anexia

DHBW
Duale Hochschule
Baden-Württemberg
Karlsruhe

# Route Injection

# Projekt T3_2000

für die Prüfung zum

Bachelor of Science

des Studienganges Informatik / Informationstechnik

an der

Dualen Hochschule Baden-Württemberg Karlsruhe

von

**Leon Louis Schoch**

Abgabedatum 1. April 2090

| | |
|---|---|
| Bearbeitungszeitraum | 20 Wochen |
| Matrikelnummer | 1015290 |
| Kurs | TINF21B5 |
| Ausbildungsfirma | Anexia Deutschland GmbH<br>Karlsruhe |
| Betreuer der Ausbildungsfirma | Stephan Peijnik-Steinwender (B.Sc.) |
| Gutachter der Studienakademie | Prof. Dr. Markus Strand |

# Erklärung

Ich versichere hiermit, dass ich meine Projekt T3_2000mit dem Thema: Route Injection selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe. Ich versichere zudem, dass die eingereichte elektronische Fassung mit der gedruckten Fassung übereinstimmt.

_____ _____

Ort Datum Unterschrift

# Sperrvermerk

Der Inhalt dieser Arbeit darf weder als Ganzes noch in Auszügen Personen außerhalb des Prüfungsprozesses und des Evaluationsverfahrens zugänglich gemacht werden, sofern keine anderslautende Genehmigung vom Dualen Partner vorliegt.

**Zusammenfassung**

Mittels Remote Triggered Route Injection können End Benutzer bequem über eine Weboberfläche, Routen mittels BGP Communities manipulieren. Um dies zu verwirklichen, wurde das Projekt in verschiedene Teilsysteme unterteilt, welche ihren eigenen Aufgabenbereich haben.

# Inhaltsverzeichnis

# Abbildungsverzeichnis

# Tabellenverzeichnis

# Liste der Algorithmen

# Formelverzeichnis

# Abkürzungsverzeichnis

# Kapitel 1

# Einleitung

## 1.1 Ziele und Motivation der Arbeit

Die zunehmende Abhängigkeit von digitalen Kommunikationsnetzwerken und die kontinuierliche Weiterentwicklung der globalen Infrastruktur haben zu einer signifikanten Steigerung des Datenverkehrs im Internet geführt. Während diese Fortschritte zahlreiche Vorteile für die Gesellschaft mit sich bringen, eröffnen sie auch neue Herausforderungen im Hinblick auf die Sicherheit und Stabilität des Netzwerkbetriebs. In diesem Zusammenhang gewinnt die Fähigkeit, den Datenverkehr effektiv zu leiten und gleichzeitig gegen potenzielle Bedrohungen zu schützen, zunehmend an Bedeutung. Das Border Gateway Protocol (BGP), als das fundamentalste Routing-Protokoll im Internet, spielt eine kritische Rolle bei der Bestimmung der optimalen Routen für den Datenverkehr zwischen Autonomen Systemen (ASen). Allerdings hat die BGP-Protokollsuite bisher nur begrenzte Möglichkeiten zur gezielten Beeinflussung des Datenverkehrs in Ausnahmesituationen oder bei Sicherheitsvorfällen geboten. Eine solche Ausnahmesituation tritt beispielsweise auf, wenn ein Netzwerkressourcen-Engpass aufweist oder wenn bösartige Akteure versuchen, den Datenverkehr abzufangen oder zu manipulieren. Die vorliegende Forschung widmet sich daher der Entwicklung eines innovativen Ansatzes, der es ermöglicht, Internet-Routen über BGP gezielt in sogenannte „Blackholes“zu lenken. Dieses Konzept zielt darauf ab, den Datenverkehr von bestimmten Quellen oder zu bestimmten Zielen hinzuleiten, indem die betreffenden Routen im Netzwerk auf Blackholes abgebildet werden. Diese Blackholes repräsentieren Pfade im Netzwerk, die keinen tatsächlichen Datenaustausch ermöglichen, sondern den Verkehr effektiv abfangen und isolieren. Durch die Einrichtung dieser Blackholes wird

eine maßgeschneiderte Methode zur Verteidigung gegen Distributed Denial of Service (DDoS)-Angriffe sowie zur effizienten Nutzung von Ressourcen in Überlastsituationen geschaffen. Die Motivation für dieses Projekt liegt darin, die Flexibilität und die Sicherheitsaspekte von BGP-Routings zu erweitern, um den heutigen Anforderungen an die Netzwerksicherheit und -stabilität gerecht zu werden. Durch die Schaffung eines Mechanismus zur Blackhole-Routing kann das Risiko von Datenverkehrsumleitung durch bösartige Einflüsse minimiert und die Möglichkeit zur gezielten Netzwerkressourcenlenkung maximiert werden. Die Ergebnisse dieses Projekts haben das Potenzial, die bestehenden Ansätze zur Netzwerkverwaltung und -sicherheit zu erweitern und somit einen bedeutenden Beitrag zur Aufrechterhaltung der Integrität und Effizienz globaler Kommunikationsnetzwerke zu leisten.

# Kapitel 2

# Grundlagen

## 2.1 Aufgabenstellung

Um im Falle eines DDoS Angriffs schnell reagieren zu können, muss es eine bequeme und einfache Möglichkeit geben, Routen zu manipulieren. Hierfür wurde das Projekt Remote Triggered Blackholing gestartet. Im Falle eines DDoS Angriffs, könnten somit IP Präfixe des Angreifers gezielt in ein Blackhole geroutet werden. Eine Belastung der Zielsysteme könnte somit verhindert werden, da die boshaften Pakete des Angreifers somit nicht beim Zielsystem ankommen würden, sondern in das schwarze Loch (Blackhole) weitergeleitet werden. Um die Routen in Routern manipulieren zu können, müssen diese über Injektoren in diese injiziert werden. Im Verlaufe dieser Projektarbeit wird die Entwicklung der Injektoren Komponente und der Aufbau einer Staging(Testing) Umgebung genauer dargelegt. Der Aufbau und die Entwicklung der Application Programming Interface (API) Komponente wurde bereits in der T1000 erläutert.

## 2.2 Genutze Technologien

### 2.2.1 Django Rest Framework

Django ist ein Web-Framework, dessen Ziel es ist, die Entwicklung von Web Applikationen schnell, einfach und übersichtlich zu machen. Das Django Representational State Transfer (REST) Framework, hier nachfolgend als Django Rest Framework (DRF) bezeichnet, ist ein REST Framework welches auf Django basiert. Mit DRF lassen sich REST-ful APIs schnell und einfach gestalten. Hierfür bietet Django eine Reihe an vorgefertigten Hilfestellung an, welche im Verlaufe dieser Projektarbeit näher erläutert werden. Datenbankmodelle werden hier einfach programmatisch deklariert und werden anschließend von Django automatisch verwaltet. Über Objekte können somit einzelne Werte aus der Datenbank entnommen werden, ohne sich mühsam mit Structured Query Language (SQL) Queries auseinandersetzen zu müssen. Sowohl Django als auch DRF basieren auf der Programmiersprache Python.

### 2.2.2 Hashicorp Consul

Consul, entwickelt von Hashicorp, ist eine Netzwerk Service Lösung, welche eine sichere Kommunikation zwischen Services und Applikation erlaubt. Consul kann sowohl redundant mit mehreren Nodes, als auch standalone genutzt werden. Für diese Projektarbeit, wird eine standalone Lösung eingesetzt und es wird lediglich die Key-Value Store Funktion genutzt. Mit dieser Funktion können Key-Value Paare über das Netzwerk in Consul gespeichert werden.

### 2.2.3 Docker

Docker ist Platform zur Containerisierung von Anwendungen. Hierdurch wird die Möglichkeit geschaffen eine isoliertes und leichtgewichtige Umgebung zu schaffen, welche sonst lediglich mittels Virtuellen Maschinen (VMs) möglich wäre. Durch Docker wird auf produktiven System durch die zusätzliche Isolationsschicht der Containerisierung eine weitere Sicherheitsstufe hinzugefügt, welche potenziellen Angreifern den Zugriff auf das Hostsystem erschwert.

## 2.3 Stand der Technik

Das BGP ist ein Protokoll des Internet-Routings, das die besten Wege für den Datenverkehr zwischen ASen bestimmt. Es verwendet Peering-Verbindungen zwischen Routern, um Informationen über erreichbare Netzwerke auszutauschen und die optimalen Pfade für den Datenaustausch zu ermitteln. Anders als bei herkömmlichen Routing Protokollen wie RIP oder OSPF, wird hier eine direkte TCP Verbindung zwischen Routern(Neighbours/Nachbarn) hergestellt. BGP-Communities sind ein Mechanismus, mit dem Netzwerkbetreiber spezifische Gruppen oder Kategorien von Präfixen markieren können. Diese Markierungen, als „Communities“bezeichnet, können verwendet werden, um Routen zu identifizieren und zu beeinflussen, wie sie von anderen ASen interpretiert werden. Durch die Verwendung von Communities können Netzwerkbetreiber das Routing auf feinere Weise steuern und anpassen, ohne die Kernstruktur des BGP-Netzwerks zu verändern. Die Manipulation von Routen mittels BGP Communities erfolgt, indem einem bestimmten Präfix eine oder mehrere Community-Markierungen zugewiesen werden. Andere AS können dann diese Community-Markierungen verwenden, um spezifische Aktionen auszuführen, wie z.B.:

- Pfadwahl beeinflussen: Durch das Zuweisen von Communities zu bestimmten Präfixen können Netzwerkbetreiber festlegen, wie andere AS ihre Routen interpretieren sollen. Dies kann dazu verwendet werden, den bevorzugten Weg für den Datenverkehr zu beeinflussen.

- Traffic-Engineering: Netzwerkbetreiber können Communities verwenden, um den Datenverkehrsfluss zu steuern. Durch Markieren von Präfixen können sie bestimmte AS dazu anleiten, den Datenverkehr auf bestimmten Wegen zu leiten, um Netzwerkressourcen effizienter zu nutzen.

- Blackhole-Routing: BGP Communities können dazu genutzt werden, bestimmte Präfixe zu markieren und den Datenverkehr über Blackholes zu lenken, um Angriffe oder Überlastungen zu bewältigen.

- Routenfilterung: AS können Community-Markierungen verwenden, um präzise Routenfilterung durchzuführen. Damit können sie bestimmte Routen von bestimmten Quellen oder für bestimmte Zwecke filtern oder akzeptieren.

Die Verwendung von BGP Communities ermöglicht eine flexiblere und zielgerichtete Steuerung des Internet-Routings. Netzwerkbetreiber können so gezielt

auf unterschiedliche Anforderungen reagieren und gleichzeitig die Integrität und Stabilität des BGP-Netzwerks aufrechterhalten. *Building Reliable Networks with the Border Gateway Protocol* vlg. [Beijnum 2002]

Durch den nahezu identischen Technologiestack wie bei der T1000 und um den Lesefluss zu wahren, wurden einige Kurzbeschreibungen in abgeänderter Form wiederverwendet.

# Kapitel 3

# Injector Komponente

## 3.1 Aufgaben

## 3.2 Umsetzung

### 3.2.1 Generieren der Config Files für Bird

#### Integrität der Konfigurationsdatei sicherstellen

### 3.2.2 Status der Routen von Bird abfragen

#### Evaluation der pybird Bibliothek

### 3.2.3 Bird und Bird6 aufteilen

### 3.2.4 Realisierung des Heartbeats

### 3.2.5 Emergency Mode implementieren

## 3.3 Testen

# Kapitel 4

# Staging Umgebung

## 4.1 Konzeption

## 4.2 Umsetzung

# Kapitel 5

# Fazit

## 5.1 Fazit

## 5.2 Ausblick

# Literatur

Beijnum, Iljitsch van [2002]. *Building Reliable Networks with the Border Gateway Protocol*. O'Reilly [siehe S. 13].

Li, Tony, Ravi Chandra und Paul S. Traina [Aug. 1996]. *BGP Communities Attribute*. RFC 1997. doi: 10.17487/RFC1997. url: https://www.rfc-editor.org/info/rfc1997.