wikipedia.org/wiki/Border_Gateway_Protocol

Wikipedia Eintrag zum EGP:
wikipedia.org/wiki/Exterior-Gateway-Protokoll

Mehr Basiswissen zum BGP:
linkedin.com/pulse/understanding-bgp

Basiswissen BGP Hijacking:
catchpoint.com/bgp-monitoring/bgp-hijacking

Youtube Hijacking Incident:
research.google/pubs/youtube-hijacking

ripe.net/about-us/news/youtube-hijacking

Basiswissen RPKI:
lancom-systems.de/docs/LCOS/Refmanual/DE/topics/bgp-rpki

Basiswissen BGPsec:
wikipedia.org/wiki/BGPsec

Basiswissen Route Filtering:
noction.com/knowledge-base/bgp-filtering

8 To Do

- Vollständige Übersetzung des Textes in Englisch. Erfolgt bei der späteren überarbeitung des Textes, bei der auch die Verbesserungsvorschläge aus dem Review mit einfließen.
- Einfügen der Referenzen an den entsprechenden Textstellen.
- Aussagekräftigen Titel für das Paper finden.
- BGPsec Part noch weiter ausarbeiten. Meinung Reviewer?
- Event Timeline für den YouTube Hijack noch etwas umschreiben und vereinfachen, da diese bis jetzt fast eine 1:1 Kopie aus der Originalquelle ist. Die AS Nummern tragen vermutlich wenig zur Verständlichkeit des Ablaufs bei. Meinung Reviewer?