Distributed-Denial-of-Service Attack Detection

Jasper Eumann
Betreut durch Prof. Dr. Thomas C. Schmidt

{jasper.eumann|t.schmidt}@haw-hamburg.de

Studiengang Master of Science Informatik
Department Informatik
Hochschule für Angewandte Wissenschaften Hamburg

Zusammenfassung. Distributed-Denial-of-Service (DDoS) Angriffe sind nur schwer abzuwehren und machen einen großen Teil der modernen netzwerkbasierten Angriffe auf die Verfügbarkeit der Infrastruktur aus. Ein gängiger Mechanismus, um die durch einen Angriff erzeugte Last zu vergrößern, sind Amplification-Attacks (Verstärkungsangriffe). Diese Angriffsart wird häufig mit Reflektions-Attacke (Spiegelungsangriff) kombiniert. Im Falle eines Reflection-Angriffes erhält das Opfer die Antworten des Servers, obwohl es die Anfragen nicht gestellt hat. Dies wird erreicht, indem Netzwerkpakete mit der IP-Adresse des Opfers als Absenderadresse (IP-Spoofing) an reguläre Server geschickt werden. Es existieren verschiedene Schutzmechanismen einen Service gegen DDoS-Angriffe zu schützen. Eine generelle Lösung existiert nicht und viele Schutzmechanismen wirken nur ad hoc und partiell oder sind mit Kollateralschäden behaftet (Bsp.: Blackholing).

Schlüsselwörter: DoS, DDoS, IP-Spoofing, reflection attack, amplification attack, Inter-domain traffic

1 Einführung

Erstes Auftreten des Begriffs Denial-of-Service gehen bis ins Jahr 1983 zurück [Gli83]. Er beschreibt einen Service in einem Computernetzwerk, der durch einen Cyberangriff nicht mehr zur Verfügung steht und somit keine Anfragen mehr entgegennehmen kann. Die Gründe für einen Systemausfall können sehr unterschiedlich sein. Es werden beispielsweise Fehler in der Software des Services oder Eigenarten der Übertragungsprotokolle verwendet, um ihn zu stören. Angriffsszenarien, in denen Implementierungs- oder Architekturfehler durch den Angreifer ausgenutzt werden, sind nicht Teil dieser Ausarbeitung. Es wird ausschließlich auf verteilte Distributed-Denial-of-Service (DDoS) flooding attacks eingegangen. Sie haben die Eigenschaft, dass ein Service oder die gesamte Infrastruktur mit Netzwerkpaketen geflutet werden und diese unter der Last zusammenbricht.

Es ist nur begrenzt möglich, sich vor DDoS-Angriffen zu schützen. Einige Vorfälle in der jüngsten Vergangenheit belegen diese Aussage. Am 20. September 2016 wurde die Internetpräsenz des freien Journalisten Brian Krebs mit

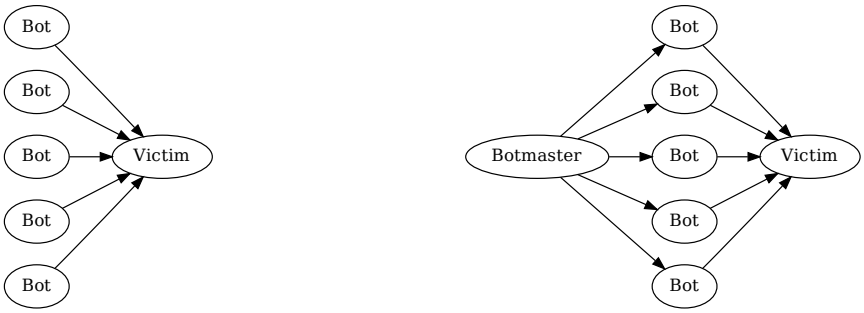
einer gewaltigen DDoS-Attacke des Mirai Botnetzes aus dem Internet genommen [Kre16], obwohl diese von Akamai, einem der größten Anbieter für DDoS-Schutz, gesichert wurde.

Die Ausarbeitung ist wie folgt gegliedert. Zu Beginn werden im Abschnitt 2 unterschiedliche Angriffstypen beschrieben und folgend im Abschnitt 3 auf die Erkennung und mögliche Abwehrmechanismen eingegangen. Aufbauend gibt der Abschnitt 4 einen Überblick über einschlägige Sicherheitskonferenzen und aktuelle Publikationen.

2 Angriffstypen

Um einen möglichst hohen Durchsatz bei einem Angriff zu erzielen, werden in der Regel DoS-Angriffe nicht nur von einem einzelnen Angreifer ausgeführt, sondern parallel von unterschiedlichen Angreifern getätigt. Diese verteilten Attacken nennen sich Distributed-Denial-of-Service (DDoS)-Angriffe.

In der Abb. 1a ist ein einfacher DDoS-Angriff zu sehen, in welchem die Angreifer das Opfer direkt ansprechen.



(a) Direkter Angriff (b) Angriff durch ein Botnetz

Abb. 1: Mögliche Anordnungen der Teilnehmer eines DDoS-Angriffes

Der Ansatz ist sehr wirkungsvoll, die Verteilung führt jedoch zum Verteilungsproblem, da der Angriff nur effektiv ist, wenn alle Teilnehmer gleichzeitig agieren. Früher wurde dieses Problem durch sorgfältige Planung und Absprache gelöst, später mit sogenannten DDoS-Tools. Dies sind Programme, die meistens mit der Zustimmung des Besitzers eines Computers für Angriffe verwendet werden. Die populärsten DDoS-Tools waren die Low Orbit Ion Canon (LOIC) und die High Orbit Cannon (HOIC), welche im Zusammenhang mit dem Hacker-Kollektiv Anonymous in den Medien präsent waren [Clo18b; Clo18a].

Die Steigerung der DDoS-Tools sind Botnetze. Botnetze sind aus sehr vielen Computern oder anderen Systemen mit Internetzugang zusammengesetzt und werden von einem oder mehreren Kontrollservern gesteuert. Die einzelnen Knoten eines Botnetzes sind in der Regel ohne das Wissen ihres Besitzers Teil des Netzes und wurden durch Schwachstellen in den einzelnen Systemen übernommen [Kol+17].

Die Abb. 1b zeigt einen durch den Botmaster initiierten Angriff. Dieser sendet die Informationen über das Opfer an die einzelnen Bots, welche das Opfer attackieren. Der Botmaster ist für das Opfer nicht sichtbar und versendet ausschließlich Kontrollpakete.

Neben der Anordnung und Anzahl der Angreifer existieren unterschiedliche Arten von Angriffen. Einige basieren darauf, dass der Angreifer ein Paket sendet, indem er das Opfer als Absender einträgt. Dieses Verfahren wird im Abschnitt 3.1 detaillierter beschrieben und zur Umsetzung von Reflection-Angriff genutzt. Mit Reflection (spiegeln) ist gemeint, dass das Opfer nicht direkt, sondern über einen Dritten angesprochen wird. Die dritte Partei erhält eine Anfrage, welche vermeintlich vom Opfer versendet wurde und beantwortet diese. Somit sieht das Opfer nicht die IP des Angreifers und ist nicht direkt in der Lage die Quelle des Angriffs zu ermitteln. Zusätzlich zur Verschleierung der Adresse des Angreifers kann eine Verstärkung erzielt werden. In diesem Fall handelt es sich um einen Amplification- (Verstärkungs-) und Reflection-Angriff. Geeignet für einen Verstärkungsangriff sind alle Anfragen, in denen die Antwort größer als die Frage ist. Je höher der Verstärkungsfaktor, desto höher ist die verursachte Last beim Opfer. Weit verbreitet sind beispielsweise Domain Name System (DNS)- oder Network Time Protocol (NTP)-Anfragen.

Eine weitere Gruppe von Angriffstypen nutzt die Eigenarten in Übertragungsprotokollen aus (Protocol exploitation attack). Bekannte Angriffe dieser Kategorie sind zum Beispiel Slowlaris- oder SYN-flood-Angriffe. Slowlaris versucht solange Verbindungen zu einem Webserver aufzubauen, bis die maximale Anzahl möglicher Verbindungen erreicht ist [BNI17]. Im Falle eines SYN-flood Angriffes wird das TCP-Protokoll genutzt, in welchem mittels einer großen Anzahl an TCP-SYN-Paketen der TCP-Verbindungsaufbau begonnen, aber nie tatsächlich aufgebaut wird. Das Opfer hält den Status der geöffneten Verbindungen bis zum Timeout [ZJT13].

Andere Angriffsarten zielen auf Fehler und Schwächen in den Opfersystemen oder in dem bereitgestellten Dienst ab, beispielsweise gegen Webserver (Vulnerability attacks). Diese werden im Rahmen dieser Ausarbeitung nicht detaillierter betrachtet.

Erkennungsmechanismen für Pakete mit manipulierter Absenderadresse sind die Hauptfragestellung dieser Auseinandersetzung. Es existieren eine Vielzahl von Angriffstypen und Kombinationen. Detailliertere Informationen finden sich beispielsweise in dem Artikel *A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks* [ZJT13].

3 Erkennung/ Abwehr von DDoS-Angriffen

Um einen DDoS-Angriff abwehren zu können, muss dieser erst identifiziert werden. Dies ist nicht trivial. Gerade im Fall von Überflutungsangriffen ist der bösartige Traffic kaum bis gar nicht von legitimen Anfragen zu unterscheiden. Mögliche Erkennungsmerkmale sind:

- die Paketsignaturen (Protokoll, Port, Header, ...)
- bekannte Absenderadressen
- auffallend viele Requests von einer geringen Anzahl an IP-Adressen
- überdurchschnittlich viele Zugriffe ohne einen erklärbaren Grund (Werbemaßnahmen, ...)
- die Intensität bestimmter Verkehrsmuster (z.B. TCP SYN).

Um die identifizierten Absenderadressen oder sonstige Auffälligkeiten auszutauschen, werden DDoS Information Sharing Systems [Kam+17] entwickelt und genutzt. Diese Systeme machen es möglich, bekannte Angreifer oder Angriffstechniken einfacher zu erkennen und abzuwehren, ähnlich wie es von Antiviren-Programmen für die Abwehr von Schadsoftware praktiziert wird.

Nach der erfolgreichen Identifizierung eines Angriffs gibt es unterschiedliche Methoden diesen abzuwehren. Die direkteste Lösung ist es, die Pakete zu verwerfen oder im Falle von anwendungsspezifischen Angriffen, den Angriffspunkt in der Anwendung zu beheben. Fehler in einer Anwendung zu finden, ist zeitaufwendig und kann teilweise nur reaktiv geschehen. Dies kann in der eigenen Infrastruktur durchgeführt werden, wenn ausreichend Ressourcen vorhanden sind. Alternativ ist es möglich, Cloud-basierten DDoS-Schutz von beispielsweise Akamai oder Cloudflare [Kum17] einzukaufen. In diesem Fall wird der gesamte Traffic durch sogenannte Scrubbing Center geleitet, welche bösartige Pakete herausfiltern und Traffic-Spitzen kompensiert.

Als letztes Mittel ist es möglich, den Service (die IP-Adresse des betreffenden Servers) mittels Border Gateway Protocol (BGP) Blackholding aus dem Netz zu nehmen. Diese Maßnahme macht den Service jedoch auch für legitime Anfragen nicht mehr erreichbar und wird in der Regel nur genutzt, wenn die Infrastruktur dem Angriff nicht gewachsen ist.

Auf die Möglichkeiten, Angriffe an unterschiedlichen Stellen auf ihrem Weg zum Opfer abzuwehren oder einzudämmen, wird im Abschnitt 3.4 detaillierter eingegangen.

3.1 IP-Spoofing

Der Begriff IP-Spoofing beschreibt das Modifizieren der Absenderadresse eines Netzwerkpaketes. In der Regel wird die Adresse des Opfers eingetragen, um wie im Abschnitt 3 vorgestellte Spiegel- und Verstärkungs-Angriffe auszuführen. Diese Verfälschung wird auf der IP-Ebene durchgeführt und verhindert den vollständigen Aufbau von verbindungsorientierter Kommunikation (TCP), da zwischen den Kommunikationspartnern eine Session aufgebaut wird. IP-Spoofing

wird häufig im Zusammenhang mit UDP basierter verbindungsloser Kommunikation eingesetzt und teilweise lediglich, um die Adresse des Angreifers zu verschleiern. Dieses Verhalten ist beispielsweise in Zusammenhang mit TCP-SYN Angriffen zu beobachten [ZJT13], die den Aufbau einer TCP-Verbindung initiieren, aber nicht abschließen und somit mit IP-Spoofing kombiniert werden können.

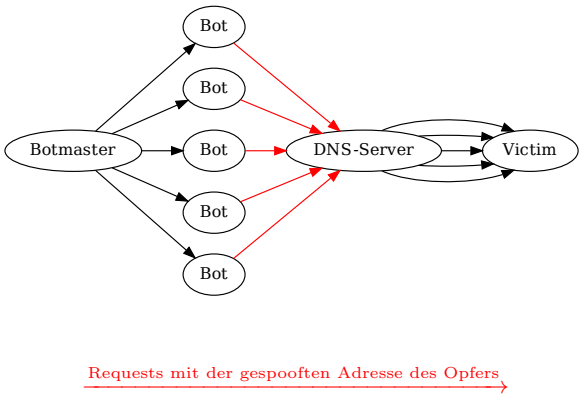


Abb. 2: Durch ein Botnetz ausgeführter DNS-Amplification/Reflection Angriff

Mittels IP-Spoofing manipulierte Pakete sind im Zusammenhang mit Amplification-Angriffen nur bis zum Spiegelserver als gespoofte Pakete identifizierbar. Die Antwort des Spiegelservers adressiert direkt das Opfer und enthält dessen Anschrift als Absenderadresse und ist somit ein legitimes Netzwerkpaket.

In der Abb. 2 ist der Ablauf eines gängigen DNS-Verstärkungsangriffes zu sehen. Der Botmaster initiiert einen Angriff auf das Opfer, welcher mittels gespoofter Pakete zum DNS-Server ausgeführt wird. Die DNS-Server Antworten des DNS-Servers werden als reguläre Netzwerkpakete an das Opfer gesendet.

3.2 Ingress- / Egress-Filterungsverfahren

Eine wirkungsvolle Methode zur Unterbindung von DDoS-Attacken, die auf IP-Spoofing setzen, ist es, die einzelnen Angreifer direkt in ihren Ursprungsnetzen zu identifizieren und ihren Traffic zu verwerfen. Dieses Vorgehen hat den Vorteil, dass der Angriff dezentral am Ursprung unterbunden werden kann und sorgt für eine Verteilung der Last, sodass diese an den einzelnen Routern geringer ist. Eine Möglichkeit dies zu erreichen, ist das Ingress- und Egress-Filterungsverfahren.

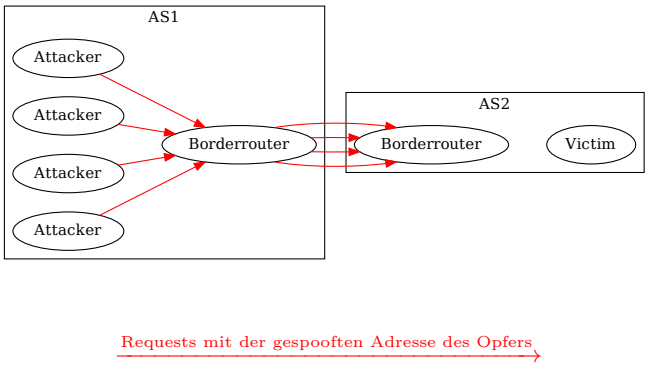


Abb. 3: Ingress/Egress Filtering verhinderter einen DDoS Angriff

Das im RFC-2827 [FS00] und RFC-3704 [BS04] beschriebene Ingress-Verfahren unterbindet allen Traffic, der aus bekannten Netzen mit unbekannter IP-Adresse versucht in ein Netz zu gelangen. Im Gegensatz dazu, verhindert das Egress-Filterungsverfahren [Dis08], dass Traffic mit einer nicht aus dem eigenen Netz stammenden IP-Adresse das Netz verlässt. Beide Verfahren können nur umgesetzt werden, wenn die von den angrenzenden Autonomen Systemen gerouteten IP-Prefixe bekannt sind.

In der Abb. 3 ist zu sehen, wie mittels Ingress-Filterung Pakete mit gespoofften Adressen gefiltert werden, indem sie vom Borderrouter des AS2 verworfen werden.

Die vorgestellten Filterungsverfahren sind sehr wirkungsvoll, aber nicht flächendeckend im Einsatz. Bei 20% der in der Arbeit von Lichtblau u. a. betrachteten autonomen Systeme wurde Ingress und bei 50% Egress-Filterung angewendet [Lic+17] und in 74% aller ASe wurde gespoofter Traffic entdeckt.

3.3 IP-Spoofing an IXPs

Pakete mit gefälschter Absenderadresse im Kernnetz, also in Transportnetzen, an IXPs oder dem Zielnetz zu erkennen, ist sehr komplex. Ein Paket passiert eine Vielzahl von Routern und autonomen Systemen (AS) auf seinem Weg zum Ziel.

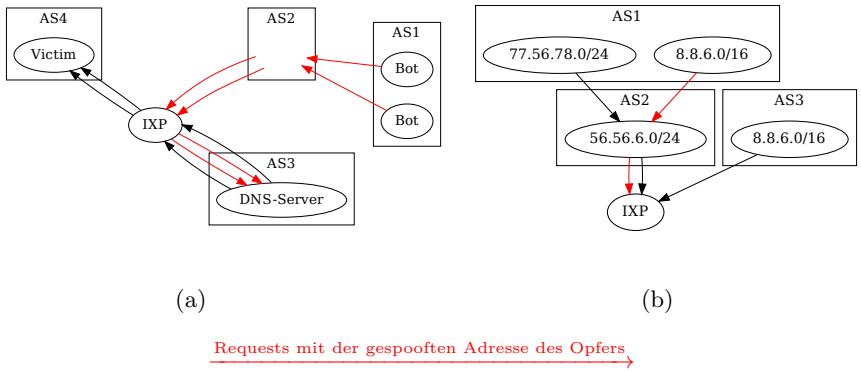


Abb. 4: DNS-Amplification/Reflection Angriff an IXPs

In der Abb. 4a ist zu sehen, dass Pakete unterschiedliche ASe und Internet Exchange Points (IXPs) passieren. Ein gespooftes Paket kann lediglich auf dem Weg von den Bots zum DNS-Server im AS3 einfach identifiziert werden. Der Borderrouter des AS4 kann somit das Paket nicht als bösartiges Netzwerkpaket identifizieren.

Einfache Identifikation ist in diesem Fall nicht Möglich, da umfassendes Wissen über alle gültigen IP-Prefixe der Route benötigt wird. Zusätzlich wäre die Filterung an IXPs anstatt an den Borderroutern der Autonomen Systeme sinnvoll, weil sie zum Herzen des Internets gehören und der positive Effekt alle Teilnehmer betreffen würde.

Das Wissen über die zulässigen IP-Prefixe der Nachbarn reicht nicht aus, um Spoofing zu erkennen. Erschwerend kommt hinzu, dass das Routing dynamisch ist. Pakete mit IP-Adressen eines IP-Prefixes können legitim auf unterschiedlichen Wegen ein AS oder IXP erreichen, da Nachbarn Transit gewähren können.

Das Paper von Lichtblau u.a. [Lic+17], wurde auf der ACM Internet Measurement Conference 2017 vorgestellt und ist unter der Leitung von Prof. Dr. Anja Feldmann an der TU Berlin entstanden. Lichtblau u.a. haben ein Konzept erarbeitet, in dem anhand der Peerings von Internet Service Providern (ISPs) ermittelt wird, ob es zulässig ist, über eine gegebene Route ein Paket zu senden oder ob es sich um ein Paket mit gefälschter Absenderadresse handeln muss. Die möglichen legitimen Routen werden nach unterschiedlichen Gesichtspunkten ermittelt. Als Datenquellen dienen die BGP Route Announcements, CAIDA Customer Cones [Luc+13], einem Datensatz der die AS Zusammenhänge und Geschäftsbeziehungen aufarbeitet. Zusätzlich wird berücksichtigt, ob eine Organisationen mehre autonome Systeme betreibt. Zur Optimierung werden die Datenquellen kombiniert eingesetzt. Das Verfahren erzielte sehr gute Ergebnisse [Lic+17] und ermöglicht es, im auf der Abb. 4b abgebildeten Szenario zu

erkennen, dass der IP-Prefix *8.8.6.0/16* nicht über das AS2 den IXP erreichen dürfte. Mit diesem Wissen ist es möglich, gespoofte Pakete zu verwerfen.

3.4 Ebenen der DDoS-Abwehr

Es existieren mehrere unterschiedliche Ansätze zur Bekämpfung von DDoS-Attacken: eine Möglichkeit ist es, die Angriffe direkt in den Ursprungsnetzen zu bekämpfen. Die **zweite** Möglichkeit bekämpft die Angriffe zentralisiert vor dem Zielsystem und mit der **dritten** Möglichkeit können Angriffe auf dem weg zum Ziel dezentral abgewehrt werden.

Ein Beispiel für den **ersten** Ansatz ist im Paper *Software-Defined Edge Defense Against IoT-Based DDoS* von Özçelik u. a. [OCG17] beschrieben, in welchem mittels Software gesteuerter Netzwerkkomponenten (SDN) in IoT-Netzen Systeme mit auffälligen Verhalten automatisch separiert werden. Die separierten Systeme sind abgeschottet und nicht in der Lage andere Systeme zu infizieren oder an einem DDoS-Angriff teilzunehmen. Dieses Vorgehen wirkt der Bildung großer Botnetze wie dem Mirai-Botnetz [Kol+17] entgegen.

Die im Abschnitt 3.2 beschriebenen Filterungsverfahren sind ebenfalls Teil dieser Kategorie. Sie sind allerdings nur wirksam gegen Angriffe, in denen IP-Spoofing eingesetzt wird. Die Abwehr von Angriffen in den Ursprungsnetzen ist effektiv, wenn die Ansätze flächendeckend eingesetzt werden. Dem Abschnitt 3.2 ist zu entnehmen, dass dies nicht geschieht.

Der **zweite** Ansatz versucht DDoS-Angriffe nah an den Zielsystemen abzuwehren. Dies wird erreicht, indem die bösartigen Pakete identifiziert und verworfen werden. Dieses Verfahren ist beispielsweise bei einfachem Cloud-basiertem DDoS-Schutz im Einsatz. Der gesamte Traffic wird umgeleitet und gefiltert dem Kunden zugestellt. Für Hoster oder andere Halter von größerer Infrastruktur besteht die Möglichkeit, an den Grenzen des eigenen Netzes Systeme zur DDoS-Abwehr zu installieren. Mehr über die genaue Funktionsweise dieser Systeme zu erfahren, ist allerdings nur schwer möglich, da es sich fast ausschließlich um proprietäre Systeme handelt. Populäre Anbieter für DDoS-Schutz sind Arbor Networks [Arb18] und A10 [A1018].

Die Absicherung an den Zielsystemen kann von den Betroffenen ausgeführt werden, welche direkt vom Schutz profitieren. Dies sorgt dafür, dass dieser Ansatz in der Praxis häufig genutzt wird. Der größte Nachteil ist allerdings, dass große flooding-Angriffe auch von der stärksten Hardware nur bedingt abgefangen werden können. Dies zeigte sich beispielsweise durch den Angriff des Mirai-Botnetzes 2016 auf DYN.com [DYN16], der große Teile des Internets beeinträchtigte.

Der **dritte** Ansatz zur Abwehr von DDoS-Angriffen basiert auf der Filterung des Traffics im Kernnetz. Ein Beispiel wie bösartiger Traffic in dieser Domäne erkannt werden kann, ist in der schon beschriebenen Arbeit von Lichtblau u.a. zu finden. Es wird anhand der Peerings von Internet Service Providern (ISPs) ermittelt, welche IP-Prefixe auf einer gegebenen Route zulässig sind. Die Eindämmung von Angriffen in den Transportnetzen und IXPs verlagert die im Vorhergehen-

den beschriebene Problematik, der Paketflut Herr zu werden, an unterschiedliche Punkte im Kernnetz und macht sie somit beherrschbar.

Im Paper von Zargar u.a. wird ein Konzept vorgestellt, in dem alle drei Ansätze kombiniert werden [ZJT13]. Dieses Vorgehen macht es möglich, den Angriff auf mehreren Ebenen abzufangen und vereint die Vorteile aller drei Ansätze. Es sind allerdings Anpassungen an der vorhandenen Infrastruktur sowie die Kooperation der einzelnen Interessentengruppen erforderlich.

4 Forschung und Konferenzen

Das Thema DDoS beschäftigt schon lange die wissenschaftliche Gemeinde. Eines der frühesten Paper, das bei der Recherche auffiel, war das Paper *Distributed Denial of Service Attacks* von Lau u.a aus dem Jahr 2000 [Lau+00]. Es existieren Veröffentlichungen zu diesem Thema von fast jeder größeren Universität und sowohl die IETF als auch die IEEE beteiligen sich aktiv an der Lösungsfindung. Eine Auswahl bekannter Konferenzen, an welchen zu diesem Thema veröffentlicht wurde, können der folgenden Aufzählung entnommen werden:

- **Network and Distributed System Security Symposium (NDSS)** [NDS18] - Auf der NDSS 2016 wurden drei Paper zum Thema DDoS veröffentlicht. Unter anderem das Paper *SIBRA: Scalable Internet Bandwidth Reservation Architecture* [Bas+16] von Basescu u. a., welches sich mit dem Schutz der Transportnetze und IXPs gegen DDoS-Angriffe beschäftigt, indem mittels Zusicherung von Bandbreite pro AS verhindert wird, dass bösartiger Traffic die Links auf dem Transportweg auslastet und so der reguläre Netzwerkverkehr behindert wird. Die Autoren des Papers stammen unter anderem von der ETH Zürich in der Schweiz und der Beihang Universität in China

- **ACM Conference on Computer and Communications Security (CCS)** [CCS17] - Eins der auf der CSS 2016 veröffentlichten Paper war *Identifying the Scan and Attack Infrastructures Behind Amplification DDoS Attacks* von Krupp u.a. [KBR16]. Es befasst sich mit der Umsetzung eines Systems aus Honeypots, welches die Infrastruktur bestehend aus Scannern und Angreifern hinter Amplification/Reflection-Attacken sichtbar macht. Das Paper wurde unter der Leitung von Prof. Dr. Christian Rossow an der Universität des Saarlandes geschrieben.

- **ACM Internet Measurement Conference (IMC)** [IMC18] - Das Paper von Lichtblau u.a. sowie *Millions of Targets Under Attack: a Macroscopic Characterization of the DoS Ecosystem* von Jonker u.a [Jon+17] wurde auf der IMC 2017 veröffentlicht. Es befasst sich mit dem Aufbau und der Auswirkung von DDoS-Angriffen. Die benötigten Informationen sind durch Honeypots und zusätzliche Datenquellen beschaffen worden. Dieses Paper ist ebenfalls teilweise an der Universität des Saarlandes geschrieben worden.

– **IEEE Conference on Communications and Network Security (CNS)** [CNS18] - Eines der Paper, das auf der CNS 2016 veröffentlicht wurde, war *A Moving Target Defense Approach to Mitigate DDoS Attacks against Proxy-Based Architectures* von Venkatesan u.a. [Ven+16]. Es befasst sich mit dem Schutz von auf Proxys basierenden DDoS-Abwehrsystemen und ist an der George Mason University und der University of Michigan in den USA entstanden.

Die IETF setzt sich hauptsächlich mit übertragungsspezifischen Themen, beispielsweise Spoofing oder dem Schutz der Transportnetze, auseinander. Die Arbeitsgruppe *DDoS Open Threat Signaling (DOTS)* beschäftigt sich beispielsweise mit der Entwicklung von Echtzeit-Signalisierenungs-Protokollen zur Übertragung von DDoS Informationen.

Auf der ACM IMC wird größtenteils über Messungen und weniger über direkte Gegenmaßnahmen publiziert. Die Veröffentlichungen im Rahmen der IEEE zielen auf konkrete Lösungen ab und setzen eher auf die Absicherung und Härtung der Systeme, um beispielsweise zu verhindern, dass diese nicht Teil eines Botnetzes werden.

5 Ausblick

Aus der bisherigen Recherche geht hervor, dass DDoS-Attacken ein aktuelles Thema sind. Das Aufkommen von mehr und mehr, leider häufig ungenügend abgesicherter, Internet of Things (IoT)-Geräten sorgt für stärker werdende Angriffe. Dies zeigte sich beispielsweise durch das Mirai-Botnetz, welches hauptsächlich aus IoT-Geräten bestand, die Aufgrund von schlechter oder nicht existierender Schutzmechanismen leicht zu übernehmen waren. Es verursachte unter anderem einen Angriff mit einem maximalen Durchsatz von 1.1 Tbps, welchem der betroffene französische Web- und Cloud-Hoster OVH nicht gewachsen war [Kol+17].

Die Tatsache, dass es noch keine Lösung oder Gegenmaßnahme zu DDoS-Attacken gibt und die daraus resultierende Aktualität des Themas, haben mich darin bestärkt, mich weiterhin mit diesem auseinanderzusetzen. Im Laufe des Semesters habe ich mir einen Überblick erarbeiteten können.

Mir ist bewusst geworden, dass es sich um ein sehr breites Themengebiet handelt, welches viele Überschneidungen mit anderen Bereichen beinhaltet: Aufbau von Botnetzen, Eigenschaften von Transportprotokollen, Anwendungssicherheit, Routing, Lastverteilungsmechanismen und Infrastruktur-Dienste wie NTP oder DNS spielen eine Rolle. Für die weiterführende Auseinandersetzung mit diesem Thema wird es für mich nötig sein, das Themengebiet weiter einzuschränken, um eine tiefere Auseinandersetzung zu ermöglichen.

Konkret möchte ich auf den vorgestellten Konzepten und der Arbeit von Franziska Lichtblau u. a. aufbauen und versuchen, diese in den Projekten, welche auf das Grundseminar folgen, zu erweitern. Um diese zu erproben, möchte ich mich mit Traffic-Echtzeitanalyse im Rahmen des X-Check Projekts [XCh17] auseinandersetzen.

Literatur

[A1018] A10networks.com. *A10 - At A10 we strive to protect our customers with best-in-class solutions and services needed to win the cyberwar.* 2018. URL: https://www.a10networks.com/.

[Arb18] Arbornetworks.com. *Arbor Networks - The Security Division of NETSCOUT.* 2018. URL: https://www.arbornetworks.com/.

[BS04] F. Baker und P. Savola. *Ingress Filtering for Multihomed Networks.* RFC 3704. IETF, März 2004.

[Bas+16] Cristina Basescu u. a. „SIBRA: Scalable Internet Bandwidth Reservation Architecture". In: *23rd Annual Network and Distributed System Security Symposium, NDSS 2016, San Diego, California, USA, February 21-24, 2016.* NDSS, 2016.

[BNI17] Karuna S. Bhosale, Maria Nenova und Georgi Iliev. „The distributed denial of service attacks (DDoS) prevention mechanisms on application layer". In: IEEE, Okt. 2017.

[CCS17] CCS-ACM. *ACM Conference on Computer and Communications Security (CCS).* 2017. URL: https://www.sigsac.org/ccs/CCS2017/.

[Clo18a] Cloudflare.com. *The High Orbit Ion Cannon Is A User-Friendly Tool To Launch Dos And DDoS Attacks Using HTTP Traffic.* 2018. URL: https://www.cloudflare.com/learning/ddos/ddos-attack-tools/low-orbit-ion-cannon-loic/.

[Clo18b] Cloudflare.com. *The Low Orbit Ion Cannon Is A User-Friendly Tool To Launch Dos and DDoS Attacks Using TCP, UDP, and HTTP Traffic.* 2018. URL: https://www.cloudflare.com/learning/ddos/ddos-attack-tools/low-orbit-ion-cannon-loic/.

[CNS18] CNS-IEEE. *IEEE Conference on Communications and Network Security (CNS).* 2018. URL: http://cns2018.ieee-cns.org/.

[Dis08] Dennis Distler. *Performing Egress Filtering.* 2008. URL: https://www.sans.org/reading-room/whitepapers/firewalls/performing-egress-filtering-32878.

[DYN16] DYN.com. *Dyn Statement on 10/21/2016 DDoS Attack.* 2016. URL: https://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/.

[FS00] P. Ferguson und D. Senie. *Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing.* RFC 2827. IETF, Mai 2000.

[Gli83] Virgil D. Gligor. „A Note on the Denial-of-Service Problem". In: *Proceedings of the 1983 IEEE Symposium on Security and Privacy, Oakland, California, USA, April 25-27, 1983.* IEEE, 1983, S. 139–149.

[IMC18] IMC-ACM. *ACM Internet Measurement Conference (IMC).* 2018. URL: http://www.sigcomm.org/events/imc-conference.

[Jon+17] M. Jonker u. a. „Millions of Targets Under Attack: a Macroscopic Characterization of the DoS Ecosystem". In: *Internet Measurement Conference (IMC).* ACM, Nov. 2017.

[Kam+17] Akshat Kambli u. a. „DDoS Information Sharing System“. In: ACM, 2017.

[Kol+17] Constantinos Kolias u. a. „DDoS in the IoT: Mirai and Other Botnets“. In: Bd. 50. 7. IEEE, 2017, S. 80–84.

[Kre16] Brian Krebs. *KrebsOnSecurity Hit With Record DDoS*. 2016. URL: https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/.

[KBR16] Johannes Krupp, Michael Backes und Christian Rossow. „Identifying the Scan and Attack Infrastructures Behind Amplification DDoS Attacks“. In: *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. CCS '16. Vienna, Austria: ACM, 2016, S. 1426–1437. ISBN: 978-1-4503-4139-4.

[Kum17] Chandan Kumar. *Top 7 DDoS Attack Protection Service for Better Security Top 7 DDoS Attack Protection Service for Better Security*. 2017. URL: https://geekflare.com/ddos-protection-service/.

[Lau+00] F. Lau u. a. „Distributed denial of service attacks“. In: IEEE, Okt. 2000.

[Lic+17] Franziska Lichtblau u. a. *Detection, Classification, and Analysis of Inter-Domain Traffic with Spoofed Source IP Addresses*. 2017.

[Luc+13] M. Luckie u. a. „AS Relationships, Customer Cones, and Validation“. In: *Internet Measurement Conference (IMC)*. ACM, Okt. 2013, S. 243–256.

[NDS18] NDSS-Symposium. *NDSS Symposium*. 2018. URL: https://www.ndss-symposium.org/.

[OCG17] M. Ozcelik, N. Chalabianloo und G. Gur. „Software-Defined Edge Defense Against IoT-Based DDoS“. In: *2017 IEEE International Conference on Computer and Information Technology (CIT)*. Bd. 00. IEEE, Aug. 2017, S. 308–313.

[Ven+16] Sridhar Venkatesan u. a. „A moving target defense approach to mitigate DDoS attacks against proxy-based architectures“. In: *2016 IEEE Conference on Communications and Network Security, CNS 2016, Philadelphia, PA, USA, October 17-19, 2016*. IEEE, 2016, S. 198–206.

[XCh17] X-Check. - *Detection of Security Incidents at Internet Exchange Points*. 2017. URL: http://x-check.realmv6.org/.

[ZJT13] Saman Taghavi Zargar, James Joshi und David Tipper. „A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks.“ In: *IEEE Communications Surveys and Tutorials* 15.4 (2013), S. 2046–2069.