Towards Remediating DDoS Attacks

Arturs Lavrenovs
NATO CCDCOE, Tallinn, Estonia
Arturs.Lavrenovs@ccdcoe.org

DOI: 10.34190/IWS.21.046

Abstract: The Internet infrastructure has been struggling with distributed denial-of-service (DDoS) attacks for more than two decades. This paper reviews aspects of current remediation strategies for reflected amplified DDoS attacks and identifies elements that are insufficiently researched which might be hindering remediation efforts. It identifies additional actors who should be playing a role in these efforts and reviews their incentives and motivation. The issue has long been whether it is possible to remediate abused protocols faster than the protocols get deprecated while devices using them remain functional until the end of their life. It now appears that it is. The Memcache protocol attack capacity was only 319 Mbps in May 2020 but it was 1.7 Tbps only two years previously. Thus it can be considered fully remediated. The paper examines why this was a successful remediation effort and whether it could be applied to other commonly abused protocols by using the reflector capacity measurement methodology. In contrast, the long-term abused DNS protocol has not seen a significant drop in capacity, which is lingering around 27.5 Tbps.

Keywords: DDoS attacks, DDoS attack capacity, DDoS attack remediation, reflectors, amplifiers

1. Introduction

The first DDoS network attack was two decades ago and was soon followed by reflected amplified DDoS attacks that have been plaguing the Internet ever since. Although the number of reflectors observed by scanning projects has been steadily decreasing, the attack capacity is ever-growing and is setting new records. A reasonable observer would assume that our technological society is capable of solving this long-known technical challenge, and perhaps wonder why we have not.

This paper discusses only reflected amplified DDoS attacks and while the attackers' desired effect for the victims is the same and may be common across different types of attack, the remediation strategies differ widely. Compromised devices participating in a botnet and causing direct attacks attract more attention from law enforcement agencies, Internet service providers (ISP), and industry.

The twofold problem of the ability to spoof source IP addresses in the network and a large number of reflectors is the root cause of the issue. An attacker capable of renting or compromising a host connected to a mismanaged network can use the available upload bandwidth by sending packets with the spoofed IP address of the victim to publicly-reachable network services, which in return respond directly to the victim usually with a larger packet size. The current remediation strategy is the proliferation of network configuration, ensuring that only packets with legitimate source IP addresses enter the Internet from individual networks (BCP 38, BCP 84) and removing reflectors. Both the percentage of networks that are spoofable and the number of reflectors per commonly-abused protocols have decreased, which indicates that the remediation strategy is working, at least to some extent, while the DDoS attacks are breaking capacity records.

Addressing the DDoS problem in 2020 has become more important than ever. The global pandemic almost instantly shifted the whole education system and jobs that can be done online to the home. Accessing different remote systems has become a necessity for all those affected. DDoS attacks against many organisations could previously have had only a limited negative effect and reputational damage and the daily operations of employees and students could continue in person or via locally accessible systems. Now the attack can stop all work and education for remote users relying on the targeted system. This has become a reality; DDoS attacks against an e-learning platform by a single high school student disrupted access to online classes for a week for 170,000 users (Freed, 2020). What could be the worldwide economical impact if a new record-breaking DDoS attack targets the largest online collaboration tools?

2. Related work

DDoS is a widely researched topic. It primarily follows a typical pattern of new technology emerging, such as SDN, blockchain, AI, and researchers applying it to the DDoS problem but usually when the attack has already reached the victim. The root cause of the issue is twofold: the ability to spoof the source IP addresses and a large number of reflectors on the Internet. Researchers tend to focus on these aspects. The Center for Applied Internet Data Analysis is running a long-term project known *the Spoofer* to assess and monitor networks that allow the injection of packets with spoofed IP addresses (Beverly and Bauer, 2005). The notification efforts are tracked and provide a correlation between sent notifications and remediation, thus having a positive effect on network security, especially in the case of reflected DDoS attacks (Luckie et al., 2019). There have been attempts to filter spoofed packets by technical means without remediating the mismanaged networks (Jin et al., 2003; Mirkovic et al., 2017) but while those might demonstrate high efficiency in a simulated setting, this approach has not seen widespread adoption.

Reflector research is quantitative. It revolves around scanning the Internet for a specific port and protocol abusable for reflection. It is conducted when a protocol starts being abused (Czyz et al., 2014) or is being investigated for the possibility of future abuse (Rossow, 2014). Usually, this type of research does not investigate what the abused devices are, or their contribution to the attack capacity. Most focuses on dealing with the consequences instead of understanding and addressing the root causes. Osterweil et al. (2020a, 2020b) explored the state of affairs of DDoS attacks and recognised that fundamental changes and more research are needed to tackle the issue while relying fully on the peak attack capacities reported by mitigation services providers.

Global DDoS attack capacity estimation can identify which of the abused protocols contribute the most (Leverett and Kaplan, 2017) and which regions are at highest risk (CyberGreen Institute, 2020) and a proposed measuring methodology (Lavrenovs, 2019) enables identification of the most and least contributing hosts, networks and regions. Synthetic measurements of reflector performance in a laboratory setting (Vasques and Gondim, 2019; Gondim et al., 2020), although important for furthering the understanding of global capacity, cannot cover the whole range of devices and network conditions on the Internet.

3. Actors and motivation

Understanding some of the actors on the Internet landscape can provide clues as to why we are struggling with remediation efforts. Ordinary users merely want to access remote services offered by organisations. Malicious actors range widely in their capabilities and motivations but ultimately seek to prevent users from accessing targeted services. Most of the published research focuses on these types of actors, but there are others who either contribute to the problem or can contribute to the remediation.

3.1 ISPs and transit service providers

Many of the transit service providers and some of the ISP and data centres cannot filter out large application-layer DDoS attacks. The motivation for this type of actor is to provide network services to all their clients while maintaining customer satisfaction and fulfilling service level agreements. If the attack size is not affecting other clients, it might get passed on to the victim. The victim may or may not have the means to deal with the attack. If it is large enough to affect other clients, then the transit providers have to mitigate it, and often the only means to do that is to employ blackholing as remote from the victim in network topology as possible (King et al., 2016). As the attacked service loses connectivity, the attack can be considered successful.

ISPs are externalising the cost of having open reflectors on their networks. From their perspective, there might be no drawbacks even in network bandwidth consumption. Networks that focus on specific customer segments, such as residential or data centres usually have unbalanced network bandwidth consumption and thus unused capacity. When reflectors in a residential ISP network are generating amplified responses, they consume this unused upload capacity. As long as this consumption is relatively small and does not affect other clients or the network routers, there are no-ill effects for the ISP and therefore no incentive to fix the problem.

The targets of the DDoS attacks are often commercial services hosted in data centres and this imbalance enables reception of attack download bandwidth without any additional expense to the extent of reserve capacity. If the free capacity is sufficient and the network has an appropriate filtering solution, the attack can be mitigated. The larger the data centre is, the more free capacity its network might have meaning larger attacks could be filtered out. Some of the largest data centres in the world do offer DDoS filtering at little or no cost and can handle most of the attacks. Smaller data centres and ISPs can be overwhelmed by a single attack.

If an ISP has balanced bandwidth either by offering services to both bandwidth-generating and -consuming clients or by selling unused capacity as a transit, it can have financial incentives and thus motivation to keep wasted bandwidth to a minimum. Technical solutions or network monitoring and management can significantly reduce wasted bandwidth for the ISP.

No legislation specifically targets the negligence of having open reflectors present on the networks, and even if a DDoS attack from a specific set of reflectors caused provable damage, the liability could be shifted to the end-client hosting these reflectors. Overall, a significant number of ISPs that host open reflectors have no motivation to address this issue.

3.2 Mitigation service providers

DDoS mitigation services often attract the largest attacks on the Internet. These service providers might exclusively offer DDoS filtering or accompany it with CDN or other network services. The business model is straightforward; acquire ingress bandwidth capacity that exceeds the largest expected attacks and deploy a filtering solution that can drop the attack traffic while forwarding the legitimate packets to the client.

Whenever a new protocol is abused or a new attack size record is broken, these providers publish a technical report. These reports are the most referenced sources for DDoS capacity and largest attacks in academia, industry, and media, making them excellent sources of free worldwide marketing.

As long as expected attack capacity and future growth are manageable and no record-breaking attacks happen, these providers are in a safe market position. They have the most technical insights into the current situation and what needs to be addressed first. However, remediating it is not in their interest as they will lose competitive advantage or even their entire business model.

3.3 Device manufacturers

Often overlooked is that a large number of reflectors are not essential public services but rather residential and business devices with default configurations connected to the Internet. The problem is exacerbated by the class of devices that have router functionality with separate internal and external network interfaces. Services on the internal interface might be required, but they are not contributing to the open reflector problem while services on the external interface could contain open reflectors but generally are not needed for functionality required by users.

Residential device manufacturers often seek to make their products as cheap as possible and this is sometimes achieved by cutting corners; software quality and security have been first to suffer. If a device is compromised because the default configuration control panel exposed to the Internet and default credentials or a vulnerability in the software were exploitable, then it may at the very least become part of the botnet. Users of these devices might not even notice, or they might wonder why the CAPTCHAs have become more frequent or why the Internet sometimes slows down. In more extreme cases, the user’s information could be stolen or further exploitation conducted to take over other devices on the network. If mass exploitation of a manufacturer’s devices with tangible consequences for the users occurs, it will attract bad publicity. Manufacturers are thus incentivised to minimise such occurrences and fix them so they do not recur. A large number of devices operating as open reflectors do not harm customers directly, but the reputational damage will motivate the manufacturer to address the issue.

3.4 Policymakers and legislatures

In all developed countries, causing a DDoS attack already falls under some criminal ordinance. Malicious actors responsible for reflected DDoS attacks are the hardest to identify. The global nature of the Internet and DDoS attacks could mean a single attack against a company registered in one jurisdiction could be affecting services physically hosted in one or more other jurisdictions and caused by an attacker located in another who uses spoofing and reflectors located in any number of other jurisdictions. While charging criminals and affecting international law is a challenge, legislatures and regulators seek to improve their citizens’ lives and should be encouraged to remediate DDoS attacks.

4. Remediating DDoS attacks

The most visible remediation efforts scan for open reflectors targeting the source networks and notify network administrators. Other simple solutions might also be available.

4.1 Notifying network administrators

Much academic and industry research has focused on conducting scans for known abused services reachable on the Internet and notifying network or abuse contacts. If the network is properly managed, these notices are forwarded to the end client and maybe the client is even assisted with solving the issue. Perhaps the network has specific terms of service that mandate clients to limit or block their reflectors. Poorly managed networks do not even forward these notices. While running reflector honeypots, we have encountered a large number of forwarded notices on some of the well-managed networks, but their effectiveness might be limited.

The number of reflectors for long-abused protocols seems to be decreasing, but it is unclear the role that notification efforts have played. There is no research into this, and thus no reliable assertion can be made. An alternative explanation is that devices that are abusable are present on the Internet until the end of their lifetime or until network configuration changes and the effect is completely detached from any remediation efforts.

The repetitive nature of the notification e-mails combined with the lack of any perceived value for the networks makes its effectiveness questionable. Providing an estimate of potentially wasted bandwidth capacity calculated for each network can offer at least some perceived value. Measuring the effect of this remediation approach is not easy, but a detailed report hidden by tracked link and capacity changes in the specific network over time against the baseline could provide insights into its effectiveness.

4.2 ISPs and net neutrality

Although net neutrality has been a hot topic for several years, there are widespread precedents of it being violated in some protocols for the benefit of ISPs. While DPI and traffic shaping in residential and mobile networks have been widely investigated, the lesser-known and measured practice of ISPs and data centres blocking or limiting specific ports has not. Most commonly, it targets e-mail sending ports and blocks them by default with an opt-out ability, rate-limiting or filtering system. Why client perception differs between these two cases is open for debate; it could be that an opt-out feature is viewed as sufficient choice.

Spam was a problem even before reflected DDoS attacks became a norm. As it directly affects the productivity and safety of the users and businesses, various mitigation approaches have been developed, primarily spam filtering and blacklisting compromised hosts. However, spam filtering is not 100% precise and neither is blocking individual IP addresses of compromised hosts. If the network administrator does not take action against a spamming host, the same will happen with other spam-sending hosts on the same network. Blacklisting the whole network or decreasing its reputation seems a reasonable step to protect users and as individual blacklist management is time-consuming, global blacklists are used by many e-mail services.

If ISPs wish to offer clients the ability to directly send e-mails that are not rejected or classified as spam by most receivers, they have to keep themselves off the blacklist. Whenever an abusive host appears on the network, swift action has to be taken to stop spamming by limiting network connectivity or asking the client to solve the issue. Otherwise, clients cannot send e-mails and thus ISP can only have clients that do not need that functionality. Most ISPs elect to deal with the spam issue to avoid being added to the blacklists.

Some ISPs externalise the costs of poor network management practices and have no incentive to act otherwise. They might be susceptible to persuasion to improve the management of their networks using the blacklisting approach that is used to fight spam but that would depend on the cost of being added to the blacklist. There are already other blacklists besides the spam ones. Usually, they consist of individual hosts (or small subnets) whose behaviour is deemed malicious, such as spreading malware, aggressive scanning, probing services, or brute-forcing credentials. These blacklists are often deployed by governmental or other organisations striving for more security. Surprisingly, this might not penalise the ISP at all as non-abusive clients might not experience any limitations. Combined with the fact that reflectors are not malicious and blacklisting them is pointless, this approach seems unsuitable as a mitigation strategy.

The offences discussed above could decrease the overall reputation of the network. Greylisting the whole ISP based on its reputation can be effective as it affects many clients. A few hosts brute-forcing credentials might force websites that rely on network reputation to require all ISP clients to always solve a CAPTCHA. Credit card transactions or other activity might be delayed for manual processing or fail by default as labelled potentially fraudulent. Client satisfaction could drop and they could look for another ISP which would provide a financial incentive. Relying on the same greylists could be done for networks that allow spoofed IP packets and only if it could be proven that the spoofing was actively happening.

We might need a new type of greylist for DDoS reputation and a way to penalise ISPs. The penalty should be relevant to the DDoS issue; for example, the same CAPTCHA that many DDoS mitigation services employ could penalise a network known to allow spoofed packets or which contains a disproportionately high number of open reflectors.

Whenever there is a discussion requiring third parties to implement a new regulation, there is always a question of cost. It happens with ISPs whenever national governments require expensive DPI or data retention systems. Basic solutions for both blocking packets addressed to reflectors and IP address spoofing are simple and cheap. Blocking all packets coming from the Internet addressed to a few known abused ports is trivial and cost-free for an ISP on existing equipment. The only incurred cost is in managing or providing self-service functionality for clients to opt-out.

4.3 Devices and regulation

Open reflectors running on consumer devices is something we can start addressing now. The California state legislature has passed an act (State of California, 2018) requiring connected devices to have basic security measures to protect consumers. While this does not directly affect the consumer, there is no reason why this type of legislation could not improve overall security on the Internet by requiring external interfaces to not provide any unneeded services by default. If this regulation in at least one large market is introduced rationally, it would be more cost-effective for manufacturers of those devices to supply the same secure version to all markets.

While a legislature could also require ISPs to offer a basic firewall with an opt-out feature, it would not have as large an effect in other jurisdictions. As patching of consumer devices is done rarely, the old ones might continue contributing reflector capacity until end-of-life without ISP regulation.

To start addressing the issue from the device perspective, we need to understand which device classes and manufacturers contribute the most to the capacity. Then, the most prominent manufacturers can be addressed directly and this knowledge can be presented to legislatures to justify actions. Only if national legislation has proven to be effective is it justifiable to lobby for international laws and regulations.

5. Measuring DDoS attack capacity

Understanding DDoS attack capacity is necessary for developing and validating more efficient remediation strategies and it is one piece of information that current DDoS research is lacking. We have used the proposed methodology (Lavrenovs, 2019) to measure two very dissimilar abused protocols: Memcache and DNS.

5.1 Memcache

Memcache has been the record holder for DDoS attack size since 2018 with a reported observed attack capacity of 1.7 Tbps (Morales, 2018). We measured its attack capacity to be only 319 Mbps in May 2020, contributed by only 12 reflectors which could have been aggressive honeypots. The measuring methodology allows the exclusion of insignificantly contributing hosts from the calculation. Therefore, the protocol can be considered fully mitigated and likely will not see a resurgence. Because of how capacity is understood, decision-makers and the public could wrongly assume that the currently most referenced number in terms of capacity is relevant. For how long this protocol and attack size has been wrongly considered a major concern?

How fast was this protocol remediated? The same way as the peak attack is observed in a specific network and point in time a singular measurement is no different. The solution is to have a system continuously measuring attack capacity for each actively abused protocol where newly abused protocol monitoring could be added quickly.

This protocol is a noteworthy case not only because of the record attack size but also because of the fast remediation and deployment differences. Most of the long-term abused protocols are present on low-power consumer devices reachable on the Internet. Memcache was generally deployed in the enterprise environment where each host could have gigabit on 10-gigabit connectivity. The protocol is providing high-performance service, meaning the software was not a bottleneck either. Each reflector could fill the available bandwidth capacity, negatively affecting its primary functionality which could then be detected by the administrators. Notification efforts could also reach responsible administrators that have the incentive and capability to act upon it. As this protocol affected mitigation service providers, they actively participated in remediation efforts (Majkowski, 2018).

5.2 DNS

DNS remediation differs significantly. It was one of the first protocols abused in the wild for reflected amplified DDoS attacks and to this day remains unremediated. In May 2020, the DNS protocol global capacity was measured to be 27.5 Tbps (80% required minimum response rate, 1 Gbps per country minimum capacity; see Figure 1). This type of presentation is common for capacity estimation providing more detailed information than pure open reflector counts. It identifies China and the USA as the largest capacity contributors followed by developing and developed countries with high speeds of Internet connectivity.

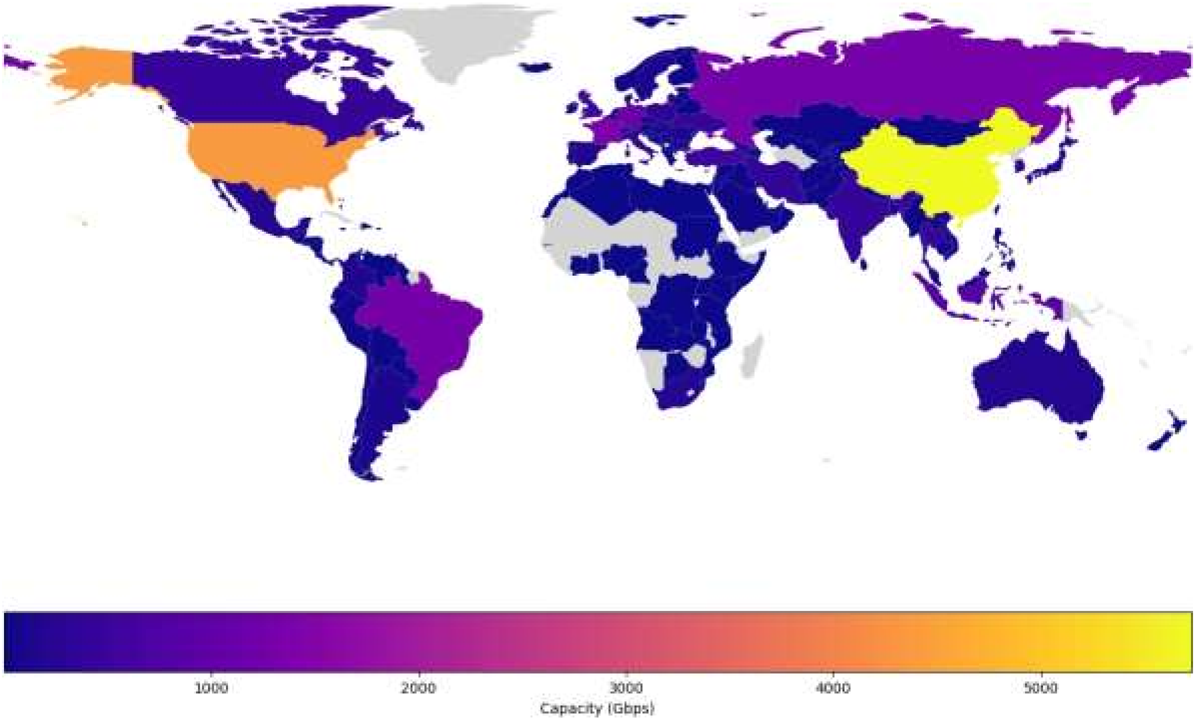

Figure 1: DNS attack capacity per country

This figure corresponds closely to our 2018 August measurement of 37.6 Tbps. While this might seem like a significant decrease, network churn, positioning of measurement points in the network topology and lack of established methodology for addressing measurement errors must all be considered. Even if we assume the measurements are comparable and have insignificant measurement errors, the change over time is low relative to the fully mitigated Memcache.

According to Cloudflare, the top two networks sending reflected Memcache packets were OVH and Digital Ocean, both of which conducted remediation work (Majkowski, 2018), possibly network firewalling the reflectors or making direct contact with clients. These networks are still major contributors to DNS protocol abuse with 1.4 Tbps and 200 Gbps of measured DNS reflection capacity respectively. They provide data centre and hosting services and should value their outgoing bandwidth capacity while understanding the effect as they are prime targets for the attacks themselves. This suggests that the type of ISP where the reflectors reside is not the determining factor in the remediation outcome, or not the only one. The reason for the remediation outcome difference may be a combination of factors – low reflector count, high connection bandwidth or, for Memcache, positioning in non-residential networks. This could significantly incentivise some actors, but there is currently no empirical evidence to support the theory.

6. Results and discussion

We know two root causes enabling reflected DDoS attacks and the appropriate technical remediation – eliminate open reflectors or IP spoofing, or both. However, we cannot implement these measures universally and instantly. Quantitatively, the remediation works on both fronts but is hampered by ever-increasing bandwidth capacity. We need to improve the remediation strategy, starting with adjustments requiring minimal effort and encountering no resistance to produce an incremental positive effect. We reviewed some additional actors (ISPs, device manufacturers, and legislatures) that should be part of the remediation strategy but lack incentives and thus motivation. The block for all of them is a lack of understanding of attack capacity and therefore the ability to measure improvements and estimate the effectiveness of any new measures taken. Mitigation service providers have monopolised this knowledge and have disincentives to improve the situation. We have confirmed through capacity measurements that full remediation is possible for a highly abused protocol (Memcache) within a reasonable timeframe which has not been observed before for other protocols. In contrast, DNS remediation has been stagnating from the capacity perspective over the last two years.

We have raised many issues that can be addressed with comprehensive research into the root causes of DDoS attacks instead of their effects. Capacity research and understanding is key to measuring the effectiveness of remediation efforts and validating proposed and possible future remediation strategies. We need to measure the capacity contributions of specific ISPs and device manufacturers to include this with the notification efforts and measure the impact of these efforts. We also need to justify any legislative efforts with reliable and independent data.

References

Beverly, R. and Bauer, S. (2005) The Spoofer project: Inferring the extent of source address filtering on the Internet, in *Usenix Sruti*, pp. 53–59.

CyberGreen Institute (2020) 'Cyber Health Statistics'. URL https://stats.cybergreen.net/ (accessed 9.19.2020).

Czyz, J. *et al.* (2014) Taming the 800 pound gorilla: The rise and decline of NTP DDoS attacks, in *Proceedings of the 2014 Conference on Internet Measurement Conference*. ACM, pp. 435–448.

Freed, B. (2020) *Miami high schooler charged in DDoS attacks against district*. URL https://edscoop.com/miami-dade-schools-ddos-attack-student-charged/ (accessed 4.9.2020).

Gondim, J. J. C., de Oliveira Albuquerque, R. and Orozco, A. L. S. (2020) Mirror saturation in amplified reflection Distributed Denial of Service: A case of study using SNMP, SSDP, NTP and DNS protocols, *Future Generation Computer Systems*.

Jin, C., Wang, H. and Shin, K. G. (2003) Hop-count filtering: an effective defense against spoofed DDoS traffic, in *Proceedings of the 10th ACM conference on Computer and communications security*. ACM, pp. 30–41.

King, T. *et al.* (2016) *BLACKHOLE Community*. RFC7999. RFC Editor, p. RFC7999.

Lavrenovs, A. (2019) Towards Measuring Global DDoS Attack Capacity, in *2019 11th International Conference on Cyber Conflict (CyCon). 2019 11th International Conference on Cyber Conflict (CyCon)*, Tallinn, Estonia: IEEE, pp. 1–15.

Leverett, E. and Kaplan, A. (2017) Towards estimating the untapped potential: a global malicious DDoS mean capacity estimate, *Journal of Cyber Policy*, 2(2), pp. 195–208.

Luckie, M. *et al.* (2019) Network Hygiene, Incentives, and Regulation: Deployment of Source Address Validation in the Internet, in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. *CCS '19: 2019 ACM SIGSAC Conference on Computer and Communications Security*, London United Kingdom: ACM, pp. 465–480.

Majkowski, M. (2018) *Memcrashed - Major amplification attacks from UDP port 11211, Cloudflare*. URL https://blog.cloudflare.com/memcrashed-major-amplification-attacks-from-port-11211/ (accessed 3.3.2018).

Mirkovic, J., Kline, E. and Reiher, P. (2017) RESECT: Self-Learning Traffic Filters for IP Spoofing Defense, in *Proceedings of the 33rd Annual Computer Security Applications Conference*. ACM, pp. 474–485.

Morales, C. (2018) *NETSCOUT Arbor Confirms 1.7 Tbps DDoS Attack; The Terabit Attack Era Is Upon Us*. URL https://asert.arbornetworks.com/netscout-arbor-confirms-1-7-tbps-ddos-attack-terabit-attack-era-upon-us/ (accessed 3.9.2018).

Osterweil, E., Stavrou, A. and Zhang, L. (2020a) 21 Years of Distributed Denial-of Service: Current State of Affairs, *Computer*, 53(7), pp. 88–92.

Osterweil, E., Stavrou, A. and Zhang, L. (2020b) 21 Years of Distributed Denial-of-Service: A Call to Action, *Computer*, 53(8), pp. 94–99.

Rossow, C. (2014) Amplification Hell: Revisiting Network Protocols for DDoS Abuse, in *Proceedings of the 2014 Network and Distributed System Security Symposium*. San Diego, CA, USA: Internet Society.

State of California (2018) *SB-327 Information privacy: connected devices.*

Vasques, A. T. and Gondim, J. J. C. (2019) Amplified Reflection DDoS Attacks over IoT Mirrors: A Saturation Analysis, in *2019 Workshop on Communication Networks and Power Systems (WCNPS). 2019 Workshop on Communication Networks and Power Systems (WCNPS)*, Brasilia, Brazil: IEEE, pp. 1–6.