Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Analyse der Verbreitung und erster Betriebsszenarien der RPKI als Sicherungsmaßnahme für das Internet Backbone Routing

Tobias Ramin

Bachelorarbeit

Fakultät Technik und Informatik
Studiendepartment Informatik

Faculty of Engineering and Computer Science
Department of Computer Science

Tobias Ramin

Analyse der Verbreitung und erster Betriebsszenarien der RPKI als Sicherungsmaßnahme für das Internet Backbone Routing

Bachelorarbeit eingereicht im Rahmen der Bachelorprüfung

im Studiengang Bachelor of Science Technische Informatik
am Department Informatik
der Fakultät Technik und Informatik
der Hochschule für Angewandte Wissenschaften Hamburg

Betreuender Prüfer: Prof. Dr. Thomas C. Schmidt
Zweitgutachter: Prof. Dr. Klaus-Peter Kossakowski

Eingereicht am: 18. Januar 2016

Tobias Ramin

Thema der Arbeit
Analyse der Verbreitung und erster Betriebsszenarien der RPKI als Sicherungsmaßnahme für das Internet Backbone Routing

Stichworte
BGP, Routing, RPKI, ROA, Analyse

Kurzzusammenfassung
Für das Internet Backbone Routing zwischen den Autonomen Systemen (AS) des Internets wird das Border-Gateway-Protokoll eingesetzt. Da BGP-Nachrichten einfach gefälscht werden können, wurde zur Absicherung des BGPs die Resource Public Key Infrastructure (RPKI) entwickelt, welche es ermöglicht, eine überprüfbare Beziehung zwischen den in den BGP-Nachrichten genannten ASen und den ASen zugeordneten IP-Bereichen aufzubauen. Hierzu werden Route Origination Authorizations (ROAs) eingesetzt, die beglaubigen, dass ein bestimmtes AS einen bestimmten IP-Bereich als seinen Ursprung ankündigen darf. Eine Analyse der Verbreitung und möglicher Schwierigkeiten der RPKI erfolgt mittels gesammelter BGP-Nachrichten sowie den dazugehörigen ROAs.

Tobias Ramin

Title of the paper
Analysis of distribution and first operational scenarios of RPKI as a safeguard for the internet backbone routing

Keywords
BGP, routing, RPKI, ROA, analysis

Abstract
The border-gateway-protocol is used for the internet backbone routing between autonomous systems (AS) of the internet . Since BGP-messages can easily be tempered with, the resource public key infrastructure (RPKI) was developed to create a verifiable relationship between the ASes and their assigned IP-ranges in the BGP-messages. To accomplish this, route origination authorizations (ROAs) are deployed, which attest, that a specific AS is entitled to announce a specific IP-range. An analysis of the distribution of RPKI and possible problems for the usage is done with collected BGP-messages and their corresponding ROAs.

Meiner Tochter

Danksagung

Großen Dank gebührt meiner Frau und meiner Familie, die mich immer unterstützt haben. Außerdem großen Dank an meine Freunde, Kommilitoninnen und Kommilitonen, Kolleginnen und Kollegen.

Inhaltsverzeichnis

1 Einleitung

Das Internet verbindet unterschiedliche Netzwerke miteinander und ermöglicht die Kommunikation über Netzwerkgrenzen hinaus. Diese Netzwerke wiederum bestehen aus Routern und Hosts. Die Aufgabe dieser Router besteht aus dem Verteilen von Datenpaketen auf die Hosts. Das Routing der Datenpakete erfordert, dass die IP-Adresse(n) der Hosts den Routern bekannt sind, so dass die Datenpakete über festgelegte Routen an die Hosts zugestellt werden können.

Wenn nun ein Host nicht Teil des Netzwerkes ist, so muss der Datenfluss über das Internet erfolgen. Dazu ist es aber notwendig, dass die Router des Internets (Internet-Backbone-Router) die Routen zu den unterschiedlichen Netzwerken kennen. Es kommt regelmäßig vor, dass Netzverbindungen unterbrochen werden oder neu hinzukommen, so dass für das Internet statisches Routing nicht ausreicht, sondern Erreichbarkeitsinformationen zwischen den Internet-Backbone-Routern ausgetauscht werden müssen.

In der vorliegenden Arbeit werden ausschließlich Internet-Backbone-Router betrachtet und diese daher zur Vereinfachung der Lesbarkeit nur noch als Router bezeichnet.

Als Autonomes System (AS) bezeichnet man den Zusammenschluss von Netzwerken, die einer gemeinsamen Administration unterliegen. Beispielsweise verwendet die Deutsche Telekom die AS-Nummer AS3320.

Ein Routing-Protokoll dient den Routern dazu, die Erreichbarkeitsinformationen der einzelnen Netzwerke untereinander auszutauschen und wird aufgrund der Dynamik der Routen benötigt. Insbesondere wird eine Zuordnung von AS zu IP-Bereichen benötigt, die über das AS erreichbar sind, sowie die Möglichkeit des Nachrichtenaustausches zwischen den ASen. Ein Präfix beschreibt einen durch CIDR-Notation festgelegten IP-Bereich.

Als Routing-Protokoll entwickelten Rekhter und Li (1994) das Border-Gateway-Protokoll (BGP), welches im folgenden Kapitel genauer erläutert wird. In RFC-4271 wurde eine revidierte Version von Rekhter u. a. (2006) beschrieben und anschließend als aktueller Standard von der Internet Engineering Task Force (IETF) festgelegt.

Über BGP-Nachrichten wird die Erreichbarkeit von Präfixen über AS-Pfade propagiert. Der AS-Pfad beschreibt den Weg der Datenpakete über unterschiedliche ASe bis zum Ursprungs-AS, über welches ein IP-Bereich direkt erreichbar ist.

Ein Schwachpunkt ist, dass keine Überprüfung der BGP-Nachrichten auf Manipulation und Fehlerhaftigkeit statt findet, so dass die darin genannte Zuordnung von Präfix zu AS verändert werden kann. Dadurch besteht die Möglichkeit, den Netzwerkverkehr von IP-Bereichen, die einem bestimmten AS zugeordnet sind, auf ein anderes AS umzuleiten.

Die Notwendigkeit der Absicherung des BGPs wurde am 24.02.2008 besonders deutlich, als die Pakistan Telecom eine Route zu youtube.com annoncierte und den daraus resultierenden Traffic verwarf (RIPE, 2008). Ziel des Routingeintrags war die Zensur von youtube.com für die pakistanische Bevölkerung. Durch die Verbreitung der fehlerhaften Annoncierung über das BGP war die Webseite teilweise mehrere Stunden für die ganze Welt nicht mehr erreichbar.

Zur Absicherung des BGPs gegen fehlerhafte Zuordnungen von Präfix zu AS wurde die Resource Public Key Infrastructure (RPKI) von Lepinski und Kent (2012) entwickelt. Sie erlaubt, eine überprüfbare Zuordnung zwischen dem in der BGP-Nachricht als Ursprung genannten AS und dem annoncierten Präfix herzustellen, so dass nur die Ankündigung der Erreichbarkeit von IP-Bereichen in der Nachricht möglich ist, für die dieses AS legitimiert ist.

In der vorliegenden Arbeit soll geprüft werden, wie verbreitet der Einsatz der RPKI zur Zeit ist, welche Probleme für das Internet-Backbone-Routing durch deren Betrieb entstehen können und welche Probleme dadurch gelöst werden. Dazu werden die von der RIPE archivierten BGP-Nachrichten von August 2013 bis Dezember 2015 analysiert und mit Hilfe der im gleichen Zeitraum gesammelten Zertifikate der RPKI auf Gültigkeit der Zuordnung von AS zu Präfix(en) überprüft. Ebenso werden diese Zertifikate verwendet, um Fehlkonfigurationen der RPKI und Probleme durch den Einsatz einer RPKI sowie daraus folgende Konsequenzen zu analysieren.

Im nächsten Kapitel werden zunächst die Grundlagen des Routings via BGP erläutert und auf die damit verbundenen Sicherheitsprobleme des Protokolls eingegangen.

Im dritten Kapitel folgt eine Einführung in den Einsatz einer RPKI, welche zur Absicherung des BGPs entwickelt wurde. Insbesondere werden mögliche Schwierigkeiten beim Betrieb der RPKI untersucht, die zu Störungen des Internet Backbone Routing führen können.

Das Verfahren zur Auswertung und die Analyse werden im vierten Kapitel entwickelt und durchgeführt. Die Routen der gesammelten BGP-Daten werden auf Gültigkeit geprüft und auf die zuvor beschriebenen Schwierigkeiten hin untersucht.

Das letzte Kapitel fasst die gewonnenen Erkenntnisse zusammen und präsentiert die verbliebenen offenen Fragen.

2 Das Border-Gateway-Protokoll (BGP)

Man unterscheidet Autonome Systeme (ASe) danach, ob sie über eine Default-Route verfügen, die gewählt wird, falls die zu routenden Pakete nicht Teil ihres Netzwerkes sind oder ob sie Routing-Informationen ausschließlich durch den Nachrichtenaustausch mit anderen BGP-Teilnehmern erhalten. Letztere Gruppe wird als Router der Default-Freien-Zone (DFZ) bezeichnet.

Das BGP ist ein sogenanntes Exterior-Gateway-Protokoll (EGP), es funktioniert im Gegensatz zu Interior-Gateway-Protokollen (IGP) über Netzwerkgrenzen hinaus auch in der DFZ und wird für den Austausch von Routing-Informationen im Internet verwendet.

Die Erreichbarkeitsinformationen der ASe werden zwischen den ASen über das BGP ausgetauscht. Durch diese Informationen ist es möglich, einen Graphen aufzubauen und so Routingschleifen zu vermeiden. Das BGP ist ein Pfadvektor-Protokoll, der AS-Pfad beschreibt die bereits durchlaufenen Pfade der ASe als Vektor.

Es existieren unterschiedliche Klassifizierungen von Internetserviceprovidern (ISPs), Tier-1, Tier-2 und Tier-3. Die Klassifizierung erfolgt anhand der Businessrolle, die diese ISPs erfüllen. Die großen Tier-1 ISPs bieten ausschließlich kostenpflichtige Anbindungen (Transit) an ihr Netzwerk an, es gibt keine Möglichkeit der kostenlosen, gegenseitigen Verbindung (Peering) zu anderen ISPs der gleichen Klasse. Tier-2 und Tier-3 beschreiben entsprechend kleinere Netzwerke, die auf Transit zu übergeordneten Tiers angewiesen sind, untereinander aber aus Kostengründen bevorzugt Peering verwenden. So entstehen die Business-Rollen “Customer (c)” und “Provider (p)”, wobei Transit c-to-p und Peering p-to-p Beziehungen beschreiben.

2.1 Aufbau des BGPs

BGP verwendet TCP (Postel, 1981) als Transportprotokoll auf Port 179. Über diesen Port werden BGP-Nachrichten zwischen Routern der ASe ausgetauscht. Die so entstehenden Verbindungen nennt man BGP-Sessions.

Die BGP-Nachrichten weisen einen Header aus 19 Byte und einen Nachrichteninhalt von 0 bis 4077 Byte auf. Damit beträgt die minimale Länge einer BGP-Nachricht 19 Byte, wenn nur

der Header geschickt wird. Die maximale Länge beträgt 4096 Byte. Der Header selbst besteht aus einem Marker mit 16 Byte, einem Feld für die Länge der Nachricht mit 2 Byte und einem Byte für die Nachrichtenart, von der es vier verschiedene gibt:

- Open: wird für den BGP-Sitzungsaufbau verwendet. Hierbei entscheiden die beiden Kommunikationspartner anhand ihrer Konfiguration, ob Routinginformationen ausgetauscht werden oder die Verbindung abgebrochen wird.
- Update: beinhaltet zurückgezogene oder neue Routen und dient sowohl dem Austausch der gesamten Routing-Tabelle als auch inkrementiellen Updates. Die Nachricht beinhaltet das Präfix und auch den AS-Pfad.
- Notification: wird im Fehlerfall ausgegeben.
- Keepalive: dient der Aufrechterhaltung der Verbindung, wenn keine Update-Nachrichten zu verschicken sind.

Kapitel 4.3 aus Rekhter und Li (1994) beschreibt "Update" genauer. Anhand eines Beispiels lassen sich die für diese Arbeit wichtigen Felder einer BGP-Update-Nachricht erläutern:

Die HAW-Hamburg ist über das deutsche Forschungsnetz (DFN) an das Internet angebunden. Das DFN hat die AS-Nummer AS680 und die HAW das Präfix 141.22.0.0/16 mit Länge 16. Zur Veranschaulichung dessen dient folgende, beispielhafte BGP-Nachricht:

```
1417392078|A|37989|141.22.0.0/16|37989 1239 10507 3320 680|IGP|0
```

Listing 2.1: BGP-Nachricht

Die BGP-Nachricht in Listing 2.1 zeigt, wie das Präfix 141.22.0.0/16 über das AS680 erreichbar ist und über welche ASe der Pfad dorthin verläuft.

2.1.1 Zeitstempel

Die Nachricht ist mit einem Zeitstempel (hier 1417392078) versehen, so dass es möglich ist, die Aktualität der Nachricht zu bestimmen. Das hier gewählte Format ist Unix-Zeit.

2.1.2 Nachrichtentyp

Es gibt drei unterschiedliche Nachrichtentypen: Announcement, Withdrawal und BGP-Table-Dump. Entsprechend der Anfangsbuchstaben werden die Typen durch "A", "W" und "B" symbo-

lisiert und bedeuten Ankündigung einer neuen Route, Zurückziehen einer bestehenden Route und kompletter Abzug der Routing-Tabelle eines Routers. Hier wird Typ “A” verwendet.

2.1.3 Präfix/Länge

Bei dem Präfix handelt es sich um den IP-Bereich, welcher über das AS erreichbar ist. Es wird in CIDR-Notation für IPv4 oder IPv6 mit der jeweiligen Präfixlänge angegegben. In diesem Beispiel lautet das Präfix 141.22.0.0/16.

2.1.4 AS-Pfad

Der AS-Pfad zählt die verschiedenen ASe auf, die bisher bei dieser Nachricht durchlaufen wurden. Jedes durchlaufene AS fügt seine Nummer von links dem Pfad hinzu, so dass am Ende des Pfades der Ursprung des Paketes steht und ein Graph aufgebaut werden kann. Hier lautet der AS-Pfad: 37989 1239 10507 3320 680. Das Origin-AS 680 kündigt die direkte Erreichbarkeit des obigen Präfixes an.

2.1.5 Ursprung

Der Ursprung beschreibt die Quelle der BGP-Ankündigung. Entweder ist diese IGP oder EGP, sonst INCOMPLETE. Hier wird IGP verwendet.

2.1.6 Multi-Exit-Descriminator

Der Multi-Exit-Descriminator (MED) dient der Möglichkeit der Bevorzugung bei benachbarten ASen und stellt so eine Entscheidungshilfe bei der Pfadauswahl dar. In diesem Beispiel ist der MED 0.

2.2 Funktionsweise des BGPs

Die über BGP-Update-Nachrichten empfangenen Routen werden für das Weiterleiten (Forwarding) der Datenpakete verwendet, indem durch eine Routing-Policy bestimmt wird, welche Route gewählt wird. Die auf diese Weise selektierten Routen werden auf Routern in Routing-Tabellen gespeichert und für das Forwarding verwendet.

2.2.1 Befüllung der Tabellen des Routers

Die Routen selber werden in unterschiedlichen Tabellen des Routers, den Routing Information Bases (RIBs) gespeichert:

- Adj-RIBs-In: speichert eingehende Routing-Informationen, die via "Update"-Nachricht von anderen BGP-Sprechern empfangen wurden. Diese Informationen dienen als Eingabe in den Entscheidungsprozess der zu wählenden Route.
- Loc-RIB: beinhaltet die lokalen Routing-Informationen, die aus der Anwendung der Routing-Policy auf die in der Adj-RIBs-In enthaltenen Routing-Informationen resultieren.
- Adj-RIBs-Out: enthält die Routing-Informationen der Loc-RIB, welche per "Update"-Nachricht wieder an andere Teilnehmer verteilt werden.

Die Forwarding Information Base (FIB) enthält die Einträge der Loc-RIB, allerdings unterscheidet sie sich dadurch, dass Präfixe nicht mehrfach vorkommen können, um so Routingschleifen zu vermeiden. Die kürzeste Länge eines AS-Pfades bestimmt zusammen mit der Routing-Policy, welche Route in die FIB übernommen wird, falls mehrere Routen existieren. Die FIB wird für das eigentliche Routing verwendet. Die RIBs dienen dem Filtern, Sortieren und Verwalten der eingehenden BGP-Updates.

2.2.2 Pfadauswahl

Viele Netzwerke unterhalten mehrere BGP-Verbindungen zu ihren Partnern, um Netzwerkausfälle kompensieren zu können. Für die Pfadauswahl der besten Route bei mehreren Routen zum gleichen Ziel wird eine Routing-Policy angewendet, die folgendes Schema durchläuft (van Beijnum (2002)):

- Wende zuerst eigene, selbst konfigurierte Policies an
- Wähle die Route mit der höchsten lokalen Präferenz, benachbarte ASe werden bevorzugt
- Wähle dann die Route mit dem kürzesten AS-Pfad
- Wähle nun die Route nach Ursprung, bevorzuge IGP, dann EGP und dann INCOMPLETE
- Wähle dann die Route mit dem niedrigsten Multi-Exit-Descriminator
- Wende tie-breaking Regeln an, um bei mehreren gleichwertigen Routen eine auszuwählen

Mit dieser Prozedur werden eventuell vorhandene Routing-Schleifen aufgelöst und trotzdem die Erreichbarkeit über unterschiedliche Wege ermöglicht.

2.2.3 Beispiel für den Aufbau einer Routingtabelle

Abbildung 2.1 (vgl. van Beijnum (2002)) zeigt einen beispielhaften Ausschnitt des Internets, bestehend aus mehreren ASen und deren Routing-Beziehungen. Das AS10 gehört zu einem größeren Tier-2 ISP, AS20 und AS30 sind Teil von zwei Tier-3 ISPs. AS40 und AS50 sind zwei unterschiedlichen Kunden zugeordnet. Eine Default-Route zeigt an, dass über sie alle Systeme des Internets erreichbar sind. AS10 besitzt keine Default-Route, sondern befindet sich in der DFZ. AS40 und AS50 annoncieren entsprechend die Präfixe 144.0.0.0 und 145.0.0.0.

Nachdem sich alle Routen im Netzwerk per BGP verbreitet haben, zeigt Abb. 2.1 die daraus resultierenden Routing-Tabellen der jeweiligen ASe. '>' zeigt die bevorzugte Route an, falls mehrere Routen zur Verfügung stehen. Der AS-Pfad ist ebenfalls aufgeführt, er ist hinter den jeweiligen Präfixen vermerkt. Die Geschäftsbeziehungen Transit und Peering zwischen den ISPs und Kunden sind ebenso mit aufgeführt. Tatsächlich sind Routing-Tabellen aber deutlich komplexer als in diesem Beispiel.

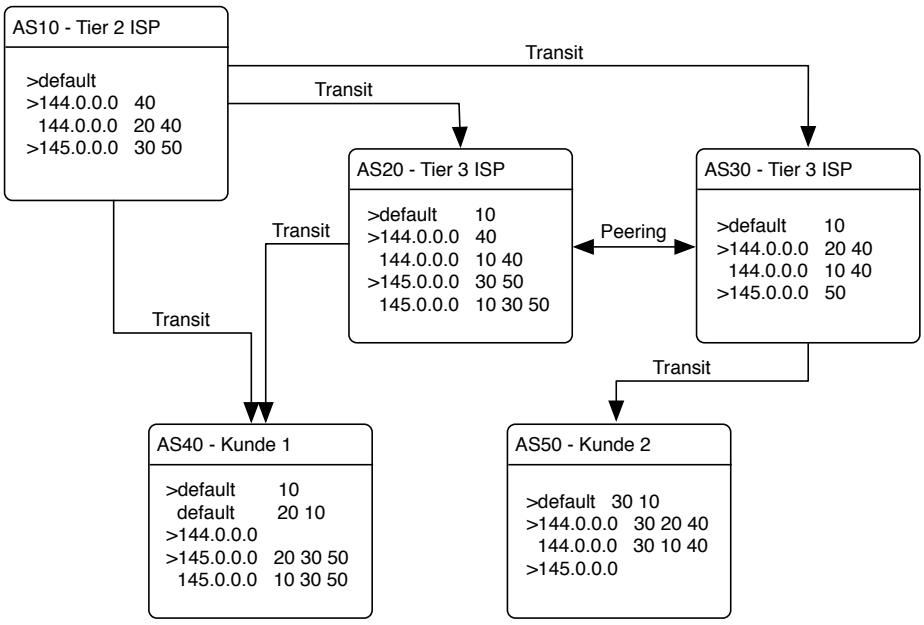

Abbildung 2.1: BGP Beispiel - Routing-Beziehungen der Teilnehmer

Routing-Tabelle von AS10:
Sie enthält eine leere Default-Route sowie die Route zum Netzwerk 144.0.0.0 und 145.0.0.0, wobei erstere doppelt vorkommt. Dies ergibt sich daraus, dass AS40 sowohl direkt als auch über AS20 erreichbar ist. Die direkte Route wird bevorzugt, da sie kürzer ist.
Routing-Tabelle von AS20:
Hier ist vermerkt, dass über die Default-Route zu AS10 das gesamte Internet erreichbar ist und wie über AS30 und AS50 der IP-Bereich 145.0.0.0 erreicht werden kann. Ebenso kann 144.0.0.0 direkt über AS40 erreicht werden. AS20 und AS30 sind über Peering miteinander verknüpft.
Routing-Tabelle von AS30:
Sie zeigt hier ebenso den Default-Eintrag über AS10 und dass das Netzwerk 145.0.0.0 direkt über AS50 erreichbar ist. Für 144.0.0.0 sind zwei Einträge vermerkt, die Verbindung über AS20 zu AS40 wird wegen des kostenneutralen Peerings bevorzugt.
Routing-Tabelle von AS40:
Das Kundennetzwerk 144.0.0.0 ist entweder direkt über AS10 oder über AS10 und AS20 erreichbar, die direkte Route wird bevorzugt. Das Netzwerk 145.0.0.0 kann auf zwei Wegen erreicht werden, die Route über AS20 und AS30 zu AS50 wird wegen des Peerings bevorzugt.
Routing-Tabelle von AS50:
Das Kundennetzwerk 145.0.0.0 besitzt nur eine Default-Route. Bei den Routen zu AS40 wird ebenfalls die Route mit dem Peering zwischen AS30 und AS20 bevorzugt.

2.3 Schwächen des BGPs

Das Border-Gateway-Protokoll birgt einige Probleme in sich, die vor allem die Skalierbarkeit und die Sicherheit von BGP-Nachrichten betreffen.

2.3.1 Skalierbarkeit des BGPs

Die Router der DFZ tauschen ihre Erreichbarkeits-Informationen untereinander aus, so dass sie einen Großteil der verfügbaren Routen des gesamten Internet-Backbones in ihren RIBs haben. Ein aktueller Abzug (09.01.2016) enthält zur Zeit 588025 Einträge, wie die Webseite des CIDR-Reports von Huston zeigt. Dies demonstriert ein Problem bezüglich der Skalierbarkeit von BGP, denn es lässt sich ein superlineares Wachstum erkennen. Daraus lässt sich ableiten, dass auch der Speicherplatz der Router mitwachsen muss, da sonst keine globale Routingtabelle mehr vorgehalten werden kann. Ebenso werden immer leistungsfähigere Router benötigt, um die anfallenden Datenmengen in angemessener Zeit verarbeiten zu können.

Am 12. August 2014 kam es zur Überschreitung der Grenze von 512k Einträgen in der Routingtabelle (Toonk, 2014), der Tag wird seit dem als 512KDay bezeichnet. Damit verbunden war ein Überlauf der Routingtabelle gerade bei älteren Routern und damit ein Ausfall der Erreichbarkeit einiger Präfixe, so dass Teile des Internets nicht erreichbar waren.

2.3.2 Sicherheitsschwächen des BGPs

Das BGP wurde ohne jegliche Form der Authentifizierung entworfen, so dass nicht sichergestellt werden kann, dass eine BGP-Nachricht wirklich von dem Sender kommt, der in der BGP-Nachricht als Origin-AS genannt wurde. Murphy bemängelt außerdem, dass das BGP ohne Verschlüsselung entworfen wurde, mit der die Integrität der Daten garantiert werden könnte.

Bereits 1989 erschien von Bellovin "Security Problems in the TCP/IP Protocol Suite", worin er Sicherheitsschwächen des EGPs, dem Vorgänger des BGPs, behandelte. Dort beschrieb er, wie mit Hilfe eines zweiten Gateways Datenströme eines AS umgeleitet (redirection) werden können. In den neueren Sicherheitsanalysen zu BGP von Butler u. a. (2010), Goldberg u. a. (2010), Ballani u. a. (2007) und Murphy (2006) sind folgende Sicherheitsprobleme des BGPs aufgeführt:

Route-Leaks

Das Durchsickern von Routen (route-leaks) über BGP-Nachrichten, obwohl diese Routen nicht per BGP an die Router der DFZ verteilt werden sollten, sondern nur an wenige lokale Nachbar-ASe. Dies führt zu einer Flut an Traffic für das Origin-AS, für den es nicht immer ausgelegt ist.

Prefix-Hijacking

Die Entführen von Präfixen (prefix-hijacking), bei dem ein AS den Besitz eines Präfixes ankündigt, welches aber einem anderen AS zugeordnet ist. Wenn nun benachbarte ASe diese Route der legitimen Route vorziehen, wird der Netzwerk-Verkehr entführt und auf das AS des Angreifers umgeleitet. Ob die Daten das eigentliche Origin-AS noch erreichen, hängt nur noch vom Angreifer ab.

Blackholing

Einen besonderen Fall des prefix-hijacking stellt das sogenannte Blackholing dar, bei dem z.B. durch Fehlkonfiguration oder einen Angreifer die Routingtabelle so manipuliert wird, dass Netzwerkverkehr an IP-Adressen geroutet wird, die entweder nicht existieren oder einem

anderen Teilnehmer zugeordnet sind. Diese umgeleiteten Pakete verschwinden in dem namensgebenden schwarzen Loch, wenn die ungewünschten Pakete dann auf dem Router des Origin-AS gelöscht bzw. verworfen werden.

Denial-of-Service-Angriff

Ein weiteres Problem betrifft Denial-of-Service-Angriffe, die die Unterbrechung des Datenstroms zur Folge haben. Hier verstopfen zu viele Pakete die Netzwerkleitung, so dass legitime Pakete nicht mehr rechtzeitig zugestellt werden können.

Verstärkungsangriff

Verstärkungsangriffe sind eine spezielle Form der DoS-Attacke, bei der ein Host mit einer gefälschten Absenderadresse eine legitime Anfrage an viele Netzwerkteilnehmer stellt und deren Antwort-Pakete deutlich größer als die Anfrage selbst sind. Durch den gefälschten Absender werden die gesamten Antworten an das attackierte Ziel gesendet.

Path-shortening-Attacke

Mit einer Path-shortening-Attacke kann der AS-Pfad so verkürzt werden, dass die Pfadauswahl der Router manipuliert wird und so eine Route gewählt wird, die über das AS eines Angreifers führt. Da das Origin-AS dabei nicht geändert wird, kommen die Datenpakete ans Ziel, erlauben aber den unberechtigten Zugriff auf die Daten, so dass die Vertraulichkeit der Kommunikation nicht mehr gegeben ist.

Impersonation-Angriff

Der Impersonation-Angriff dient ebenso dem Abhören der Datenpakete, bei dem sich ein angreifendes AS als legitimes Ziel der Routing-Informationen ausgibt, indem es die Origin-AS-Nummer des Opfers übernimmt.

2.3.3 Sicherheitsschwächen des von BGP verwendeten TCPs

Durch das Abhören von TCP-Nachrichten ist die Vertraulichkeit der Kommunikation nicht mehr gewährleistet. Eine Manipulation der TCP-Nachrichten ist ebenfalls möglich. Der Datenaustausch findet beim BGP über TCP statt, so dass auch TCP angegriffen werden kann, um das BGP zu schwächen:

Man-In-The-Middle-Attacke

Mit einer Man-In-The-Middle-Attacke lässt sich die Integrität der TCP-Nachrichten gefährden, insbesondere durch das Einfügen gefälschter TCP-Nachrichten, Löschen oder Verändern legitimer TCP-Nachrichten oder einen Wiederholungsangriff, um bereits zurückgezogene Routen wieder neu zu annoncieren.

Denial-of-Service-Angriff

Auch TCP ist anfällig für Denial-of-Service-Angriffe, um die Kommunikation einzuschränken oder zu unterbrechen, beispielsweise durch SYN-flooding beim TCP-Handshake. Auch route-flapping, das ständige Auf- und Abbauen der Verbindung, welches bedingt, dass die Routen kontinuierlich zurückgezogen und wieder angekündigt werden müssen, dient diesem Zweck.

Link-Cutting Attack

Ein weiterer Angriff ist die link-cutting attack, bei der durch eine Unterbrechung der Netzwerkverbindung neue Routen notwendig werden und so eine Route mit z.B. weniger Bandbreite genutzt werden muss.

2.3.4 Erste Ansätze zur Absicherung des BGPs

Einen Ansatz zur Absicherung des BPGs lieferten Kent u. a. (2000) mit S-BGP, welches aber bis dato nicht eingesetzt wird. Hierin wird beschrieben, wie mit Hilfe zweier PKIs sowohl die Identität und Berechtigung der BGP-Sprecher als auch die der ASe und des zugehörigen IP-Bereichs validiert werden kann. Außerdem findet die Kommunikation verschlüsselt über IPSec statt, so dass die Integrität der Nachrichten gewährleistet ist. Im Gegensatz zu S-BGP wird RPKI bereits eingesetzt und im folgenden Kapitel erläutert.

Karlin u. a. (2005) schlagen vor, dass eingehende BGP-Nachrichten geprüft und gefiltert werden sollten, indem sie mit bereits empfangenen BGP-Nachrichten verglichen werden und existierende Kombinationen aus Präfix und AS bevorzugt werden.

Zur Absicherung von TCP kann das in RFC-2385 beschriebene Verfahren von Heffernan (1998) verwendet werden, bei dem eine MD5-Hashsumme über die jeweilige TCP-Nachricht gebildet und der Nachricht hinzugefügt wird, so dass eine Manipulation der TCP-Nachrichten erschwert wird. Eine überarbeitete Version findet sich in RFC-5925 von Touch u. a. (2010).

Trotz dieser Vorschläge kommt es weiterhin zu Vorfällen, bei denen via BGP irreführende Routen annonciert werden, da der Einsatz der RPKI noch nicht sehr weit verbreitet ist:

Der Netzwerkdienstleister Renesys (2013) berichtet von zwei größeren Vorfällen von hijacking im Jahr 2013, bei denen der Netzwerkverkehr über das AS eines Angreifers geführt wurde und von diesem nach Analyse wieder zurück an das ursprüngliche Ziel gelangte, so dass es zu keinen Ausfällen oder Störungen kam.

Im Verlauf der BlackHat-Konferenz 2015 gab es gleich zwei Vorträge, die mögliche Angriffe auf die konzeptionellen Schwächen von BGP präsentierten und als Absicherung den Einsatz einer RPKI empfehlen. Der Vortrag von Remes (2015) handelt vom Stand der derzeitigen Sicherheit von BGP, der von Gavrichenkov (2015) beschreibt die Möglichkeit, TLS-Zertifikate bei der Generierung zu entführen.

3 Sicherheitserweiterung des BGPs mittels RPKI

Zur Verbesserung der Sicherheit des BGPs wurde die Resource Public Key Infrastructure (RPKI) von Lepinski und Kent (2012) entwickelt. Dazu gehörten zum einen das RPKI-Router Protokoll (RTR) zum Austausch der RPKI-Daten von Bush und Austein (2013), zum anderen die Gültigkeitsprüfung der Verknüpfung von Präfixen zu berechtigten ASen von Huston und Michaelson (2012) sowie von Mohapatra u. a. (2013). Die Beglaubigung der Zugehörigkeit eines Präfixes zu einem bestimmten AS erfolgt mittels Route Origination Authorizations (ROAs) und ist in RFC-6482 von Lepinski u. a. (2012) beschrieben. Die Beglaubigung geschieht über X.509-Zertifikate, wie sie in RFC-5280 von Cooper u. a. (2008) definiert sind.
Der Ursprung einer Route lässt sich durch den Einsatz von RPKI beglaubigen und ebenfalls überprüfen, wodurch die Sicherheit des BGPs erhöht wird.

3.1 Architektur der RPKI

Die RPKI besteht aus einer Zuteilungshierarchie von IP-Adressraum zu AS-Nummern, den ROAs und einer verteilten, replizierten Datenbank zum Speichern der RPKI- und ROA-Daten.

3.1.1 Zuteilungshierarchie mittels PKI

Die Vergabe von IP-Bereichen ist hierarchisch aufgebaut, von der IANA als Wurzel über die 5 Regionalen Internet Registries (RIRs) ARIN, AfriNIC, APNIC, LACNIC und RIPE bis zu den nationalen Registries und den Internet-Service-Providern (ISPs). Ebenso verhält es sich mit der Vergabe der AS-Nummern. Diese Hierarchie korreliert mit dem Aufbau einer PKI, bei der die Zertifikate für die Zugehörigkeit eines IP-Präfixes zu einem AS gespeichert werden können und welche daher Resource-PKI (RPKI) genannt wird.

Die X.509-Zertifikate der RPKI binden den öffentlichen Schlüssel des Zertifikats an ein Präfix und eine AS-Nummer, dienen aber nicht der Authentifizierung der Ressource, sondern ausschließlich der Beglaubigung der Berechtigung.

CA-Zertifikate beglaubigen die Zugehörigkeit eines Präfixes zu einem AS. EE-Zertifikate werden von den CAs ausgestellt und attestieren die Berechtigung eines AS, ein bestimmtes Präfix als Ursprung (Origin) zu annoncieren. Mit ihnen werden die ROAs signiert.

3.1.2 Beglaubigung mittels ROA-Zertifikaten

Das ROA ist eine Beglaubigung, die besagt, dass der Halter eines Präfixes ein bestimmtes AS autorisiert hat, Routen für dieses Präfix anzukündigen. Hierzu muss das ROA mit dem privaten Schlüssel des EE-Zertifikats signiert worden sein. Das ROA selber beinhaltet die AS-Nummer, das Präfix und die maximale Länge des Präfixes. So lässt sich die Gültigkeit des ROAs und damit auch die der Routenankündigung überprüfen. Das Ergebnis der Prüfung lautet entweder "gültig", wenn ein gültiges ROA für die Kombination aus Präfix und AS vorliegt, "ungültig", für den Fall, dass es ein ROA gibt, welches aber diese Kombination aus AS und Präfix nicht widerspiegelt oder das EE-Zertifikat zum Signieren des ROAs ungültig ist. Falls kein ROA zu der Kombination AS und Präfix gefunden werden kann, lautet das Ergebnis "nicht gefunden" und bedeutet, dass die RPKI für diese Ressource nicht genutzt wird.

3.1.3 Replizierte Datenbank

Die ISPs und RIRs müssen zum Überprüfen der BGP-Nachrichten alle zur Zeit gültigen ROAs und Zertifikate vorrätig halten. Daher ist die Nutzung einer verteilten Datenbank mit repliziertem Datenbestand unerlässlich. Diese dient auch der Manipulationsprüfung, denn alle darin enthaltenen Elemente sind durch X.509-Zertifikate signiert. Weiterhin werden Manifest-Dateien verwendet, die als Verzeichnis fungieren und so das Löschen oder Hinzufügen signierter Objekte bemerkt werden kann. Zur Synchronisation der Daten zwischen den unterschiedlichen Teilen der Datenbank wird das rsync-Protokoll verwendet.

3.1.4 Beispiel einer RPKI-Architektur

Eine Übersicht der verwendeten Elemente der RPKI zeigt Abbildung 3.1 (vgl. Wählisch (2011)). Die IANA und die 5 RIRs bilden die Vertrauensanker für die RPKI. Das AS eines ISPs beinhaltet einen oder mehrere lokale Caches als Teil der replizierten Datenbank, welche wiederum von einem RPKI-sprechenden Router verwendet werden und über das RTR-Protokoll kommunizieren. Die Synchronisation der lokalen Caches mit der globalen RPKI findet über das rsync-Protokoll statt.

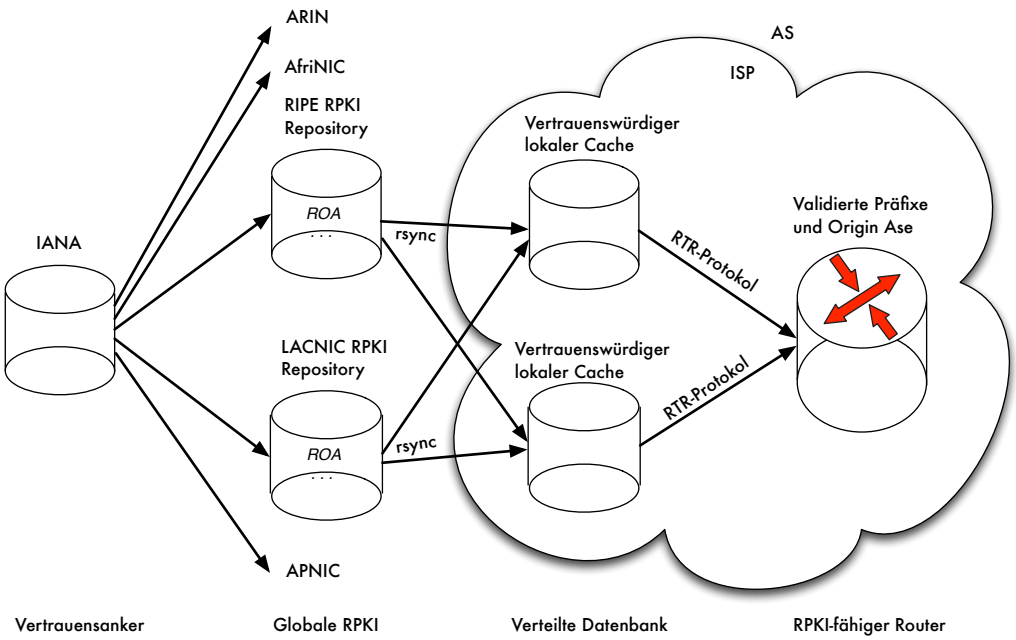

Abbildung 3.1: RPKI Architektur - Verbindungen zwischen den Teilnehmern

3.2 Funktionsweise der RPKI

Die Hauptaufgabe der RPKI ist die Bereitstellung einer Validitätsprüfung der Routinginformationen. Hierzu wird ein lokaler Cache mit den gültigen ROAs, Zertifikaten und Manifest-Dateien gefüllt und einem BGP-sprechenden Router mit RPKI-Erweiterung zur Verfügung gestellt. Dieser kann dann die eingehenden Routenankündigungen der anderen BGP-Teilnehmer auf Gültigkeit überprüfen, indem er im Cache nach einem gültigen ROA für die Kombination aus Präfix und AS-Nummer des Routingannouncements sucht. In Abhängigkeit der Gültigkeit des ROAs kann so die Gültigkeit der angekündigten Route bestimmt werden.

3.2.1 Befüllung des lokalen Caches

Um die signierten Objekte einer PKI nutzen zu können, muss ein Teilnehmer einen lokalen Cache aller gültigen EE-Zertifikate für diese PKI anlegen. Dazu sind folgende Schritte notwendig:

- aus der verteilten Datenbank eine Kopie aller Zertifikate, Manifeste und Zertifikatswiderrufslisten (CRL) herunterladen.

- Überprüfung der Gültigkeit der CA-Zertifikate mittels der Manifeste und der Ablaufdaten der jeweiligen Zertifikate.
- Anhand der Manifeste erfolgt eine Überprüfung auf Vollständigkeit und Gültigkeit der Manifeste, CRLs und Zertifikate.
- Überprüfung der EE-Zertifikate durch Konstruktion und Prüfung des Zertifizierungspfades.

Durch die sich ständig ändernden Inhalte der Datenbank muss diese Operationen regelmäßig wiederholt werden. Es ist somit effektiver, nur die zwischenzeitlich veränderten Daten von Datenbank und lokalem Cache abzugleichen. Der Austausch der Daten zwischen Router und lokalem Cache ist im RPKI-Router-Protokoll von Bush und Austein (2013) beschrieben.

3.2.2 Ausstellen eines ROAs

Ein Halter eines IP-Adress-Bereichs kann für diesen Bereich ein AS autorisieren, Routen hierzu anzukündigen. Um ein ROA für die Zuordnung von Präfix zu AS zu erstellen, muss zuerst ein EE-Zertifikat erzeugt werden, welches dieses Präfix enthält. Anschließend wird das ROA aus Präfix und AS-Nummer erstellt. Dann wird das ROA mit dem privaten Schlüssel des EE-Zertifikats signiert. Schließlich werden das ROA und das EE-Zertifikat in die verteilte Datenbank hochgeladen.

3.2.3 Validierung von BGP-Nachrichten

Huston und Michaelson (2012) sowie Mohapatra u. a. (2013) beschreiben, wie eine per BGP angekündigte Route überprüft werden kann. Wie in 2.1.4 beschrieben, ist das im AS-Pfad am weitesten rechts stehende AS das Ursprungs-AS (Origin-AS), über welches das Präfix erreichbar ist. Das Präfix und das Origin-AS werden in einem ROA beglaubigt, welches im Validierungsprozess überprüft wird. Dies geschieht, indem für die angekündigte Route nach einem gültigen ROA im lokalen Cache gesucht wird. Abhängig von der Gültigkeit des ROAs ist dementsprechend auch die Validität der Routenankündigung, welche in die Pfadauswahl mit einbezogen wird. Hierbei wird “gültig” stark bevorzugt, “nicht gefunden” leicht bevorzugt und “ungültig” nicht bevorzugt. Mit den nun dargestellten Funktionen bietet die RPKI die Möglichkeit, eingehende BGP-Nachrichten darauf zu prüfen, ob die Route vom Origin-AS überhaupt angekündigt werden durfte. Dies würde Prefix-Hijacking, Blackholing, die Impersonation-Attack und DoS-Angriffe verhindern, denn die angekündigte Route wäre immer “ungültig”.

3.3 Schwächen der RPKI

Der Einsatz einer RPKI bringt für das BGP einen nennenswerten Sicherheitsgewinn, der allerdings auch mit erheblichem Aufwand verbunden ist, denn für jede Kombination von AS zu Präfix muss ein ROA erzeugt und signiert werden. Außerdem birgt der Einsatz einer RPKI Schwächen, die im Folgenden beschrieben werden.

3.3.1 Ausschließliche Validierung des Origin-AS

RPKI stellt nur eine Beglaubigung für die Beziehung Origin-AS zu Präfix aus. Solange das Origin-AS nicht geändert wird, kann trotzdem der AS-Pfad manipuliert werden, denn es findet keine Validierung des gesamten AS-Pfades statt. Goldberg (2014) zeigt, dass eine Path-Shortening-Attacke so weiterhin möglich ist. Außerdem zeigt Goldberg, dass route leaks immer noch stattfinden können, wenn es sich um eine gültige Route handelt, für die ein ROA exisitiert.

3.3.2 Möglichkeit der Downgrade-Attacke

Eine als "gültig" deklarierte, sichere Route bedeutet nicht, dass diese kürzer und kostengünstiger ist als eine Route mit Status "nicht gefunden". Es besteht die Möglichkeit einer Downgrade-Attacke, bei der eine unsichere Route bevorzugt wird, da die sicherere länger oder teurer ist, siehe Lychev u. a. (2013). Dieses Verhalten hängt von den jeweiligen Routing-Policies ab, insbesondere ob der Fokus der ISPs mehr auf Sicherheit oder mehr auf Performance und Wirtschaftlichkeit liegt.

3.3.3 Entstehung weiterer Manipulationsmöglichkeiten

Im Falle einer fehlerhaft konfigurierten oder durch staatliche Einflussnahme veränderten RPKI entstehen laut Cooper u. a. (2013) neue Möglichkeiten der Manipulation des Routings, insbesondere Zensur, Informationskontrolle und Überwachung. Dazu kann ein eigentlich gültiges ROA invalidiert oder via CRL zurückgezogen werden, so dass die annoncierte Route "ungültig" wird und die Router daher in Abhängigkeit der Routing-Policies die Route verwerfen. So wären Teile des Internets nicht mehr erreichbar. Auch durch das Ausstellen eines ROAs mit falschen Daten kann Einfluss auf das Routing genommen werden, indem eine neue, nun gültige Route angekündigt wird, die von den Routern bevorzugt wird und der Verkehr über die neue, unsichere Route geleitet wird. Piscitello (2012) beschreibt ein Verfahren zur Beschlagnahmung einer Domain über das DNS.

3.3.4 Fehlende Differenzierungsmöglichkeit zwischen Fehler und Angriff

Wählisch u. a. (2012) zeigen, dass es schwierig ist, zwischen Fehlkonfiguration und Angriff zu differenzieren. Zur Analyse dienten hier "ungültige" BGP-Announcements, welche anhand des Origin-AS und der Präfixlänge auf ihre Gültigkeit untersucht wurden. Zu "ungültigen" Announcements kommt es, wenn entweder das Origin-AS oder die Präfixlänge nicht mit den in den ROAs deklarierten übereinstimmt, auch beides ist möglich. Auf einen Angriff deutet eine kurze Dauer des "ungültig"- Zustandes und eine kurzfristige Veränderung des Präfixes bzw. des Origin-ASes hin. Für eine Fehlkonfiguration spricht ein ungültiges Origin-AS, wenn ein gültiges AS auf dem AS-Pfad liegt sowie eine zu große Präfixlänge, wenn für eine kürzere Präfixlänge ein ROA existiert.

3.4 Mögliche Schwierigkeiten beim Einsatz der RPKI

Die Einführung und der Betrieb einer RPKI zur Absicherung des Internet-Backbone-Routings kann bei ISPs zu Problemen führen, beispielsweise durch Fehlkonfiguration oder Unerfahrenheit, auch systematische Fehler können beim Betrieb auftreten.

3.4.1 Verbreitung der RPKI

In den Arbeiten von Wählisch u. a. (2014) sowie Wählisch u. a. (2015) wird der zögerliche Einsatz der RPKI bei den großen Content-Delivery-Networks (CDN) beschrieben und auf mögliche Ursachen eingegangen. Da die CDNs einen Großteil der beliebtesten Interseiten verteilen, ist hier ein unterdurchschnittlicher Einsatz einer RPKI besonders relevant für die Verbreitung des Einsatzes.

3.4.2 Veränderungen der Gültigkeit von "gültig" zu "ungültig"

Wenn es bereits gültige Routenankündigungen für eine Kombination aus Ursprungs-AS, Präfix und Präfixlänge gab, diese jedoch ab einem bestimmten Zeitpunkt ungültig werden, beruht dieses entweder auf einem Konfigurationsfehler oder ist auf einen Angriff zurückzuführen.

3.4.3 Veränderungen der Gültigkeit zu "gültig"

Eine Veränderung von "ungültig" zu "gültig" findet statt, wenn eine Fehlkonfiguration erkannt und behoben, oder ein Angriff abgewehrt oder beendet wurde. Eine Veränderung von "nicht gefunden" zu "gültig" bedeutet, dass es nun für diese Kombination aus AS und Präfix ein gültiges ROA gibt und von diesem Zeitpunkt an die RPKI verwendet wird.

3.4.4 Fehlkonfiguration durch ein ungültiges Origin-AS im AS-Pfad

Das Ursprungs-AS auf dem AS-Pfad ist möglicherweise nur für den internen Gebrauch gedacht gewesen und durch eine Fehlkonfiguration in den AS-Pfad eingetragen worden. Das eigentliche Origin-AS liegt aber auf dem AS-Pfad und es existiert für es auch ein gültiges ROA.

3.4.5 Fehlkonfiguration durch falsche Präfixlänge

Zur Überprüfung der Gültigkeit einer Routenankündigung sind drei Elemente der Routenankündigung nötig: das Ursprungs-AS, das zu routende Präfix und dessen Länge. Beispielsweise durch Fehlkonfiguration kann es dazu kommen, dass ein ausgestelltes ROA für ein Präfix mit Länge 20 ausgestellt wurde, in der Routenankündigung aber 24 angegeben wurde. Die daraus resultierende Gültigkeitsprüfung würde trotz gültigem ROA für Präfix/20 ein "ungültig" für Präfix/24 anzeigen.

3.4.6 Fehlkonfiguration durch Routing von privaten AS-Nummern

Es gibt AS-Nummern, ähnlich den privaten IP-Adressen, die nur intern verwendet und nicht geroutet werden dürfen. Diese privaten AS-Nummern sind in Mitchell (2013) spezifiziert. Folgende AS-Nummern sind als privat gekennzeichnet: 64512 - 65534 sowie 4200000000 - 4294967294 und dürften daher nicht in BGP-Updates genannt werden.

3.4.7 Unterschiede in der Gültigkeitsprüfung verschiedener Monitore

Die BGP-Nachrichten werden von BGP-Monitoren aufgezeichnet, so dass eine nachträgliche Analyse sämtlicher Nachrichten möglich ist. Der hier hauptsächlich genutzte BGP-Monitor ist rrc00 des RIPE NCC in Amsterdam. Als zweiter Monitor dient das Route Views Archiv von der University of Oregon, insbesondere der Monitor route-views2.oregon-ix.net.

Durch die unterschiedlichen Betreiber und geographisch weit auseinander liegende Monitore könnte es vorkommen, dass es trotz DFZ zu unterschiedlichen Ergebnissen bei der Gültigkeitsprüfung der Routenankündigung kommen kann.

Die Gültigkeitsdauer der "ungültigen" Routenankündigungen wird daher in Abhängigkeit des Monitors untersucht.

3.4.8 Prüfung des Ablaufzeitpunktes der ROAs

ROAs haben eine Zeitspanne, in der sie gültig sind. Durch Unachtsamkeit oder fehlendes Monitoring kann es dazu kommen, dass die ROAs ablaufen und dann die Gültigkeit der Routenankündigungen auf "ungültig" wechselt.

3.4.9 Besonderheit des Geschwister-AS (Sibling AS)

Ein ISP kann auch mehrere AS-Nummern verwenden. Diese Geschwister-ASe können beispielsweise durch Übername eines konkurrierenden ISP entstehen. Über whois-Abfragen zu den einzelnen AS-Nummern lassen sich solche Sibling-ASe feststellen und auf unterschiedliche Ergebnisse der Gültigkeitsprüfung untersuchen.

4 Evaluation der Routingdaten

Die Datenmenge der gesammelten BGP-Daten ist erheblich, alle 5 Minuten werden die in den vergangenen 5 Minuten gesammelten BGP-Updates in ein Archiv transferiert. Die Anzahl der Einträge pro Archiv beträgt laut CIDR-Reports von Huston im Schnitt zwischen 100 und 200 Updates. Dies entspricht 12 Archiven pro Stunde, also 288 pro Tag. Pro Jahr ergeben sich so 105120 Archive. Mit 150 Einträgen pro Archiv ergeben sich damit über 15 Millionen BGP-Updates pro Jahr.

4.1 Entwicklung und Nutzung der Werkzeuge

Zur Untersuchung der Gültigkeit der Routingdaten ist es erforderlich, die BGP-Daten als auch die zeitlich dazu passenden ROA-Daten herunterzuladen und zu verarbeiten. Die dazu verwendete Skriptsprache ist Perl, mit ihr ist es dank guter Integration von regulären Ausdrücken und der Erweiterung der Funktionalität mittels des Perl CPANs möglich, die großen Datenmengen einfach zu verarbeiten. Zur Erzeugung der Grafiken wird die Matplotlib von Hunter (2007) eingesetzt. Als Betriebssystem wird Ubuntu 14.04 LTS verwendet, da alle in das Hauptprogramm zu integrierenden Programme für Linux entwickelt wurden. Auch auf anderen linuxartigen Betriebssystem sollten die Programme funktionieren, dieses wurde aber bisher nicht getestet.

4.1.1 Verarbeitung der BGP-Dumps

Mit dem Programm bgpdump der RIPE (2015) lassen sich die gesammelten Archive entpacken und anschließend nach Nachrichtentyp kategorisieren. Die hier eingesetzte Version von bgpdump stammt vom 16.07.2015. Eine beispielhafte Ausgabe kann Listing 2.1 entnommen werden. Anhand des Nachrichtentyps Announcement oder Withdrawal werden die Datensätze aus Zeitstempel, Origin-AS, Präfix, Präfixlänge, Mirror und Gültigkeit hinzugefügt oder wieder entfernt.

4.1.2 Verarbeitung der ROAs

Die gesammelten, historischen ROAs werden von der LACNIC (2015) bereitgestellt. Die LACNIC stellt unterschiedliche ROA-Daten zur Verfügung, hauptsächlich wird mit der Datei global-roa-prefixes.csv des ausgewählten Tages gearbeitet. Sollte diese nicht existieren, wird statt dessen ripe-ncc.tal-roa-prefixes.csv verwendet. Erst seit dem 13.08.2013 stellt LACNIC die global-roa-prefixes.csv zur Verfügung.

4.1.3 Verwendung der RTRLib zur Gültigkeitsprüfung

Mit Hilfe der RTRLib (Wählisch u. a., 2013) werden die ROAs der LACNIC des zu untersuchenden Zeitraums in die Präfix-Tabelle der RTRLib geladen. Die RTRLib bietet dann die Möglichkeit der Gültigkeitsprüfung der BGP-Announcements aus dem gleichen Zeitraum.

4.1.4 Gültigkeitsprüfung in der RTRLib

Nachdem die ROAs in die Präfixtabelle der RTRLib geladen wurden, kann die RTRLib zur Gültigkeitsprüfung der Routingannouncements verwendet werden. Hierzu wird die Methode *rtr_mgr_validate* der RTRLib verwendet.

```
rtr_mgr_validate(&conf, asn, &prefix, pfx_len, &result);
```

Listing 4.1: RTRLib

Das Listing 4.1 zeigt den Aufruf von *rtr_mgr_validate*, als Eingabe dienen die Werte *asn, prefix, pfx_len*. Das Ergebnis der Prüfung befindet sich in der Variable *result*, es wird an das aufrufende Hauptprogramm zurück geliefert. Die Einstellungen der RTRLib sind in *conf* abgelegt.

4.1.5 Validitätsprüfung im Hauptprogramm

Die Datensätze aus den Announcements werden erst heruntergeladen, dann entpackt und anschließend die zu dem Zeitpunkt des Announcements gültigen ROAs heruntergeladen und in die RTRLib geladen. Daraufhin wird jeder Datensatz an die RTRLib übermittelt und von ihr auf Gültigkeit geprüft. Das Ergebnis der Gültigkeitsprüfung wird von der RTRLib wieder zurückgegeben und zusammen mit Zeitstempel, Origin-AS, Präfix, Präfixlänge und Mirror gespeichert.

Abbildung 4.1 zeigt den schematischen Programmablauf sowie die beteiligten Kommunikationspartner. Als Aufrufparameter des Hauptprogramms dient der zu untersuchende Zeitraum.

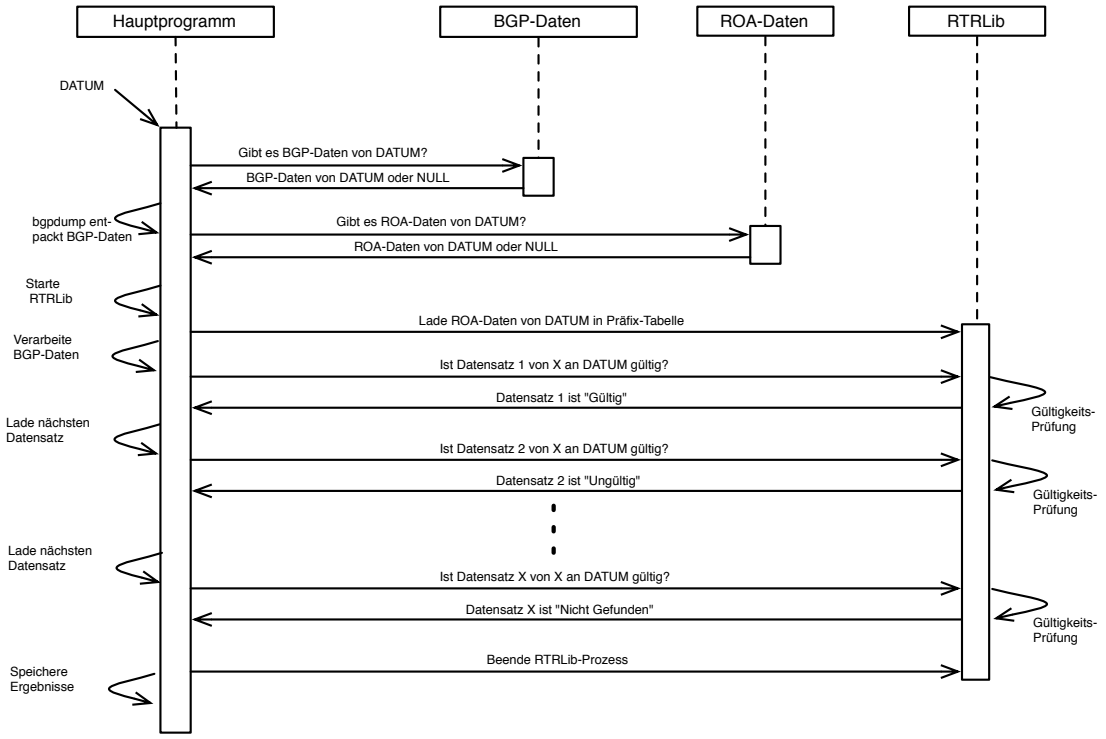

Abbildung 4.1: Ablauf des Hauptprogramms

4.2 Analyse der Daten

Folgender Programmteil des Hauptprogramms in Listing 4.2 beschreibt die Auswertung des Ergebnisses der Gültigkeitsprüfung und wird in einer Schleife für jeden Datensatz durchgeführt:

```
1  my $reiterate_count = 0;
2  my $j = $#tmp;  # letztes Element in AS-Pfad, Origin-AS
3  REVALUATE:
4  $data_out = "$oas,$pfx, $pln\n" # Uebertragung an RTRLib
5  my $valid = $data_in;   # Ergebnis der Pruefung der RTRLib
6
7  if ($valid == 0) { # valid
8      $valid_count++;
9      if ($reiterate_count != 0){
10         print $inv2val_file "NOW-VALID -> $oas -> $line";
11         $reiterate_count = 0;
12         }else{
```

```
13              if(!defined $dbhash2{"$pfx\/$pln\/$asn"} ||
14              $dbhash2{"$pfx\/$pln\/$asn"} ne $valid){
15                  $dbhash2{"$pfx\/$pln\/$asn"} = $valid; # change
16                  print $resf "$pfx\/$pln\/$asn;$ts;$monitor;$valid\n"
17              } #else: identischer Eintrag existiert bereits
18          }
19  elsif ($valid == 2) { # invalid
20      if ($reiterate_count == 0){
21          $invalid_count++;
22          print $inv_file $line;
23          if(!defined $dbhash2{"$pfx\/$pln\/$asn"} ||
24          $dbhash2{"$pfx\/$pln\/$asn"} ne $valid){
25              $dbhash2{"$pfx\/$pln\/$asn"} = $valid; # change
26              print $resf "$pfx\/$pln\/$asn;$ts;$monitor;$valid\n"
27          } #else: identischer Eintrag existiert bereits
28      }
29      while($j>0){ # solange AS-Pfad von rechts nach links durchgehen
30          $j--;        # bis valid oder links angekommen
31          $oas = $tmp[$j];
32          $reiterate_count++;
33          goto REVALUATE;
34      }
35  }
36  elsif ($valid == 1) { # not found
37      $not_found_count++;
38      if(!defined $dbhash2{"$pfx\/$pln\/$asn"} ||
39      $dbhash2{"$pfx\/$pln\/$asn"} ne $valid){
40          $dbhash2{"$pfx\/$pln\/$asn"} = $valid; # change
41          print $resf "$pfx\/$pln\/$asn;$ts;$monitor;$valid\n"
42      } #else: identischer Eintrag existiert bereits
43  }else{    $error_count++; }
```

Listing 4.2: Gültigkeitsprüfung

In die Ergebnisliste gehen die Einträge nur ein, wenn sie entweder vorher noch nicht erfasst wurden oder sich eine Veränderung der Gültigkeit ergibt. Dazu wird *dbhash2* verwendet, in den *pfx, pln* und *asn* als Key und *valid* als Value eingehen. So werden mehrfache, gleiche Einträge vermieden, die sich nur anhand des Zeitstempels unterscheiden. Sobald in der Ergebnisliste Einträge mehrfach vorkommen, muss es sich also um Gültigkeitswechsel handeln.

Einen Ausschnitt der Ergebnisliste zeigt Listing 4.3, die Spaltenbezeichnung kann Zeile 1 entnommen werden.

```
1 prefix/pln/OAS;timestamp;mirror;valid
2 ...
3 46.182.32.0/21/197426;1372636831;rrc00;0
4 46.182.32.0/21/197426;1377045673;rrc00;1
5 46.182.32.0/21/197426;1377216126;rrc00;0
6 46.182.32.0/24/197426;1381241875;rrc00;2
7 46.182.32.0/21/197426;1392542515;rrc00;1
8 46.182.32.0/21/197426;1392685434;rrc00;0
9 ...
```

Listing 4.3: Ausschnitt der Ergebnisliste

4.2.1 Analyse der Verbreitung des RPKI-Einsatzes

Für die Analyse der Verbreitung des Einsatzes einer RPKI werden stichprobenartig alle 30 Tage die Abzüge der Routingtabelle der RIPE untersucht. In diesen Dateien befinden sich alle zu diesem Zeitpunkt aktiven Routen, die dann auf ihre Gültigkeit geprüft werden. In der ersten Hälfte des Jahres 2013 sind die gesammelten ROA-Daten der LACNIC nur lückenhaft vorhanden, daher wurden dort nicht immer genau das 30-Tage-Intervall eingehalten, sondern der nächste Tag mit existierenden ROAs gewählt. So ist es trotz teilweise fehlender ROAs möglich, eine Übersicht von Januar 2013 bis Dezember 2015 zu erzeugen.

4.2.2 Veränderungen der Gültigkeit von “gültig” zu “ungültig”

Die ermittelten Gültigkeitswechsel ermöglichen eine Aussage über Wechsel von “gültig” zu “ungültig”, wenn sich das Ergebnis der Prüfung von 0 zu 2 ändert. In diesen Fällen wurde entweder eine ungültige Präfixlänge oder ein nicht durch ein gültiges ROA abgedecktes Origin-AS angegeben. Ursächlich dafür können sowohl Angriffe als auch Fehlkonfigurationen sein. Anhand der Dauer des ungültigen Zustandes lassen sich eingeschränkt Rückschlüsse auf die Ursache ziehen, da Angriffe meistens kurz andauern, während Fehlkonfigurationen auch länger aktiv sein können. Für Angriffe spricht auch eine Veränderung des Origin-AS, weil nur auf diese Weise Datenpakete entführt werden können. Bei einer ungültigen Präfixlänge und gültigem Origin-AS liegt eher eine Fehlkonfiguration zu Grunde. Listing 4.3 zeigt in den Zeilen 5 bis 6 einen entsprechenden Übergang, der durch eine falsche Präfixlänge verursacht wurde.

4.2.3 Veränderungen der Gültigkeit zu “gültig”

Im Fall eines Gültigkeitswechsels von “nicht gefunden” zu “gültig” ändert sich das Ergebnis der Prüfung von 1 zu 0. Bei einer Änderung von “ungültig” zu “gültig” wechselt das Ergebnis der Prüfung von 2 auf 0. Der erste Fall tritt auf, wenn ab einem bestimmten Zeitpunkt die RPKI erfolgreich eingesetzt wird. Der zweite Fall entsteht, nachdem eine Fehlkonfiguration behoben oder ein Angriff beendet oder abgewehrt wurde und bereits vor der Fehlkonfiguration bzw. dem Angriff die RPKI zum Einsatz kam. Listing 4.3 zeigt in den Zeilen 4 bis 5 und 7 bis 8 Übergange von “nicht gefunden” zu “gültig”.

4.2.4 Fehlkonfiguration durch ein ungültiges Origin-AS im AS-Pfad

Liefert das Ergebnis der Gültigkeitsprüfung “ungültig”, so wird die Prüfung erneut gestartet, dieses Mal wird aber nicht das hinterste AS im AS-Pfad, sondern das vorletzte an die RTRLib übertragen und das Ergebnis erneut bestimmt. Sollte dieses Ergebnis nun “gültig” sein, so handelt es sich um eine zu erkennende Fehlkonfiguration. Das Listing 4.2 zeigt diese Prüfung in Zeile 29-34.

4.2.5 Fehlkonfiguration durch falsche Präfixlänge

Durch die falsche Präfixlänge kann das Ergebnis der Gültigkeitsprüfung nicht “gültig” sein. Die maximale Präfixlänge für IPv4-Präfixe beträgt 24, für IPv6 48. Längere Präfixe sind für die RPKI nicht zulässig.

```
# BGP-Update mit Origin-AS 680, Praefix 141.22.0.0/24
#
# whois -h whois.cymru.com " -v -f -b -s -o -d 141.22.0.0/24"
# 680     | 141.22.0.0       | 141.22.0.0/16
```

Listing 4.4: Falsche Präfixlänge

Das Listing 4.4 zeigt, wie sich die korrekte Präfixlänge herausfinden lässt.

4.2.6 Fehlkonfiguration durch Routing von privaten AS-Nummern

Private AS-Nummern dürfen nur intern verwendet werden und sollten nicht in der DFZ geroutet werden. Trotzdem kann es durch route-leaks dazu kommen, dass es Routenankündigungen mit privaten AS-Nummern gibt.

```
# BGP-Update mit Origin-AS 65005, Praefix 141.22.0.0/16
#
```

```
# whois -h whois.cymru.com " -v -f -b -s -o -d 141.22.0.0/16"
# 680     | 141.22.0.0        | 141.22.0.0/16
```

Listing 4.5: Private-AS

Das Listing 4.5 zeigt an, welche AS-Nummer und welche Präfixlänge das Präfix 141.22.0.0/24 tatsächlich besitzt, denn die in der BGP-Nachricht genannte AS-Nummer 65005 hätte nicht verwendet werden sollen, sondern stattdessen die AS-Nummer 680.

4.2.7 Unterschiede in der Gültigkeitsprüfung verschiedener Monitore

Für die BGP-Daten stehen zwei unterschiedliche Datenquellen zur Verfügung. Die RPKI-Daten werden ausschließlich von der LACNIC bezogen, aber durch den Datenabgleich über rsync sollten sich hier keine Unterschiede bemerkbar machen.

Es finden daher zwei Prüfungen der BGP-Daten auf Gültigkeit statt, einmal mit den BGP-Daten der RIPE und ein zweites Mal mit den BGP-Daten des Route Views Archivs.

4.2.8 Prüfung des Ablaufzeitpunktes der ROAs

Jedes ROA hat ein Beginn- und einen End-Zeitpunkt seiner Gültigkeit. Aus den ROAs vom 24.12.2014 folgt ein zur Verdeutlichung gekürzter Auszug in Listing 4.6. Hier wird ein ROA für das AS1234 und das Präfix 198.48.0.0/22 mit maximaler Präfixlänge von 22 verwendet. Das ROA ist ab dem 31.01.2014 gültig, es läuft aber am 31.03.2015 ab.

```
rsync://rpki.apnic.net/A91...8.roa,AS1234,198.48.0.0/22,22,
2014-01-31 02:20:05,2015-03-31 23:59:59
```

Listing 4.6: Ablaufdatum eines ROAs

Sollte das ROA nun nicht bis zum 31.03.2015 durch ein länger gültiges ersetzt werden, so würde sich die Gültigkeit eines Routingannouncements ab dem 01.04.2015 von “gültig” zu “ungültig” ändern.

Die Prüfung findet statt, indem das Verwendungsdatum des ROAs mit seinem Ablaufdatum verglichen wird. Sollte das Ablaufdatum kleiner sein, handelt es sich um ein abgelaufenes ROA.

4.2.9 Besonderheit des Geschwister-AS

Geschwister-ASe gehören der selben Organisation an, haben aber unterschiedliche AS-Nummern und Präfixe. Als Datenquellen liegen die whois-Daten der RIPE und CYMRU vor, wobei die Daten der RIPE nur die ASe beinhalten, die sich auch in der Verwaltung der RIPE befinden.

```
whois -h whois.ripe.net "AS2595" | grep "org\-name" | cut -d " " -f8-
# CSP s.c. a r.l.

whois -h whois.ripe.net "AS2596" | grep "org\-name" | cut -d " " -f8-
# CSP s.c. a r.l.
```

Listing 4.7: Geschwister-AS

Das Listing 4.7 zeigt, wie über eine whois-Abfrage an whois.ripe.net zu einer AS-Nummer die dazu registrierte Organisation herausgefunden werden kann.

Durch den Vergleich der bis dato verwendeten AS-Nummern sowie deren zugehörigem Attribut der Organisation lassen sich bei Übereinstimmung der Organisation Geschwister-ASe erkennen. Da die beiden Organisationen die Daten unanhängig von einander gesammelt haben, sind Unterschiede in den Ergebnissen möglich.

4.3 Ergebnisse der Analyse

Zuerst werden alle Routenankündigungen der BGP-Updates von Juli 2013 bis Dezember 2015 auf Gültigkeit geprüft. Nur dort, wo es einen Wechsel bei der Gültigkeit gibt, gehen die Datensätze in die Analyse ein.

Zeitliche Lücken gibt es bei den von der LACNIC gesammelten ROAs. Sowohl zwischen dem 20.02.2015 und dem 02.03.2015, zwischen dem 04.04.2015 und dem 06.04.2015, als auch zwischen dem 27.10.2015 und dem 02.11.2015 fehlen die Daten. Für die Auswertung wurden in diesem Zeitraum die letzten gültigen ROAs vom 19.02.2015, 03.04.2015 bzw. 26.10.2015 verwendet. Die gesammelten BGP-Daten weisen keine Lücken auf.

4.3.1 Verbreitung des RPKI-Einsatzes

Die absolute Anzahl der als “gültig”, “ungültig” oder als “nicht gefunden” deklarierten Einträge in der Routingtabelle der RIPE kann in einem 30-Tage-Intervall von Anfang 2013 bis Ende 2015 ermittelt werden, da die in der ersten Hälfte des Jahres 2013 nur lückenhaft vorliegenden ROA-Daten in die Lücken des Intervalls fallen.

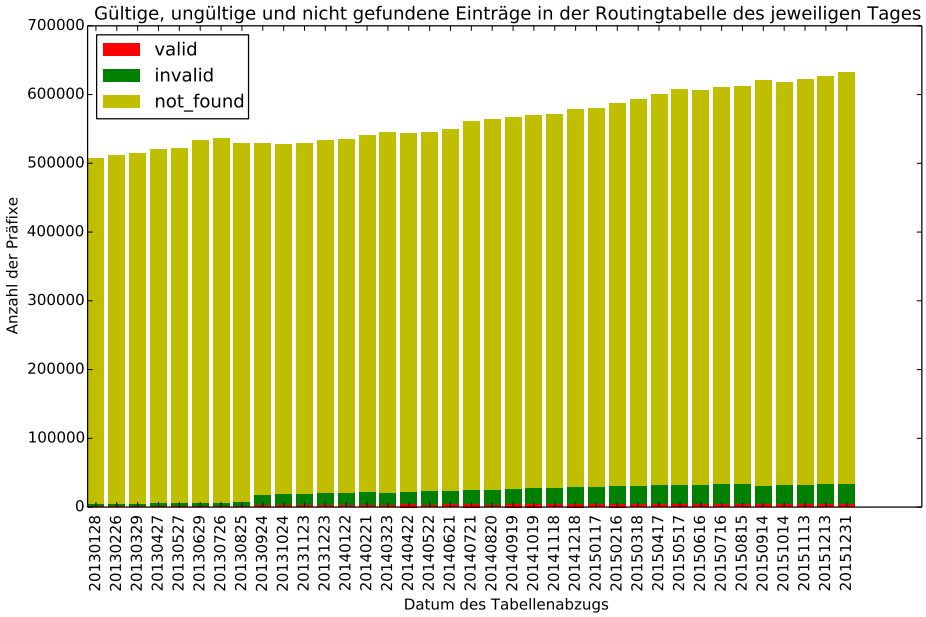

Abbildung 4.2: Ergebnisse der Gültigkeitsprüfung mit den BGP-Daten der Ripe

Abbildung 4.2 zeigt die Anzahl der als “gültig”, “ungültig” oder “nicht gefunden” bewerteten Routen aus den Tabellenabzügen des jeweiligen Tages. Man erkennt eine kontinuierliche Zunahme der “nicht gefunden” deklarierten Routen seit Oktober 2013. Da das Verhältnis von “gültig” und “ungültig” zu “nicht gefunden” recht klein ist, zeigt Abbildung 4.3 die gleichen Ergebnisse mit ausgeblendeten “nicht gefunden” Werten (vgl. Iamartino u. a. (2015)).

In Abbildung 4.3 erkennt man eine kontinuierliche Zunahme der als “gültig” deklarierten Routen, ebenso einen Sprung zwischen August und September 2013 sowie einen leichten Einbruch im September 2015. Der Sprung ist laut Iamartino u. a. darauf zurückzuführen, dass das X.509-Zertifikat der LACNIC Ende Dezember 2012 abgelaufen war und erst Mitte August 2013 erneuert wurde. Bei der APNIC gab es eine ähnliche Störung zwischen Januar und August 2013. Alle in diesem Zeitraum eigentlich “gültigen” Routenankündigungen waren damit nun “nicht gefunden”. Seit September 2013 ist das Problem behoben, daher steigen dort die “gültigen” Einträge um zehntausend, während die “nicht gefundenen” um zehntausend sinken.

Der Anteil der als “ungültig” deklarierten Routen liegt seit ca. April 2014 gleichbleibend zwischen vier- und fünftausend Einträgen.

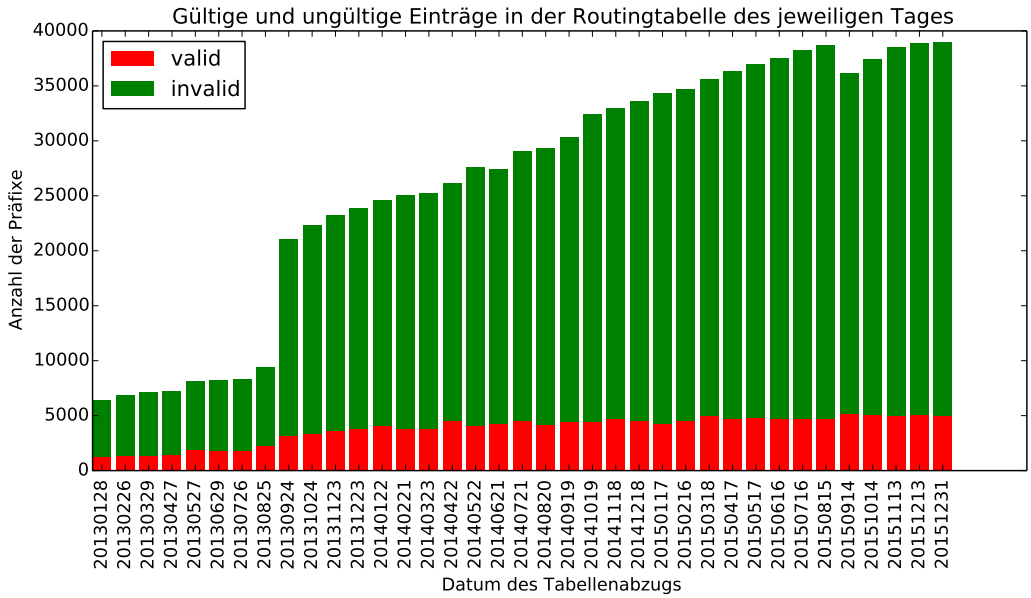

Abbildung 4.3: Ausgewählte Ergebnisse der Gültigkeitsprüfung mit den BGP-Daten der Ripe

4.3.2 Veränderungen der Gültigkeit von “gültig” zu “ungültig”

Im untersuchten Zeitraum fanden 746 Gültigkeitswechsel von “gültig” zu “ungültig” statt. Aufgeteilt nach dem Stichtag des Datenbankabzuges ergibt sich folgende Verteilung:

Datum	Anzahl
20130726	3
20130825	1
20130924	11
20131024	8
20131123	23
20131223	9
20140122	16
20140221	1
20140323	6
20140422	48
20140522	25
20140621	11
20140721	8

20140820	5
20140919	13
20141019	12
20141118	170
20141218	5
20150117	15
20150216	11
20150318	91
20150417	9
20150517	7
20150616	21
20150716	7
20150815	4
20150914	154
20151014	20
20151113	11
20151213	9
20151231	12

Tabelle 4.1: Gültigkeitswechsel von “gültig” zu “ungültig”

In Tabelle 4.1 fallen zwei Zeiträume auf, in denen es besonders viele Gültigkeitswechsel gegeben hat, zwischen dem 19.10.2014 und dem 18.11.2014 sowie zwischen dem 15.08.2015 und dem 14.09.2015. Die 170 Gültigkeitswechsel des ersten Zeitraums wurden nach Häufigkeit der in den Routenankündigungen genannten Origin-ASe sortiert, dabei wurden 7 Blöcke mit 10 oder mehr identischen Origin-ASen gefunden. All diese Blöcke gehören zu französischen ASen und bilden mit 153 Gültigkeitswechseln den Großteil dieses Zeitraums.

Letzterer passt zeitlich zum eben erwähnten Einbruch im September 2015, die Anzahl ist aber zu gering für den Rückgang von ca. dreitausend “gültigen” Routen. Die 154 Gültigkeitswechsel dieses Zeitraums wurden ebenfalls nach Häufigkeit des Vorkommens der Origin-ASe sortiert, hier wurden 3 Blöcke mit mehr als 10 identischen Origin-ASen gefunden. Diese Blöcke gehören alle zu equdorianischen ASen und weisen mit 130 Gültigkeitswechseln den Hauptteil dieses Zaitraums aus.

4.3.3 Veränderungen der Gültigkeit zu “gültig”

Eine Übersicht über alle Gültigkeitswechsel zeigt Abbildung 4.4

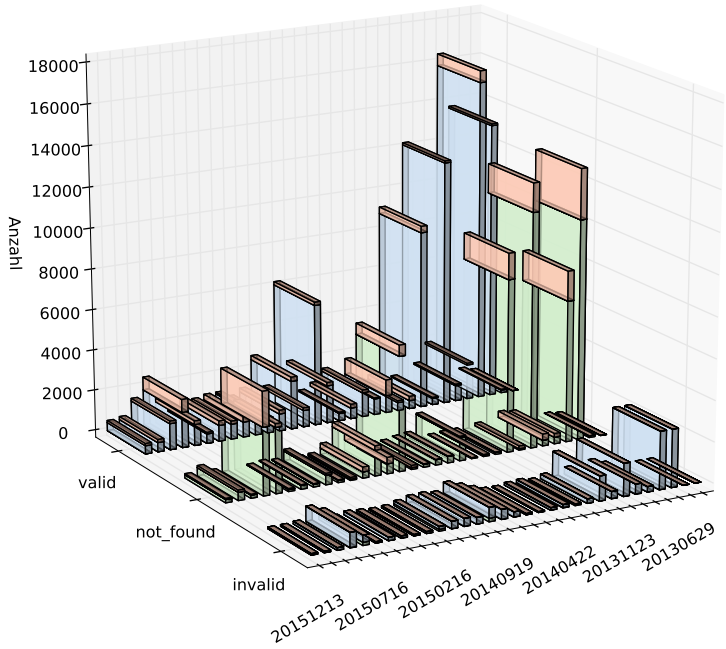

Abbildung 4.4: Alle Gültigkeitsveränderungen. Status vor dem Wechsel: blau - nicht gefunden, grün - gültig, rot - ungültig. Nach dem Wechsel: Sortierung in die entprechenden Spalten

Die linke Spalte zeigt die “gültigen”, die mittlere Spalte die “nicht gefundenen” und die rechte Spalte die “ungültigen” Routenankündigungen. Die Farbe beschreibt den vorherigen Status, blau bedeutet “nicht gefunden”, grün bedeutet “gültig” und rot bedeutet “ungültig”.

Deutlich erkennbar ist, dass von August bis September 2013 eine große Anzahl an Gültigkeitsveränderungen von “nicht gefunden” (blau) in der linken Spalte für “gültige” Routenankündigungen erscheint. Ebenso gibt es im gleichen Zeiraum in der mittleren Spalte für die “nicht gefundenen” Routenankündigungen einen großen Zuwachs, der aus vormals “gültigen” und “ungültigen” Routenankündigungen besteht.

Das Absinken der “gültigen” Einträge im September 2015 ist hier ebenfalls dargestellt, diese sind nun in der Spalte “nicht gefunden” dargestellt.

Die Veränderungen der Gültigkeit von “ungültig” zu “gültig” entspricht den roten Blöcken in der Spalte gültig.

4.3.4 Fehlkonfiguration durch ein ungültiges Origin-AS im AS-Pfad

Zur Analyse wurden alle als “ungültig” deklarierten Routenankündigungen gesammelt und noch einmal geprüft, dieses Mal aber mit dem vorletzten AS im AS-Pfad als Origin-AS.

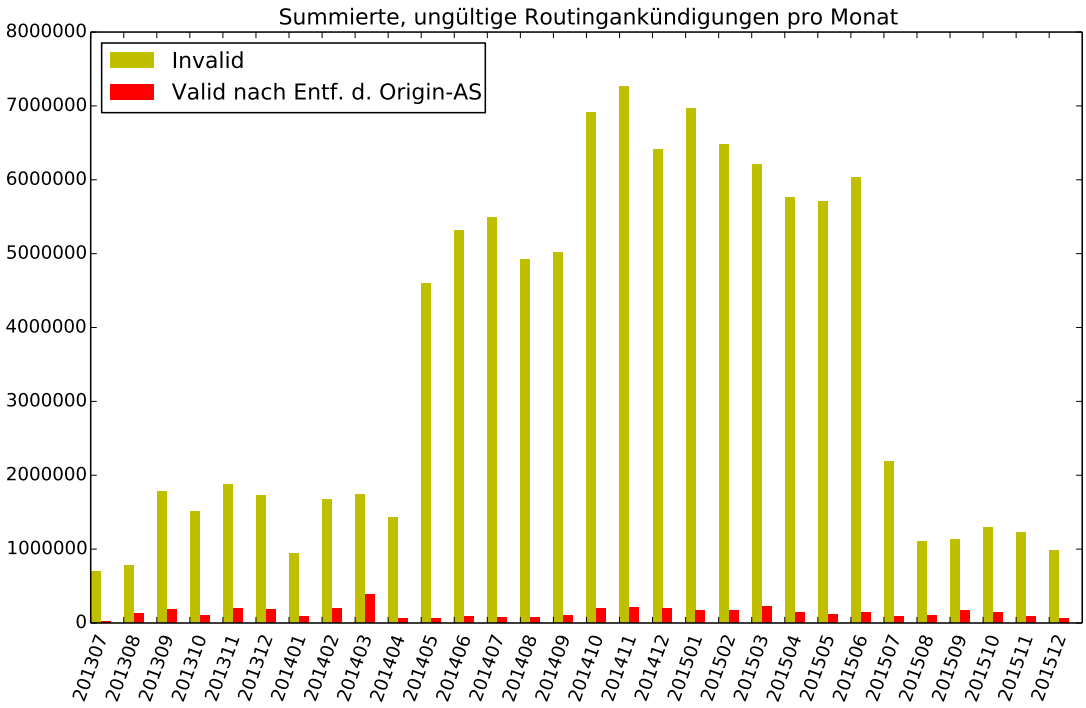

Abbildung 4.5: Alle ungültigen Routenankündigungen (gelb) sowie ungültige Routenankündigungen mit gültigem Origin-AS auf dem AS-Pfad (rot)

Abbildung 4.5 zeigt die nach Monaten aufsummierten “ungültigen” Routenankündigungen in gelb. Die roten Werte entsprechen der Teilmenge der “ungültigen” Routenankündigungen, die nach Entfernung des Origin-AS bei erneuter Prüfung als “gültig” bewertet werden.

4.3.5 Fehlkonfiguration durch falsche Präfixlänge

Es werden alle ungültigen Routenankündigungen auf ihre Präfixlänge hin untersucht.

Aus allen 54061 ungültigen Routenankündigungen überschreiten 11757 die maximale Präfixlänge für IPv4 und IPv6. Dieses entspricht ca. 21% aller ungültigen Routenankündigungen.

4.3.6 Fehlkonfiguration durch Routing von privaten AS-Nummern

Insgesamt wurden in 57427 Routenankündigungen private AS-Nummern gefunden. Hiervon hat die Gültigkeitsprüfung 379 als "ungültig", 5 als "gültig" und 57043 als "nicht gefunden" ergeben. Für den Großteil der als "nicht gefunden" deklarierten Routenankündigungen existiert also kein ROA. Besonders auffällig sind die 5 gültigen Einträge in Listing 4.8, für die es keine ROAs geben dürfte.

```
1 2a02:d58:200a::/48/64520;1413837912;rrc00;0
2 179.0.20.0/25/65105;1404498378;rrc00;0
3 179.0.20.128/25/65105;1404498378;rrc00;0
4 179.0.21.128/26/65104;1404498378;rrc00;0
5 179.0.22.64/26/65105;1404498378;rrc00;0
```

Listing 4.8: gültige, private-ASN

Laut whois.lacnic.net gehören die Präfixe in Zeile 2-5 aus Listing 4.8 eigentlich zum AS52470, welches der Organisation CONARE in Costa Rica zugeordnet ist. Die vier Einträge weisen auch den identischen Zeitstempel auf, es handelt sich um den 04.07.2014, 20:26:18 Uhr. Es existieren ebenfalls als "gültig" deklarierte Routenankündigungen für die genannten Präfixe mit dem Origin-AS 52470. Fragt man whois.ripe.net nach dem Präfix in Zeile 1, erfährt man, dass dieses dem AS44919 zugeordnet ist. Die zugehörige Organisation heißt eqipe GmbH aus der Schweiz. Für das hier genannte Präfix wurde keine weitere Routenankündigung annonciert.

4.3.7 Unterschiede in der Gültigkeitsprüfung verschiedener Monitore

Die Daten von der RIPE kommen aus Amsterdam, die Daten von Route Views aus Oregon. Durch diese geographisch weit auseinanderliegenden Orte besteht die Möglichkeit, zu untersuchen, ob die Distanz Einfluss hat auf die Verbreitung der Routingdaten und auf die Ergebnisse der Gültigkeitsprüfung.

Abbildung 4.6 zeigt die Anzahl der als "gültig", "ungültig" oder "nicht gefunden" bewerteten Routen aus den Tabellenabzügen des jeweiligen Tages. Man erkennt auch hier eine kontinuierliche Zunahme der als "nicht gefunden" deklarierten Routen seit Oktober 2013. Zur besseren

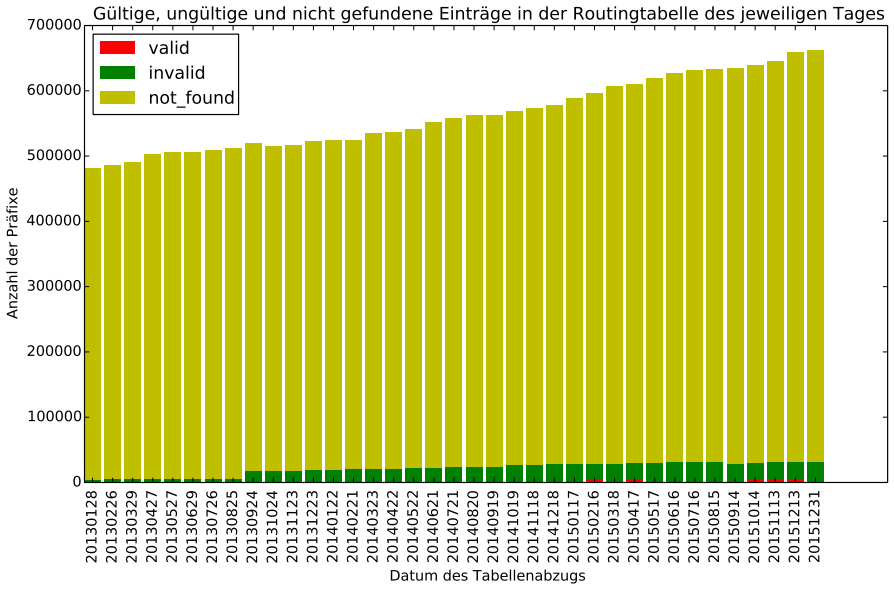

Abbildung 4.6: Ergebnisse der Gültigkeitsprüfung mit den BGP-Daten des Route Views Archive

Übersicht zeigt Abbildung 4.7 die gleichen Ergebnisse mit ausgeblendeten “nicht gefunden” Werten.

Abbildung 4.7 mit den Route-Views-Daten zeigt ein ähnliches Diagramm wie die Abbildung 4.3 mit den RIPE-Daten.

Die in den Abbildungen 4.2 und 4.6 dargestellten Werte können folgender Tabelle entnommen werden.

		RIPE			Route Views	
Datum	gültig	ungültig	nicht gefunden	gültig	ungültig	nicht gefunden
20130128	5137	1306	502894	4599	612	476414
20130226	5541	1322	506223	5002	617	480908
20130329	5746	1368	509125	5172	632	485516
20130427	5809	1444	513838	5242	704	496883
20130527	6213	1866	516338	5731	819	500115
20130629	6382	1865	526557	5818	698	499445
20130726	6470	1821	530420	5869	649	502971
20130825	7178	2206	521823	6486	996	505904
20130924	17892	3204	511922	17153	1951	502153

20131024	18977	3303	508760	18345	2029	496831
20131123	19613	3613	510080	18764	2200	498162
20131223	20096	3821	513105	19177	2340	503676
20140122	20492	4061	514514	19516	2473	505111
20140221	21286	3810	519206	20073	2555	503903
20140323	21439	3800	523951	20438	2502	514437
20140422	21620	4531	521546	20748	3181	515471
20140522	23523	4035	521180	22516	2751	519044
20140621	23197	4266	526223	22083	2962	529446
20140721	24557	4508	535965	23480	2906	534156
20140820	25167	4153	538197	24027	2826	538902
20140919	25868	4470	541058	24686	3176	538153
20141019	27983	4464	541401	26950	2962	541695
20141118	28246	4697	543644	27221	3186	546864
20141218	29111	4478	549650	27944	2938	549380
20150117	30057	4294	550868	28968	3089	559466
20150216	30189	4477	556992	29035	3264	567836
20150318	30646	4955	562851	29382	3521	577914
20150417	31629	4694	568432	30303	3545	579606
20150517	32184	4775	575163	30817	3099	589182
20150616	32794	4710	573816	31429	3042	594443
20150716	33497	4719	576838	31978	2966	599816
20150815	33963	4729	577949	32560	3028	600560
20150914	30976	5128	589210	29303	3230	605339
20151014	32300	5058	585846	30614	3275	608568
20151113	33499	5038	589093	31707	3370	613271
20151213	33817	5055	593227	32004	3597	627201
20151231	34009	4964	599089	32194	3431	630701

Tabelle 4.2: Ergebnisse der Gültigkeitsanalyse der Routingtabellenabzüge

Tabelle 4.2 zeigt die in den Abbildungen 4.2 und 4.6 dargestellten Gültigkeitswerte an den angegebenen Tagen. Man erkennt eine relativ gute Übereinstimmung der Ergebnisse von RIPE und Route Views, wobei die Werte für “gültig” und “ungültig” ca. um eintausend Einträge höher

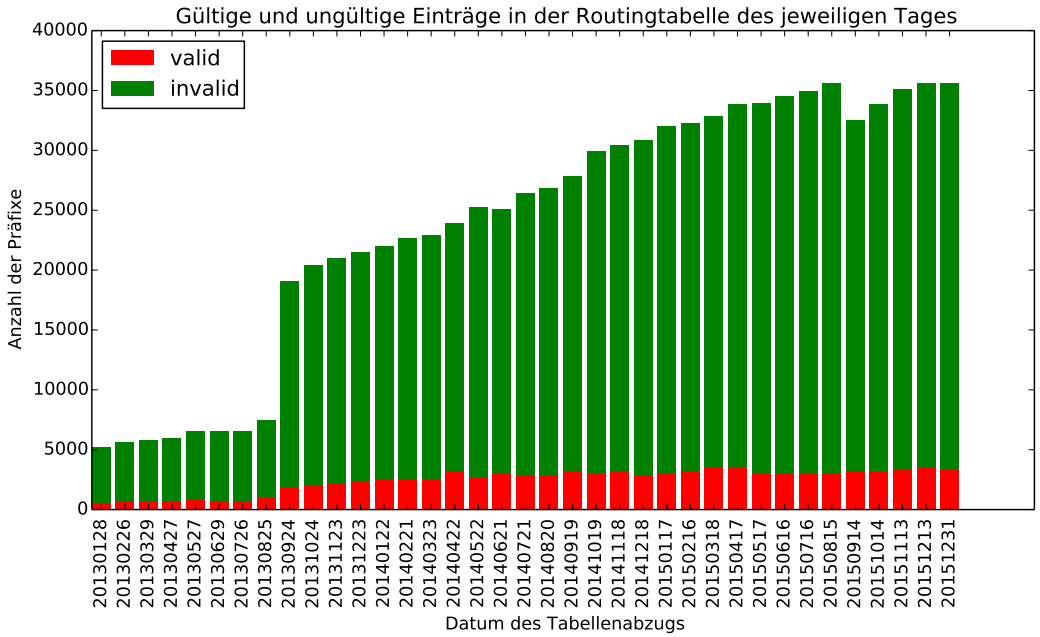

Abbildung 4.7: Ausgewählte Ergebnisse der Gültigkeitsprüfung mit den BGP-Daten des Route Views Archive

sind für die RIPE. Trotzdem weisen die Einträge die gleichen Trends auf, wie beispielsweise den sprunghaften Anstieg im September 2013 bei den “gültigen” Routen.

4.3.8 Untersuchter Ablaufzeitpunkt der ROAs

Alle ROA-Daten der LACNIC wurden auf ein bereits überschrittenes Ablaufdatum am Tag ihres Einsatzes kontrolliert, es wurde kein einziges abgelaufenes ROA gefunden. Die gesamte Zertifikatskette der ROAs bis hinauf zum Vertrauensanker wurde nicht geprüft, lediglich das Ablaufdatum des ROAs selber. Es besteht also die Möglichkeit, dass durch ein abgelaufenes Zertifikat eines RIRs alle von diesem RIR signierten ROAs ungültig werden.

4.3.9 Besonderheit des Geschwister-AS

Folgende ASe gehören laut cymru.com zur gleichen Organistion:

ASN	Organisation
4262	California Education and Research Federation Network
4263	California Education and Research Federation Network
4264	California Education and Research Federation Network
4265	California Education and Research Federation Network
4266	California Education and Research Federation Network
4267	California Education and Research Federation Network
4269	California Education and Research Federation Network
8068	Microsoft Corporation,US
8075	Microsoft Corporation,US
17225	AT&T Enhanced Network Services,US
17226	AT&T Enhanced Network Services,US
17227	AT&T Enhanced Network Services,US
17228	AT&T Enhanced Network Services,US
17229	AT&T Enhanced Network Services,US
17230	AT&T Enhanced Network Services,US
17231	AT&T Enhanced Network Services,US
17232	AT&T Enhanced Network Services,US
17233	AT&T Enhanced Network Services,US
28000	LACNIC - Latin American and Caribbean IP address,UY
28001	LACNIC - Latin American and Caribbean IP address,UY
28002	LACNIC - Latin American and Caribbean IP address,UY
52224	LACNIC - Latin American and Caribbean IP address,UY
58691	DELTA-IIG-BD Delta Infocom Limited.,BD
58749	DELTA-IIG-BD Delta Infocom Limited.,BD
58752	DELTA-IIG-BD Delta Infocom Limited.,BD
58886	DELTA-IIG-BD Delta Infocom Limited.,BD
58892	DELTA-IIG-BD Delta Infocom Limited.,BD
58953	DELTA-IIG-BD Delta Infocom Limited.,BD
59375	DELTA-IIG-BD Delta Infocom Limited.,BD
133109	DELTA-IIG-BD Delta Infocom Limited.,BD

133153	DELTA-IIG-BD Delta Infocom Limited.,BD
133180	DELTA-IIG-BD Delta Infocom Limited.,BD
133608	DELTA-IIG-BD Delta Infocom Limited.,BD
37674	Millenium,MU
327913	Millenium,MU
327914	Millenium,MU

Tabelle 4.3: Geschwister-ASe laut den Daten von cymru.com

Bei all den genannten Geschwister-ASen in Tabelle 4.3 fand im untersuchten Zeitraum mindestens ein Gültigkeitswechsel statt.

Folgende ASe gehören laut ripe.net zur gleichen Organistion:

ASN	Organisation	ROAs vorhanden
2595	CSP s.c. a r.l.	ja
2596	CSP s.c. a r.l.	nein
5483	Magyar Telekom plc.	ja
15545	Magyar Telekom plc.	ja
15555	Magyar Telekom plc.	ja
15752	BP International Ltd	ja
15753	BP International Ltd	ja
8972	PlusServer AG	nein
21499	PlusServer AG	ja
21501	PlusServer AG	ja
25074	PlusServer AG	ja
35329	PlusServer AG	ja
13110	INEA S.A.	ja
33868	INEA S.A.	ja
33869	INEA S.A.	ja
8674	NETNOD Internet Exchange i Sverige AB	ja
20943	NETNOD Internet Exchange i Sverige AB	ja
29216	NETNOD Internet Exchange i Sverige AB	ja
39840	NETNOD Internet Exchange i Sverige AB	ja
39870	NETNOD Internet Exchange i Sverige AB	ja
39871	NETNOD Internet Exchange i Sverige AB	ja

57021	NETNOD Internet Exchange i Sverige AB	ja
44574	AS44574 Networks Limited	ja
59676	AS44574 Networks Limited	ja
30746	Esgob Ltd	ja
60035	Esgob Ltd	ja
60036	Esgob Ltd	ja
60564	Esgob Ltd	ja
42044	CentralNic Ltd	ja
60890	CentralNic Ltd	ja
199330	CentralNic Ltd	ja
201303	CentralNic Ltd	ja
201304	CentralNic Ltd	ja
203961	CentralNic Ltd	ja
204055	CentralNic Ltd	ja

Tabelle 4.4: Geschwister-ASe laut den Daten von ripe.net

Auch bei all den genannten Geschwister-ASen in Tabelle 4.4 fand im untersuchten Zeitraum mindestens ein Gültigkeitswechsel statt. Bei den Daten der Ripe wurde zusätzlich geprüft, ob für alle Geschwister ROAs ausgestellt wurden.

Die ersten beiden Einträge in Tabelle 4.4 zeigen, dass nur für AS2595 ROAs ausgestellt wurden, für AS2596 ist dies nicht geschehen. Ebenso sind nicht für alle ASe der PlusServer AG ROAs ausgestellt worden.

```
# cat results.csv | egrep -e "/2595;"
194.116.0.0/18/2595;1372636840;rrc00;0
194.116.0.0/18/2595;1377064309;rrc00;1
194.116.0.0/18/2595;1377216124;rrc00;0
194.116.0.0/18/2595;1392542594;rrc00;1
194.116.0.0/18/2595;1392685565;rrc00;0
2001:848::/32/2595;1372636845;rrc00;0
2001:848::/32/2595;1377066014;rrc00;1
2001:848::/32/2595;1377256044;rrc00;0
2001:848::/32/2595;1392530446;rrc00;1
2001:848::/32/2595;1392719453;rrc00;0
```

```
# cat results.csv | egrep -e "/2596;"
194.116.60.0/22/2596;1383834404;rrc00;2
194.116.60.0/22/2596;1392478353;rrc00;1
194.116.60.0/22/2596;1392684760;rrc00;2
2001:848:804::/48/2596;1384167186;rrc00;2
2001:848:804::/48/2596;1392478350;rrc00;1
2001:848:804::/48/2596;1392694820;rrc00;2
```

Listing 4.9: Geschwister-AS-Gültigkeitsprüfung

Das Listing 4.9 zeigt die unterschiedlichen Gültigkeitswechsel für verschiedene Präfixe für die beiden Geschwister-ASe AS2595 und AS2596. Da für AS2596 kein gültiges ROA ausgestellt wurde, kann das Ergebnis der Gültigkeitsprüfung nicht "gültig" sein. Äquivalent verhält es sich mit dem AS8972 der PlusServer AG.

4.3.10 Ergebnisse der Gültigkeitsprüfung

Eine Übersicht über alle Gültigkeitsergebnisse zeigt Abbildung 4.8. "Gültige" Routenankündigungen sind grün markiert, "ungültige" rot und dort, wo die Prüfung "nicht gefunden" ergibt, sind diese blau markiert.

Man erkennt in Abbildung 4.8, dass die Anzahl der "gültigen" Routenankündigungen kontinuierlich steigt. Ebenso wächst die Anzahl der "nicht gefundenen" Routenankündigungen seit Oktober 2013 kontinuierlich. Die "ungültigen" nehmen von Januar 2013 bis April 2014 zu und stagnieren dann bis Dezember 2015 zwischen vier- und fünftausend Einträgen.

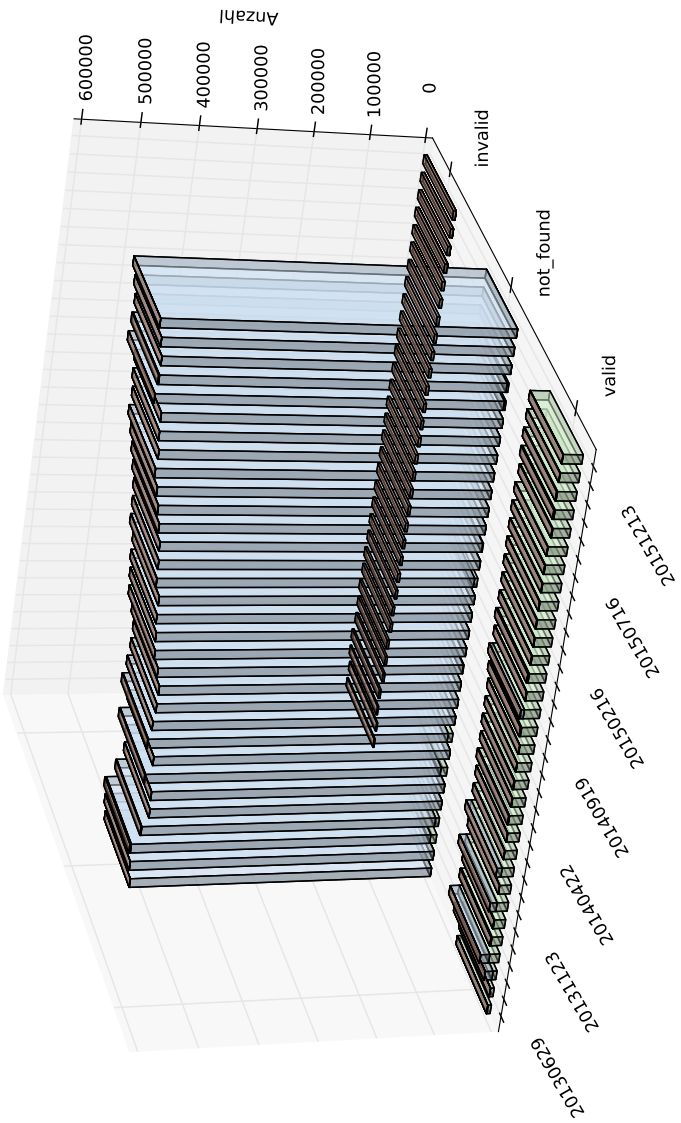

Abbildung 4.8: Alle Ergebnisse der Gültigkeitsprüfung mit Markierungen der Veränderungen. Gültige Routenankündigungen sind grün markiert, ungültige Routenankündigungen rot und in der Gültigkeitsprüfung nicht gefundene Routenankündigungen blau

5 Fazit und Ausblick

5.1 Zusammenfassung und Fazit

Die Adaption der RPKI findet bisher nur sehr langsam statt, das Verhältnis von "gültigen" zu "nicht gefundenen" Einträgen stieg von 1,02% im Januar 2013 auf 5,76% im Dezember 2015. Die Quote der "ungültigen" Routenankündigungen liegt in Bezug auf "nicht gefundene" Einträge deutlich unter 1%. Die Anzahl der "ungültigen" Routenannouncements ist relativ konstant und nicht rückläufig, wie man nach dem Abbau einer anfänglichen Verunsicherung erwarten würde. Gehäufte Gültigkeitsveränderungen fanden nur in der zweiten Jahreshälfte von 2013 statt. Ursächlich dafür war die Zertifikatserneuerung der LACNIC und der APNIC, nachdem deren Zertifikat ca. ein halbes Jahr lang abgelaufen war. Anschließend gab es nur noch wenige Gültigkeitswechsel. Auch Unterschiedliche Monitore zum Aufzeichnen der BGP-Daten haben keinen Einfluss auf die Ergebnisse der Gültigkeitsprüfung, die Daten von der RIPE und vom Route Views Archive weisen eine große Übereinstimmung auf.

Der Einsatz einer RPKI birgt Risiken durch Fehlkonfigurationen. Die Analyse der "ungültigen" Routenankündigungen ergibt, dass nur ein kleiner Teil durch ein weiter links im AS-Pfad stehendes, alternatives Origin-AS in eine "gültige" Routenankündigung gewandelt werden kann. Es handelt sich hierbei um ein selten auftretendes Konfigurationsproblem, bei dem das eigentliche Origin-AS erst als zweites AS im AS-Pfad erscheint. Verbreiteter sind überschrittene maximale Präfixlängen, die nicht durch ein gültiges ROA abgedeckt sein können. Dies betrifft ca. ein Fünftel aller "ungültigen" Routenankündigungen. Auch das Routen von privaten AS-Nummern ist eine Fehlkonfiguration, trotzdem wurden 57427 Routenankündigungen mit privaten AS-Nummern gefunden, von denen sogar 5 ein gültiges ROA aufwiesen. Es wurden keine ROAs mit überschrittenem Ablaufdatum gefunden, dies zeigt, dass die ROAs bisher immer fristgerecht verlängert wurden. Anders sieht es mit den Zertifikaten zum Signieren der ROAs aus, hier gab es seit Januar 2013 Probleme mit abgelaufenen Zertifikaten, die erst im August 2013 behoben wurden. Ein letztes Konfigurationsproblem betrifft die Geschwister-ASe, deren Zahl aber gering ist. Es kommt vor, dass nicht für jedes Geschwisterteil ROAs ausgestellt wurden und Präfixe mit dem Origin-AS annonciert werden, für welches eben kein ROA vorhanden

ist. Diese Routeankündigungen können nicht "gültig" sein. Für all diese Fehlkonfigurationen gibt es kein Monitoring, so dass die ISPs über fehlgeschlagene Gültigkeitsprüfungen nicht informiert werden und nur wenig Übersicht über die Gültigkeit ihrer Präfixe haben.

Als "ungültig" geprüfte Routenankündigungen haben für das Routing zur Zeit keine Konsequenzen, da diese Routen in den Routingpolicies nicht abgelehnt werden. Würde es bei einer Routingpolicy, die als "ungültig" erkannte Routenankündigung verwirft, zu Fehlkonfigurationen der RPKI wie zu große Präfixlängen oder route-leaks mit privaten AS-Nummern kommen, so käme es zu Ausfällen der Erreichbarkeit dieser Präfixe. Weiterhin ist der Aufwand zur Absicherung der Routenankündigungen recht hoch, da für jede Kombination von Präfix zu AS ein ROA erstellt und signiert werden muss. Durch einen höheren Automatisierungsgrad könnte das Erstellen der ROAs vereinfacht werden und so die Verbreitung der RPKI vorangetrieben werden. Dies wäre wünschenswert, da der Einsatz einer RPKI wirkungsvoll Manipulationen des Origin-AS bei den Routenankündigungen und damit fast alle hier gezeigten Angriffe verhindert. Nur die path-shortening-attack, bei der das Origin-AS nicht verändert wird, lässt sich nicht durch den Einsatz einer RPKI verhindern, da nicht der gesamte AS-Pfad in die Gültigkeitsprüfung eingeht. Außerdem sind nur dort, wo es bereits gültige ROAs gibt, die Origin-ASe gegen Manipulation geschützt. Da aber ca. 95% der Routenankündigung als Ergebnis der Gültigkeitsprüfung "nicht gefunden" aufweisen, profitieren diese 95% bisher nicht vom Einsatz einer RPKI. Selbst wenn einige ISPs nicht vorhaben, ihre Routenauswahl mittels des Einsatzes einer RPKI abzusichern, wäre es vorteilhaft, für ihre Präfixe ROAs auszustellen und so Anhaltspunkte für die Legitimität von Routenankündigungen für ihre Präfixe zu liefern.

Als Ergebnis der vorliegenden Arbeit lässt sich feststellen, dass der Einsatz einer RPKI deutlich zur Sicherheit des BGPs beitragen würde, wenn die Verbreitung der RPKI schneller voranschreiten würde. Gerade die großen Webseiten und CDNs setzen für ihre ASe unterdurchschnittlich auf den Einsatz einer RPKI

5.2 Ausblick und offene Fragen

Die bereits erwähnte path-shortening-attack könnte durch den Einsatz von BGPSEC (Lepinski, 2015) verhindert werden. BGPSEC bietet eine Validierung des gesamten AS-Pfades, nicht nur des Origin-ASes. Jedes AS signiert hier die BGP-Nachricht, so dass das Präfix und der komplette AS-Pfad überprüfbar werden. Auch die Signaturen der anderen ASe im AS-Pfad sind an die Nachricht angehängt. Path-shortening-Angriffe werden somit verhindert.

Fraglich bleibt, wie die Adaption der RPKI durch die ISPs beschleunigt werden könnte. Eventuell fehlt auch Vertrauen auf die Sicherheit und Zuverlässigkeit der RPKI. Zunächst entstehende Kosten für Personal, Hard- und Software mögen vielleicht manche ISPs vom Einsatz einer RPKI abhalten, die sich jedoch im Laufe der Zeit aufgrund der erhöhten Sicherheit und daraus resultierend weniger Ausfälle im Routing amortisieren.

Auch die fehlende Transparenz bei den Routingpolicies und der Mangel an Konsequenzen für als "ungültig" geprüfte Routenankündigungen mögen zur langsamen Verbreitung des Einsatzes der RPKI beitragen. Durch die Ablehnung dieser als "ungültig" deklarierten Routenankündigungen in den Routingpolicies könnte die Nutzung der RPKI beschleunigt werden.

Zukünftig könnten Ausfälle, wie die durch die Pakistan Telecom verursachte Sperrung von Youtube, durch den Einsatz einer RPKI verhindert werden.

Literaturverzeichnis

[Ballani u. a. 2007] Ballani, Hitesh ; Francis, Paul ; Zhang, Xinyang: A Study of Prefix Hijacking and Interception in the Internet. In: *SIGCOMM Comput. Commun. Rev.* 37 (2007), August, Nr. 4, S. 265–276. – ISSN 0146-4833

[van Beijnum 2002] Beijnum, Iljitsch van: *BGP - building reliable networks with the border gateway protocol.* O'Reilly, 2002. – ISBN 978-0-596-00254-1

[Bellovin 1989] Bellovin, S. M.: Security Problems in the TCP/IP Protocol Suite. In: *SIGCOMM Comput. Commun. Rev.* 19 (1989), April, Nr. 2, S. 32–48. – ISSN 0146-4833

[Bush und Austein 2013] Bush, R. ; Austein, R.: The Resource Public Key Infrastructure (RPKI) to Router Protocol / IETF. January 2013 (6810). – RFC

[Butler u. a. 2010] Butler, Kevin ; Farley, Toni R. ; McDaniel, Patrick ; Rexford, Jennifer: A survey of BGP security issues and solutions. In: *Proceedings of the IEEE* 98 (2010), Nr. 1, S. 100–122

[Cooper u. a. 2008] Cooper, D. ; Santesson, S. ; Farrell, S. ; Boeyen, S. ; Housley, R. ; Polk, W.: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile / IETF. May 2008 (5280). – RFC

[Cooper u. a. 2013] Cooper, Danny ; Heilman, Ethan ; Brogle, Kyle ; Reyzin, Leonid ; Goldberg, Sharon: On the Risk of Misbehaving RPKI Authorities. In: *Proceedings of the Twelfth ACM Workshop on Hot Topics in Networks.* New York, NY, USA : ACM, 2013 (HotNets-XII), S. 16:1–16:7. – ISBN 978-1-4503-2596-7

[Gavrichenkov 2015] Gavrichenkov, Artyom: Breaking HTTPS with BGP hijacking. In: *BlackHat USA. Briefings* (2015)

[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. – ISSN 1542-7730

[Goldberg u. a. 2010] Goldberg, Sharon ; Schapira, Michael ; Hummon, Peter ; Rexford, Jennifer: How Secure Are Secure Interdomain Routing Protocols. In: *Proceedings of the ACM SIGCOMM 2010 Conference*. New York, NY, USA : ACM, 2010 (SIGCOMM '10), S. 87–98. – ISBN 978-1-4503-0201-2

[Heffernan 1998] Heffernan, A.: Protection of BGP Sessions via the TCP MD5 Signature Option / IETF. August 1998 (2385). – RFC

[Hunter 2007] Hunter, J. D.: Matplotlib: A 2D graphics environment. In: *Computing In Science & Engineering* 9 (2007), Nr. 3, S. 90–95

[Huston und Michaelson 2012] Huston, G. ; Michaelson, G.: Validation of Route Origination Using the Resource Certificate Public Key Infrastructure (PKI) and Route Origin Authorizations (ROAs) / IETF. February 2012 (6483). – RFC

[Huston 2015] Huston, Geoff: *CIDR REPORT for 4 Oct 15*. 2015. – URL http://www.cidr-report.org/as2.0/. – Zugriffsdatum: 04.10.2015

[Iamartino u. a. 2015] Iamartino, Daniele ; Pelsser, Cristel ; Bush, Randy: Measuring BGP Route Origin Registration and Validation. In: Mirkovic, Jelena (Hrsg.) ; Liu, Yong (Hrsg.): *Passive and Active Measurement* Bd. 8995. Springer International Publishing, 2015, S. 28–40. – ISBN 978-3-319-15508-1

[Karlin u. a. 2005] Karlin, Josh ; Forrest, Stephanie ; Rexford, Jennifer: Pretty good bgp: Protecting bgp by cautiously selecting routes / University of New Mexico, Octber. 2005. – Forschungsbericht

[Kent u. a. 2000] Kent, Stephen ; Lynn, Charles ; Mikkelson, Joanne ; Seo, Karen: Secure Border Gateway Protocol (S-BGP. In: *IEEE Journal on Selected Areas in Communications* 18 (2000), S. 103–116

[LACNIC 2015] LACNIC: *rpki/batch-validation*. 2015. – URL http://mvuy10.labs.lacnic.net/rpki/batch-validation/. – Zugriffsdatum: 02.12.2015

[Lepinski und Kent 2012] Lepinski, M. ; Kent, S.: An Infrastructure to Support Secure Internet Routing / IETF. February 2012 (6480). – RFC

[Lepinski u. a. 2012] Lepinski, M. ; Kent, S. ; Kong, D.: A Profile for Route Origin Authorizations (ROAs) / IETF. February 2012 (6482). – RFC

[Lepinski 2015] Lepinski, Matthew: BGPsec Protocol Specification / Internet Engineering Task Force. Internet Engineering Task Force, Dezember 2015 (draft-ietf-sidr-bgpsec-protocol-14). – Internet-Draft. – URL https://tools.ietf.org/html/draft-ietf-sidr-bgpsec-protocol-14. Work in Progress

[Lychev u. a. 2013] Lychev, Robert ; Goldberg, Sharon ; Schapira, Michael: BGP Security in Partial Deployment: Is the Juice Worth the Squeeze? In: *CoRR* abs/1307.2690 (2013)

[Mitchell 2013] Mitchell, J.: Autonomous System (AS) Reservation for Private Use / IETF. July 2013 (6996). – RFC

[Mohapatra u. a. 2013] Mohapatra, P. ; Scudder, J. ; Ward, D. ; Bush, R. ; Austein, R.: BGP Prefix Origin Validation / IETF. January 2013 (6811). – RFC

[Murphy 2006] Murphy, S.: BGP Security Vulnerabilities Analysis / IETF. January 2006 (4272). – RFC

[Piscitello 2012] Piscitello, D: Guidance for preparing domain name orders, seizures takedowns / ICANN. März 2012. – Forschungsbericht

[Postel 1981] Postel, J.: Transmission Control Protocol / IETF. September 1981 (793). – RFC

[Rekhter und Li 1994] Rekhter, Y. ; Li, T.: A Border Gateway Protocol 4 (BGP-4) / IETF. July 1994 (1654). – RFC

[Rekhter u. a. 2006] Rekhter, Y. ; Li, T. ; Hares, S.: A Border Gateway Protocol 4 (BGP-4) / IETF. January 2006 (4271). – RFC

[Remes 2015] Remes, Wim: Internet Plumbing For Security Professionals: The State Of BGP Security. In: *BlackHat USA. Briefings* (2015)

[Renesys 2013] Renesys: *The New Threat: Targeted Internet Traffic Misdirection.* 2013. – URL http://research.dyn.com/2013/11/mitm-internet-hijacking/. – Zugriffsdatum: 25.08.2015

[RIPE 2008] RIPE, NCC: *YouTube Hijacking: A RIPE NCC RIS case study.* 2008. – URL https://www.ripe.net/publications/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study. – Zugriffsdatum: 10.10.2015

[RIPE 2015] RIPE, NCC: *libBGPdump*. 2015. – URL https://bitbucket.org/ripencc/bgpdump/wiki/Home. – Zugriffsdatum: 04.12.2015

[Toonk 2014] Toonk, Andree: *What caused today's Internet hiccup*. 2014. – URL http://www.bgpmon.net/what-caused-todays-internet-hiccup/. – Zugriffsdatum: 08.11.2015

[Touch u. a. 2010] Touch, J. ; Mankin, A. ; Bonica, R.: The TCP Authentication Option / IETF. June 2010 (5925). – RFC

[Wählisch 2011] Wählisch, Matthias: *Beta Version of the RPKI RTR Client C Library Released*. 2011. – URL https://labs.ripe.net/Members/waehlisch/beta-version-of-the-rpki-rtr-client-c-library-released. – Zugriffsdatum: 29.11.2015

[Wählisch u. a. 2013] Wählisch, Matthias ; Holler, Fabian ; Schmidt, Thomas C. ; Schiller, Jochen H.: RTRlib: An Open-Source Library in C for RPKI-based Prefix Origin Validation. In: *Presented as part of the 6th Workshop on Cyber Security Experimentation and Test*. Berkeley, CA : USENIX, 2013

[Wählisch u. a. 2012] Wählisch, Matthias ; Maennel, Olaf ; Schmidt, Thomas C.: Towards Detecting BGP Route Hijacking Using the RPKI. In: *SIGCOMM Comput. Commun. Rev.* 42 (2012), August, Nr. 4, S. 103–104. – ISSN 0146-4833

[Wählisch u. a. 2014] Wählisch, Matthias ; Schmidt, Robert ; Schmidt, Thomas C. ; Maennel, Olaf ; Uhlig, Steve: When BGP Security Meets Content Deployment: Measuring and Analysing RPKI-Protection of Websites. In: *CoRR* abs/1408.0391 (2014)

[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: *Proceedings of the 14th ACM Workshop on Hot Topics in Networks*. New York, NY, USA : ACM, 2015 (HotNets-XIV), S. 11:1–11:7. – ISBN 978-1-4503-4047-2

Abbildungsverzeichnis

Listings

Tabellenverzeichnis

Hiermit versichere ich, dass ich die vorliegende Arbeit ohne fremde Hilfe selbständig verfasst und nur die angegebenen Hilfsmittel benutzt habe.

Hamburg, 18. Januar 2016 Tobias Ramin