Distributed DDoS Defense:A collaborative Approach at Internet Scale

Jessica Steinberger*†, Anna Sperotto†, Harald Baier*, Aiko Pras†

*da/sec - Biometrics and Internet Security Research Group
University of Applied Sciences Darmstadt
Darmstadt, Germany
Email:{Jessica.Steinberger, Harald.Baier}@h-da.de

†Design and Analysis of Communication Systems
University of Twente
Enschede, The Netherlands
Email:{A.Sperotto,A.Pras}@utwente.nl

***Abstract*—Distributed large-scale cyber attacks targeting the availability of computing and network resources still remain a serious threat. To limit the effects caused by those attacks and to provide a proactive defense, mitigation should move to the networks of Internet Service Providers (ISPs). In this context, this thesis focuses on a development of a collaborative, automated approach to mitigate the effects of Distributed Denial of Service (DDoS) attacks at Internet Scale. This thesis has the following contributions: i) a systematic and multifaceted study on mitigation of large-scale cyber attacks at ISPs. ii) A detailed guidance selecting an exchange format and protocol suitable to use to disseminate threat information. iii) To overcome the shortcomings of missing flow-based interoperability of current exchange formats, a development of the exchange format Flow-based Event Exchange Format (FLEX). iv) A communication process to facilitate the automated defense in response to ongoing network-based attacks, v) a model to select and perform a semi-automatic deployment of suitable response actions. vi) An investigation of the effectiveness of the defense techniques moving-target using Software Defined Networking (SDN) and their applicability in context of large-scale cyber attacks and the networks of ISPs. Finally, a trust model that determines a trust and a knowledge level of a security event to deploy semi-automated remediations and facilitate the dissemination of security event information using the exchange format FLEX in context of ISP networks.**

***Index Terms*—DDoS, Mitigation, Reaction, Dissemination, future attacks, attack intensities**

I. Introduction

Being originally described by J. C. R. Licklider of the Massachusetts Institute of Technology (MIT) in August 1962 [1], the Internet has evolved to a vital component that heavily influences our daily life. Large majorities of users rely on the Internet on a regular basis for financial services (e.g., online banking), shopping and other customer services (e.g., access health care information, governments communication, locate jobs, watch movies) [2]. Besides the communication and information aspect of the Internet, it has become a crucial component for millions of businesses, stock markets, public facilities and transportation hubs, power grids and water delivery systems that are controlled by networked devices [3]. The Internet Society defines Internet as a world-wide broadcasting capability, a mechanism for information dissemination, and a medium for collaboration and interaction between individuals and their computers without regard for geographic location [4]. This description primarily summarizes the benefits of the emerging technologies provided within the Internet. However, emerging technologies are also opening up new vulnerabilities that might be exploited by attackers to perform large-scale cyber attacks.

In recent years, large-scale cyber attacks targeting the availability of network infrastructure and service have been constantly reported [3], [5], [6]. These large-scale cyber attacks could lead to enormous financial loss [6], [7], potentially triggering sustained power outages over large portions of the electric grid [8] and prolonged disruptions in communications, food and water supplies, and health care delivery. An evolution of the attack intensities and related security events have been published in [9] and are shown in Figure 1.

One common characteristic of these attacks is that they are referred to as large-scale cyber attacks. According to the definition of the Tallinn Manual on the International Law Applicable to Cyber Warfare [10] large-scale cyber attacks involve many devices that connote a relationship with information technology and are distributed over a large geographic area.

The majority of these large-scale cyber attacks are using reflection and amplification techniques while performing an attack. First, reflection is used to make publicly available network devices send attack traffic to the attack target to hide the attacker's identity. Usually, the attacker sets the source IP address to the target IP address and thus makes use of spoofing. As a result, the attack target receives all response packets of the publicly available network device. Second, amplification is used to increase the network packet size to overwhelm the target network. Amplification exploits the fact that response packets usually are significantly larger than the initial request packet.

Besides the geographic distribution and the techniques used to strengthen the attack, the attacks are either based on the two most popular transport layer protocols: Transmission Control Protocol (TCP) or User Datagram Protocol (UDP). The majority of large-scale cyber attacks rely on UDP, because many UDP-based protocols are vulnerable to amplification due

978-1-7281-4973-8/20/$31.00

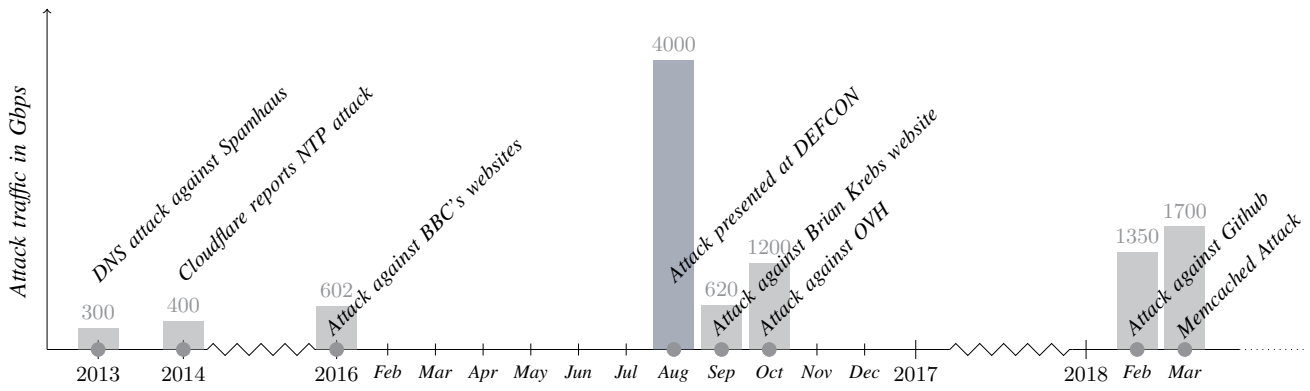

Fig. 1. DDoS evolution is partially based on [9], [11]–[13]

to the lack of verification of the participating communication partners [14] and thus support spoofing. Using UDP-based protocols, an attacker can achieve network traffic up to a factor of 4670 [15]. Even though TCP employs a three-way-handshake, it is also vulnerable for amplification as reported in [14], [16]. As reported in [17], the attacker can amplify TCP traffic by a factor of 20. Both, UDP and TCP-based attacks are volumetric attacks (floods) and are intended to reach bandwidth or connection limits of hosts or networking devices [18].

One type of large-scale cyber attacks are DDoS attacks that still remain the top concern responsible for network infrastructure and service outages [19]. The reason is that DDoS attacks are getting larger, more sophisticated (e.g. multi-vector attacks) and frequent as shown in Figure 1.

At the same time it has never been easier to execute DDoS attacks, e.g., Booter services offer paying customers without any technical knowledge the possibility to perform DDoS attacks as a service via a web page [20], [21]. Besides Booter services, it is also possible to hire a whole botnet (e.g., hire-a-botnet-services [22]) for a DDoS campaign at low price [23], [24]. Moreover, new technology trends in the development of the Internet such as Internet of Things (IoT) focus to connect billions of everyday devices. These devices are designed to be user-friendly and accessible and often do not have a stringent security standard. Currently, 4.9 billion IoT units are in use [25] and will reach 25 billion by 2020. However, the lack of missing security standards, the ease of manipulation and the amount of available everyday devices encourage attackers to perform large-scale DDoS attacks [26].

The well-known DDoS attacks that attracted large public attention are: (a) the "SpamHaus" attack in March 2013 where SpamHaus faced a DDoS attack targeting the Spamhaus's Domain Name System (DNS) servers with traffic peaks of 300 Gbps [12], [27], [28], (b) the "NTP" attack in february 2014 where the attacker only used 4 529 Network Time Protocol (NTP) servers running on 1 298 different networks to create an attack traffic of 400 Gbps [13], [29], (c) the attack targeting the web site of the journalist Brian Krebs in September 2016 with traffic peaks of 620 Gbps [11], [30] launched by 100 000 poorly secured IoT devices that have been compromised by the Mirai malware and (d) the OVH attack in September 2016 where the French Web hoster OVH faced a 1.1 Tbps DDoS attack. This attack was launched by a collection of hacked Internet-connected cameras and digital video recorders [31].

Considering the quantity of everyday devices connected to the Internet, their mobile speed and the trend of recent attack intensities, theoretically a devastating large-scale DDoS attack might be launched [32], [33]. To be prepared for future DDoS attacks, a new paradigm is required to mitigate their effects.

A. Research Goal and Research Questions

The main research goal of the thesis is to develop a collaborative, automated approach to mitigate the effects of DDoS attacks at Internet Scale. To achieve the research goal the following research question have been defined:

1) Is distributed and automatic mitigation at ISP level performed and if yes, how?
2) How are security events currently exchanged and do they satisfy the requirements of ISPs?
3) Is mitigation currently done in a proactive or reactive approach? If reactive, would it be possible to do it in a proactive approach?
4) Is mitigation currently done manually or automatically? If manually, would it be possible to perform mitigation in an automated way?
5) How can trust among collaborative partners be arranged?

B. Publications

This thesis is published in [34]. The motivation to the dissertation, the conceptual background of the research context and the use-case scenario have been published in [35]–[37]. The analysis to what extent countermeasures are set up and which mitigation approaches are adopted by ISPs and their own view on collaboration have been published in [38], [39]. A structured overview of exchange formats and protocols

used to share security event related information in context of intrusion detection and incident handling was published in [40]. Based on the results of this structured overview, the exchange format FLEX that was developed to overcome the shortcomings of missing flow-based interoperability was published in [41], [42]. Further, a communication process that facilitates the dissemination of threat information that are created in conjunction with widely adopted monitoring technologies e.g., NetFlow was presented and published in [43]. In addition, a process of selecting an appropriate response related to the identified network-based attack to initiate a suitable reaction was published in [37], [44]. The defense techniques Moving Target Defense (MTD) using SDN was presented and published in [45]. Finally, a trust model that determines a trust and a knowledge level of a security event to deploy semi-automated remediations and facilitate the dissemination of security event information using the exchange format FLEX in the context of ISPs was published in [46].

C. Awards

The publication [35] was awarded the prize for best student poster at the Trans-European Research and Education Networking Association (TERENA) Networking Conference (TNC2014) by Cisco Systems and the Internet Society. Further, this thesis [34] was awarded the price for the best PhD thesis at the Fachbereichstag Informatik (FBTI).

D. Contributions

The main contribution of this thesis is a systematic and multifaceted study on mitigation of large-scale cyber attacks at ISPs. By performing two surveys, we got in contact with experienced networking operators and thus gained insight into processes, structures and capabilities of ISPs to mitigate and respond to network-based attacks. Using the contact with experienced networking operators revealed potentials for improvement in their mitigation and response capabilities and it ensured that the distributed DDoS defense paradigm will be both fine-tuned and used by the intended audience. Based upon these finding, multiple aspects of a distributed DDoS defense at ISP networks were scrutinized and resulted in a multifaceted approach.

The first aspect of a distributed DDoS defense is the dissemination of threat information. We provided network operators a detailed guidance selecting an exchange format and protocol suitable to use in their network to disseminate threat information. To overcome the shortcomings of missing flow-based interoperability, we developed the exchange format FLEX.

The second aspect of distributed DDoS defense is the collaboration of ISP networks. To establish collaboration among ISP networks, a proactive and semi-automatic approach is needed and trust among collaborating partners is required.

In a first step, a communication process was developed to facilitate the automated defense in response to ongoing network-based attacks. This communication process supports the dissemination of threat information based on FLEX and helps organizations to speed up their mitigation and response capabilities without the need to modify the current network infrastructure. We demonstrated that our communication process supports achieving the situational awareness of the current threat landscape, pools expertise and resources at ISP networks, facilitates the automated defense in response to ongoing network-based attacks and thus lessens the time to respond.

In a second step, we analyze the initiation of a suitable reaction. This initiation is a process of selecting an appropriate response related to the identified network-based attack. The process of selecting a response requires to take into account the economics of an reaction e.g., risks and benefits. We provided a response selection model that allows to mitigate network-based attacks by incorporating an intuitive response selection process that evaluates negative and positive impacts associated with each countermeasure. In addition to the process of selecting an appropriate response, the semi-automatic deployment of response actions were analyzed. Therefore, we investigate the effectiveness of the defense techniques moving-target using SDN and their applicability in context of large-scale cyber attacks and the networks of ISPs.

Besides sharing threat information and the selection of an appropriate response to ongoing network-based attacks, establishing trust among collaborative partners is deemed of critical importance to semi-automatically deploy mitigation. Therefore, we developed a trust model that determines a trust and a knowledge level of a security event to deploy semi-automated remediations and facilitate the dissemination of security event information using the exchange format FLEX in context of ISP networks.

The contribution in this thesis can be used by network administrators, network operators and network security engineers to better limit the effects of current and future DDoS attacks and thus prevent network infrastructure and service outages.

II. Current DDoS Detection & Mitigation: A Survey

To achieve insight into real-world processes, structures and capabilities of IT companies and their computer networks and investigate how network operators detect, mitigate and respond to network-based attacks in practice, we set up a survey research according to the common procedures and standards for good practice of survey research described in [47], [48]. Thus, we performed a survey research on the basis of two surveys conducted in the year 2013 and 2015.

We collected empirical data about current detection and mitigation approaches. This data was provided by the expertise and experience of network administrators, network operators and network security engineers gathered through a cross-sectional and a repeated cross-sectional survey. Even though survey research remains most used in applied social research, this thesis relies on those well-known empirical methods to enrich the quality and fine-tune its research results to satisfy the requirements of ISP networks. The cross-sectional survey performed in the year 2013 determined the state of the art in attack detection and mitigation in ISP networks and resulted

in four main findings. These four main findings serve as a starting point of Research questions (RQs) 2 - 5. The repeated cross-sectional survey was conducted in the year 2015 with the main intention to add additional evidence to the findings of the first survey and re-evaluate the results of the first survey to ensure that our research results two years ago are still valid.

We found that current detection and mitigation approaches in ISP networks use flow-based data (e.g., NetFlow, Internet Protocol Flow Information Export (IPFIX)) and are performed primarily within single Autonomous Systems (ASs) and thus not distributed. Further, the survey revealed that in case of a large-scale cyber attack collaboration among partners is done on an ad-hoc-basis via telephone or email without the use of well-defined processes or standards for security managements (e.g., Information Technology Infrastructure Library (ITIL)). We recognized that automatic mitigation to limit the effects of an ongoing large-scale attack is not a requirement of ISPs, because ISPs are afraid that automatic mitigation systems gain increasing interest to be compromised and thus perform unwanted automatic actions within the network. However, ISPs prefer semi-automatic mitigation.

In order to achieve the overall research goal of this thesis, the survey provides the following 4 main findings:

a) Finding 1: Many exchange formats available but unknown: For ISPs to collaborate, a common data representation to describe security-related data is important. Further, an exchange protocol to transmit security events over network borders is also required. Even though, various exchange formats and protocols have been published in context of intrusion detection and incident management, it is still a challenge to find a standardized exchange format that is thoroughly validated and tested in full scale of industry trials. In addition, exchange formats and protocols are often unknown for ISPs.

b) Finding 2: Collaborative mitigation is done on an ad-hoc and reactive basis: To counteract large-scale network-based attacks, ISP networks have been identified as a key position within the Internet infrastructure. Even though collaboration of trusted partners and their exchange of threat information to mitigate and respond to a network-based attack is regarded as valuable, exchanging threat information is currently done on an ad-hoc basis via email or telephone. As a consequence, mitigation is only performed in case a large-scale network-based attack occurred and already caused effects within the network and thus can be described as reactive mitigation.

c) Finding 3: Mitigation is done manually: Although network-based attacks are getting larger, more frequent and sophisticated and thus the number of related security events increases, network operators often manually analyze and initiate possible countermeasures against ongoing network-based attacks to recover normal operations. Automatic mitigation and response systems to speed up mitigation and response capabilities within ISP networks are not widely deployed. Even though network operators are afraid that automatic mitigation systems gain increasing interest to be compromised, network operators prefer semi-automatic mitigation and would like to make use of it.

d) Finding 4: Collaboration requires the establishment of trust: Security event sharing is deemed of critical importance to counteract large-scale attacks at ISP networks. On the one hand, security event sharing is regarded to speed up organization's mitigation and response capabilities. On the other hand, it is currently done on an ad-hoc basis via email, member calls or in personal meetings only under the premise that participating partners are personally known to each other. As a consequence, mitigation and response actions are delayed and thus security events are not processed in time. However, collaboration of trusted partners to mitigate and respond to a network-based attack is regarded as valuable, but the personal knowledge of each sharing partner to develop trust to share security events does not scale very well.

We will now revisit each one of the RQs 2-5, which stem from the aforementioned findings.

III. Revising the Research Questions

To answer RQ 2, we reviewed 10 exchange formats and 7 exchange protocols used in context of intrusion detection and incident management. The security event exchange formats can be categorized into four groups: S-expressions, XML-based and MIMEMessage-based formats and syslog. The security event exchange protocols can be categorized into the two groups: Secured and unsecured. Our conclusion is that even though various exchange formats and protocols have been presented, it is still a challenge to find a standardized exchange format and protocol that is thoroughly validated and tested in full scale of industry trials. In addition, none of the exchange formats has been used in conjunction with flow-based data despite RQ 1 revealed that current detection and mitigation approaches in ISP networks rely on flow-based data.

To satisfy the requirement of flow-based interoperability of an ISP, we present the new exchange format FLEX. FLEX is suitable to carry data of flow export technologies (e.g. Cisco NetFlow, IPFIX) that are used to identify, track and mitigate malicious traffic. Further, FLEX is intended to facilitate the cooperation among network operators and focus on an automated threat information exchange. In addition, since FLEX messages are disseminated using Simple Mail Transfer Protocol (SMTP), FLEX is easy to deploy and it integrates with existing infrastructure.

To answer RQ 3, Section II revealed that current mitigation is done on an ad-hoc and reactive basis. To limit the effects of an ongoing large-scale cyber attack and to perform mitigation in a proactive approach, a communication process was introduced that supports an automated dissemination of threat information based on FLEX in context of ISPs. Further, this communication process supports achieving the situational awareness of the current threat landscape, pools expertise and resources and facilitates the automated defense. Even though some collaborating partners have not been actively involved in an ongoing attack, the communication process ensures that all collaborating partners are informed about the

effects of the attack. As a result, this communication process helps organizations to speed up their mitigation and response capabilities.

To answer RQ 4, we found in Section II that current mitigation is done manually. One approach to counteract the proliferation of network-based attacks is a generalized and automated process that initiates mitigation and response measures. Traditionally, automated mitigation and response processes make use of an Intrusion Response System (IRS) that provides a distinct response selection process, and is able to collaborate with other security appliances, such as firewalls to block and terminate suspicious traffic. However, available solutions proposed by the scientific community are not widely adopted. Further, each IRS uses different metrics to select an appropriate response and some of the metrics are only applicable for specific system environments. To mitigate network-based attacks by incorporating an intuitive response selection process, a new response selection model, called Response Effectiveness Assessment (REASSESS) was introduced that evaluates negative and positive impacts associated with each countermeasure and selects the most appropriate response action to limit the effects of an large-scale network-based attack.

We combined the defense techniques moving-target using SDN. This combination increases the attackers uncertainty due to an ever-changing attack surface. We found that the effects of a large-scale cyber attack can be significantly reduced using MTD and SDN.

To answer RQ 5, Section II revealed that collaboration requires the establishment of trust. Current collaborative approaches take place under the premise that participating partners are personally known to each other. As a consequence, mitigation and response actions are delayed and thus security events are not processed in time. Therefore, a trust model was presented that determines a trust and a knowledge level of a security event to deploy semi-automated remediations and facilitate the dissemination of security event information using the exchange format FLEX in the context collaborating ISPs. This trust model is scalable and helps to build a trust community to share sensitive information about threats and its remediation suggestions.

IV. Conclusion

The key terms in the thesis research goal were *collaboration* and *automation*. However, our research revealed that collaboration among ISPs is often not performed for three reasons. First, ISPs regard themselves as competitors in the same market segment. Second, at the time the research was started, ISPs did not see themselves responsible to perform attack detection and mitigation as they did not see financial incentives for themselves. Removing attack traffic reduces the overall network traffic in an ISP network, while ISPs are payed based on the amount of transferred traffic [49], [50]. Third, the results from our surveys showed that only a minority of ISPs adhere to established IT processes, security standards and frameworks (e.g., ITIL, Control Objectives for Information and Related Technology (COBIT), ISO/IEC 27000), even though being compliant to security standards and frameworks is known to enhance security and ensures reproducible workflow outputs.

The absence of security standard compliance of ISPs also contradicts the establishment of automated processes to detect and mitigate DDoS attacks. Moreover, the results of our surveys show that ISPs fear to face a huge amount of false positive alarms or to deploy a new attack target within their own network infrastructure and services in case of an automated detection and mitigation approach. As a result, ISPs are afraid to lose control over their own network infrastructure and services.

Nevertheless, we consider ISPs to be key points for DDoS attack detection and mitigation. Therefore, the main contribution of this thesis is to leverage synergies and opportunities arising from the combination of the key terms to mitigate the effects of DDoS attacks at Internet scale.

Acknowledgment

This work was partly supported by the German Federal Ministry of Education and Research (BMBF) under grant number 16BY1201F (iAID), 03FH005PB2 (INSAIN) and the Center for Advanced Security Research Darmstadt (CASED), the Hessen State Ministry for Higher Education, Research and the Arts (HMWK) within the Center of Research in Security and Privacy (CRISP) and the Hessen Agentur GmbH under grant number 473/15-15 (ROBUST). In addition it was funded by FLAMINGO, a Network of Excellence project (318488) supported by the European Commission under its Seventh Framework Programme and by the Netherlands Organisation for Scientific Research (NWO) Distributed Denial-of-Service Defense: Protecting Schools and other public organizations (D3) Project.

References

[1] Internet Hall of Fame®, "Internet Hall of Frame Pioneer - J.C.R. Licklider," Website, 2016. [Online]. Available: https://www.internethalloffame.org/inductees/jcr-licklider

[2] National Telecommunications and Information Administration and Economics and Statistics Administration, "Exploring the Digital Nation: America's Emerging Online Experience," Website, 2013. [Online]. Available: https://www.ntia.doc.gov/files/ntia/publications/exploring_the_digital_nation_-_americas_emerging_online_experience.pdf

[3] C. Baylon and D. Livingstone, "Cyber Security at Civil Nuclear Facilities: Understanding the Risks," Website, 2015. [Online]. Available: https://www.chathamhouse.org/publication/cyber-security-civil-nuclear-facilities-understanding-risks

[4] B. M. Leiner, V. G. Cerf, D. D. Clark, R. E. Kahn, L. Kleinrock, D. C. Lynch, J. Postel, L. G. Roberts, and S. Wolff, "Brief History of the Internet," Website, 2012. [Online]. Available: http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet

[5] S. Greengard, "The war against botnets," *Commun. ACM*, vol. 55, no. 2, pp. 16–18, 2 2012.

[6] Z. Whittaker, "Sony takes $15M hit after North Korea cyberattack," Website, 2015. [Online]. Available: http://www.zdnet.com/article/sony-hack-cost-it-15-million-so-far/

[7] Verizon Enterprise, "2015 Data Breach Investigations Report," Website, 2015. [Online]. Available: http://www.verizonenterprise.com/DBIR/2015/pdf.xml

[8] C. Q. Choi, "Nuclear Cybersecurity Woefully Inadequate," Website, 2015. [Online]. Available: http://spectrum.ieee.org/energywise/telecom/security/nuclear-cybersecurity-woefully-inadequate

[9] F. J. Ryba, M. Orlinski, M. Wählisch, C. Rossow, and T. C. Schmidt, "Amplification and drdos attack defense - a survey and new perspectives," *CoRR*, 2015. [Online]. Available: http://arxiv.org/abs/1505.07892

[10] Michael N. Schmitt, "Tallinn Manual on the International Law Applicable to Cyber Warfare," Website, 2013. [Online]. Available: https://ccdcoe.org/tallinn-manual.html

[11] B. Krebs, "Krebsonsecurity hit with record ddos," Website, 2016. [Online]. Available: https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/

[12] M. Prince, "The DDoS That Knocked Spamhaus Offline (And How We Mitigated It)," Website, 2013. [Online]. Available: https://blog.cloudflare.com/the-ddos-that-knocked-spamhaus-offline-and-ho/

[13] ——, "Technical Details Behind a 400Gbps NTP Amplification DDoS Attack," Website, 2014. [Online]. Available: https://blog.cloudflare.com/technical-details-behind-a-400gbps-ntp-amplification-ddos-attack/

[14] M. Kührer, "Large-scale analysis of network-based threats and potential countermeasures," Ph.D. dissertation, Ruhr University Bochum, 2016. [Online]. Available: http://nbn-resolving.de/urn:nbn:de:hbz:294-45217

[15] C. Rossow, "Amplification Hell: Revisiting Network Protocols for DDoS Abuse," in *Proceedings of the 2014 Network and Distributed System Security (NDSS) Symposium*, 2 2014. [Online]. Available: http://www.internetsociety.org/doc/amplification-hell-revisiting-network-protocols-ddos-abuse

[16] M. Kührer, T. Hupperich, C. Rossow, and T. Holz, "Hell of a handshake: Abusing tcp for reflective amplification ddos attacks," in *Proceedings of the 8th USENIX Workshop on Offensive Technologies (WOOT 14)*. San Diego, CA: USENIX Association, 8 2014. [Online]. Available: https://www.usenix.org/conference/woot14/workshop-program/presentation/kuhrer

[17] ——, "Exit from hell? reducing the impact of amplification ddos attacks," in *Proceedings of the 23rd USENIX Security Symposium (USENIX Security 14)*. San Diego, CA: USENIX Association, 2014, pp. 111–125. [Online]. Available: https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/kuhrer

[18] US-CERT of the Department of Homeland Security, "DDoS Quick Guide," Website, 2014. [Online]. Available: https://www.us-cert.gov/security-publications/DDoS-Quick-Guide

[19] D. Anstee, P. Bowen, C. Chui, and G. Sockrider, "Worldwide infrastructure security report," Arbor Networks Inc., Tech. Rep. XI, 1 2015. [Online]. Available: http://www.arbornetworks.com/resources/annual-security-report

[20] J. J. Santanna, R. van Rijswijk-Deij, R. Hofstede, A. Sperotto, M. Wierbosch, L. Zambenedetti Granville, and A. Pras, "Booters - An analysis of DDoS-as-a-service attacks," in *Proceedings of the 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM)*, 5 2015, pp. 243–251.

[21] Hacker's List, "Hacker's List," Website, 2015. [Online]. Available: https://hackerslist.com/

[22] T. Gallo, "Renting a zombie farm: Botnets and the hacker economy," Website, 2014. [Online]. Available: http://www.symantec.com/connect/blogs/renting-zombie-farm-botnets-and-hacker-economy

[23] P. Paganini, "Finding Hacking Services and More in the Deep Web," Website, 2015. [Online]. Available: http://darkmatters.norsecorp.com/2015/06/16/finding-hacking-services-and-more-in-the-deep-web/

[24] M. Goncharov, "Russian Underground 101," Website, 2012. [Online]. Available: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf

[25] J. Rivera and R. van der Meulen, "Gartner Says 4.9 Billion Connected "Things" Will Be in Use in 2015," Website, 2014. [Online]. Available: http://www.gartner.com/newsroom/id/2905717

[26] M. Majkowski, "Mobile Ad Networks as DDoS Vectors: A Case Study," Website, 2015. [Online]. Available: https://blog.cloudflare.com/mobile-ad-networks-as-ddos-vectors

[27] Q. Jenkins, "Answers about recent DDoS attack on Spamhaus," Website, 2013. [Online]. Available: https://www.spamhaus.org/news/article/695/answers-about-recent-ddos-attack-on-spamhaus

[28] M. Prince, "The DDoS That Almost Broke the Internet," Website, 2013. [Online]. Available: https://blog.cloudflare.com/the-ddos-that-almost-broke-the-internet/

[29] J. Graham-Cumming, "Understanding and mitigating NTP-based DDoS attacks," Website, 2014. [Online]. Available: https://blog.cloudflare.com/understanding-and-mitigating-ntp-based-ddos-attacks/

[30] S. Hilton, "Dyn Analysis Summary Of Friday October 21 Attack," Website, 2016. [Online]. Available: http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/

[31] D. Goodin, "Record-breaking ddos reportedly delivered by ¿145k hacked cameras," Website, 2016. [Online]. Available: https://arstechnica.com/information-technology/2016/09/botnet-of-145k-cameras-reportedly-deliver-internets-biggest-ddos-ever/

[32] A. Pras, J. J. Santanna, J. Steinberger, and A. Sperotto, *DDoS 3.0 - How Terrorists Bring Down the Internet*. Cham: Springer International Publishing, 11 2016, pp. 1–4. [Online]. Available: http://dx.doi.org/10.1007/978-3-319-31559-1_1

[33] L. Young, "Attacking Network Infrastructure to Generate a 4 Tb's DDoS for $5," Website, 2016. [Online]. Available: https://www.defcon.org/html/defcon-24/dc-24-speakers.html#Young

[34] J. Steinberger, "Distributed ddos defense: A collaborative approach at internet scale," Ph.D. dissertation, University of Twente, 2018, **Best PhD Thesis Award**. [Online]. Available: https://research.utwente.nl/files/52663811/Dissertation_JSteinberger.pdf

[35] J. Steinberger, A. Sperotto, H. Baier, and A. Pras, "Real-time DDoS Defense: A collaborative Approach at Internet Scale," Website, 5 2014, **Best Student Poster**. [Online]. Available: https://tnc2014.terena.org/core/poster/21

[36] J. Steinberger, A. Sperotto, A. Pras, and H. Baier, "Real-time DDoS Defense: A collaborative Approach at Internet Scale," in *Proceedings of the 10th SPRING of the SIG Security - Intrusion Detection and Response of the German Informatics Society SIG SIDAR*, 7 2015. [Online]. Available: http://www.gi-fg-sidar.de/spring/SIDAR-Reports/SIDAR-Report-SR-2015-01.pdf

[37] J. Steinberger, J. J. Santanna, E. Spatharas, H. Amler, N. Breuer, K. Graul, B. Kuhnert, U. Piontek, A. Sperotto, H. Baier, and A. Pras, ""Ludo" - Kids playing Distributed Denial of Service," in *Proceedings of the TNC16*, K. Wierenga, Ed. GÉANT Ltd, 11 2016. [Online]. Available: http://www.terena.org/publications/tnc16-proceedings/

[38] J. Steinberger, L. Schehlmann, S. Abt, and H. Baier, "Anomaly detection and mitigation at internet scale: A survey," in *Proceedings of the 7th IFIP International Conference on Autonomous Infrastructure, Management and Security (AIMS 2013): Emerging Management Mechanisms for the Future Internet*, ser. Lecture Notes in Computer Science, G. Doyen, M. Waldburger, P. Čeleda, A. Sperotto, and B. Stiller, Eds. Springer Berlin Heidelberg, 2013, vol. 7943, pp. 49–60. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-38998-6_7

[39] J. Steinberger, A. Sperotto, H. Baier, and A. Pras, "Collaborative Attack Mitigation and Response: A survey," in *Proceedings of the 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM 2015)*, 5 2015.

[40] J. Steinberger, A. Sperotto, M. Golling, and H. Baier, "How to exchange security events? overview and evaluation of formats and protocols," in *Proceedings of the 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM)*, 5 2015, pp. 261–269.

[41] J. Steinberger, A. Sperotto, H. Baier, and A. Pras, "Exchanging Security Events of flow-based Intrusion Detection Systems at Internet Scale," Website, 6 2015. [Online]. Available: https://www.iab.org/wp-content/IAB-uploads/2015/04/CARIS_2015_submission_3.pdf

[42] J. Steinberger, "FLEX," Website, 7 2015. [Online]. Available: https://datatracker.ietf.org/meeting/93/materials/agenda-93-mile/

[43] J. Steinberger, B. Kuhnert, A. Sperotto, H. Baier, and A. Pras, "Collaborative DDoS Defense using Flow-based Security Event Information," in *Proceedings of the 2016 IEEE/IFIP Network Operations and Management Symposium (NOMS 2016)*, 4 2016.

[44] S. Ossenbühl, J. Steinberger, and H. Baier, "Towards automated incident handling: How to select an appropriate response against a network-based attack?" in *Proceedings of the Ninth International Conference on IT Security Incident Management IT Forensics (IMF)*, 5 2015, pp. 51–67.

[45] J. Steinberger, B. Kuhnert, C. Dietz, L. Ball, A. Sperotto, H. Baier, A. Pras, and G. Dreo, "DDoS Defense using MTD and SDN," in *Proceedings of the 2018 IEEE/IFIP Network Operations and Management Symposium (NOMS 2018)*, 5 2018.

[46] J. Steinberger, B. Kuhnert, A. Sperotto, H. Baier, and A. Pras, *In Whom Do We Trust - Sharing Security Events*. Cham: Springer International Publishing, 2016, pp. 111–124. [Online]. Available: http://dx.doi.org/10.1007/978-3-319-39814-3_11

[47] F. J. Fowler, *Survey Research Methods*, 5th ed. London: Sage Publications, 2013.

[48] L. M. Rea and R. A. Parker, *Designing and Conducting Survey Research - A Comprehensive Guide*, 4th ed. New York: John Wiley & Sons, 2014.

[49] I. Cloudflare, "The Relative Cost of Bandwidth Around the World," Website, 2014. [Online]. Available: https://blog.cloudflare.com/the-relative-cost-of-bandwidth-around-the-world/

[50] T. Scholl, "Internet routing and traffic engineering," Website, 2014. [Online]. Available: https://aws.amazon.com/de/blogs/architecture/internet-routing-and-traffic-engineering/