An Introduction to the Border Gateway Protocol and how Malicious Actors Exploit its Weaknesses

Mark Klement
Goethe Universität
Frankfurt, Germany
s6840520@stud.uni-frankfurt.de

Abstract

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. Ziel dieses Papers ist es die systematischen Schwächen des Protokolls zu beleuchten. Es soll die Frage geklärt werden, welche Ursachen den Schwächen des Protokolls zugrunde liegen und wie Malicious Actors sich diese zu Nutzen machen. Zu diesem Zweck werden wir zunächst auf die Herkunft und Anforderungen an das Protokoll, dessen Entwicklung und den Stellenwert für moderne, verteilte Informationssysteme eingehen. Nach der Klärung der Grundlagen erfolgt eine Beschreibung der zwei Hauptangriffsvektoren "Origin Hijacks" und "Path Hijacks". Wir werden anhand eines realen, möglichst anschaulichen Vorfalls verdeutlichen, wie die beschriebenen Angriffsvektoren für das Protokoll in seiner Reinform ohne zusätzliche Sicherheitsmechanismen zum Problem werden können. Darauf aufbauend werden wir anschließend sowohl die gängigen Sicherheitsmaßnahmen, die der Prävention dienen, als auch moderne Hilfsmittel für die Erkennung und Analyse von aktiven und vergangenen Incidents erklären. Abschließend werden wir die aktuelle Gesamtsituation bewerten und versuchen einen kleinen Ausblick auf zukünftige Entwicklungen zu geben.

Keywords

BGP, Border Gateway Protocol, Origin Hijacking, Path Hijacking, RPKI, BGPSec

ACM Reference Format:
Mark Klement. 2025. An Introduction to the Border Gateway Protocol and how Malicious Actors Exploit its Weaknesses. In . ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 Introduction

Gateway Protokolle lassen sich allgemein in zwei Klassen einteilen, die sich im Wesentlichen darin unterscheiden, ob sie sich für das Routing innerhalb eines Autonomen Systems (kurz AS) oder zwischen verschiedenen Autonomen Systemen eignen. Innerhalb eines Autonomen Systems werden sogenannte Interior Gateway Protokolle (kurz IGPs) verwendet, während für das Routing zwischen Autonomen Systemen, auch genannt "Inter Domain Routing", 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.* Das BGP existiert sowohl in der Version iBGP für Intra Domain Routing als auch als eBGP für Inter Domain Routing. Innerhalb dieses Papers werden wir uns mit der Version für das Inter Domain Routing beschäftigen und diese allgemein als BGP bezeichnen.
Die sich heute im Einsatz befindliche Variante des BGP ist eine erweiterte Version des BGP-4 [19] dessen aktuelle Spezifikation zu diesem Zeitpunkt fast 20 Jahre alt ist. Das Hauptziel bei der Entwicklung des BGP war es, ein Protokoll zu erschaffen, das zuverlässig in besonders großen und komplexen Netzwerken funktioniert. Die wichtigsten Anforderungen waren entsprechend eine hohe Performance bei quasi unbegrenzter Skalierbarkeit sowie eine hohe Zuverlässigkeit und Flexibilität bei der Nutzung des Netzwerkes. Das BGP sollte sowohl die Durchsetzung von Routing Policies der ISPs ermöglichen, als auch in der Lage sein, Veränderungen oder Ausfälle von Routen dynamisch und dezentral zu kompensieren. Tatsächlich erfüllt das BGP diese Anforderungen so gut, dass es heute praktisch das einzige für Inter Domain Routing genutzte Protokoll ist.
Unglücklicherweise resultieren aus diesen Anforderungen aber auch die größten Schwächen des Protokolls [16]. Diverse Sicherheitsmaßnahmen wie kryptografische Verschlüsselungen, Ausstellung von Zertifikaten oder ähnliches kosten wertvolle Systemressourcen [13]. Je nach Verfahren kann es sich bei diesen Ressourcen um Speicherplatz, Rechenleistung oder auch Bandbreite 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, Effizienz und Geschwindigkeit sind in der Praxis oft Anforderungen, die nur schwer gleichzeitig erfüllbar sind. Entsprechend sind in der "Basisversion" des BGP keine nennenswerten Sicherheitsmechanismen integriert, da diese den anderen Anforderungen an das Protokoll im Wege stehen würden. Lediglich die Nutzung von TCP als Transport-Layer-Protokoll bietet minimalen Schutz vor Wiretapping Angriffen bei bereits etablierten Verbindungen zwischen zwei Routern [19]. Es hindert Angreifer aber nichts daran eine neue Verbindung zu einem Border-Router aufzubauen und diesem dann gänzlich erfundene BGP-Nachrichten zu senden.
Die Einfachheit das auf Vertrauen basierende Prinzip 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

Conference'17, Washington, DC, USA

ACM ISBN 978-x-xxxx-xxxx-x/YYYY/MM
https://doi.org/10.1145/nnnnnnn.nnnnnnn

Informationen können auf einen Schlag riesige Mengen an Traffic umgeleitet werden. Um BGP zu sichern sind daher zusätzliche Maßnahmen und Protokolle wie SBGP [10], BGPSec [12] oder RPKI [11] notwendig.

2 Threat Modeling

Dieses Kapitel soll ein etwas besseres Verständnis dafür vermitteln, welche Ziele besonders lukrativ sind und ob es sich bei BGP-Hijacking gemessen an der Anzahl der bekannten Vorfälle wirklich um ein ernstzunehmendes Problem handelt.

Wer wird Ziel
BGP-Hijacking hat generell eher große Unternehmen aus der Wirtschaft oder Regierungsnahe Institutionen zum Ziel. Privatpersonen sind in der Regel nur indirekt betroffen, wenn Beispielsweise die Daten eines großen Unternehmens abgefangen werden und dazu auch Kundendaten gehören. Die Kriterien, warum man als Unternehmen oder Organisation zur Zielscheibe wird sind vielfältig. Die Motive der Angreifer reichen von der Absicht der Sabotage von Services oder Netzwerken [2] (DOS Angriffe) bis hin zu staatlich organisierter Spionage. Aber auch Angriffe aus finanziellen Gründen sind insbesondere seit dem Aufleben von Kryptowährungen wie Bitcoin keine Seltenheit mehr [3].

Frequenz der Angriffe
Es ist nicht einfach Eine genaue Anzahl tatsächlicher Angriffe zu benennen, da nicht alle Angriffe als solche erkannt werden und es entsprechend eine gewisse Dunkelziffer gibt. Die Tendenz zeigt aber, dass mit dem generellen Wachstum des Internets und der Verlegung von immer mehr Services und Diensten in das Internet auch die Zahl der Vorfälle zunimmt [15] Auch moderne Sicherheitsmaßnahmen wie RPKI und BGPSec scheinen nicht in der Lage zu sein die absolute Anzahl der jährlichen Vorfälle zu senken. Obwohl auch sie keinen garantierten Schutz vor erfolgreichen Angriffen bieten, können sie dennoch helfen Angriffe gegen das eigene Netzwerk oder Unternehmen zumindest deutlich zu erschweren, sofern sie korrekt implementiert werden.

Einschätzung der Netzwerkbetreiber
Eine Interessante Studie [22] aus 2018 mit 75 befragten Netzwerkbetreibern hat ergeben, dass BGP-Hijacking von den Netzwerkbetreibern als ein ernstzunehmendes Problem bezeichnet wird. Mehr als 40% der Befragten Betreiber gaben an bereits zum Ziel von Hijacking Angriffen geworden zu sein. Die Dauer der Angriffe betrug in 57% der Fälle mehr als eine Stunde, in 25% der Fälle sogar mehr als einen Tag. Etwa 71% gaben damals an unter anderem aus Kostengründen kein RPKI zu verwenden und setzten stattdessen eher auf verstärktes Peering mit anderen Netzwerken um die Auswirkungen von Hijacking Incidents abzumildern.

3 Austausch von BGP Informationen

In seiner ursprünglichen Form funktioniert der Austausch von BGP Daten wie bereits erwähnt auf Vertrauensbasis, da das Unterlassen einer stringenten Prüfung der versendeten/ erhaltenen Daten beträchtliche mengen 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.

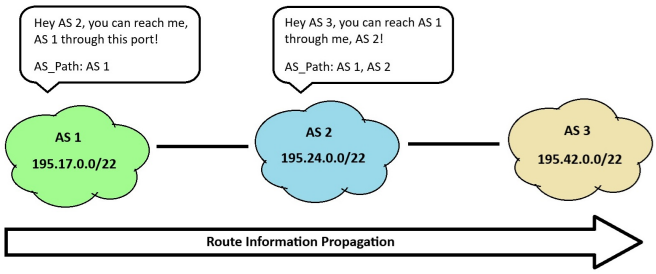

Figure 1: ASes exchanging Routing information

BGP-4 unterstützt CIDR (Classless Inter Domain Routing) sowohl für IPv4 als auch für IPv6 [19]. Es gibt 4 Nachrichtentypen, wovon 3 der Verwaltung der Verbindung zu unmittelbaren Nachbarn (Peers) dienen. Der eigentliche Austausch der Routen erfolgt über Nachrichten vom Typ "UPDATE". Routen können sowohl bekannt gegeben, als auch zurückgezogen werden.
Die wichtigsten Attribute innerhalb der BGP-Nachrichten sind:

- Die "AS_Number", die der eindeutigen Identifikation von Autonomen Systemen dient
- Ein "AS_Path" bestehend aus einer Kette von AS_Numbers, der zu einem anderen, erreichbaren AS führt
- Die "NRLI" Network Layer Reachability Information, also der Prefix des Adressbereichs, zu dem der AS_Path führt

Es gibt zwar noch weitere Attribute, aber im Wesentlichen lässt sich der Internetgraph aus den oben genannten Attributen erstellen, weshalb wir es für den Kontext dieses Papers dabei belassen.

4 Kategorien von Angriffen

Manche Quellen [9] teilen BGP Hijacking incidents grob in die Kategorien "Prefix Hijacks" und "Path Hijacks" ein, während andere Quellen diese Unterscheidung nicht vornehmen und allgemein von "BGP Hijacks" sprechen. Manche Quellen nehmen sogar noch feinere Einteilungen vor und zerlegen Beispielsweise die Klasse der Prefix Hijacks in "Black-Hole-Attacks" und "Interception-Attacks" [17]. Außerdem werden teils unterschiedliche Begriffe für die Gleichen Angriffe verwendet, wie es zum Beispiel bei "Prefix Hijacking" und "Origin Hijacking" der Fall ist. Insgesamt haben sowohl unsere eigene Literaturrecherche als auch die anderer Autoren ergeben, dass die Kategorisierungen und Bezeichnungen von Angriffen teilweise inkonsistent sind [18]. In diesem Paper werden wir deshalb die relativ gängige Einteilung in "Prefix Hijacks" und "Path Hijacks" verwenden, je nachdem, ob der Angriff sich hauptsächlich über den Adressraum selbst oder über den Pfad zu einem entsprechenden Adressraum definiert.

4.1 Prefix Hijacking

Generell bevorzugen Router bei der Erstellung ihrer Routingtabellen Announcements mit möglichst präzisen Prefixes [9]. Ein

Announcement wird immer dann präziser, wenn der Prefix in der CIDR Notation länger, also die Zahl nach dem "/" größer wird.

Example in IPv4:

`192.232.0.0/22` → less precise

`192.232.0.0/24` → more precise

Angreifer Nutzen diese sogenannte "longest-prefix-matching-rule" für sich aus, indem sie präzisere Prefixes in ihren BGP-Nachrichten verschicken als die legitimen Eigentümer eines Adressraumes. So überreden sie quasi andere Border-Router ihre gefälschten Announcements zu akzeptieren und zu bevorzugen.

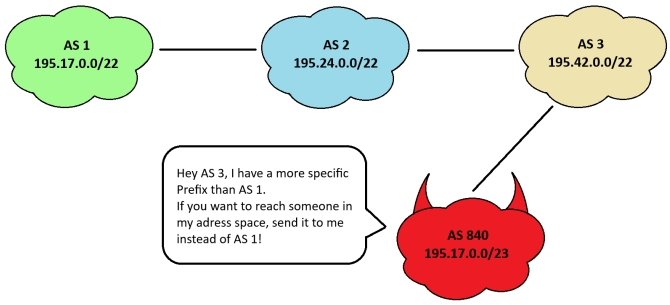

Figure 2: Prefix hijack

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 übernehmen will und die Empfänger seiner Announcements alle zu unspezifischen Announcements verwerfen. Um sein Ziel zu erreichen muss er dann eine auffällig hohe Menge an sehr spezifischen Announcements versenden, was schnell dazu führen kann, dass der Angriff als solcher erkannt wird.
Wenn ein legitimer Besitzer eines Adressraumes den Verdacht hat, dass er das Opfer eines Prefix-Hijacks ist, kann er diese Methode tatsächlich genauso anwenden wie der Angreifer und dadurch versuchen seinen gekaperten Adressraum zurückzuerobern.
Dies war zum Beispiel 2008 der Fall, als Pakistan Telecom versucht hat die Verfügbarkeit von YouTube innerhalb von Pakistan einzuschränken [20].
Dabei hat Youtube ursprünglich einen /22er Prefix verwendet, der dann von Pakistan Telecom durch einen /24er Prefix gehijacked wurde. YouTube versuchte zunächst den Adressraum zurückzuerobern, indem es ebenfalls einen /24er Prefix announced hat. Mit zwei Prefixen identischer Länge im Umlauf konnte YouTube jedoch nur einen Teil des Traffics zurückerobern. Schlussendlich musste YouTube zwei /25er Prefixes announcen, um den vollständigen Adressraum des /24er Prefixes abzudecken und wieder den gesamten Traffic zu erhalten.

4.2 Path Hijacking

Ein weiteres extrem relevantes Attribut bei der erstellung der Routingtabellen ist der sogenannte "AS_Path" und seine Länge. Um Pakete möglichst schnell und zuverlässig zuzustellen 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 [9]. Angreifer Nutzen dieses Grundprinzip also aus, indem sie behaupten, dass sie einen besonders kurzen Weg zu einem bestimmten Adressraum kennen.
Die Pfadlänge ist zwar wichtig, allerdings hat die "longest-prefix-

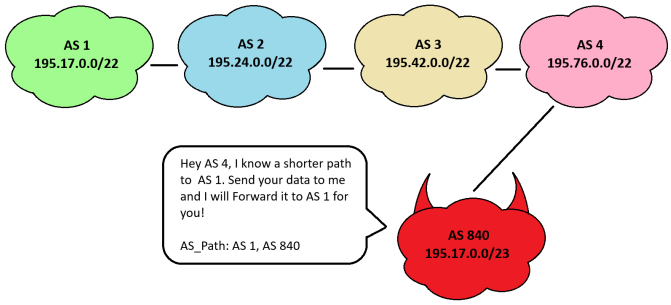

Figure 3: BGP Path Hijack

matching-rule" eine noch höhere Priorität. Path Hijacks werden deshalb unter anderem dann interessant, wenn Angreifer aus irgendeinem Grund (Beispielsweise wegen RPKI) nicht in der Lage sind, noch spezifischere Announcements zu versenden als die legitimen Besitzer des Adressraumes. Wenn die Angreifer nur in der Lage sind einen Prefix der gleichen Länge zu versenden wie die legitimen Besitzer eines Adressraumes dient die Pfadlänge als tie-breaker. In diesem Fall wird der Teil des Traffics an den Angreifer umgeleitet, der von Absendern kommt, die näher an dem AS des Angreifers liegen als an dem des tatsächlichen Besitzers des Adressraumes. Auch diese Situation konnte 2008 während dem Youtube Hijacking [20] beobachtet werden, als der gleiche /24er Prefix sowohl von Pakistan Telecom als auch von Youtube announced wurde. Hat ein Angreifer nicht einmal die Möglichkeit den gleichen Prefix wie ein legitimer Besitzer zu announcen, kann er durch die Behauptung einen besonders kurzen Pfad zum Ziel zu kennen aber immer noch Versuchen zu erreichen, dass andere ASes ihren Traffic dem Angreifer schicken, weil sie denken, dass der Angreifer ihn besonders schnell weiterleiten könne. In diesem Fall würde das AS des Angreifers dann nicht mehr vorgeben das Ziel des traffics zu sein, sondern lediglich als besonders attraktives Transit-AS auftreten.
Das Hauptziel des Angreifers ist es allerdings immer irgendwie in den Besitz des Traffics zu kommen. Ob er sich als Transit-AS oder als Ziel-AS ausgibt ist aus seiner Sicht in der Regel zweitrangig, da er in beiden Fällen die gleichen Möglichkeiten hat, was er mit dem erhaltenen Traffic anstellen kann. Er kann ihn in der Rolle des Ziel-AS verwerfen oder ihn als Transit-AS einfach nicht mehr weiterleiten. Genauso gut kann er den Traffic nachdem er ihn beispielsweise inspiziert oder modifiziert hat auch in beiden Fällen an den legitimen empfänger weiterleiten, um nicht so schnell aufzufallen und noch mehr Informationen abzugreifen.

5 Sicherheitsmaßnahmen

Die Sicherheitsmaßnahmen lassen sich im Wesentlichen in zwei Kategorien unterteilen [24]. Zum einen gibt es die präventiven Maßnahmen, die verhindern sollen, dass es überhaupt zu Hijacks und Route Leaks kommt. Zu diesen Methoden gehören RPKI, BGPSec und RouteFiltering. Die zweite Kategorie beinhaltet die Maßnahmen, die der Erkennung von Hijacks dienen, sobald diese auftreten. In dieser Kategorie befinden sich Verfahren, die sich mit dem Monitoring und der Anomalieerkennung beschäftigen.

RPKI (Resource Public Key Infrastructure)
RPKI ist ein kryptografisches Verfahren, das der Authentifizierung von Routing Informationen dient [11]. Dabei werden Kombinationen von AS Nummern und Präfixen durch Certificate Authorities (CAs) in einer Kette signiert und validiert, sodass eine möglichst stabile Trust-Chain mit einem Trust-Anchor am Anfang entsteht. Auf diese Weise wird verhindert, dass Autonome Systeme Prefixes announcen, die sie nicht kontrollieren, was folglich insbesondere die Vermeidung von "Origin Hijacks" bewirken soll. Ein aus Prefix und AS_Number bestehender Datensatz wird auch als Route Origin Authorization Object (ROA Objekt) bezeichnet, das für alle Border-Router zugänglich in einer verteilten Datenbank liegt. ROA Objekte können zusätzlich ein optionales Attribut enthalten, mit dem die maximal erlaubte Länge eines Prefix announcements für einen gegebenen Adressraum spezifiziert wird. Dadurch soll verhindert werden, dass Angreifer RPKI aushebeln, indem sie korrekte Kombinationen aus AS_Number und Adressraum verwenden und den eigentlichen Besitzer einfach mit einem oder mehreren, spezifischeren Subprefix announcements ausstechen. Bei der Verwendung dieses Attributs müssen Besitzer von Adressräumen deshalb aufpassen, dass sie die maximale Prefix Länge nicht höher ansetzen als es bei den Prefixen, die in den entsprechenden ROA Objekten enthalten sind, der Fall ist [4]. Wenn diese Regel nicht eingehalten wird und ein AS Beispielsweise einen Prefix der Länge /16 in ein ROA Objekt schreibt und das max_Length Attribut dann aber auf /24 setzt, nennt man das "Loose ROA". Loose ROAs sind besonders gefährlich, wenn kein Verfahren zur Verifikation von AS_Paths eingesetzt wird, da Angreifer dann die Möglichkeit haben, einen sogenannten "Forged-Origin Subprefix Hijack" durchzuführen, bei dem der Hijack sogar durch eine eigentliche Sicherheitsmaßnahme (RPKI) validiert werden kann. Obwohl die Verwendung von RPKI in seiner noch nicht vollständig standardisierten Anfangszeit in 2011 recht selten war, hat sich diese Situation mittlerweile deutlich verbessert und auch die Anzahl der Miskonfigurationen hat stark abgenommen [6, 9].

BGPsec
Ähnlich wie RPKI ist auch BGPsec [12] 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. Eines der Probleme ist, dass diese Signatur in jedem Schritt auf dem Pfad vom Origin AS bis zum Ziel AS erfolgen muss. Dadurch ist nicht nur der Rechenaufwand im Vergleich zu ROV mittels RPKI relativ hoch, sondern es reicht auch noch ein einziger Router ohne BGPSec auf dem Pfad aus, um potenzielle Sicherheitsvorteile zu verlieren. Und selbst wenn BGPSec auf dem vollständigen Pfad erfolgreich implementiert wird, demonstrieren [13], dass es trotzdem noch Möglichkeiten gibt Traffic abzufangen. Wenn zwei kompromittierte ASes miteinander kooperieren, können sie mittels einer Remote-BGP Session einen direkten Link und damit auch einen sehr kurzen Pfad simulieren. Sofern das AS, das auf dem Pfad näher am Ziel liegt den erhaltenen Pfad signiert, können die folgenden ASes nicht feststellen, dass kein echter Link vorhanden ist und die simulierte Verbindung wird gegenüber einer scheinbar längeren aber echten Route bevorzugt.
Weiterhin kann über eine hohe Frequenz an Announcements und Withdrawals einer Route durch einen Angreifer die Instabilität dieser Route vorgetäuscht werden. Das kann der Angreifer mit allen Routen machen, bis die scheinbar stabilste und attraktivste Route aus Sicht des Opfers durch das AS des Angreifers führt.
BGPSec ist zwar in der lage zumindest einige Sicherheitsbedenken auszuräumen, aber es keine Optimallösung die vollständige Sicherheit garantiert [13, 17].

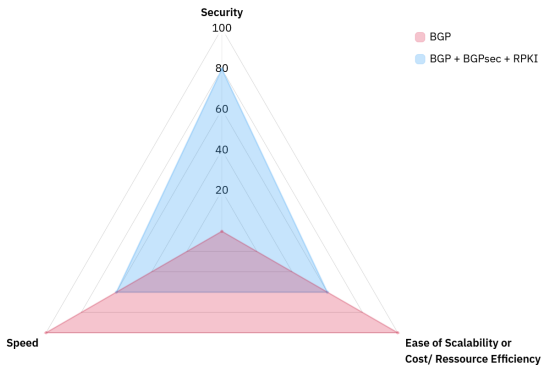

Figure 4: Pure BGP vs. BGP with additional security measures (Graph Scale more arbitrary than exact)

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. Speziell zu diesem Zweck

entwickelt gibt es eine Reihe von Monitoring-Tools, die die Identifikation von Incidents deutlich erleichtern soll. Beispiel hierfür sind Tools die der Visualisierung von Routen dienen, wodurch plötzlich auftretende Veränderungen leichter erkennbar sind [18].
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.
Um bösartige Angriffe von "normalen" Vorfällen zu unterscheiden, kann eine Analyse der von einer Umleitung betroffenen prefixes helfen[5]. Die meisten ASes announcen mehrere Prefixes wodurch im Falle eines gewöhnlichen technischen Defektes auch der Traffic für all diese Prefixe umgeleitet wird. Gezielte Angriffe konzentrieren sich aber oft nur auf ein Subset der Prefixes eines ASes, wodurch letztendlich auch nur das entsprechende Subset an Traffic umgeleitet wird, während der Traffic der nicht betroffenen Prefixes weiterhin die übliche Route nimmt. Ein solcher Angriff lässt sich dann möglicherweise daran erkennen, dass die Pakete, die an einen gehijackten Teil des Adressraumes gesendet werden eine höhere Latenz beziehungsweise Round Trip Time haben.

KI-Basierte Anomalieerkennung
Wie in vielen anderen technischen Bereichen gewinnen auch bei der Anomalieerkennung KI-basierte Methoden zunehmend an Bedeutung. Das Internet entspricht einem Graphen, bei dem die (BGP) Router die Knoten und die Verbindungen zwischen ihnen die Kanten darstellen. Entsprechend gut lassen sich Graphenbasierte Machine Learning Architekturen auf das Problem anwenden[7].
Ein alternativer Ansatz ist ein NLP-basiertes Verfahren, das in Anlehnung an Word2Vec AP2Vec[24] getauft wurde. Es basiert auf der Annahme, dass ASes verschiedene Rollen wie tier-1 oder tier-2 Provider oder auch cloud Provider besitzen und sich die Verteilung der Rollen auf einer Route im Falle eines Angriffs stärker verändert als dies bei einer regulären Routenänderung normal ist. Das Verfahren betrachtet die Routen als Sätze deren Wörter den Rollen der ASes auf den jeweiligen Ruten entsprechen. Aufgrund des Embeddings dieser Sätze kann dann darauf geschlossen werden, ob es sich bei dem gegebenen Satz beziehungsweise der entsprechenden Route um einen Hijack handelt oder nicht.

6 Conclusion

Das BGP ist das Protokoll, das unser modernes Internet zusammenhält und daran wird sich auf absehbare Zeit auch nichts ändern. Aufgrund seiner Bedeutsamkeit und der scheinbar unaufhörlich wachsenden Größe des Internets wird das Protokoll entsprechend auch in Zukunft ein lukratives Ziel für Angreifer bleiben.
Obwohl BGP allein ein äußerst anfälliges Protokoll ist, gibt es mittlerweile recht effektive Präventionsmaßnahmen wie RPKI, BGPsec und RouteFiltering, die Angriffe zwar nicht gänzlich verhindern, aber zumindest erschweren können.
Bedauerlicherweise scheitert es aber in der Praxis häufig an der Implementierung und Anwendung dieser Maßnahmen. Die Gründe dafür reichen von mangelnden Kenntnissen und Fähigkeiten der Administratoren bis hin zu finanziellen Überlegungen der Netzwerkbetreiber. Während mangelnde Fachkenntnisse durch gezielte Schulungen von Administratoren und Betreibern behoben werden können, lässt sich der finanzielle Aspekt nur schwer eliminieren. Die letzte und vielleicht einzige Möglichkeit besonders kostenoptimiert arbeitenden Betreibern zu begegnen wäre das Schaffen eines gesetzlichen Rahmens, der fahrlässiges Handeln unter so hohe Strafen stellt, dass die Implementierung von Sicherheitsmaßnahmen die günstigere Option ist. Solche Gesetze international zu erlassen und anschließend auch durchzusetzen ist aber schier unmöglich, insbesondere da einige Staaten beispielsweise zwecks Spionage oder Zensur auch gar kein Interesse an der vollständigen Schließung sämtlicher Sicherheitslücken haben.

7 To Do

- Vollständige Übersetzung des Textes in Englisch
- Referenzen häufiger in den Text einbinden

References

[1] Bahaa Al-Musawi, Philip Branch, and Grenville Armitage. 2016. BGP Anomaly Detection Techniques: A Survey. *IEEE Communications Surveys and Tutorials* PP (10 2016), 1–1. doi:10.1109/COMST.2016.2622240 [Online; accessed 5-December-2025].

[2] Antony Antony, Daniel Karrenberg, Robert Kisteleki, Tiziana Refice, and Rene Wilhelm. 2008. YouTube Hijacking (February 24th 2008) Analysis of BGP Routing Dynamics. https://research.google/pubs/youtube-hijacking-february-24th-2008-analysis-of-bgp-routing-dynamics/ [Online; accessed 3-December-2025].

[3] Maria Apostolaki, Aviv Zohar, and Laurent Vanbever. 2017. Hijacking bitcoin: Routing attacks on cryptocurrencies. In *2017 IEEE symposium on security and privacy (SP)*. IEEE, 375–392. https://arxiv.org/pdf/1605.07524 [Online; accessed 5-December-2025].

[4] Randy Bush. 2014. *Origin validation operation based on the Resource Public Key Infrastructure (RPKI)*. Technical Report. IETF. https://www.rfc-editor.org/rfc/rfc7115.html [Online; accessed 6-December-2025].

[5] Tobias Bühler, Alexandros Milolidakis, Romain Jacob, Marco Chiesa, Stefano Vissicchio, and Laurent Vanbever. 2023. Oscilloscope: Detecting BGP Hijacks in the Data Plane. *arXiv preprint arXiv:2301.12843* (2023). arXiv:2301.12843 [cs.NI] https://arxiv.org/abs/2301.12843 [Online; accessed 3-December-2025].

[6] Taejoong Chung, Emile Aben, Tim Bruijnzeels, Balakrishnan Chandrasekaran, David Choffnes, Dave Levin, Bruce M Maggs, Alan Mislove, Roland van Rijswijk-Deij, John Rula, et al. 2019. RPKI is coming of age: A longitudinal study of RPKI deployment and invalid route origins. In *Proceedings of the Internet Measurement Conference*. 406–419. https://dl.acm.org/doi/pdf/10.1145/3355369.3355596 [Online; accessed 3-December-2025].

[7] Kevin Hoarau, Pierre Ugo Tournoux, and Tahiry Razafindralambo. 2021. Suitability of graph representation for bgp anomaly detection. In *2021 IEEE 46th Conference on Local Computer Networks (LCN)*. IEEE, 305–310. https://hal.science/hal-03398624v1/file/Suitability.pdf [Online; accessed 3-December-2025].

[8] Thomas Holterbach, Thomas Alfroy, Amreesh Phokeer, Alberto Dainotti, and Cristel Pelsser. 2024. A System to Detect Forged-Origin BGP Hijacks. In *21st USENIX Symposium on Networked Systems Design and Implementation (NSDI 24)*. USENIX Association, Santa Clara, CA, 1751–1770. https://www.usenix.org/conference/nsdi24/presentation/holterbach [Online; accessed 5-December-2025].

[9] Ebrima Jaw, Moritz Müller, Cristian Hesselman, and Lambert Nieuwenhuis. 2024. Serial BGP hijackers: A reproducibility study and assessment of current dynamics. In *2024 8th Network Traffic Measurement and Analysis Conference (TMA)*. IEEE, 1–10. https://ris.utwente.nl/ws/portalfiles/portal/454762901/Serial_BGP_Hijackers_A_Reproducibility_Study_and_Assessment_of_Current_Dynamics.pdf [Online; accessed 3-December-2025].

[10] Stephen Kent, Charles Lynn, and Karen Seo. 2002. Secure border gateway protocol (S-BGP). *IEEE Journal on Selected areas in Communications* 18, 4 (2002), 582–592. http://dpnm.postech.ac.kr/research/08/KT_BGP/BGP_Security/SecureBorderGatewayProtocol.pdf [Online; accessed 5-December-2025].

[11] Matt Lepinski and Stephen Kent. 2012. *An infrastructure to support secure internet routing*. Technical Report. IETF. https://www.rfc-editor.org/rfc/rfc6480.html [Online; accessed 5-December-2025].

[12] Matt Lepinski and Kotikalapudi Sriram. 2017. *BGPSEC protocol specification*. Technical Report. IETF. https://www.rfc-editor.org/rfc/rfc8205.html [Online; accessed 3-December-2025].

[13] Qi Li, Jiajia Liu, Yih-Chun Hu, Mingwei Xu, and Jianping Wu. 2018. Bgp with bgpsec: Attacks and countermeasures. *IEEE Network* 33, 4 (2018), 194–200. https://yihchun.com/papers/ieee-net-19.pdf [Online; accessed 5-December-2025].

[14] Stephanos Matsumoto, Raphael M Reischuk, Pawel Szalachowski, Tiffany Hyun-Jin Kim, and Adrian Perrig. 2017. Authentication challenges in a global environment. *ACM Transactions on Privacy and Security (TOPS)* 20, 1 (2017), 1–34. https://dl.acm.org/doi/pdf/10.1145/3007208 [Online; accessed 5-December-2025].

[15] Alexandros Milolidakis, Tobias Bühler, Kunyu Wang, Marco Chiesa, Laurent Vanbever, and Stefano Vissicchio. 2023. On the Effectiveness of BGP Hijackers That Evade Public Route Collectors. *IEEE Access* 11 (2023), 31092–31124. doi:10.1109/ACCESS.2023.3261128 [Online; accessed 3-December-2025].

[16] Sandra Murphy. 2006. *BGP security vulnerabilities analysis*. Technical Report. Network Working Group. https://www.rfc-editor.org/rfc/rfc4272 [Online; accessed 5-December-2025].

[17] Jan Oesterle, Holger Kinkelin, and Filip Rezabek. 2021. Challenges with BGPSec. *Network* 5 (2021). https://www.net.in.tum.de/fileadmin/TUM/NET/NET-2022-01-1/NET-2022-01-1_02.pdf [Online; accessed 8-December-2025].

[18] Justin Raynor, Tarik Crnovrsanin, Sara Di Bartolomeo, Laura South, David Saffo, and Cody Dunne. 2022. The state of the art in BGP visualization tools: A mapping of visualization techniques to cyberattack types. *IEEE Transactions on Visualization and Computer Graphics* 29, 1 (2022), 1059–1069. https://www.researchgate.net/profile/Justin-Raynor/publication/363898023_The_State_of_the_Art_in_BGP_Visualization_Tools_A_Mapping_of_Visualization_Techniques_to_Cyberattack_Types/links/633d8632ff870c55ce0261f1/The-State-of-the-Art-in-BGP-Visualization-Tools-A-Mapping-of-Visualization-Techniques-to-Cyberattack-Types.pdf [Online; accessed 5-December-2025].

[19] Yakov Rekhter, Tony Li, and Susan Hares. 2006. *A border gateway protocol 4 (BGP-4)*. Technical Report. Network Working Group. https://www.rfc-editor.org/rfc/rfc4271 [Online; accessed 5-December-2025].

[20] RIPE NCC RIS. 2008. YouTube Hijacking: A RIPE NCC RIS case study. https://www.ripe.net/about-us/news/youtube-hijacking-a-ripe-ncc-ris-case-study/ [Online; accessed 3-December-2025].

[21] Nils Rodday, Ítalo Cunha, Randy Bush, Ethan Katz-Bassett, Gabi D Rodosek, Thomas C Schmidt, and Matthias Wählisch. 2021. Revisiting rpki route origin validation on the data plane. In *Proc. of Network Traffic Measurement and Analysis Conference (TMA), IFIP*. https://dl.ifip.org/db/conf/tma/tma2021/tma2021-paper11.pdf [Online; accessed 5-December-2025].

[22] Pavlos Sermpezis, Vasileios Kotronis, Alberto Dainotti, and Xenofontas Dimitropoulos. 2018. A survey among network operators on BGP prefix hijacking. *ACM SIGCOMM Computer Communication Review* 48, 1 (2018), 64–69. https://arxiv.org/pdf/1801.02918 [Online; accessed 5-December-2025].

[23] Pavlos Sermpezis, Vasileios Kotronis, Petros Gigis, Xenofontas Dimitropoulos, Danilo Cicalese, Alistair King, and Alberto Dainotti. 2018. ARTEMIS: Neutralizing BGP hijacking within a minute. *IEEE/ACM transactions on networking* 26, 6 (2018), 2471–2486. https://arxiv.org/pdf/1801.01085v4 [Online; accessed 5-December-2025].

[24] Tal Shapira and Yuval Shavitt. 2022. AP2Vec: an unsupervised approach for BGP hijacking detection. *IEEE Transactions on Network and Service Management* 19, 3 (2022), 2255–2268. https://www.researchgate.net/publication/359892012_AP2Vec_an_Unsupervised_Approach_for_BGP_Hijacking_Detection [Online; accessed 5-December-2025].