DDoS defence mechanisims

Alexander Haar
Haaralexander3@gmail.com
Universität Kassel
Kassel, Hessen, Deutschland

Abstract

Distributed Denial of Service (DDoS)-Attacken sind beliebt, weil sie einfach in der Anwendung sind und großen Schaden anrichten können. Um dies zu Verhindern kann einmal an einem Internetknotenpunkt (IXP) mit Hilfe eines Machine Learning System (MLS) der schädliche Datenverkehr gefiltert werden. Eine andere Methode ist es Source Address Validation (SAV) zu nutzen, aber es wird nicht flächendeckend eingesetzt, aufgrund finanzieller Hindernisse. Aktuelle Forschungen bei der Internet Engineering Task Force (IEFT) haben das Ziel, diese Probleme zu bekämpfen und neue SAV-Methoden zu erarbeiten, die sicher und einfach zu implementieren sind. In China, das eine enorm ausgedehnte Infrastruktur aufweist, besteht jedoch ein Mangel an effektivem Schutz vor DDoS-Angriffen. Dies macht das Land beliebt sowohl zum Ausgangspunkt als auch zum Ziel solcher Angriffe. Durch eine umfassende Anwendung beider Methoden könnten DDoS-Attacken vollständig unterbunden werden.

Keywords: Source Address Validation, IP-Spoofing, IXP, Scrubber, Machine Learning, DDoS

ACM Reference Format:
Alexander Haar. 2024. DDoS defence mechanisims. In *Proceedings of ACM Conference (Conference'17).* ACM, New York, NY, USA, 7 pages.
https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 Einleitung

Cyberkriminalität ist in der modernen Gesellschaft allgegenwärtig. Insbesondere DDoS-Attacken auf Unternehmen und staatliche Institutionen haben in den letzten Jahren stark zugenommen. Bereits seit Ende des letzten Jahrhunderts sind derartige Angriffe bekannt [15]. Die mangelnde Authentifizierung im Internetprotokoll, beim Senden von Datenpaketen ermöglicht diese Angriffe.

Conference'17, July 2017, Washington, DC, USA

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

Das Ziel dieser Analyse ist es herauszufinden, wie durch einen "Scrubber" am IXP DDoS-Angriffe nachträglich gefiltert werden können, ähnlich wie es bei Spam-Filtern geschieht. Ein weiterer Aspekt betrifft SAV, die darauf abzielt, das Spoofen von IP-Adressen zu verhindern. Jedoch setzen nicht alle Netzwerke SAV ein, was verschiedene Arten von DDoS-Angriffen begünstigt. Die Frage lautet hier: Wie ist der aktuelle Stand von SAV, und in welche Richtung wird weiter geforscht?

Eine Antwort auf diese Fragen wurde in den frühen 2000er Jahren mit der Einführung von SAV präsentiert. Mit Basic Control Program (BCP) 38 [19] wurde der "Ingress Filter" vorgestellt. Daraufhin wurde mit BCP 84 [20] weitere Methoden wie Access Control List (ACL) und reverse-path-forwarding (RPF) für den Filter vorgestellt. Diese Veröffentlichungen zielen darauf ab, IP-Spoofing zu verhindern und damit auch DDoS-Attacken entgegenzuwirken. Sie gelten heutzutage immer noch als "Best Practie" [16].

SAV kann in zwei Richtungen implementiert werden: outbound SAV (oSAV), wenn Datenverkehr das Netzwerk verlässt und inbound SAV (iSAV), wenn Datenverkehr in ein Netzwerk gelangt. Untersuchungen zeigen jedoch, dass die Mehrheit des Internets keine umfassende SAV implementiert hat [2] [13]. Dies wird durch verschiedene Einflüsse wie finanzielle Ressourcen, gesetzliche Rahmenbedingungen und weitere Faktoren behindert [16]. Eine Steigerung der Präsenz von SAV wird als notwendig erachtet, um diese Herausforderung zu bewältigen [15].

Der flächendeckende Einsatz von oSAV könnte DDoS-Attacken, insbesondere Reflection-Angriffe, wirksam unterbinden [10]. Außerdem können DDoS-Angriffe auch an anderen Stellen des Internets bekämpft werden. Der IXP-Scrubber [11] filtert schädlichen Verkehr an einem IXP.

Eine umfassende Implementierung dieser Maßnahmen würde dazu beitragen, die Lücke bei der Authentifizierung im Protokoll zu schließen und DDoS-Angriffe vollständig zu bekämpfen. Jedoch weisen aktuelle Forschungen darauf hin, dass die bestehenden Methoden nicht mehr geeignet sind, da sie sich dem dynamischen Internet einfach nicht genug anpassen können.

2 IXP-Scrubber

Ein Internet Exchange Point (IXP) fungiert als zentraler Knotenpunkt im Internet, durch den ein erheblicher Datenverkehr fließt. Angesichts der wachsenden Menge an erzeugtem Internetverkehr gibt es weltweit viele dieser Knotenpunkte.

Gleichzeitig nehmen DDoS-Angriffe weiter zu. Daher erscheint es sinnvoll, an diesen Knotenpunkten eine Art "Staubsauger" zu implementieren, der schädlichen Verkehr effektiv herausfiltert. Im Folgenden wird ein IXP und der IXP-Scrubber näher betrachtet.

2.1 Internet Exchange Point

Das Internet besteht aus einer Vielzahl von miteinander verbundenen Netzwerken. Um diese Netzwerke effizient zu verknüpfen, werden sogenannte IXPs am Rand dieser platziert. Die IXPs fungieren als zentrale Knotenpunkte im Internet und ermöglichen es, den Internetverkehr von einem Netzwerk auf ein anderes zu leiten. Praktisch betrachtet handelt es sich bei IXPs um Schaltstellen, die als Bindeglieder zwischen verschiedenen Netzwerken dienen. Daraus folgt, dass durch einen IXP sehr viel Internetverkehr durchläuft. Die Funktionsweise eines IXPs kann mit der eines Internet-Switches verglichen werden, wobei dieser auf der zweiten Ebene des OSI-Modells positioniert ist. Zur Kommunikation mit einem IXP verwenden Netzwerke das sogenannte Backbone-Protokoll [4].

Ein wesentlicher Vorteil von einem IXP leigt in der geringen Latenz und der kurzen Roundtrip-Zeit. Darüber hinaus ermöglicht es ein IXP, den Verkehr im Falle eines Ausfalls auf alternative Routen umzuleiten, was die Robustheit des Netzwerks erhöht. Dies trägt dazu bei, dass ein Netzwerk weniger anfällig für Fehler und Störungen ist [1].

2.2 Scrubber

Im Jahr 2022 haben Matthias Wichtlhuber (u.a.) [11] einen IXP-Scrubber vorgestellt, der im Folgenden näher betrachtet wird. Der IXP-Scrubber, im Folgenden als "Scrubber" bezeichnet, wird innerhalb eines IXP eingesetzt. Seine Hauptaufgabe ist es, bösartigen Internetverkehr zu erkennen und herauszufiltern. Der Scrubber basiert auf einem Machine Learning System (MLS). Die primäre Motivation hinter diesem Scrubber ist die Abwehr von DDoS-Attacken. DDoS-Attacken sind besonders problematisch, da es Unternehmen gibt, bei denen der Kauf von Internetverkehr kostengünstig ist. Dies führt dazu, dass dieser Angriffsvektor häufig genutzt wird und das Volumen solcher Angriffe könne bis zu 3,5 Tbit/s erreichen.

Das MLS des Scrubbers besteht aus zwei Hauptschritten. Zunächst erfolgt das Training des Systems. Danach die Klassifizierung der Daten. In Figure 1 wird gezeigt, wie der Scrubber anschließend den Verkehr filtert und neue Daten zum weiter lernen erhält. Der Grundgedanke des Scrubbers ist es, präzise zu arbeiten und gleichzeitig die Übersichtlichkeit zu wahren. Im Anschluss wird der Scrubber evaluiert.

2.2.1 Mikroskopische Ebene. Um zuverlässig zu funktionieren, braucht das MLS viele Trainingsdaten. Aus diesem Grund ist dem MLS von fünf Partner IXPs in Europa und den USA Daten zur Verfügung gestellt worden, die bis zu zwei Jahre alt sein können. Diese Daten sind in gutartigen und

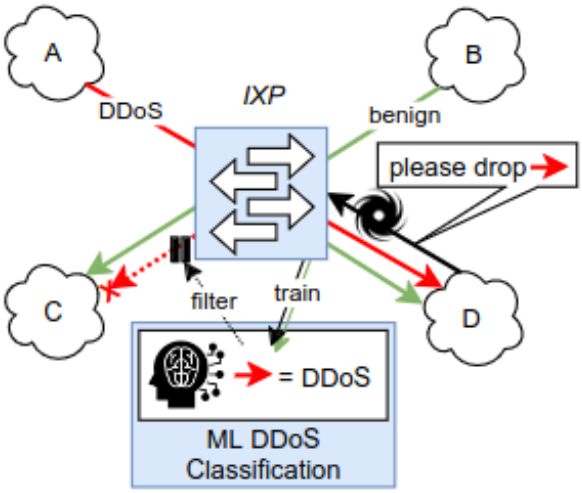

Figure 1. Das MLS filtert an einem IXP und lernt ständig von benachbarten ASes (A-D). Von Matthias Wichtlhuber (u.a.) (https://shorturl.at/mnS14). Seite 1.

bösartigen Verkehr unterteilt. Der Internetverkehr, der automatisch vom System oder von benachbarten IXPs manuell als schädlich gekennzeichnet ist, erhält das Label "blackholed".

Verkehr mit diesem Label wird in ein Schwarzes Loch geleitet, was dazu führt, dass sie verschwinden und das Ziel nicht beeinträchtigt wird. Durch die Verwendung des Border Gateway Protocol (BGP) werden diese Labels an andere IXPs weitergegeben [3].

Daten, die dieses Label nicht erhalten haben, werden als gutartig eingestuft. Die Trainingsmenge ist aus ungefähr dem gleichen Anteil aus gutartigem und bösartigem Verkehr zusammengesetzt. Auf den Trainingsdaten ist der Association Rule Mining (ARM)-Algorithmus angewendet. ARM ist ein bekanntes Data-Mining-Verfahren, das Assoziation-Regeln anhand der Daten in der Form A -> C lernt. Die Anwendung des Verfahrens auf den Testdaten ergibt 7859 Regeln. Anschließend werden alle Regeln eliminiert, die keinen Mehrwert haben, weil sie eine zu geringe Konfidenz aufweisen. Nach dieser Minimierung sind 367 Regeln übriggeblieben. Diese Anzahl ist gering genug, damit die Regeln manuell überprüft werden können. In einem User Interface (UI) werden die Regeln angezeigt und Administratoren können zu den Regeln Kommentare hinzufügen sowie diese akzeptieren oder ablehnen.

Die zuvor gewonnen Regeln sind im nächsten Schritt unabhängig geprüft worden, damit sichergestellt werden kann, dass sie keine Voreingenommenheit aufweisen und akkurat sind. Hierfür ist eine neue Testmenge erstellt wurden, die als "Self Attack Set" (SAS) bezeichnet wird. Das Wichtige, bei diesen Testdaten, ist es zu wissen, ob sie wahr oder falsch sind. Um dies zu garantieren, wurden DDoS-Attacken

bei einem Unternehmen, wie Anfangs beschrieben, gekauft und auf einem speziell dafür ausgelegten und abgegrenzten Internetbereich ausgeführt. Zusätzlich ist gutartiger Internetverkehr ebenfalls simuliert und der SAS hinzugefügt wurden.

In einem zusätzlichen Experiment wurde der ARM-Algorithmus auf dem SAS ausgeführt. Die gewonnen Regeln wurden von fünf Domänen Experten ausgewertet. Nach der Überprüfung sind 38 Regeln übriggeblieben. Im Anschluss wurde gemessen, wie lange die Regeln benötigt haben und wie effektiv sie sind. Die Regeln weisen eine kurze Laufzeit und zeigen dabei eine hohe Effizienz auf. Unter einem Prozent gutartiger Verkehr wurde als bösartiger Verkehr gekennzeichnet und 75 Prozent des DDoS Verkehrs erfolgreich erkannt. Die Ergebnisse zeigen, dass der Ansatz eine gute Durchführbarkeit besitzt.

2.2.2 Makroskopische Ebene. Das Ziel des zweiten Schrittes ist es korrekt zu identifizieren, ob ein Ziel angegriffen wurde oder nicht. Zusätzliche soll gelten, dass die Identifizierung ortsunabhängig ist und übersichtlich bleibt. Um dieses Ziel zu erreichen, werden Kategorien gewichtet. Die Gewichtung findet vor der Klassifikation in der Vorverarbeitung statt. Kategorien, die häufig in blackhole Labels auftreten, erhalten eine positive Gewichtung, während Kategorien, die nicht in blackhole Labels auftreten, eine negative Gewichtung erhalten. Mögliche Kategorien sind IPs, Transportports, MAC-Adressen etc. Zudem sind die Daten normalisiert.

Die Klassifikation wurde mit fünf verschiedenen Klassifikatoren durchgeführt, somit können die fünf Klassifikatoren am Ende miteinander vergliechen werden. Die Daten hierfür wurden erneut in eine Trainingsmenge und Testmenge unterteilt, wobei gilt, dass die zwei Mengen disjunkt sind. Die Klassifikatoren sollen bestmöglich abschneiden. Um dieses zu erreichen, wurden die Daten, wie im letzten Absatz erläutert, in die Vorverarbeitung geschickt. Zusätzlich wurden die Hyperparameter in jedem Schritt überprüft und angepasst, wobei die 3-Fold-Cross-Validation auf allen Daten verwendet werden. Das bedeutet, dass die Daten in drei Mengen aufgeteilt sind und für jede Kombination wurden zwei Mengen als Trainingsdaten und die verbleibende Menge für Testdaten verwendet. Als letzte Optimierung wurden Korrelationen betrachtet.

2.2.3 Evaluation. Der Srubber wurde mit allen fünf Klassifikatoren und mit jedem Angriffsvektor getestet. Dabei habe der XGB Klassifikator am besten abgeschnitten. Je länger der Scrubber trainiert wurde, desto besser schneidet er ab. Zusätzlich soll das Model täglich mit neuen Daten weiter lernen, damit dieses effektiv bleibt. Geographische Änderung machen dem Model sehr wenig aus, aber für die Effizienz ist es besser, wenn alle IXPs zu einem großen XGB-Model zusammengefügt werden.

Neue Angriffsvektoren können ohne manuellen Eingriff von Administratoren erlernt werden. Aufgrund der Minimierung von Regeln, behält ein Netzwerk-Administrator den Überblick über das MLS und kann verstehen, wie die Regeln entstanden und entscheiden, ob sie sinnvoll sind.

3 Source Address Validation

IP-Spoofing, das Versenden von Internetpaketen unter Vortäuschung einer falschen Absenderadresse, stellt ein erhebliches Problem für das Internet dar. Das Fehlen einer Authentifizierung beim Senden von Internetpaketen hat zur Folge, dass es schwierig ist zu identifizieren, ob der angegebene Absender des Pakets authentisch ist oder ob sich dahinter jemand anderes verbirgt. Die dadurch gewonnene Anonymität wird gezielt ausgenutzt, um verschiedene Arten von Angriffen durchzuführen, darunter insbesondere DDoS-Angriffe [24] [7].

Die Notwendigkeit von Authentifizierungsmethoden und Schutzmechanismen gegen IP-Spoofing wird immer deutlicher, um die Integrität und Sicherheit des Internets zu gewährleisten. Unternehmen und Institutionen müssen fortlaufend daran arbeiten, effektive Maßnahmen zu entwickeln, um sich vor den potenziell verheerenden Auswirkungen von IP-Spoofing und den damit verbundenen Angriffen zu schützen.

3.1 IP-Spoofing

IP-Spoofing ist im Kern eine Täuschungstechnik, bei der der Empfänger eines Datenpakets fälschlicherweise glaubt, dass es von einem bestimmten Absender stammt, während es tatsächlich von einem anderen gesendet wurde. Dieser trickreiche Vorgang hat weitreichende Auswirkungen auf die Sicherheit im Netzwerkumfeld und ermöglicht es Angreifern, ihre wahre Identität zu verschleiern. Technisch betrachtet manipuliert der Angreifer bei IP-Spoofing seine IP-Adresse, um sie, als die eines anderen Senders erscheinen zu lassen. Dieser Prozess birgt erhebliche Sicherheitsrisiken, da er es dem Angreifer ermöglicht, verschiedene Angriffe auf ein Ziel auszuüben. Die fehlende Authentifizierung bei der Übermittlung von Datenpaketen trägt dazu bei, dass der Empfänger diese gefälschten Absenderinformationen nicht zuverlässig überprüfen kann [12].

Diese Täuschungstechnik besteht bereits seit mehr als 25 Jahren und hat sich in dieser Zeit als beliebt für Anonymität und verschiedene DDoS-Angriffsvektoren wie Redirection und Amplification etabliert [15].

3.2 Validation

SAV fungiert als Schutzmaßnahme gegen IP-Spoofing. Die Hauptabsicht von SAV besteht darin, die Echtheit der Absenderadresse eines Datenpakets zu überprüfen. In der aktuellen Internetarchitektur fehlt eine Authentifizierungsoption beim Senden von Datenpaketen. Diese Sicherheitslücke

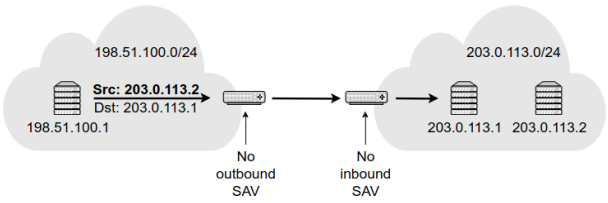

Figure 2. Angriffs Szenario: Der Angreifer betreibt IP-Spoofing und auf dem Weg zur der Zieladresse ist kein SAV in Betrieb, also erhält das Ziel das gefälschte Paket. Von Yevheniya Nosyk (u.a.) (https://shorturl.at/duzB8). Seite 2591.

ermöglicht IP-Spoofing, was wiederum zu einer Zunahme von DDoS-Angriffen führt [16].

3.2.1 Outband SAV und inbound SAV. Je nachdem, in welche Richtung des Internetflusses der SAV eingesetzt wird, erfüllt es unterschiedliche Funktionen und Ziele. Outbound SAV (oSAV) prüft die Echtheit der Absenderadresse, wenn Datenpakete das interne Netzwerk verlassen, während inbound SAV (iSAV) die Absenderadresse für eingehende Datenpakete aus externen Netzwerken prüft. Diese Unterscheidung ist wichtig für die Implementierung von Sicherheitsmaßnahmen und die daraus resultierten Reduzierungen von Angriffsvektoren in beide Richtungen des Datenverkehrs [16].

In Figure 2 ist ersichtlich, dass aufgrund von fehlendem SAV in beide Richtungen, der Angreifer ungestört seinen Angriff durchführen kann. Zusätzlich ist ersichtlich an welcher Stelle oSAV und iSAV im Internet eingesetzt werden können.

Die Nichtumsetzung von oSAV erleichtert Angreifern die Durchführung von DDoS-Angriffen, insbesondere reflection-Angriffen über offene Domain Name Systems (DNS) oder das Network Time Protocol (NTP). Bei diesen Angriffen nutzen Angreifer öffentliche Server, um Schaden anzurichten, indem sie manipulierte IP-Adressen verwenden, um Anfragen zu senden und den Empfänger mit Antworten zu überlasten. Zudem erhält der „Absender" ebenfalls Antworten aufgrund des Transmission Control Protocol (TCP) Handshake. Darüber hinaus bleibt der Angreifer aufgrund der fehlenden Identifikation unerkannt [15] [16] [19]. Bei fehlendem iSAV zusammen mit neuen Attacken wie Water Torture Attack (Lou (u.a.) [9]) könnte es zu erheblichen Konsequenzen führen.

3.2.2 Ingress Filter. In den 1990er Jahren wurden die ersten DDoS-Angriffe öffentlich bekannt, die auf IP-Spoofing basierten [13]. Die daraus resultierende Unsicherheit und die Befürchtung, wenig dagegen unternehmen zu können, führten dazu, dass Fergusan und Senie (BCP 38) [19] im Jahr 2000 den sogenannten "Ingress Filter" vorstellten. Dieser sollte dazu dienen, die Auswirkungen von IP-Spoofing und den daraus resultierenden DDoS-Angriffen zu minimieren. Dieser Filter setzt voraus, dass eine Liste aller gültigen IP-Präfixe vorhanden ist. Seine Funktionsweise besteht darin, IP-Spoofing-Angriffe zu unterbinden, indem er nur den Datenverkehr passieren lässt, dessen IP-Präfix in seiner Liste aufgeführt ist. Falls das Präfix nicht aufgeführt ist, wird der Datenverkehr blockiert. Um einen erfolgreichen Angriff zu starten, muss ein Angreifer eine gültige IP-Adresse aus seinem regionalen Bereich übernehmen, um den Filter zu umgehen.

Ein Nachteil dieses Angriffs-Ansatzes besteht darin, dass die übernommene IP-Adresse möglicherweise von einem Internetdienstanbieter (ISP) blockiert wird. Dies könnte dazu führen, dass der legitime Sender Schaden erleidet, obwohl er nichts mit dem Angriff zu tun hat. Andererseits bietet der Filter den Vorteil, dass Angreifer aufgrund der regionalen Einschränkung einfacher identifiziert werden können. Zusätzlich profitieren Unternehmen von einem verbesserten Schutz, da sie einem geringeren Risiko für DDoS-Angriffe ausgesetzt sind [19].

Es wird dringend empfohlen, dass Internetdienstanbieter und Netzwerkadministratoren den Ingress Filter an den Rändern ihrer Netzwerke implementieren, um das Problem effektiv anzugehen. Netzwerke, die auf diesen Filter verzichten, unterstützen potenzielle Angreifer und tragen somit zu der Problematik bei [15].

3.2.3 Erweiterung des Ingress Filters. Der zuvor präsentierte Filter weist einige Schwächen auf. Insbesondere kann es dazu kommen, dass der Internetverkehr blockiert wird, obwohl er legitim ist, weil zum Beispiel die Liste der IP-Präfixe nicht auf dem neuesten Stand ist. Um dieses Problem zu einzudämmen, stellen F. Baker und P. Savola (BCP 84) [20] vier Jahre später Erweiterungen für den Filter vor. Statische Access Control Lists (ACLs) sind eine davon. Eine weitere ist Strict Reverse Path Forwarding (Strict RPF). Hierbei wird die Quelladresse eines Pakets im Forwarding Information Base (FIB) überprüft. Die Überprüfung ist erfolgreich, wenn das Paket über die Schnittstelle empfangen wird, die normalerweise für die Weiterleitung zum Ursprungsort des Pakets verwendet wird.

3.3 Aktueller Stand von SAV

IP-Spoofing und die daraus resultierende DDoS-Angriffe existieren bereits länger als 25 Jahre [15]. Obwohl das Internet vor 25 Jahren noch nicht die gleiche Relevanz wie heutzutage hatte, waren die Angriffe bereites ein Problem. Der 2000 vorgestellte „Ingress Filter" [19] und die 2004 Erweiterung des Filters [20] gelten aktuell immer noch als Best Practice [13] [21] [16] [15].

3.3.1 Spoofer Project. Robert Beverly (u.a.) [2] haben 2005 den ersten Versuch unternommen, das Internet in Bezug auf SAV zu messen, und ihre Ergebnisse im sogenannten *Spoofer Project* vorgestellt. Im Rahmen des Projekts wurden Freiwillige gesucht, die eine Software installierten, um das Netzwerk, an das ihre Computer angeschlossen waren, auf

SAV zu überprüfen. Die Software sandte regelmäßig Anfragen mit sowohl verfälschten als auch nicht verfälschten IP-Adressen an einen bestimmten Server. Dieser Server überprüfte die empfangenen Anfragen und analysierte, ob Spoofing erlaubt war. Die gewonnenen Daten wurden öffentlich im Internet zugänglich gemacht. Ein Vorteil dieser Messungen besteht darin, dass sie nicht nur Netzwerke aufdecken, die IP-Spoofing erlauben, sondern auch solche, die es nicht erlauben. Ein Nachteil des Projekts ist jedoch, dass Daten nur gewonnen werden können, wenn es Freiwillige gibt, die sie sammeln. Dadurch herrscht eine unabsichtliche Auswahlverzerrung in den Regionen von ISPs, in denen es mehr Nutzer gibt, die diese Software installiert haben. Zusätzlich sind einige ISPs unterrepräsentiert oder gar nicht vertreten in Regionen, wo das Projekt keine Bekanntheit hat. Darüber hinaus werden Netzwerke, die bewusst auf SAV verzichten, nicht freiwillig an solchen Messungen teilnehmen.

3.3.2 The Closed Resolver Project. In einer aktuellen Studie von Yevheniya Nosyk (u.a.) aus dem Jahr 2023 [13] wurde das Internet erneut hinsichtlich SAV gemessen. Das Hauptziel dieser Messung bestand darin, den Einsatz von iSAV zu überprüfen. Während in der Vergangenheit viele Studien den Einsatz von oSAV gemessen haben, wurde die andere Richtung bisher nur selten untersucht. Die Messmethode ähnelte dabei dem Spoofer Project. Die Studie umfasste sowohl IPv4- als auch IPv6-Messungen. Zudem wurden aktuelle Daten aus dem Spoofer Project herangezogen. Die Ergebnisse zeigen, dass die Mehrheit der Autonomous System (AS) kein iSAV implementiert hat. Als AS werden in der Regel größere IP-Netzwerkverbände bezeichnet, die über eine einzige Routing-Richtlinie verwaltet werden und eine eindeutige Nummer besitzen [18]. Des Weiteren wurde die geografische Verteilung der AS berücksichtigt, wobei festgestellt wurde, dass China über ein sehr umfangreiches DNS-Resolver-Netz im IPv4 verfügt, wovon jedoch ein Achtel keine oder fehlerhafte iSAV-Implementierungen aufweist. Im IPv6 hat die USA das größte DNS-Netz mit 260.047 Resolvern, von denen 1319 anfällig für IP-Spoofing sind. Kleinere Länder wie der Kosovo zeigen prozentual eine besonders hohe Anfälligkeit für IP-Spoofing.

3.3.3 DDOS in Bezug auf China. Omer Yoachimik und Jorge Pacheco [22] analysierten in einem Online-Artikel die DDoS-Angriffe auf die Cloudflare-Infrastruktur im dritten Quartal 2023. Cloudflare bietet umfassende Internetdienstleistungen, darunter einen robusten Schutz vor DDoS-Angriffen, eine Web Application Firewall und ein globales Content Delivery Network (CDN). Die Autoren stellten fest, dass China mit erheblichen Herausforderungen durch DDoS-Angriffe konfrontiert ist. Ein Großteil des auf China ausgerichteten Datenverkehrs, wurde von Cloudflare als DDoS-Angriff eingestuft und entsprechend herausgefiltert. In einem weiteren Artikel aus dem Jahr 2019 hielt Eliza Gkritsi [14] fest, dass die Mehrheit der DDoS-Angriffe aus China stammt.

3.3.4 Verbreitung von SAV. Die Erkenntnisse aus beiden Projekten zeichnen ein wenig ermutigendes Bild für Internetnutzer. Ein Großteil der Internetinfrastruktur implementiert kein umfassendes SAV. Diese Situation führt zu einem anhaltenden Anstieg von DDoS-Angriffen [13]. SAV steht vor mehreren Herausforderungen, die dessen weitreichende Implementierung behindern.

Ein wesentlicher Wirtschaftsreiz fehlt, da der Einsatz von SAV keinen direkten finanziellen Gewinn für die implementierende Organisation bringt, denn das Einsetzen von SAV verhindert im Vorhinein DDoS-Attacken. Die Vorteile, die durch oSAV entstehen sind indirekter Natur, da sie verdächtigen Verkehr am Anfang filtern und benachbarte Netzwerke sich nicht mehr damit auseinandersetzen müssen. Dadurch profitieren andere Netzwerke, anstatt das eigene [13].

Ein weiterer Faktor, der die Verbreitung von SAV einschränkt, ist der Kostenaspekt. Die Implementierung und Aufrechterhaltung von SAV-Maßnahmen erfordert kontinuierliche Aktualisierungen und Wartungen, um die Effektivität zu gewährleisten [21]. Zudem benötigen Unternehmen nicht nur Software, sondern auch Rechenleistung, um das umzusetzen. Dieser Prozess ist nicht nur zeit- und ressourcenintensiv, sondern auch kostspielig. Unternehmen könnten aufgrund dieser finanziellen Belastung zögern, SAV in ihren Netzwerken zu implementieren.

Neben den finanziellen Überlegungen hemmt die Sorge vor übermäßigem Filtern die Verbreitung von SAV. Kein Netzwerk strebt danach, legitimen Verkehr aus dem Internet zu blockieren [10].

Ein entscheidender Faktor, der die Verbreitung von SAV weiter hemmt, ist das Fehlen von Anreizen und Regularien. Unternehmen und Netzwerkbetreiber sehen möglicherweise keine klaren Belohnungen und Vorgaben für den Einsatz von SAV-Maßnahmen. Da es keinen unmittelbaren Bonus für die Implementierung gibt, könnte die Motivation SAV einzusetzen, gering sein. Ein weiterer Aspekt ist das Fehlen von Sanktionen für den Nicht-Einsatz von SAV. Ohne klare Strafen oder negative Auswirkungen für Unternehmen, die auf SAV verzichten, fehlt ein Anreiz, diese Sicherheitsmaßnahmen zu implementieren [21].

Es existiert eine weltweite Initiative namens "Mutually Agreed Norms for Routing Security" (MANRS), die sich zum Ziel gesetzt hat, Lösungen für die gängigsten Bedrohungen im Internetverkehr bereitzustellen. Im Rahmen dieser Initiative werden unterschiedliche Programme für Netzwerkadministratoren angeboten. Ein weiteres Ziel besteht darin, der SAV eine größere Reichweite zu verschaffen, um die Implementierung von SAV in mehr Netzwerken zu fördern [15]. Ebenfalls bieten sie eine Anleitung [17] an, wie gegen Spoofing vorgegangen wird. Die bisherigen Best Practice Methoden (BCP 38 und BCP 84), um SAV zu implementieren, wurden bereits vor einer langen Zeit veröffentlicht. Das Internet hat sich in dieser Zeit vergrößert und ist komplexer

geworden. Jedoch sind diese Methoden nicht darauf ausgelegt diese Komplexität mit abzubilden. Aufgrund dessen braucht das Internet neue Standards in der SAV [5].

3.4 Die Zukunft von SAV

IETF ist eine Initiative, die es sich zur Aufgabe gemacht hat, das Internet zu verbessern, indem sie neue Internetstandards und Best Practices, die die Funktionsweise des Internets verbessern sollen, entwickeln. Eine Arbeitsgruppe der IEFT mit dem Namen Source Address Validation in Intra-domain and Inter-domain Networks (SAVNET) hat sich am 08. November 2023 in Prag zum 118. Treffen der IEFT getroffen, um neue Internetstandards zu präsentieren und zu diskutieren. Diese Ergebnisse werden im Folgenden erläutert.

Jianping Wu (u.a.) [5] hat Anforderungen an neue SAV Methoden im Bereich der Intra-domain präsentiert. SAV-Architecture (SAVA) (RFC5210) teilt ein Netzwerk in 3 Stufen auf: acces, intra-domain und inter-domain. Der Vorteil dieser Architektur ist, dass wenn SAV nicht vollständig implementiert ist, SAVA Ablöse für das Problem sein kann, indem SAVA einspringt, wenn SAV nicht greift. Dadurch ist das Internet sicherer vor DDoS-Angriffen. Inter-domain SAV (interSAV) wird zwischen ASes betrieben. Ein Vorteil von interSAV ist es, dass verschiedene ASes keine Kommunikation brauchen, um effektiv zu filtern. Intra-domain SAV (intraSAV) wird innerhalb eines AS betrieben.

Um die Herausforderungen der aktuellen Methoden zu überwinden, wurden für neue Standards im SAV-Bereich folgende Anforderungen definiert:

1. Der SAV-Mechanismus aktualisiert sich automatisch, entsprechend der sich ändernden Netzwerkdynamik.
2. Präzise Validierung der Source Address, um legitimen Datenverkehr möglichst wenig zu filtern.
3. Effektivität des Mechanismus, selbst wenn er nicht vollständig implementiert ist.
4. Validierung sowohl von IPv4- als auch von IPv6-Adressen.
5. Vermeidung von neuen Sicherheitslücken.

InterSAV hat zu dem noch ein paar weitere Anforderungen, die spezifisch für den Bereich zwischen ASes gelten, weil dort einige Details unterschiedlich sein können.

Dan Li (u.a.) [6] hat einen Vorschlag für intraSAV entwickelt, der auf den zuvor definierten Anforderungen basiert. Ihr Ansatz beinhaltet die Einführung eines dezidierten Austauschkanals. Um die Sicherheit dieses Kanals zu gewährleisten, muss dieser immer vor dem Austausch verschlüsselt werden, und zwar durch ein sicheres Verschlüsselungsverfahren. Über diesen Kanal können Router innerhalb eines AS spezifische SAV-Inhalte austauschen, wie beispielsweise lokale IP-Präfixe. Auf Basis dieser spezifischen SAV-Inhalte werden neue SAV-Regeln generiert.

Falls der Kanal keine Informationen bereitstellt, kann die Lücke mit den eigenen lokalen Beständen gefüllt werden. Der Kommunikationskanal bietet den Vorteil, dass Router automatisch aktualisiert werden und in beide Fließrichtungen genutzt werden können. Router A kann seine Präfixe an Router B senden, sodass Router B diese Präfixe für oSAV benutzen kann und umgekehrt. Dies fördert einen effizienten Austausch von SAV-relevanten Informationen innerhalb des AS.

Im Bereich interSAV haben Jianping Wu (u.a.) [8] im Wesentlichen denselben Ansatz verfolgt. In diesem Szenario wird ein Kommunikationskanal zwischen ASes eingerichtet, anstatt innerhalb eines AS.

In der Präsentation *"A Large-scale Measurement of IP Source Spoofing on the Internet"* stellte Shuai Wang [23] seine Ergebnisse einer SAV-Messung vor, die mithilfe eines lokal installierbaren Programms durchgeführt wurde. Das Programm etabliert eine Verbindung zu einem speziellen Server. Dabei sendet der Computer gefälschte Pakete an den Server und der Server sendet ebenfalls gefälschte Pakete an den Computer. Auf diese Weise lässt sich erkennen, ob iSAV oder oSAV implementiert ist. Die Resultate zeigen, dass inbound-Spoofing deutlich häufiger vorkommt als outbound-Spoofing.

Des Weiteren ergab die Untersuchung, dass China einige ASes besitzt, die im IPv4-Adressraum unzureichenden Schutz gegen Outbound-Spoofing bieten. Im Vergleich dazu verfügt der Westen über umfassendere Schutzmaßnahmen gegen Spoofing.

4 Fazit

DDoS-Angriffe bleiben eine aktuelle Herausforderung, die vorerst nicht vollständig behoben werden kann. Durch die fehlende Authentifizierung des Absenders, sind sie zu einer beliebten Bedrohung geworden. Ihre einfache Ausführung und die damit verbundenen erheblichen Schäden, machen sie besonders attraktiv.

Aufgrund dieser Herausforderung braucht das Internet Methoden, um DDoS-Angriffe effektiv zu bekämpfen. Der IXP-Scrubber [11] ist eine Methode dieses Ziel zu erreichen in dem er an einem IXP schädlichen Verkehr filtert. Der Scrubber ist ein MLS. Nach dem Training und der Validierung mit gesammelten Daten von IXPs ist er in der Lage, eigenständig und effektiv neue Regeln, zur Filterung schädlichen Internetverkehrs, zu bestimmen. Dabei sind die Regeln übersichtlich, damit ein Netzwerk-Administrator schnell entscheiden kann, ob die gefundenen Regeln effektiv sind oder nicht. Tägliches Training sorgt dafür, dass das MLS effektiv bleibt und auch neue Angriffsvektoren erkennt und filtert. Der Einsatz des MLS an verschiedenen IXPs, insbesondere in anderen Regionen, ist möglich, wobei minimale Effizienzverluste auftreten können. Eine optimale Lösung wäre die Zusammenarbeit aller IXPs, um ein umfassendes gemeinsames MLS aufzubauen.

Obwohl mit BCP 38 und BPC 84 die ersten SAV-Methoden eingeführt wurden, sind sie bisher nicht weit verbreitet. Das wurde in mehreren Versuchen gemessen [2] [13] [23]. Dies

liegt daran, dass sie erheblichen Aufwand erfordern und nur effektiv sind, wenn sie regelmäßig von Experten aktualisiert werden. Vernachlässigt man diese Aktualisierungen, besteht die Gefahr, dass legitimer Internetverkehr blockiert wird [5]. Zudem fehlen klare Vorschriften, die festlegen, ob die Implementierung von SAV verpflichtend ist.

Um die Schwächen aktueller SAV-Methoden zu überwinden, wurden spezifische Anforderungen definiert, die in einer umfassenden Liste festgehalten sind [5]. Neue Methoden, die diesen Kriterien entsprechen, wurden auf einer IETF-Konferenz vorgestellt. Eine dieser Methoden beinhaltet einen zusätzlichen Informationskanal zwischen Netzwerken, auf dem SAV spezifische Inhalte ausgetauscht werden können. Das hat den Vorteil, dass nicht mehr Experten diese Inhalte aktualisieren müssen, sondern die SAV-Methoden es automatisch selbst machen können. Um die Sicherheit zu gewährleisten, muss dieser Kanal verschlüsselt werden, um Abhörversuchen durch Angreifer vorzubeugen. Ein weiterer Vorteil dieser Methode ist die direkte Kommunikation zwischen Router. Dadurch können iSAV und oSAV parallel betrieben werden, was zur besseren Effektivität führt.

China hat ein großes Problem mit DDoS. Die meisten DDoS-Angriffe stammen aus dem Land [14] und zusätzlich wird deren Internetinfrastruktur stark angegriffen [22]. Außerdem hat eine aktuelle Überprüfung [23] herausgefunden, dass die ASes in China wenig SAV im Einsatz hat. Interessanterweise sind viele Autoren, der auf der letzten IETF-Konferenz in Prag eingereichten Dokumente, in Unternehmen oder Institutionen mit Sitz in China tätig. Dies lässt darauf schließen, dass China die Problematik erkannt hat und Maßnahmen ergreifen möchte, um sie zu bekämpfen.

Insgesamt ist es entscheidend zu betonen, dass das Bewusstsein für die Problematik von IP-Spoofing in Verbindung mit DDoS-Angriffen gestärkt werden muss. Dies könnte dazu beitragen, dass die Forschung in dem Bereich vorangetrieben wird und zudem mehr SAV im gesamtem Internet eingesetzt wird.

References

[1] Timm Böttger al. 2019. Shaping the Internet: 10 Years of IXP Growth. *arxiv* 3, 1 (July 2019), 1–20. https://datatracker.ietf.org/doc/draft-li-savnet-intra-domain-architecture/

[2] Robert Beverly and Steven Bauer. 2005. The Spoofer Project: Inferring the Extent of Source Address Filtering on the Internet. *usenix* 1, 1 (July 2005), 1–8. https://www.usenix.org/legacy/event/sruti05/tech/full_papers/beverly/beverly.pdf

[3] cloudflare. [n. d.]. *Was ist Blackhole-Routing?* Retrieved Januar 19, 2024 from https://www.cloudflare.com/de-de/learning/ddos/glossary/ddos-blackhole-routing/

[4] cloudflare. [n. d.]. *Was ist ein Internet Exchange Point? | Cloudflare.* Retrieved Januar 14, 2024 from https://www.cloudflare.com/de-de/learning/cdn/glossary/internet-exchange-point-ixp/

[5] Dan Li et al. 2023. Source Address Validation in Intra-domain Networks Gap Analysis, Problem Statement, and Requirements. *IEFT SAVNET* 2, 1 (Aug. 2023), 1–13. https://datatracker.ietf.org/doc/draft-ietf-savnet-intra-domain-problem-statement/

[6] Dan Li et al. 2024. Intra-domain Source Address Validation (SAVNET) Architecture. *IEFT SAVNET* 1, 1 (Jan. 2024), 1–20. https://datatracker.ietf.org/doc/draft-li-savnet-intra-domain-architecture/

[7] Jakub Czyz et al. 2014. Taming the 800 Pound Gorilla: The Rise and Decline of NTP DDoS Attacks. *ACM Internet Meas. Conf.* 1 (2014), 435–448. https://doi.org/10.1145/2663716.2663717

[8] Jianping Wu et al. 2024. Inter-domain Source Address Validation (SAVNET) Architecture. *IEFT SAVNET* 1, 1 (Feb. 2024), 1–40. https://datatracker.ietf.org/doc/draft-wu-savnet-inter-domain-architecture/

[9] Luo Xi et al. 2018. A Large Scale Analysis of DNS Water Torture Attack. *Association for Computing Machinery* 1, 1 (2018), 168–173. https://doi.org/10.1145/3297156.3297272

[10] Maciej Korczy´nski et al. 2020. Don't Forget to Lock the Front Door! Inferring the Deployment of Source Address Validation of Inbound Traffic. *Proceedings of the Passive and Active Network Measurement Conference* 1, 1 (Feb. 2020), 1–15. https://doi.org/10.48550/arXiv.2002.00441

[11] Matthias Wichtlhuber et al. 2022. IXP Scrubber: Learning from Blackholing Traffic for ML-Driven DDoS Detection at Scale. *SIGCOMM* 14, 1 (Aug. 2022), 1–16. https://doi.org/10.1145/3544216.3544268

[12] Robert Beverly et al. 2009. Understanding the efficacy of deployed internet source address validation filtering. *SIGCOMM* 14, 1 (Nov. 2009), 1–14. https://doi.org/10.1145/1644893.1644936

[13] Yevheniya Nosyk et al. 2023. The Closed Resolver Project: Measuring the Deployment of Inbound Source Address Validation. *IEEE/ACM Transactions on Networking* 31, 6 (July 2023), 2589–2603. https://doi.org/10.1109/TNET.2023.3257413

[14] Eliza Gkritsi. 2019. *China is the world's largest source of DDOS attacks, but its share is falling.* Retrieved Februar 7, 2024 from hhttps://technode.com/2019/07/08/china-is-the-worlds-largest-source-of-ddos-attacks-but-its-share-is-falling/

[15] Qasim Lone. 2023. *Why is Source Address Validation Still a Problem?* Retrieved Februar 01, 2024 from https://www.manrs.org/2023/04/why-is-source-address-validation-still-a-problem/

[16] Yevheniya Nosyk Maciej Korczyński. 2021. Source Address Validation. *Springer Berlin Heidelberg*, 1 (2021), 1–5. https://hal.science/hal-04027475/document

[17] MANRS. 23. *MANRS Implementation Guide.* Retrieved Februar 05, 2024 from https://manrs.org/netops/guide/antispoofing/

[18] Myra. 2021. *Was ist ein Autonomes System und was sind AS-Nummern (ASN)?* Retrieved Februar 06, 2024 from https://www.myrasecurity.com/de/knowledge-hub/asn/

[19] D. Senie P. Ferguson. 2000. Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing. *BCP 38, RFC 2827* 1, 1 (May 2000), 1–10. https://www.rfc-editor.org/info/bcp38

[20] D. Senie P. Ferguson. 2004. Ingress Filtering for Multihomed Networks. *BCP 84, RFC 3704* 1 (March 2004), 1–16. https://www.rfc-editor.org/info/rfc3704

[21] Qasim Lone (u.a.). 2022. SAVing the Internet Measuring the adoption of Source Address Validation (SAV) by network providers. *[Dissertation (TU Delft), Delft University of Technology]* 1, 1 (2022), 37–62. https://doi.org/10.4233/uuid:cfed8540-76cf-4d35-b528-b03230ef98e0

[22] Omer Yoachimik und Jorge Pacheco. 2024. *DDoS threat report for 2023 Q4.* Retrieved Februar 7, 2024 from https://blog.cloudflare.com/ddos-threat-report-2023-q4

[23] Shuai Wang. 2023. *A Large-scale Measurement of IP Source Spoofing on the Internet?* Retrieved Februar 06, 2024 from https://datatracker.ietf.org/meeting/118/materials/slides-118-savnet-a-large-scale-measurement-of-ip-source-spoofing-on-the-internet

[24] Maciej Korczy ´nski and Yevheniya Nosyk. 2023. Source Address Validation. *Encyclopedia of Cryptography, Security and Privacy* 1 (Jan. 2023), 1–6. https://doi.org/10.48550/arXiv.2301.09952