Hell of a Handshake: Abusing TCP for Reflective Amplification DDoS Attacks

Marc Kührer, Thomas Hupperich, Christian Rossow, Thorsten Holz
Horst Görtz Institute for IT-Security, Ruhr-University Bochum, Germany

Abstract

Nowadays, a common way for attackers to perform *Distributed Denial-of-Service* (DDoS) attacks is via so called *amplification attacks*. The basic idea is to send relatively small requests with spoofed source address to public hosts (e.g., NTP servers), which reflect significantly larger responses to the victim of the attack. Recent studies focused on UDP-based attacks and analyzed the attack surface in detail. First results also suggested that TCP-based protocols are in principle vulnerable to such attacks, despite the three-way-handshake mechanism.

In this paper, we continue this line of work and demonstrate that TCP protocols indeed can be abused in practice. More specifically, we show that the handshake itself often yields amplification, especially since a lot of devices on the Internet react in unforeseen ways during the connection establishment. To estimate the landscape of Internet devices vulnerable to TCP amplification attacks, we performed Internet-wide scans for common TCP-based protocols and identified thousands of amplifiers that allow an amplification of factor 50x and higher.

1 Introduction

Different kinds of *Distributed Denial-of-Service* (DDoS) attacks are known for a long time [1, 2, 11]. As a consequence, multiple countermeasures were proposed (e.g., [4, 5, 7, 9, 12]) that reduce the impact of traditional DDoS attacks such as *TCP SYN* and *UDP flooding*. Recently, miscreants elevated their DDoS attacks to attack bandwidth of up to 400 Gbps by switching to so called *amplification attacks*, in which vulnerable (typically UDP-based) protocols are abused to amplify the attack traffic by a factor of up to 4,670 [10]. In such an amplification attack, the attacker sends relatively small requests with spoofed source address to so called *amplifiers*—often public hosts offering services such as DNS or NTP—that *reflect* [8] considerably larger responses to the attack victim, exhausting the capacity of the victim's network. As UDP lacks any verification of the communication partners by design, many UDP protocols are vulnerable to such reflection attacks.

On the contrary, TCP-based protocols employ a three-way-handshake, in which the two communication partners are validated by interchanging three sequential, equally-sized TCP packets before the actual payload data is transmitted. As we assume the end hosts to randomly select the initial sequence numbers, the handshake thus cannot be completed by sending TCP segments with spoofed source addresses. More specifically, when a spoofed `SYN` packet is sent to an end host, only a single `SYN/ACK` or `RST` segment should be reflected to the victim's network.

As a consequence, TCP thus should not permit traffic amplification. In prior work, we have shown that TCP can in general be abused for amplification attacks [6]. In that work, we enumerated the `SYN/ACK` responses upon sending a single `SYN` packet to HTTP and Telnet hosts and revealed hundreds of thousands of systems (mostly business and consumer routing devices) that repeatedly sent up to 20 `SYN/ACK` packets in response.

In this paper, we extend this work and consider the general threat of TCP-based amplification attacks. More specifically, we do not limit our focus on the obvious threat of `SYN/ACK` retransmissions, but rather dissect all kinds of unexpected responses received upon sending a single `SYN` packet. We performed scans in the entire IPv4 address space for common TCP-based protocols. Inspecting the response traffic revealed that there are other, more severe amplification vulnerabilities than the `SYN/ACK` retransmissions studied before. In fact, we identified hosts that respond with an excessive number of `RST` packets and others that transmit actual payload data via `PSH` packets—even before the three-way-handshake has completed. In total, our scans exposed more than 4.8 million devices vulnerable to an average amplification factor of 112x. However, we also identified thousands of hosts that can be abused for amplification up to a factor of almost 80,000x, respectively, reflect more than 5,000 packets within 60 seconds, causing a serious impact on a victim's network. Leveraging fine-granular fingerprint techniques, we assigned thousands of vulnerable devices to various manufacturers and device models, showing a high diversity in the landscape of TCP-based amplifiers.

To summarize, our contributions are as follows:

- We performed scans in the entire IPv4 address space for common TCP-based protocols to identify hosts vulnerable to reflective amplification attacks.
- We classified the amplifiers into categories based on the monitored network traffic and determined the number of hosts, the average amplification factor, and the packet frequency for each category.
- We applied protocol-specific fingerprinting to obtain as much information as possible about the amplifiers, showing a high diversity in the landscape of vulnerable systems.
- Lastly, we evaluated potential countermeasures to mitigate TCP-based amplification attacks.

2 Related Work

Our work is based on the analysis of UDP-based amplification attacks [10]. Rossow identified 14 network protocols with amplification vectors and gave an overview of potential countermeasures. TCP-based amplification attacks are not tackled in this work, though.

We continued this line of research and enumerated the number of potential amplifiers for TCP- and UDP-based protocols [6]. Inter alia, we focused on HTTP and Telnet hosts that repeatedly transmit `SYN/ACK` packets, allowing an amplification factor of up to 20. In this work, we thoroughly analyze the TCP responses and identify further TCP vulnerabilities such as payload exchange prior the handshake or aggressive `RST` segment storms.

Paxson [8] labeled end hosts that respond to arbitrary TCP packets with `SYN/ACK` or `RST` segments as *reflectors*, which can be abused for spoofing attacks. In such an attack, a high number of spoofed TCP packets are transmitted to a large number of reflectors, which in turn forward the responses to a target host in the victim's network. While this attack reflects TCP traffic to the victim, no amplification is achieved. An attacker thus is required to generate an enormous number of spoofed packets to achieve a high impact on the victim's network.

3 TCP Handshake Amplification

Our goal is to quantify the threat landscape of devices vulnerable to TCP handshake amplification attacks. In this section, we explain our experimental TCP scanning setup and the results in terms of amplification. The general methodology is similar to our previous work on this topic [6] and we refer to that paper for further details.

3.1 Amplifier Magnitude

We determine the number of Internet devices that are vulnerable to TCP handshake amplification in a two-step approach. First, we performed sampled TCP scans in IPv4 on 20 million randomly chosen hosts (about 0.5% of the IPv4 address space) for a set of widely distributed protocols. We then dissected the received network traffic to identify and enumerate the hosts that are vulnerable (i.e., in our context, hosts that reflect and amplify network traffic). Second, based on the number of estimated amplifiers from the sampled scans, we performed scans in the entire IPv4 address space for the most popular TCP-based protocols.

Scanning Setup. We use the same scanning tool that we developed for our previous work on this topic [6]. In the following, we briefly recap the scanning setup. The scanner employs a linear feedback shift register that generates a pseudo-random permutation of the IPv4 address space, thus limits the number of packets a network receives within a short time span, as suggested by Durumeric et al. [3]. We also distributed a scan of one protocol over 14 hours to refrain from aggressive scanning.

For every protocol, the scanner sends a single `SYN` packet to each target host (i.e., either 20 million random hosts or all addresses in the IPv4 address space) while we record the corresponding responses. Note that we do not complete a TCP handshake with valid `ACK` segments.

We further do not reply with `RST` packets, i.e., we do not cancel a connection when receiving `SYN/ACK` segments. This simulates the same situation as if a victim suffers from network overload and thus cannot reply with `RST` segments. Similarly, an attacker might target unassigned IP addresses in the victim's network so that also no `RST` packets are generated to cancel the connections.

Results. We scanned 20 million random IP addresses for 13 common TCP-based protocols. To enumerate the hosts that transmit payload data before the three-way-handshake is finished, we mainly focused on protocols, in which a server sends payload data first once the handshake is completed (e.g., banner information). When analyzing the received network traffic, we only considered hosts that amplify our `SYN` packet by a factor > 20, whereas the amplification factor is defined by the number of layer-2 bytes sent by an amplifier divided by the size of our initial `SYN` packet of 54 bytes. The factor thus also takes into account the TCP, IP, and Ethernet headers.

Table 1 shows the number of vulnerable hosts that we identified in the sampled scans. We found the highest number of amplifiers for FTP and Telnet, while most of the other protocols had a few amplifiers at all. We considered protocols for an Internet-wide scan if we estimated to find at least 5,000 amplifiers in the entire IPv4 space (i.e., FTP, HTTP, NetBIOS, SIP, SSH, and Telnet).

Table 1: Number of potential amplifiers with an amplification factor > 20 based on scans of 20 million hosts

	20 million random hosts			Estimation (IPv4)
Protocol	# Responsive	# Amplifiers	Amplifier Ratio	# Amplifiers
FTP	705,371	13,701	1 : 51	2,945,715
HTTP	715,354	1,746	1 : 409	375,390
IMAP	683,567	9	1 : 75,951	1,935
IPP	702,590	19	1 : 36,978	4,085
IRC	648,688	7	1 : 92,669	1,505
MySQL	672,336	8	1 : 84,042	1,720
NetBIOS	517,482	44	1 : 11,760	9,460
NNTP	667,598	8	1 : 83,449	1,720
POP3	689,716	7	1 : 98,530	1,505
SIP	711,210	87	1 : 8,174	18,705
SMTP	674,815	12	1 : 56,234	2,580
SSH	657,916	384	1 : 1,713	82,560
Telnet	575,067	9,315	1 : 61	2,002,725

Table 2: Number of potential amplifiers per protocol based on scans in the entire IPv4 address space

		# Amplifiers with amplification factor					
Protocol	# Responsive	> 20	> 50	> 100	> 500	$> 1,000$	$> 2,500$
FTP	152,026,322	2,913,353	3,500	1,868	1,032	937	847
HTTP	149,521,309	427,370	15,426	6,687	1,596	649	347
NetBIOS	82,706,193	12,244	2,449	1,463	873	811	783
SIP	154,030,015	22,830	5,158	3,913	3,289	3,123	2,889
SSH	141,858,473	87,715	4,611	2,141	1,275	1,176	1,082
Telnet	126,133,112	2,120,175	16,469	7,147	2,008	1,393	994

Table 2 illustrates the results obtained for the Internet-wide scans. For FTP and Telnet, we find almost 2% of the responsive hosts to be vulnerable for amplification higher than 20x. That is, the number of bytes received from the amplifiers (including packet headers of Ethernet, IP, and TCP) is more than 20 times higher than the size of the SYN packet that we sent. The number of amplifiers drops rapidly for higher amplification rates. At an amplification factor of $> 2,500$, though, attackers can still abuse almost 2,900 hosts—using the SIP protocol.

Table 3 outlines the intersection between the protocols relative to the overall number of vulnerable hosts for the protocols stated in the first table column. We observe the largest overlap for NetBIOS and SIP: more than 50% of the NetBIOS amplifiers can also be abused using SIP. The share between HTTP and FTP, respectively, Telnet ranges from a 1/4 to 1/3. In total, we find 4.8 million distinct IP addresses of amplifiers for the six protocols.

3.2 Amplification Type

In face of this problem's impact, we need to ascertain what TCP implementation artifacts cause such high amplification rates. In general, we would expect to see either a single RST packet upon our SYN segment when a port is closed or a SYN/ACK packet when a service is listening for connections and the second step of the handshake is completed. SYN/ACK segments, however, might

Table 3: Intersection of potential amplifiers

	Intersection (in %)					
Protocol	*FTP*	*HTTP*	*NetBIOS*	*SIP*	*SSH*	*Telnet*
FTP	-	4.5	0.1	0.2	0.6	19.2
HTTP	30.8	-	0.6	1.1	4.3	26.7
NetBIOS	20.9	21.9	-	53.8	14.7	22.5
SIP	21.9	21.4	28.9	-	22.5	26.0
SSH	19.8	21.1	2.1	5.9	-	21.0
Telnet	26.3	5.4	0.1	0.3	0.9	-

Table 4: Number of vulnerable hosts and average amplification factor (AF) per protocol and amplification type

	SYN/ACK		PSH		RST	
Protocol	# Ampl.	AF	# Ampl.	AF	# Ampl.	AF
FTP	2,907,279	22x	274	103x	5,577	53,927x
HTTP	421,487	60x	241	147x	3,411	432x
NetBIOS	8,863	54x	64	71x	3,087	78,042x
SIP	16,496	1,596x	2	696x	6,306	32,411x
SSH	81,256	80x	391	57x	5,889	29,705x
Telnet	2,112,706	28x	2,353	3,272x	4,242	79,625x

be retransmitted multiple times until i) an ACK segment is received, ii) a threshold is met and the half-open connection is terminated by the initial recipient, or iii) the connection attempt is aborted by the initial sender (e.g., by transmitting a RST segment).

Motivated by the fact that the observed behavior diverged from our initial assumption for thousands of hosts, we analyzed the recorded network packets in more detail. In particular, we studied the distribution of TCP flags and identified three main categories of flags that caused most of the amplification. We identified amplifiers that i) aggressively retransmit SYN/ACK packets, or ii) transmit payload data via PSH packets even though the three-way-handshake is never actually completed, or iii) send many RST segments to refuse our connection attempt. Table 4 outlines the number of hosts per amplification type and the average amplification factor.

SYN/ACK: The majority of amplifiers cause amplification by repeatedly retransmitting SYN/ACK packets upon our SYN segments. This attack type amplifies traffic up to 80x on average, and for SIP even up to 1,596x.

PSH: The number of amplifiers that transmit payload data via PSH (without a completed handshake) is low for most protocols. Nevertheless, the amplification factor is higher compared to the SYN/ACK amplifiers.

RST: The by far highest amplification is observed for hosts that transmit a tremendous number of RST segments. As such, an attacker could abuse the 4,242 vulnerable Telnet hosts to achieve an average amplification rate of 79,625x. Compared to SYN/ACK, the RST amplifiers of most protocols also have a much higher traffic volume—even though the number of hosts is significantly lower. That is, the 8,863 SYN/ACK amplifiers of

Table 5: Number of packets transmitted by the amplifiers within 10, 30, and 60 seconds after the first response

	SYN/ACK			PSH			RST		
Protocol	< 10	< 30	< 60	< 10	< 30	< 60	< 10	< 30	< 60
FTP	2	5	10	5	10	14	561	1,584	3,055
HTTP	2	6	11	5	10	16	140	224	264
NetBIOS	8	17	22	5	6	8	976	2,748	5,291
SIP	2	6	12	1	1	1	562	1,360	2,497
SSH	3	6	11	6	9	10	595	1,394	2,523
Telnet	2	5	10	52	154	277	996	2,345	4,254

NetBIOS transmitted about 25 MB of traffic, while the RST amplifiers caused traffic of more than 12 GB. Similarly, even though we observed most of the FTP amplifiers sending SYN/ACK packets (causing a total of 3.2 GB of traffic), the RST amplifiers transferred 15.1 GB of traffic in the same amount of time, a multitude of factor 5x.

Unknown: Note that we could not assign 3,763 hosts (less than 0.1% of the identified amplifiers) to one of the main amplification types, as these devices replied with seemingly arbitrary TCP flags. More specifically, we identified 1,841, respectively, 712 amplifiers repeatedly transmitting ACK segments for HTTP and Telnet that caused amplification from factor 265x to 405x. The number of unclassified hosts, however, is negligible compared to the overall number of amplifiers.

Packet Frequency. A high amplification factor is important to achieving a high impact on a victim's network. However, the impact is also affected by the number of packets that reach the target host simultaneously. We thus also determine the initial packet frequency for the different types of TCP-based amplifiers. More specifically, we measure the number of packets that were transmitted by each amplifier within 10, 30, and 60 seconds after observing the first response from the host. As illustrated in Table 5, the average number of packets reflected by SYN/ACK amplifiers within the first 60 seconds is rather low for all protocols. We suspect the majority of hosts to implement common delays to distribute the retransmission of SYN/ACK packets over time.

The PSH amplifiers draw a similar picture—with a single exception for Telnet. The Telnet PSH amplifiers send 52 packets on average within the first 10 seconds. Within 60 seconds, almost 280 packets are transmitted per amplifier, causing a significant impact on the target host.

We observe completely different results for the RST amplifiers. For most protocols, we find the RST amplifiers to transmit more than 500 packets within the first 10 seconds and up to 5,300 packets (NetBIOS) in the first 60 seconds. Considering that we found 3,087 NetBIOS amplifiers with an average amplification factor of 78,042x, this poses a serious threat to the Internet community.

Real-world TCP-based attacks. We also determine whether the identified amplifiers can be abused for real-world DDoS attacks, in which an attacker would repeatedly send spoofed SYN packets to the amplifiers to flood the victim's network with reflected traffic. That is, we create a subset of 100,000 randomly chosen SYN/ACK amplifiers and all PSH and RST amplifiers we found to be vulnerable for the Telnet protocol and send a single, respectively, 5 and 10 SYN packets to each of the individual hosts using different source ports for all SYN packets. Our analysis is based on all responses that arrive up to 60 seconds after sending the last SYN segment. In total, we find up to 62,736 SYN/ACK, 2,203 PSH, and 1,593 RST amplifiers responding to our SYN segments (the remaining hosts presumably went offline in the mean-time).

For SYN/ACK, we find an almost negligible increase in the attack volume. More specifically, the SYN/ACK amplifiers transmitted 34.2 MB of traffic when sending a single SYN segment. Transmitting 5 SYN segments resulted in traffic of 55.1 MB, while 10 SYN segments caused 76.0 MB of traffic, an increase of factor 2.2x.

We observe completely different results for the hosts vulnerable to PSH amplification. That is, we received 11.2 MB of network data when sending a single SYN segment, while 110.8 MB of traffic was transmitted when sending ten SYN segments, a multitude of factor 10x.

We find similar results for the RST amplifiers. Of the 1,593 responding RST amplifiers, we find 1,391 hosts to amplify a single SYN packet by a factor of 1,250x within 60 seconds, causing network traffic of 89.6 MB. We find a rise of traffic volume by factor 4.4x when sending five SYN packets (resulting in 392.4 MB of reflected traffic) and observe another rise of factor 2x in the attack volume for 10 SYN packets. More specifically, within 60 seconds after sending the last SYN segment, we recorded 789.2 MB of network traffic.

We thus conclude that SYN/ACK amplifiers are not suitable to be used in large-scale amplification attacks. PSH and RST amplifiers, in contrast, can indeed be abused when repeatedly sending SYN segments to exhaust the capacity of a victim's network with reflected traffic.

3.3 Amplifier Classification

After determining the amplification factor and packet frequency of each amplification type, we try to shed light onto the types of systems that permit amplification via the TCP protocol. More specifically, we request information via the protocols FTP, HTTP, HTTPS, SSH, and Telnet from each previously identified amplifier to leverage details in protocol banners and payload fragments. Based on the returned payload, we applied 1,873 regular expressions we already utilized in previous work [6], respectively, manually compiled 279 additional regular ex-

Table 6: Device fingerprinting results of the identified TCP-based amplifiers

	Hardware (in %)							Operating System (in %)								
Protocol	Router	Embedded	Printer	Camera	DVR	Others	Unknown	Unix	Linux	Solaris	Windows	ZyNOS	Cisco IOS	SmartWare	Others	Unknown
FTP	83.5	15.5	0.0	0.1	0.1	0.8	0.0	3.3	15.3	0.0	0.0	64.8	0.0	0.0	0.2	16.4
HTTP	48.8	44.5	0.9	0.5	0.9	0.3	4.1	1.1	24.8	0.1	0.4	63.8	0.2	0.1	0.4	9.1
NetBIOS	25.3	35.1	12.8	4.7	2.6	3.2	16.3	5.0	31.4	0.0	2.9	21.5	0.5	0.0	4.7	34.0
SIP	14.4	74.2	0.2	1.8	1.0	1.0	7.4	2.7	64.0	0.0	1.2	16.6	4.3	0.1	1.7	9.4
SSH	10.1	77.3	0.0	0.3	0.4	1.2	10.7	7.1	36.5	3.0	0.7	1.3	4.8	12.9	4.7	29.0
Telnet	93.3	3.8	0.2	0.2	0.4	0.6	1.5	8.7	0.3	0.0	0.0	85.4	0.1	1.0	0.4	4.1

pressions to perform fine-granular device fingerprinting, i.e., a classification into two categories: the underlying hardware (e.g., routers, cameras, or printers) and the OS.

Results. Table 6 illustrates the fingerprinting results obtained for all enumerated amplifiers. Note that the category *Router* also covers similar devices such as gateways, switches, and modems. Further, the category *Embedded* includes various kinds of embedded systems such as *serial to LAN* devices.

In general, we observed many routing devices. Particularly for FTP and Telnet, most of the vulnerable devices are consumer routers running Linux or ZyNOS, an OS that is distributed on ZyXEL devices. We further find 996 (12.9%) of the SSH amplifiers use SmartWare, which is running on SmartNode VoIP gateways. Besides a high number of routing devices and embedded systems, we identified miscellaneous types of printers and surveillance cameras. We also observed a surprisingly wide distribution of devices running the NetBIOS protocol.

When looking at the hosts of specific amplification types, we find a diversity of devices for `RST` amplifiers such as routers, camera systems, and DVRs of various manufacturers. We thus cannot determine a specific device or vendor that causes the high amplification rates.

However, we find the `SYN/ACK` amplifiers for the SIP protocol to be specific Wireless ADSL2 VoIP devices manufactured by ZyXEL. Further, the majority of Telnet `PSH` amplifiers can be assigned to SmartNode VoIP gateways transmitting a specific message each second. A minority of `PSH` amplifiers was found to be a specific routing device of Avocent Cyclades, while we also observed several printing servers transmitting actual payload data before completing the TCP handshake. As part of responsible disclosure, we have notified the vendors about these protocol implementation deficiencies.

In general, though, we found the fingerprints to show a high diversity of devices and manufacturers, thus the TCP amplification vulnerabilities are not caused by a single manufacturer and represent a generic attack vector.

3.4 Countermeasures

After classifying the individual amplifiers, we discuss potential countermeasures to either mitigate or completely stop TCP-based amplification attacks.

As previously stated, we do not reply with TCP `RST` packets during our scans, thus potential amplifiers will not refrain from continuously retransmitting packets. To evaluate the impact of `RST`, we repeated the Internet-wide scan for the FTP protocol with `RST` transmission enabled. We clearly observed a large diversity between the numbers of amplifiers. While the number of `SYN/ACK` amplifiers dropped to 2,222 hosts (a decrease of 99.9%), we still monitored 5,187 amplifiers distributing a large number of `RST` packets (a decline of 7.0%), resulting in an average amplification of 19,149x. Further on, the number of hosts that amplify traffic of factor > 50x remains stable compared to the results in Table 2.

In an attempt to also stop the remaining hosts from distributing large amounts of packets, we evaluated the effects of specific types of network packets on the behavior of the amplifiers. More specifically, we sent a single `SYN` packet to each remaining amplifier and replied with a predefined message upon received packets. In particular, we responded with TCP `ACK`, `PSH`, or `FIN` segments to eventually trigger specific behavior that stops the hosts from amplifying the initial `SYN` packet. We further replied with ICMP `host prohibited` and ICMP `port/host/protocol unreachable` messages.

We obtained responses from about 3,500 amplifiers upon our `SYN` packets (the remaining hosts presumably went offline) and observed the highest decrease of amplifiers when transmitting ICMP `port unreachable` messages. That is, we merely found 742 hosts (21.2% of the responsive hosts) to still amplify traffic. For the remaining TCP and ICMP messages, we found in-between 1,218 (TCP `ACK`) and 1,728 (ICMP `host prohibited`) hosts to still transmit an excessive number of packets. We thus conclude that particularly TCP `RST` and ICMP `port unreachable` messages help to mitigate the attack traffic, however, are not a general solution to remediate the root causes for TCP-based amplification vulnerabilities.

3.5 TCP- and UDP-based Amplifiers

The majority of vulnerable UDP-based protocols amplify the number of UDP payload bytes from 3.8x (NetBIOS) to 556.9x (NTP `monlist`) on average [10]. When intentionally selecting the most responsive 10% of the amplifiers an attacker could achieve an amplification factor up to 4,670x for NTP `monlist` requests while the amplification remains in-between 4.9x (NetBIOS) and 98.3x (DNS) for the other dissected UDP protocols. However, in terms of actual bandwidth amplification (including Ethernet, IP, and UDP headers), the amplification factor is actually significantly lower, e.g., less than 1,000x in the worst case of NTP `monlist` amplifiers. On the contrary, many common TCP-based protocols allow much higher bandwidth amplification. Particularly for `RST`, we identified thousands of vulnerable hosts that amplify a single `SYN` packet by a factor of up to 79,625x, causing a serious impact on a victim's network.

From the viewpoint of an attacker, also the number of amplifiers is important to scale up the overall attack bandwidth. For UDP, approximately 2.8 million NetBIOS amplifiers, 30.5 million DNS amplifiers, and 87,463 NTP `monlist` amplifiers could be found [6]. Especially the huge number of DNS amplifiers can cause a considerably higher impact (about 10x compared to an attack using FTP) than any TCP protocol in Table 4. Further, the number of TCP-based amplifiers that can cause serious impact on a victim's network is rather low, particularly for `RST`. An attacker thus has to scan a high number of hosts in the IPv4 address space to find the most effective amplifiers. It is thus likely that attackers currently stick to vulnerable UDP protocols to perform large-scale amplification attacks. However, TCP-based attacks are attractive for attackers who only have little bandwidth available and want to amplify it as much as possible. Similarly, TCP traffic is considerably harder to block or filter at the network edges than protocols like the UDP-based NTP—this holds especially for widely distributed protocols such as HTTP or FTP. Distinguishing legitimate and harmful TCP packets requires DDoS defense appliances to keep state of TCP connections, and simple port-based filtering techniques cannot be applied to most networks, as these would also block benign communication. Moreover, in contrast to attacks abusing UDP-based protocols, TCP-based amplification traffic typically does not carry payload that can be inspected for validity.

4 Conclusion

In this paper, we have shown that reflective DDoS attacks are not limited to UDP-based protocols only. Our in-depth analysis of common TCP protocols identified millions of hosts that are vulnerable for TCP-based amplification. While for the majority of amplifiers the impact can be mitigated by sending `RST` segments on unexpected TCP segments, we also observed devices that do not respect this common TCP behavior and can therefore be abused. We further showed that TCP-based amplification attacks can induce similar impact than UDP-based attacks, although the number of amplifiers is lower. TCP thus permits reflective amplification attacks causing high attack traffic despite its three-way-handshake.

Acknowledgment

We would like to thank the anonymous reviewers for their constructive and valuable comments. This work was supported by the German Federal Ministry of Education and Research (BMBF Grants 16BY1110 (MoBE) and 16BY1201D (iAID)).

References

[1] COMPUTER EMERGENCY RESPONSE TEAM. CERT advisory CA-1996-21: TCP SYN Flooding and IP Spoofing Attacks. `https://www.cert.org/historical/advisories/CA-1996-21.cfm`, 1996.

[2] DITTRICH, D. Distributed Denial of Service (DDoS) Attacks/tools. `http://staff.washington.edu/dittrich/misc/ddos/`, 2000.

[3] DURUMERIC, Z., WUSTROW, E., AND HALDERMAN, J. A. ZMap: Fast Internet-Wide Scanning and its Security Applications. In *USENIX Security Symposium* (2013).

[4] FREILING, F. C., HOLZ, T., AND WICHERSKI, G. Botnet Tracking: Exploring a Root-cause Methodology to Prevent Distributed Denial-of-service Attacks. In *European Symposium on Research in Computer Security (ESORICS)* (2005).

[5] IOANNIDIS, J., AND BELLOVIN, S. M. Implementing Pushback: Router-Based Defense Against DDoS Attacks. In *Symposium on Network and Distributed System Security (NDSS)* (2002).

[6] KÜHRER, M., HUPPERICH, T., ROSSOW, C., AND HOLZ, T. Exit from Hell? Reducing the Impact of Amplification DDoS Attacks. In *USENIX Security Symposium* (2014).

[7] MIRKOVIC, J., AND REIHER, P. A Taxonomy of DDoS Attack and DDoS Defense Mechanisms. *SIGCOMM Comput. Commun. Rev. 34*, 2 (Apr. 2004).

[8] PAXSON, V. An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks. In *Computer Communication Review 31(3)* (July 2001).

[9] PENG, T., LECKIE, C., AND RAMAMOHANARAO, K. Survey of Network-based Defense Mechanisms Countering the DoS and DDoS Problems. *ACM Comput. Surv. 39*, 1 (Apr. 2007).

[10] ROSSOW, C. Amplification Hell: Revisiting Network Protocols for DDoS Abuse. In *Symposium on Network and Distributed System Security (NDSS)* (2014).

[11] SCHUBA, C. L., KRSUL, I. V., KUHN, M. G., SPAFFORD, E. H., SUNDARAM, A., AND ZAMBONI, D. Analysis of a Denial of Service Attack on TCP. In *IEEE S&P* (1997).

[12] YAAR, A., PERRIG, A., AND SONG, D. Pi: A Path Identification Mechanism to Defend Against DDoS Attacks. In *IEEE S&P* (2003).