Strategie zur Verfolgung einzelner IP-Pakete zur Datenflussanalyse

Themenkreis II: ITC Management & Sicherheit

Vortragender:
Name: Hillmann
Vorname: Peter
Akad. Titel: Dipl.-Ing.
Telefon: +49 89 6004 2251
E-Mail: peter.hillmann@unibw.de

Details zu den übrigen Autoren:
Name: Tietze
Vorname: Frank
Akad. Titel: Dipl.-Inf.
Telefon: +49 89 6004 2280
E-Mail: frank.tietze@unibw.de

Name: Dreo Rodosek
Vorname: Gabi
Akad. Titel: Prof. Dr.
Telefon: +49 89 6004 2826
E-Mail: gabi.dreo@unibw.de

Dienstanschrift aller Autoren:
Hochschule: Universität der Bundeswehr München
Straße: Werner-Heisenberg-Weg 39
PLZ: 85577
Stadt: Neubiberg

Strategie zur Verfolgung einzelner IP-Pakete zur Datenflussanalyse

Frank Tietze, Peter Hillmann and Gabi Dreo Rodosek

Lehrstuhl für Kommunikationssysteme und Netzsicherheit
Fakultät für Informatik
Universität der Bundeswehr München
Werner-Heisenberg-Weg 39
D-85577 Neubiberg
{frank.tietze, peter.hillmann, gabi.dreo}@unibw.de

Abstract: Die Identifizierung des genauen Übertragungsweges, welches ein Datenpaket im Netz genommen hat, stellt eine große Herausforderung dar. Dieses Paper präsentiert eine neue und effiziente Strategie zur Verfolgung einzelner IP Pakete namens *Tracemax*. Die präsentierte Technik ermöglicht die direkte Verfolgung einzelner Pakete über mehrere Netzknoten hinweg. Dabei können wesentlich längere Pfade für ein einzelnes Paket mitprotokolliert werden als bei bisherigen Techniken. In Kombination mit einem Intrusion Prevention System lassen sich dadurch die ungewollten von den gewünschten Datenverbindungen unterscheiden und filtern. Das neue Konzept ermöglicht genauere Analysen des Datenverkehrs und der Übertragungswege in einem Netz. Es kann die Auswirkung von Bandbreiten-Auslastenden Angriffen, wie die von Distributed Denial of Service (DDoS), effektiv reduzieren sowie Frühwarnsysteme und Präventionsmaßnahmen unterstützen als auch Angreifer identifizieren.

1 Einleitung

Eine der öffentlich wirksamsten DDoS Angriffe fand 2007 gegen Estland statt. In dem modernen Land mit E-Government Diensten hatte der Angriff einen großen Einfluss auf die Bevölkerung und das öffentliche Leben [Tra07]. Weitere massive DDoS Attacken gegen MasterCard, Visa und PayPal sowie weitere große Finanzunternehmen gab im Jahre 2010 im Zuge der Sperrung der Bankkonten von WikiLeaks [Ols10]. Die koordinierte Protestaktion „Operation Payback“ hat die Dienste der genannten Unternehmen mit erheblichen finanziellen Verlusten für mehrere Stunden zum Erliegen gebracht.

Die Mächtigkeit und Gefahr von DDoS Angriffen sind durch die vergangenen Ereignisse offensichtlich und stellen ein Problem des heutigen Internets dar. Die Notwendigkeit adäquater Abwehrmechanismen besteht in der Skalierung der Angriffe gegen einzelne Dienste bis hin zu Infrastrukturen ganzer Länder. Die bisher größte detektierte DDoS Attacke fand 2014 statt und verursachte eine Datenlast mit einer Bandbreite von über 500 GBits/s [Ols14]. Solch ein massives Datenaufkommen würde jeden Netzwerkknoten zur Unternehmensanbindung überfordern. Der Datenverkehr eines solchen Angriffs stammt

oft von einer hohen Anzahl, unterschiedlicher Quellen, wie z. B. von Bot-Netzen, Protestgruppen oder militärischen Einheiten. DDoS Angriffe sind schwer abzuwehren, da diese keine spezifische Sicherheitslücke eines Systems ausnutzen und die Initiatoren meist unerkannt bleiben.

Zur Abwehr solcher Angriffe ist es notwendig, die verschiedenen Quellen und Verursacher zu erkennen. Dabei ist die Vertrauenswürdigkeit und die Genauigkeit des Verfolgungssystems von maßgebender Bedeutung. Letztendlich besteht das Ziel in der eindeutigen und beweisbaren Identifizierung des Angreifers für Strafverfolgungsbehörden sowie für forensische Analysen unter Sicherstellung der Nachvollziehbarkeit. Die präsentierte Technik zur Datenpaketverfolgung kann ferner zur Erkennung von verborgenen Kanälen genutzt werden. Weiterhin lassen sich die Daten als nutzbringende Eingangsinformationen für Intrusion Detection Systeme (IDS) verwerten. Lastausgleichssysteme, Zonen Routing als auch weitergehende Netzanalysen können von Daten der Paketverfolgung profitieren.

2 Anwendungsgebiet

Die Konzeptidee einer effizienten Paketverfolgungsstrategie bei autonomen Transitnetzen (Transit AS) und Stub Systemen (Stub AS) wird anhand des folgenden realen Beispielszenarios erläutert. An einem Endgerät wird bösartiger Datenverkehr bzw. ein DDoS Angriff festgestellt (z. B. Flooding). Hierbei ist von gefälschten Absender-IP-Adressen auszugehen. Der Angriff lässt sich am Endgerät des Opfers z. B. mittels IDS und entsprechenden Signaturen erkennen [LL03], welche u. a. eingehenden Datenverkehr, genutzte Bandbreiten sowie Verzögerungen. Das IDS generiert einen Alarm und der zugehörige Erkennungsvektor aktiviert den Dienst zur Paketverfolgung am Edge-Router zum Opfer. Dieser propagiert die Nachricht zur IP Paketverfolgung an alle weiteren Netzkomponenten. Die Aktivierung der Paketverfolgung ist mittels Authentifikation und Verschlüsselung abgesichert und könnte auch automatisiert über den ISP erfolgen. Dazu ist eine spezifische Anfrage zur Unterstützung der Angreiferidentifikation vom Opfer an den ISP zu senden. Nach der Konfiguration der Netzkomponenten, können alle IP Pakete zurückverfolgt werden. Die Informationen werden entsprechend den Bedürfnissen der Forensik und der Strafverfolgungsbehörden aufgearbeitet und gespeichert. Nachdem ausreichend Daten gesammelt wurden und die Angreifer identifiziert sind, werden Gegenmaßnahmen eingeleitet. Die Daten der Signatur zur bösartigen Kommunikation, z. B. Informationen zur IP Adresse, Port und Protokoll, wird an alle Netzkomponenten weitergegeben. Diese nutzen die Information, um die entsprechenden Pakete zu filtern, zu verzögern und zu blockieren. Darüber hinaus kann Flow Sampling und Protokollierung auf den Netzkomponenten an den Angriff angepasst werden. Dies ist jedoch nicht Bestandteil der Betrachtung in dieser Veröffentlichung.

Die Markierung der Pakete erweitert die Datengrundlage um notwendige Informationen für anspruchsvolle Echtzeit Reaktionen und Nachweisbarkeit. Weiterhin profitiert ein ISP von den Verfolgungsinformationen indem Angriffsvektoren und Angreifer besser identifizierbar und zukünftig erkennbar sind. Bots innerhalb des eignen ISP-Netzes und fremde Netze, welche als Quelle von Schadsoftware dienen, können besser erkannt werden.

Darüber hinaus stellt das Verfahren einen Ansatz zur Erkennung von Coremelt[1] Angriffen dar, wogegen derzeit keine Verteidigungsmaßnahmen existieren. Weitere Anwendungsfälle für *Tracemax* sind die Verifikation von Lastausgleichs- oder Bündelungsverfahren sowie Netzkonfigurationen von Netzmanagementsystemen.

3 Annahmen und Anforderungen

Eine praktisch anwendbare Strategie zur Paketverfolgung muss realistischen Annahmen entsprechen. Dazu gehört u. a., dass sich Routen von Datenverbindungen während eines Angriffs dynamisch ändern können. Datenpakete gehen bei der Übertragung verloren und die Reihenfolge der Pakete ändert sich. Darüber hinaus sind Angreifer in der Lage sehr viele Datenpaket von unterschiedlicher Zusammensetzung zu generieren und die Absender-IP- Adressen zu fälschen.

Entsprechend den Anwendungsanforderungen muss eine effektive Strategie zur Paketverfolgung folgende Hauptaspekte erfüllen:

- **Einzelpaketverfolgung** (zur Erkennung intelligenter Angreifer)
- Erkennen und differenzieren von **mehreren Angreifern**
- Schnelle Pfadrekonstruktion, auch während eines Angriffs
  (Kurze **Angriffserkennungszeit** und **Präventive Maßnahmen**)
- Geringe zusätzliche Netzlast und Leistungsanforderungen (**Effizienz, Kosten**)
- **Paketverfolgung über mehr als 50 Hops**
  (Notwendig für Verbindungen über viele Netzknoten)

Als ein Hop wird die routende Netzkomponente bezeichnet, welche ein Paket bei der Übertragung passiert. Hintergrund für die notwendige hohe Hop Anzahl wird anhand des folgenden Beispiels deutlich. Der direkte Aufruf der Website von www.torproject.org vom Standort der *Universität der Bundeswehr München* wird über mehr als 18 Router geleitet[2]. Diese Verbindung beinhaltet weder Anonymisierungstechniken noch andere spezielle Konfigurationen wie z. B. manuell gewählte Proxy Server. Im Jahr 1996 betrug die höchste Anzahl an durchlaufenen Netzknoten von einem Datenpaket 39 Hops, die erwartete Anzahl in 2011 liegt bei 56 Hops [CH10].

Weitere grundlegende Anforderungen bestehen hinsichtlich der **Effektivität** der Paketmarkierung und der Pfadrekonstruktion, der **Skalierbarkeit** und Übertragbarkeit zu großflächigeren Anwendungsgebieten sowie in der **Zuverlässigkeit** des Algorithmus. Zusätzlich darf zwischen den ISPs **keine Kooperation notwendig** sein. Die angestrebte Lösung sollte keine **gesamte Netzkonfiguration erfordern**. Die zusätzlich benötigten Ressourcen des Systems muss möglichst geringe ausfallen.

[1] Ein Botnetz generiert pseudorealisitischen Datenverkehr zwischen den einzelnen Bots an einem bestimmten Netzknoten, sodass dieser Überlastet wird.

[2] Windows Befehl: tracert www.torproject.org

4 Stand der Wissenschaft und Technik

In den letzten Jahren wurden verschiedene Paketverfolgungsstrategien und Verteidigungstechniken entwickelt. Tabelle 1 stellt die verschiedenen Lösungen bewertend gegenüber und vergleicht das hier vorgestellte *Tracemax* System mit den existierenden Ansätzen entsprechend der identifizierten Anforderungen.

Eine präventive Technik gegen anonymisierte Angriffe ist Ingress Filtering (IF) [FS98]. Es verhindert IP Spoofing, stellt jedoch kein Paketverfolgungssystem dar. Es ist wird oft in Kombination mit anderen Techniken eingesetzt und trägt zur besseren Identifizierung der Angreifer bei.

Eines der bekanntesten Paketverfolgungsstrategien ist Router Stamping (RS), welches aus zwei Teilen besteht [VR10]. Der erste Teil ist die Markierung der IP Pakete, der zweite Teil ist der Pfadrekonstruktion. RS schreibt die Markierungsinformationen in das *Option Field* des IP Headers. Zur Markierung gibt es zwei Algorithmen: Deterministisches RS (DRS) und Probabilistisches RS (PRS). DRS ermöglicht es IP Pakete entsprechend den Anforderungen zu markieren. Allerdings können unter Beachtung von Headerbeschränkungen nur maximal 9 Hops protokolliert werden. PRS ist die Erweiterung von DRS um eine Wahrscheinlichkeitskomponente. Durch RS werden Informationen über die Topologie eines Netzes veröffentlicht. Die Verfahren erfüllen auf Grund der geringen Hop Reichweite bzw. der Wahrscheinlichkeitskomponente nicht die Anforderungen.

Ein weiteres Verfahren ist Packet Marking (PM), welches sich in Node-Sampling und Edge-Sampling unterteilt ist. Beim Node-Sampling [BA03] schreibt jede Netzkomponente seine eigene IP Adresse an das Ende des Payloads eines Paketes. Dies kann jedoch zu Fehlern beim Empfänger führen. Des Weiteren besteht die Möglichkeit einer Überschreitung der maximalen IP Paketgröße, welche weitere Probleme verursacht. Edge-Sampling [BA03] speichert Informationen einer einzelnen Teilverbindung in ein IP Paket. Die PM Schema benötigen eine hohe Rechenleistung, führen zu größeren Verzögerungszeiten bei der Übertragung und haben die gleichen Nachteile wie RS.

Der Ansatz von Link Testing (LT) unterscheidet zwei Prinzipien: LT mittels Input Debugging (LTID) [Sto00] und LT über Controlled Flooding (LTCF) [Bur00]. Diese Strategien erfordern einen fortlaufenden Angriff, um den Angriffspfad rekonstruieren zu können. Darüber hinaus ist es nicht zielführend bei einem DDoS Angriff das Netz mit übermäßigem Datenverkehr weiter zu belasten. LT setzt ferner eine hohe Leistungsfähigkeit der Netzkomponenten voraus.

Mittels standardisiertem *Internet Control Message Protocol* (ICMP) ist eine Verbindungsanalyse möglich [IOR07]. Dabei wird der Pfad rückwärts anhand der Senderinformation und zu geringer *Time to Live* identifiziert. Allerdings blockieren die meisten Router ICMP Nachrichten, was die Verwendung erschwert [Alj03]. Der nachträglich iterativ identifizierte Pfad referenziert nicht zwingend den tatsächlich passierten Hinpfad eines Paketes.

Ein weiterer Ansatz ist ISP Traceback [Ste13]. Es schreibt die „Autonome System Nummer“ eines ISPs in das *Option Field* des IP Paketes. Dies ermöglicht die Erkennung des Quell ISPs, jedoch aber keine direkte Pfadverfolgung. Weitere Ansätze und Hybride Lösungen zur Pfadverfolgung werden in [VR10] betrachtet.

Zusammenfassend entspricht keine Paketverfolgungstechnik den identifizierten Anforderungen. Manche Verfahren können die Pakete nicht über ausreichend viele Hops verfolgen. Andere benötigen mehrere Datenpakete oder basieren auf Wahrscheinlichkeiten.

5 Neuer Ansatz: Tracemax

Mit Bezug zum Beispiel im Abschnitt 2 wird eine spezifische Anfrage zur Paketverfolgung vom Nutzer an den ISP gesendet. Dies kann z. B. über ein Service-Interface geschehen. Daraufhin wird die Paketverfolgungstechnik *Tracemax* aktiviert. Die Technik besteht aus einem Markierungsschema und einer Rekonstrutionsmethode. Diese und auch alle weiteren Komponenten von *Tracemax* werden im Folgenden detailliert erläutert. Die Netzkomponenten markieren die IP Pakete während der Übertragung und die Rekonstrutionsmethode bestimmt den genommenen Pfad im Nachhinein.

5.1 Markierungsschema

Jede routende Netzkomponenten schreibt eine zugewiesene ID Nummer in das *Option Field* des IP *Headers*. Trotz sehr begrenzter Größe (40 Byte) können ausreichend Informationen gespeichert werden. Das *Option Field* stellt eine geeignete Wahl dar, weil die Netzlast nur geringfügig erhöht wird und keine Nebeneffekte entstehen. Die eindeutigen ID Nummern von *Tracemax* zur Markierung haben weniger als 6 Bits und sind somit wesentlich kleiner als die vollständigen IP Adressen. Dadurch lassen sich mehr IDs im *Option Field* speichern als IP Adressen. Die genaue Bit Größe einer ID ist situationsabhängig und kann angepasst werden. Die Größe hängt indirekt von der Netzkomponente mit den meisten physischen Verbindungen ab, bei der *Tracemax* verwendet wird. Zur weiteren Verkleinerung können physische Komponenten in mehrere virtuelle Hops mit kleineren IDs aufgeteilt werden. Die ID orientiert sich an den Layer 1 oder 2 ISO/OSI Informationen, z. B. der Portnummer einer physischen Verbindung. Jedoch ist die ID unabhängig davon und als abstrakte Nummer definiert. Dies ermöglicht Optimierungen während der ID Zuweisung und kann zu einer reduzierten Bit Größe führen. Die IDs werden am ausgehenden Interface in das *Option Field* geschrieben.

5.2 ID Zuweisung

Wenn *Tracemax* eingesetzt wird, erhält jeder physische Port eines Routers seine eigene ID, welche nicht zwingend im ganzen System eindeutig ist. Die ID Nummern werden vorab so zugewiesen, dass eine eindeutige Pfadrekonstruktion möglich ist. Dies kann manuell oder automatisch mittels Algorithmus geschehen. In Abhängigkeit eines gewählten Routers ist zu verhindern, dass dieser von zwei Nachbarknoten die gleiche ID auf eingehenden Verbindungen erhält. Dies wird durch Inkrementieren einer der IDs gelöst. Nichtsdesto-

trotz benötigt eine ID weniger Bits als eine IP Adresse. Eine gültige ID Zuweisung ist in der Abbildung 1 zu sehen. Abbildung 2 zeigt eine ungültige Zuweisung, da der markierte Router anhand der ID nicht eindeutig den Vorgänger identifizieren kann.

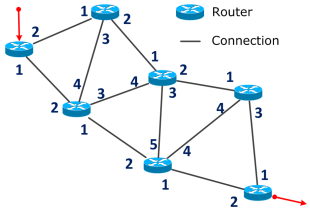

Abbildung 1: Gültige Zuweisung.

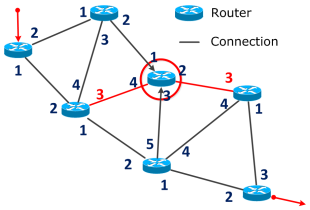

Abbildung 2: Ungültige Zuweisung.

In der vereinfachten Version von *Tracemax* erhält jede Netzkomponente eine ID anstatt jedes physisches Interface oder jede Verbindung. Dadurch sind jedoch oft größere ID Nummern notwendig, um eine eindeutige Pfadrekonstruktion zu ermöglichen. Daher ist die komplexere Variante mit IDs für jedes physische Interface zu bevorzugen.

Die Rekonstruktionsmethode extrahiert die IDs aus dem IP *Header*. Die Reihenfolge definiert die verwendeten Verbindungen zwischen den Routern und dadurch den Weg des Pakets durchs Netz. Zur Rekonstruktion muss die Methode den letzten markierten Endpunkt des Paketes als Anhaltspunkt kennen. Diese Information kann auch im *Option Field* gespeichert werden, indem die IP Adresse des Endpunktes mit vermerkt wird. Die Rekonstruktion des Pfades kann an einem unabhängigen System ausgeführt werden.

5.3 Rekonstruktionsmethode

Die Rekonstruktionsmethode korreliert die Sequenz der IDs mit dem Wissen über die Netzinfrastruktur und den zugewiesenen IDs. Dazu wird für jede ID einzeln die entsprechende Verbindung rückwärts ermittelt, angefangen beim letzten markierten Endpunkt. Alle notwendigen Informationen zur vollständigen Pfadrekonstruktion im Einsatzbereich der Technik sind dem Betreiber bekannt. Mit der Kenntnis der IDs und des Pfades lassen sich die IP Adressen der zugehörigen Netzkomponenten ermitteln, sodass die Reihenfolge der Router, die IP Adressen und der Pfad bekannt werden.

An den Übergängen von ISPs bzw. unabhängig eingesetzter *Tracemax* Systeme ist das *Option Field* zu löschen, sodass keine Informationen weitergegeben werden und das Netz nicht unnötig belastet wird. An einer solchen Netzkomponente sind die Markierungsinformationen zu speichern oder an einen zentralen Sammelpunkt zu senden, wo die Informationen ausgewertet und analysiert werden können. Bei eingehenden IP Paketen mit *Option Field* in das *Tracemax* Systems sind diese durch den ersten Router zu überschreiben. Dies verhindert das Einfügen falscher Informationen und sichert den Speicherplatz zur eigenen Verwendung. Zur Steigerung der Leistungsfähigkeit kann bei einem eingehenden IP Pakete am Übergangsrouter die Sender IP Adresse von der Routentabelle zusätzlich gespeichert

werden. Dadurch lässt sich die Markierungsreichweite um den ersten, nicht zu *Tracemax* zugehörigen, externen Router erweitern.

Zusammenfassend besteht das *Option Field* aus den folgenden Informationen:
Präambel : IP Sender : 1. ID : 2. ID : ..... : n. ID : IP Endpunkt

Ein wesentlicher Vorteil von *Tracemax* ist, dass bei diesem Ansatz mit den IDs keine schützenswerten Informationen über die private Netztopologie eines ISPs veröffentlicht werden. Zur weiteren Anonymisierung lassen sich die IDs in einem kurzen Intervall wechseln. Beim Anwendungsgebiet von DDoS muss davon ausgegangen werden, dass die Angreifer IP Spoofing einsetzen. Dies hat jedoch keinen Einfluss auf die Markierungsinformationen von *Tracemax*, da es nicht auf den Absender IP Adressen basiert. Jedes einzelne Paket wird markiert und lässt sich dadurch unabhängig von anderen Paketen zurück verfolgen. Dynamische Routen werden in kürzester Zeit erkannt. Weiterhin hat die Technik keinen Einfluss auf die Nutzdaten des Paketes und dessen Empfänger.

6 Speicherung der Markierungsinformationen im IP Header

Im Folgenden wird der Aufbau des *Option Field* nähere erläutert, da nicht alle Bits frei und flexibel verwendet werden dürfen. Der IP *Header* in Version 4 kann ein *Option Field* variabler Größe (unter Beachtung vom *Padding*) von bis zu 40 Byte besitzen.

Es gibt zwei zulässige Formate, um Informationen im *Option Field* zu speichern. Die Daten können entweder in der vordefinierten Größe eines Oktets oder mittels selbstdefinierter Größenangabe gespeichert werden. *Tracemax* nutzt die zweite Variante, um mehr Speicherplatz zur Verfügung zu haben. Alle Formate müssen mit der Angabe des *Option Typs* beginnen: 1 Bit *Copy Flag*, 2 Bit *Option Class* und 5 Bits *Option Number*. [Net81]

Das *Copy Flag* gibt an, ob das gleiche *Option Field* in allen Paket Fragmenten erscheint. Da sich hierdurch kein Vorteil ergibt, wird das Flag auf 0_2 gesetzt. Bei der *Option Class* gibt es eine vordefinierte Auswahl, wobei die Klasse der *Messung* mit 10_2 zur Paketverfolgung am Besten geeignet ist. Für die *Option Number* wird ein Wert gewählt, welcher keine Konflikte erzeugt. Hierzu nutzt *Tracemax* die unzugewiesene *Option Number* 10110_2 (22_{10}). Somit ergibt sich für das erste Oktet: 86_{10} = 0x56 = 01010110_2 . Bei der flexiblen Formatierungsmöglichkeit der Größe folgt ein weiteres Oktet zur *Option Length*. Dieses gibt die Länge des Optionsteils inklusive des *Option Headers* an, welcher bis zu 40 Byte lang sein darf. *Tracemax* definiert den gesamten Bereich für die Eigennutzung, wodurch sich das zweite Oktet ergibt: 40_{10} = 0x28 = 00101000_2 .

Die Einhaltung der Formatierung ist notwendig, da ansonsten fehlerhafte IP Pakete entstehen, unerwünschte Nebeneffekte auftreten oder Verwechselungen mit anderen Optionsparametern. So werden beispielsweise Pakete mit den Optionsparameter *Loses Sender-Routing* und *Striktes Sender-Routing* wegen Sicherheitsbedenken blockiert[3]. Das Konzept lässt sich einfach auf IP Version 6 übertragen. Dazu ist ein neuer *Next Header* zu definieren, indem die Markierungsinformationen gespeichert werden.

[3]Cisco FAQ. What *is* source routing?, 2014.

7 Evaluierung und Bewertung

Zur Evaluierung von *Tracemax* erfolgten mehrere Experimente mit einer prototypischen Implementierung. Diese wurde mittels der in Python geschriebenen Software *Scapy* realisiert, welches zur Paketgenerierung und -manipulation dient. Die Teststellung besteht aus mehreren Netzkomponenten und Rechnern. Die Netzkomponenten zur Paketmarkierung wurden durch Rechner mit entsprechender Routerkonfiguration abgebildet, wodurch die Tests sehr realitätsnah sind. Auf allen Systemen und Komponenten wird Wireshark zur Paketerfassung und Analyse eingesetzt. Die Pfadrekonstruktion erfolgte manuell.

Das folgende Python Skript 1 beschreibt die Paketmarkierung, welche bei den Routern eingesetzt wird. Es erkennt ob ein eingehendes Paket bereits ein *Option Field* besitzt. Dementsprechend wird das bisherige *Option Field* kopiert oder ein neues mit dem *Header* '\x56\x28' erstellt. Dem neu generierten Paket mit dem reservierten *Option Field* wird abschließend die definierte ID hinzugefügt. Die IDs bestehen auf Grund der Vermeidung komplexer Bittransformationen mittels *Scapy* aus doppelten Hexwerten für den experimentellen Nachweis. In dem Skript ist die Interfacespezifische ID in 'myindex' gespeichert, hier der Wert '\x09'. Nach der Paketgenerierung erfolgt die Weiterleitung an den nächsten Hop. Für die Analyse filtert das Skript auf ICMP Nachrichten.

Listing 1: Python script for Tracemax.

```
1  from scapy.all import *
2  def chgSend(x):
3          myindex = '\x09'                          # Zugewiesene ID
4          optionsarray = x[IP].options              # Option Field
5          if optionsarray.count(1) == 0 and str(optionsarray) != '[]':
6                optionsstring = str(optionsarray[0])
7          else: optionsstring = '\x56\x28'
8
9          # Paketgenerierung
10         y=IP(src=x[IP].src,dst=x[IP].dst,len=60,options=
11                       IPOption(optionsstring+myindex))/x[IP].payload
12         send(y)
13 while 1:  # Lauschen auf dem Netzinterface
14         sniff(prn=chgSend, lfilter=lambda x: x.haslayer(ICMP), count=1)
```

Die während des Tests durch Wireshark aufgezeichneten Daten dienen als Referenz. Diese belegen die Paketmarkierung im *Option Field* nach jedem Hop. Zusammen mit den bekannten Informationen der ID Zuweisung von *Tracemax* lässt sich der Übertragungsweg im Netz rekonstruieren. Die Experimente validieren das präsentierte Konzept.

Zur Zusammenfassung der Ergebnisse stellt die folgende Tabelle 1 das *Tracemax* System vergleichend den bisherigen Ansätzen gegenüber. Dies zeigt die Vorteile der entwickelten Technik. Die Symbole haben folgende Bedeutung stets in Relation zu den anderen Ansätzen: + Vorteil, - Nachteil, o Neutral.

Mit *Tracemax* lassen sich in Abhängigkeit der ID Zuweisung über 50 Hops für ein einzelnes IP Paket verfolgen. Dennoch arbeitet das System sehr effizient und die Erkennungszeit von mehreren Sendern ist gering. Darüber hinaus kann die Technik auf Grund der geringen zusätzlichen Netzbelastung präventiv eingesetzt werden.

Tabelle 1: Vergleich verschiedener Paketverfolgungsstrategien

Algorithmus	**Maximale Hops**	**Effektivität**	**Effizienz**	**Skalierbarkeit**	**Kosten**	**Notwendige Kooperation**	**Robustheit**	**Gesamte Netzkonfiguration**	**Rekonstruktionszeit**	**Präventive nutzbar**	**Einzelpaket Verfolgung**	**Erkennung mehrerer Sender**
RS-DRS	9	+	o	o	+	+	o	+	+	+	+	+
RS-PRS	∞	+	o	o	+	+	o	+	-	+	-	-
PM-Node	∞	+	+	+	o	+	-	o	o	+	+	+
PM-Edge	1 Kante	o	o	+	o	+	o	-	-	+	-	-
LT-Debug.	∞	o	-	o	o	-	+	-	-	-	-	-
LT-Flood.	∞	-	-	-	+	o	o	+	-	-	-	-
ICMP	<256	o	o	+	+	+	-	+	+	-	+	+
ISP Trace	ISP	-	o	+	+	+	-	+	+	+	+	o
Tracemax	**>50**	**+**	**+**	**+**	**+**	**+**	**+**	**-**	**+**	**+**	**+**	**+**

8 Zusammenfassung

Dieses Paper präsentiert mit *Tracemax* eine neuartige Technik zur Verfolgung und Pfadrekonsturktion einzelner IP Pakete durchs Netz. Es lassen sich wesentlich längere Pfade detektieren als mit bisherigen Verfahren. Die Technik hat keinen Einfluss auf die Nutzdaten im Paket, sodass Markierungsinformationen eines verfolgten Paketes nicht vor der Zustellung zu löschen sind. Es ist einfach realisierbar. Ein ISP veröffentlicht keine privaten Informationen über seine Netztopologie. Die zusätzliche Netzlast ist sehr gering, wodurch eine gute Skalierbarkeit erreicht wird. Variierende Routen von Kommunikationsverbindungen werden erkannt. Weiterhin lassen sich verschiedene Sender unterscheiden, womit es zur Abwehr und Identifizierung von Angreifern geeignet ist. In weiterführenden Arbeiten sind Konzepte zur Verwendung von *Tracemax* mit konkurrierenden Anwendungen um das *Option Field* zu erstellen und Einfluss von Multiprotocol Label Switching zu untersuchen. Darüber hinaus ist die Notwendigkeit eines flächendeckende Einsatzes zu Flexibilisieren, sodass sich nicht markierende Hops überspringen lassen. Die Auswirkung der Paketmarkierung auf die Leistungsfähigkeit der Router ist genauer zu betrachten. Abschließend wird die Spezifikation des Systems in einem RFC angestrebt.

Danksagung

Die Arbeit wurde durch das siebente Rahmenprogramm des Exzellenznetzwerkes (ICT-318488) über das Projekt Flamingo durch die europäische Kommission gefördert.

Literatur

[Alj03] Hassan Aljifri. IP Traceback: A New Denial-of-Service Deterrent? In *Proc. IEEE Security and Privacy*, Jgg. 1, Seiten 24 – 31, Piscataway, New Jersey, May 2003. Institute of Electrical and Electronics Engineers, Inc.

[BA03] Andrey Belenky und Nirwan Ansari. IP Traceback With Deterministic Packet Marking. In *Proc. IEEE Communications Letters*, Jgg. 7, Seiten 162 – 164, Piscataway, New Jersey, April 2003. Institute of Electrical and Electronics Engineers, Inc.

[Bur00] Hal Burch. Tracing Anonymous Packets to Their Approximate Source. In *Proc. 14th Systems Administration Conference (LISA 2000)*, Seiten 319–327, New Orleans, Louisiana, USA, December 2000.

[CH10] David Chinnery und Ben Horowitz. A Network Hub Architecture in 2011, Januar 2010.

[FS98] P. Ferguson und D. Senie. Network Ingress Filtering: Defeating Denial of Service Attacks Which Employ IP Source Address Spoofing. Network Working Group: RFC 2267, January 1998.

[IOR07] A. Izaddoost, M. Othman und M. Rasid. Accurate ICMP Traceback Model Under DoS/DDoS Attack. In *Proc. Advanced Computing and Communications (ADCOM '07)*, Seiten 441–446, Washington, DC, USA, 2007 2007. IEEE Computer Society.

[LL03] L. Li und G. Lee. DDoS attack detection and wavelets. In *Proc. IEEE Computer Communications and Networks (ICCCN'03)*, Seiten 421 – 427, Piscataway, New Jersey, October 2003. Institute of Electrical and Electronics Engineers, Inc.

[Net81] Network Working Group, Darpa Internet Programm. Internet Protocol: RFC 791, September 1981. Online: http://tools.ietf.org/html/rfc791 (08.04.2015).

[Ols10] Parmy Olson. DDoS Attacks On Visa, MasterCard Were 'Symbolic,' More To Come, Dezember 2010. Online: http://www.forbes.com/sites/parmyolson/2010/12/24/ddos-attacks-on-visa-mastercard-were-symbolic-more-to-come/ (08.04.2015).

[Ols14] Parmy Olson. The Largest Cyber Attack In History Has Been Hitting Hong Kong Sites, November 2014. Online: http://www.forbes.com/sites/parmyolson/2014/11/20/the-largest-cyber-attack-in-history-has-been-hitting-hong-kong-sites/ (08.04.2015).

[Ste13] Björn Stelte. ISP Traceback - Attack Path Detection. In *Proc. IEEE Communications and Network Securit*, Piscataway, New Jersey, 2013. Institute of Electrical and Electronics Engineers, Inc.

[Sto00] R. Stone. CenterTrack: An IP Overlay Network for Tracking DoS Floods. In *Proc. USENIX Security Symposium (SSYM'00)*, Jgg. 9, Seiten 1–15, Denver, Colorado, USA, August 2000. USENIX Association.

[Tra07] Ian Traynor. Russia accused of unleashing cyberwar to disable Estonia, Mai 2007. Online: http://www.theguardian.com/ world/2007/may/17/topstories3.russia (08.04.2015).

[VR10] S. Vincent und J. Raja. A Survey of IP Traceback Mechanisms to overcome Denial-of-Service Attacks. In India Karunya University, Hrsg., *Proc. Networking, VLSI and signal processing (ICNVS'10)*, Seiten 93–98, Stevens Point, Wisconsin, USA, 2010. World Scientific and Engineering Academy and Society (WSEAS).