Department: Head
Editor: Name, xxxx@email

Distributed Denial of Service (DDoS): A History

R. R. Brooks
Clemson University, Holcombe Department of Electrical and Computer Engineering

Lu Yu
Clemson University, Holcombe Department of Electrical and Computer Engineering

Ilker Ozcelik
Recep Tayyip Erdogan University, Department of Computer Engineering

Jon Oakley
Clemson University, Holcombe Department of Electrical and Computer Engineering

Nathan Tusing
Clemson University, Holcombe Department of Electrical and Computer Engineering

***Abstract*—Distributed Denial of Service (DDoS) attacks remain a persistent nuisance on the Internet. They exploit the fact that the Internet lacks centralized access control. Since this vulnerability was a core design decision of the early Internet, DDoS attacks have persisted. This article presents the technologies and tools that are used in DDoS, followed by a time-line of the major DDoS incidents. This is followed by a discussion of the primary classes of DDoS incidents and how the computing ecosystem enables DDoS. Early attacks were related to hacker culture, but their focus quickly changed to commercial exploitation. There have also been a number of political uses of DDoS, including cyberwar, hacktivism, and terrorism.**

Introduction

Distributed Denial of Service (DDoS) refers to using multiple computers to stage Denial of Service (DoS) attacks. DDoS attacks coordinate the actions of many computers to deprive users access to the resources of a victim machine(s). DDoS has become a persistent threat to the Internet. Although this threat is well known, current countermeasures do not adequately reduce the volume, magnitude, or number of attacks. Quite the contrary, Arbor networks reported an average of 1300 DDoS attacks per day in 2010 [52] growing to an average of 28,700 attacks per day, almost 20 every minute, in 2017 [19]. DDoS traffic volume has increased; reaching terabytes of data per second in 2017 [38]. The number of individuals impacted by DDoS attacks has grown consistently. In DDoS's early days, isolated servers would be disabled. Since 2007, entire countries are being deprived of Internet

access [34].

DDoS is not only a persistent problem, it is interesting historically. The evolution of DDoS has the following stages

1) The first attacks were made as social protests, which continue to this day;
2) Protests were followed by pranks, and idiosyncratic events;
3) Organized crime then discovered attack monetization, leading to investing resources into DDoS exploitation;
4) Nation-states found ways to leverage increasingly wide-spread DDoS attacks, using existing criminal activity as a cover to avoid retribution [17]; and
5) Governments use DDoS attacks to increase control over their populations [35], [52].

With the exception of the initial protest phase, this evolution mirrors the history of computer network abuse [9], [39], [51], [36]. This history stops at 2008, since not enough time has elapsed to maintain historical objectivity. This history, therefore, covers only the first 3 stages in the list above. We cover the progression of DDoS attacks from isolated pranks to cyber warfare tools. The evolution after 2007, when states started using Internet blackouts to control information dissemination [35] is out of this paper's scope.

The history we present is novel, since other descriptions of DDoS deal with only technical, social, criminal, or political aspects of DDoS. Attack motivations drove technical innovations in this realm. This article combines these aspects into a coherent whole. These attacks exist only because of the co-evolution of technology and society. To understand these attacks, readers need to know all aspects of the problem. This history of DDoS attacks starts with a section describing the evolution of DDoS tools and techniques, which includes a table of the networking technologies and tools most relevant to DDoS. The next section gives a narrative of the major DDoS events, including a tabular presentation. We group major DDoS events into related categories. One subsection discusses attacks tied to the emerging hacker culture. Commercial exploitation quickly replaced hacker culture, which we discuss in the next subsection. Political uses of DDoS are as important as commercial exploitation. The following subsection explains cyberwar. Cyberwar consists of both military and information operations. The final subsection describing DDoS attack events considers attacks performed by hacktivist and/or terrorist groups. We then provide a subsection explaining how the current computing ecosystem enables DDoS by allowing the production and dissemination of vulnerable computing nodes. The final section of this article provides our conclusions. By presenting how and why people are intentionally deprived of access to the Internet, and how DDoS evolved over time, this paper provides evidence of the growing importance of the Internet to society.

DDoS tools and technologies

Table 1 lists tools and technologies commonly used for DDoS. There have been a number of important DDoS tools.

Trin00 was a first generation DDoS tool. Trin00's internal communications used TCP/IP[1] with no encryption. Trin00 attacked random UDP[2] ports. It was the simplest first generation DDoS tool, with simple commands for command and control[3] (C&C) centers and bots[4]. Trin00 infections were usually detected through their repeated use of crontab[5] for startup. The C&C nodes could usually be detected by searching for file "...".

Tool	Description
DDoS bots	Software used to send attack traffic.
Stressers	Current generation of DDoS bots.
Botnet	Set of machines coordinating attacks.
Worms	Malicious processes migrating between hosts.

Table 1. DDoS relevant tools and technologies

[1] *Transmission Control Protocol* (TCP) is the connection oriented networking protocol used by most *Internet Protocol* (IP) traffic. TCP is frequently referred to as TCP/IP. It provides error free transmission of data from one computer to another.

[2] *User Datagram Protocol* (UDP) is an alternative to TCP/IP that sends information from one computer to another, but does not guarantee that data transfers are error free.

[3] *Command and control* (C2) or (C&C) refers to attack coordination infrastructure coordinating multiple nodes to perform a single attack

[4] Bots, abbreviation of robots, refers to individual compromised computers that execute attacks in response to commands from C&C infrastructure

[5] *crontab* is a UNIX system command used to schedule programs to run automatically in the future.

Tribal Flood network (TFN) was similar to Trin00, but supported four attacks: UDP, SYN [6], and ICMP[7] floods, as well as smurf[8] indirection. TFN C&C nodes were controlled through remote shells bound to TCP, ssh[9], telnet[10] or LOKI[11] sessions. **TFN2K** was part of the second generation of these tools. In addition to the original TFN attacks, it allowed mixed attacks. TFN2K included Targa3 attacks that used malformed IP headers to crash the IP stacks of victims. TFN2K encrypted communications, spoofed[12] IP addresses, and randomized the protocols used for transmitting information. Each packet in the communications protocol was sent to multiple decoy addresses as well as the IP address of the target. There were no default passwords. Passwords were requested at make time. Shell commands could be triggered remotely and used to update remote node software.

Stacheldraht was another second generation tool. It updated the capabilities of Trin00 and TFN by supporting encrypted communications and automatic software updates. Communications between C&C nodes and bots were encrypted using symmetric key encryption. Communications payloads were embedded in ICMP packets. These versatile tools were used by script kiddies[13] to attack systems worldwide, including universities. Although these tools are well known and easily detected, they have not faded from use. In 2014, IBM detected an increase in Stacheldraht probes coming from China [22].

[6]SYN floods takes advantage of TCP/IP requiring a "three way handshake" to open a connection. By starting the handshake, but not sending the final packet to complete the connection, the attacker occupies resources on the victim node. When the available "half-open connections" are all occupied, the node can not accept any new connections. SYN flood countermeasures exist.

[7]*Internet Control Message Protocol* (ICMP) is, like UDP, a datagram protocol for IP networks. ICMP is used for passing control messages, like error logging data, through the network.

[8]Smurf attacks replace packet source IP addresses with victim IP address. Attackers send attack packets to multiple destinations that respond to the victim. Coordinated smurf attacks cause multiple data streams to converge on the victim

[9]*ssh* is the secure shell software that provides encrypted remote connections.

[10]*telnet* software provides unencrypted remote connections.

[11]*LOKI* software establishes remote connections using ICMP packets.

[12]*Spoofing* refers to forging packets making them look different from what they really are.

[13]*Script kiddie* is a derogative term used to refer to unskilled attackers that use exploit code acquired from others.

The current generation of DDoS bot software is frequently referred to as *stressers*[14] rather than bots. Stressers have a more sophisticated design and can legitimately be used either to analyze web server performance or to generate DDoS attack traffic.

Botnets are networks of compromised computers working in harmony. Some botnets have been estimated to include millions of machines. Although it is difficult to verify, the largest botnet in 2009 was estimated to have between 580,000 to 1,600,000 nodes [36]. The Torpig botnet in 2010 was estimated to collect between $8,300.00 and $830,000.00 per day [4]. Since botnets act as an ongoing source of illegal income, botnet *herders* invest resources into avoiding detection. Large scale DDoS attacks typically require botnet support.

DDoS attacks may, or may not, be intentional. In the early 2000's, around the same time as the distribution of DDoS tools like TFN and Stacheldraht, a series of Internet worms hit the Internet.[15] The idea of a network worm first appeared in John Brunner's 1975 dystopian science fiction novel *Shockwave Rider* [10]. Xerox PARC implemented prototype worms within their network for system maintenance tasks in the 1980's. The first worm considered malicious by the Internet community was released by Robert Tappan Morris in 1988 [46].

The years 2001-2003 suffered multiple worm incidents, including Nimda, Blaster, Code Red I, and Code Red II. It is unclear what types of damage can be attributed to this malware. The generated attack traffic caused many major network disturbances. Leading to the supposition that they inadvertently triggered a number of DoS events. Notable events in this series of worm attacks include:

July 2001 – Code Red spread using a buffer overflow. After 3 weeks of spreading, it launched a DDoS attack on WhiteHouse.gov. The attack was ineffective, since hard coded IP addresses were used. Changing the site's IP address disabled the attack.

[14]The term stresser started being used around 2014. Stresser services are also called *booters*.

[15]A *worm* is malicious software that works as an independent process. Worms copy themselves to new hosts where they execute independently.

January 2003 – Slammer exploited a buffer overflow vulnerability in SQL-Server. The Internet slowed down due to the volume of traffic and many routers crashed.

August 2003 – Blaster exploited an RPC buffer overflow. It included a *SYN flood* attack on Microsoft update servers.

August 2003 – Blaster coincided with a blackout in the Northeastern USA. There was debate as to whether or not Blaster slowing utilities SCADA traffic helped cause this blackout.

Collateral damage that has been attributed to these worms include disruption of automated teller machine networks, airplane flight schedules, elections, and a blackout of the Northeastern US power grid [37], [33], [5]. While it is doubtful that these outages were intentionally triggered by the worm authors, it is very likely that the massive volume of traffic they generated played a role.

DDoS History

Table 2 lists influential DDoS events. In this section, we group these events into classes depending on their purpose and motivation.

Hackers

With the growth of the Internet during the 1980s, the advent of the world-wide web in the 1990s, and the invention of Mosaic in 1993, the first graphical browser, the Internet became a public space. The first documented DDoS attacks came shortly thereafter.

In 1996, the aptly named New York ISP, Panix, was hit with a SYN flood attack for several days. Panix was attacked in retaliation for installing one of the first spam filters on their email system [11]. This vulnerability was first discovered in 1994 by Cheswick and Bellovin, who decided not to include it in their book [12]. It was, however, publicized in a 1996 *Phrack* article that gave precise explanations on how it could be exploited [14]. In 1996, there were a total of about 20 million Internet users. Notable DDoS events related to hacker culture include:

L0pht The hacker collective L0pht, worked to raise awareness of the lack of computer security on the Internet. L0pht started as an informal collection of people interested in computers and security problems. It eventually morphed into a security consulting business [31]. L0pht members testified before congress in 1998. During that testimony, L0pht member Mudge testified that the members of L0pht could shut down the entire Internet within 30 minutes [23]. Suspicion is that they referred to DDoS, although they never publicly provided details on how they would have disabled the Internet.

Mafiaboy In February 2000, 15 year old Michael Calce from Montreal, Canada launched a major DDoS attack on Yahoo, Amazon, Dell, eBay, CNN, and others using the alias Mafiaboy. The Mafiaboy attack was a packet flooding assault on nascent e-commerce sites. Estimates of the damage inflicted by this attack vary; ranging from $1.7 billion to the $7.5 million claimed by the state prosecutor at trial [1]. After conviction, Mafiaboy was sentenced to a $250 fine, one year "open" detention, and eight months probation.This was much less than the maximum possible sentence. The light sentence was criticized, partly because the case's social worker felt the likelihood of recidivism was high [16].

Date	Description
Pre-1989	Non-computer DoS using sabotage and sit-ins
1995	German government blocks access to sexual material.
1995	Strano Network DDoS protests French nuclear weapons tests.
1996	Panix ISP in New York disabled by SYN flood attack.
1997	Electronic Disturbance Theater (EDT) uses Floodnet to protest Mexican government attacks on Mayan anarchists.
1998	US DoD DDoS attack on EDT during *Ars Technica* festival.
1998	L0pht testify to Congress that total Internet disruption is easy.
1999	Electro-hippies use EDT Floodnet to attack WTO.
1999-2000	Trin00, TFN, TFN2K and Stacheldraht available online.
2000	Mafiaboy takes down Yahoo, Amazon, Dell, eBay, CNN, etc.
2001	Code Red worm DDoS of WhiteHouse.gov.
2001	After Hainan incident, Chinese group launches DDoS on US military sites.
2001	German protesters use Floodnet to attack Lufthansa.
2003	Blaster worm SYN flood of Microsoft update servers.
2003	Blaster worm during blackout of US power grid.
2005	Gpcoder ransomware.
2007	Russian population launches Cyberwar with DDoS on Estonia.
2007	Pro-Putin botnets launch DDoS attacks.

Table 2. Chronology of denial of service. Detailed descriptions of events are in text.

Commercial exploitation

After black hat hackers launched DoS events for fun, others realized the commercial potential of DoS attacks. For-profit DoS attacks may be under-represented in Table 2 for many reasons. Victims of extortion do not want to publicize the events. Victims may not realize they are under attack. If their websites crash, or are slow, this may be attributed to poor design, network problems, etc. Small scale attacks will not be newsworthy, so only attacks that are larger than normal are reported.

DDoS attacks can be launched by individuals who are recruited and provided with custom software developed for the attack, Botnets either hired or provided by like-minded criminal groups, or both.

Recruiting individuals to run a DDoS is not very effective and makes the individuals vulnerable to criminal prosecution [6]. Most large volume DDoS attacks include botnets. Since running a botnet is criminal, bot-herders are prepared to hide their identities.

A survey of DDoS botnets [18] finds that almost half of the non-mobile device botnets provide DDoS for-hire services. Unlike the media, political, and strategic targets, DDoS for-hire victims tend to be commercial enterprises. DDoS attacks have been used as a distraction to hide other criminal activities attacking the victim. DDoS tends to be more costly for the victim than other attacks. Although, use of DDoS to sabotage competitors should not be discounted. For example, there are reports of Minecraft server providers DDoSing competitors to increase their market share. Extortion is a common reason for DDoS attacks on commercial sites.

The cost of hiring a botnet for DDoS is quite reasonable. Cost varies based on the victim, their DDoS protection, the volume of traffic desired, and how long the attack should be maintained [26].

Cyberwar

A major shift in DDoS attacks occurred around 2007, when they became an instrument in interstate warfare. Communications has always been an essential part of warfare. Martin van Creveld has meticulously documented the co-evolution of communications technologies and military strategy [48], [49]. Denying your opponent the ability to communicate is useful during war; making DDoS attacks part of the cyberwarfare arsenal. We differentiate between hacktivism and cyberwar, by considering cyberwar to be attacks between states and hacktivism to be attacks due to (primarily internal) political divisions. Attacks given are in chronological order.

In April 2001, a US Navy spy plane was intercepted by multiple Chinese planes off the coast of China. An in-air collision between the US plane and one Chinese plane killed the pilot. One aftermath of this confrontation was a number of DDoS attacks on US military sites. It is believed that the Chinese hacking group "Honker Union"performed the attacks [35]. This skirmish predated the attacks considered officially as cyberwarfare.

The conflict between Russia and Estonia in April 2007 is usually considered the first true cyberwar. Estonia is an independent country and a part of NATO. It had been a part of the USSR before the USSR's collapse. About 25% of the Estonian population are ethnic Russian.

The Estonian government removed a statue honoring Soviet troops, which insulted many ethnic Russians. At 10:00 PM on April 26, 2007, Estonia was subjected to a major DDoS attack. Estonia was particularly vulnerable to DDoS attacks, since their government and economic sectors are dependent on the Internet. It is considered the most Internet connected country on Earth. On May 9, the attack escalated to 4 million packets per second.

Estonia's economy was stopped for a number of weeks. All government, banking, news, media, and university Internet sites were disabled.

Attacks were coordinated using Internet Relay Chat (IRC) channels.[16] DDoS instructions, scripts, and lists of victim IP addresses were widely distributed by ethnic Russian groups. This included enlisting world-wide botnets.

Eventually, the Estonian government realized that the majority of the attack traffic came from outside Estonia. They isolated the Estonian Internet from the rest of the world and traffic become manageable. The attack stopped on May 19, 2007.

[16]*IRC* is a system allowing multiple users to exchange text over the internet in real time.

It is accepted that the attacks originated in Russia and were coordinated by Russian nationals. Originally, NATO blamed the Russian government. It remains unclear, whether or not the Russian government was directly involved. It is now thought that Russian nationalists launched the attack on their own. This may have included some coordination with Kremlin friendly groups [34], [2].

Georgia is another independent country that had been part of the former Soviet Union. As with Estonia, the country of Georgia has a sizable ethnic Russian population. The Russian and Georgian ethnic groups are not evenly distributed throughout the country. The Georgian regions of Abkhazia and South Ossetia had large Russian populations. The ethnic Russians in these regions expressed their preference to leave Georgia and become part of Russia. For months leading up to July 2008, these political differences were exacerbated by military actions undertaken by NATO and Russia on both sides of the border. These maneuvers escalated the conflict [13] .

On August 1 the Russian population started shelling Georgian villages in these regions. The tensions increased. On the night of August 6, Russian hackers attacked Georgian news and government websites.[17] Russian military officials claimed the network attacks were in response to Georgians hacking South Ossetia websites earlier in the week. The Russian attacks were mainly brute force DDoS flooding attacks powered by large botnets. The botnets used in this attack were primarily affiliated with botnets run by known Russian criminal groups, including the Russian Business Network (RBN). Concurrently, SQL injection attacks were used to deface Georgian media sites [44].

The Russian military invaded Georgia on August 7, which triggered the widespread belief that these DDoS attacks were coordinated with the military invasion. Other than the suspicious timing, there is scant evidence of coordination. The DDoS attacks peeked on August 8 at 843 Megabytes per second. A program for running DDoS bots could be downloaded with a list of IP addresses to attack from "StopGeorgia.ru." Users had to enter an address into the program and press a button saying "start flood."

This campaign apparently aimed at isolating Georgia, keeping Georgia from presenting its narrative to the international community, and inflecting short term financial damage. For the most part, minimal damage was inflicted on Georgia's physical Internet infrastructure, as well as its industrial control systems. There was a gas pipeline explosion in Georgia that coincided with the invasion, but the connection to hacking has not been established [25]. It appears that the cyberwar was primarily information warfare and preparations for war started up to two years previously [44].

Russia claimed that their invasion was a peace keeping mission to protect the Russian civilian populations in South Ossetia. They stopped all military activity on August 12, since all of their military objectives had been met. Normal banking could not resume until August 18 [13].

In spite of the suspicious timing and other circumstantial evidence, it has not been established that the Russian government was involved in these network attacks. Other theories explaining the attacks attribute them to: Russian patriots working alone, Russian organized crime working alone, or Russian organized crime working with the Kremlin [44]. According to Dr. Deibert, who runs the University of Toronto's Citizen Lab, it has been established that the servers coordinating these attacks were all located inside of Russia. The botnets used in the attack had previously been active in multiple DDoS for-hire schemes [13].

Hacktivism and/or terrorism

In parallel with the use of DDoS in cyberwar, a number of groups expanded on the early activist idea of using DDoS as a form of civil disobedience. They see the DDoS as a form of sit-in. There are arguments both for [43] and against [52] DDoS being a legitimate form of *Electronic Civil disobedience* (ECD). We note that the labels hacktivist and terrorist are both very subjective. The label used to describe a political collective often depends mainly on the author's view of the group's political goals.

Opinions on the meaning and legitimacy of ECD are nuanced. On the one extreme, Dorothy

[17]Some reports say DDoS attacks started earlier, possibly as early as July 20 [28], [20].

Denning frequently equates ECD and cyberterrorism. She sees no clear boundary. On the other hand, Graham Meikle sees ECD as activists exercising "symbolic power." Symbolic power is different from both physical violence, and economic power. It is a new type of power, which has emerged with the Intrnet's information society. ECD is primarily a way of raising consciousness and awareness. DDoS by a swarm of activists lets them express their views, which would have otherwise been excluded or ignored by society at large [30]. This differs significantly from MacKenzie Wark's view. Wark agrees on the Internet producing a new culture, which has different values than society before the Internet. He uses a Marxist dialectic to derive a culture of exploited hackers in conflict with an exploitative *vectoralist class*. Where hackers create innovations, while vectoralists are what economists would term *rent seekers.*[18] In order to innovate, hackers must continuously perform ECD. Wark is, however, very critical of DDoS. They voice the opinion that denial of information is hard to reconcile with the inherent hacker goal of innovation [50]. Instead of viewing ECD as either an exercise of power or an ongoing class struggle, Rita Raley takes a view held by many activist presented in this Section. ECD is a form of performance art [40]. Both Raley and Meikle emphasize that art collectives originated the concept of ECD. For art collectives, ECD is not a struggle. ECD is a form of self-expression. ECD can be a theatrical farce that robs the opponent of their encumbent power. By ridiculing their opponents, art collectives rob their oppressors of the trappings of power. ECD, which often uses DDoS, empowers the oppressed. The viewpoints of [40], [30], [50] add nuance beyond the traditional roles of white and black hat hacking. Their views do not, however, overcome the concerns expressed by Denning. DDoS is not always a tool of the oppressed. It is frequently a tool of oppression, as feared by Wark. This section sees DDoS progress from an almost whimsical tool of protest used by Zappatistas and Electro-hippies to a weapon used by the Russian government to hinder another state's defense.

[18]An economics term refering to parties that coerce economic advantages, without increasing productivity.

We include in this section attacks that deal more with internal political issues. We try to put attacks between nation states were listed in the cyberwar section. Since effective attribution is almost impossible and we cannot always know the true motives behind an attack, the line between cyberwar and hacktivism is not clear. The list we provide here is selective. In [52], researchers found 815 sites had been attacked by hacktivists between 1998 and 2010.

In 1995 an Italian hacker group called the Strano Network performed the first major DDoS political protest. They attacked French government sites for one hour after the French government tested nuclear weapons in the Pacific. Since this attack had only limited success, either the Panix or Strano Network attacks could be considered the first legitimate DDoS attack.

Shortly after the Strano Network attack, performance artist Ricardo Dominguez created the idea of a virtual sit-in. He lead a small group of *Electronic Disturbance Theater* (EDT) activists to create the *FloodNet* HTML page that includes a java applet [24].

The EDT wanted to support the revolutionary Zapatista Army's rebellion in Chiapas against the Mexican government. The Zapatistas were a leftist rebel group of Anarchist Mayans who were involved in an armed struggle with the Mexican government. The EDT was particularly incensed when the Mexican government's attempts to suppress the rebellion killed 45 civilians. The EDT used e-mail and the Internet to recruit participants to use Floodnet to attack the Mexican government. FloodNet performed a simple packet flooding attack on the website of Mexican President Zedillo and US President Bill Clinton. Packets could request items like "truth" or "justice" which would leave error messages on the server saying:

- "Truth not found", or
- "Justice not found".

Later versions of Floodnet requested the names of Zapatista martyrs killed by the Mexican government. While they claimed the participation of more then 8000 individuals in attacks lasting two hours at a time, they did not entirely disable the site. The Mexican President's site was unreachable occasionally [24].

Dominguez planned on presenting this work

at the 1998 Ars Electronica arts festival in Linz, Austria with an attack on Zedillo, the German stock exchange and the Pentagon. Unfortunately, he was unable to do this due to a DDoS attack on his own infrastructure. The US Department of Defense later took credit for the counter-attack [24]. The DDoS counter-attack was found to be the largest attack up to that time [29].

Virtual sit-ins continue. With people attacking other targets, such as an attack by 13000 individuals on Lufthansa [24].

Shortly after the EDT, a group of activists protested World Trade Organization (WTO) conference in Seattle. One sub-group, the *electro-hippies*, took the EDT software and used it to attack the WTO websites. Participants had to download the software and run it. Activists claim that there were over 450,000 people using their tool. There seems to have been down time and response delays due to this activity [43].

EDT's Floodnet was used in 2001 in Germany. Protesters were upset about the German government's deportation policy. To protest this, they launched DDoS attacks against the German airline Lufthansa. The government had been using the airline to deport individuals. This action was coordinated with physical protests and press releases. It did lead to Lufthansa stopping its participation in deportations [43]

Leading up to the 2007 Russian elections, botnets run by pro-government cyber-criminals launched DDoS attacks against dissident chess master Gary Kasparov and his political party. The opposition websites were inaccessible during the attacks [35]. Attacks on the pro-Kremlin youth group Nashi by the Russian newspaper Kommersant led to it being attacked in March 2008.

COMPUTING ECOSYSTEM

While this paper concentrates on networking aspects of DDoS, the larger computing ecosystem plays a role. Some attacks, like smurfing, and LAND[19] do not require attackers to gain unauthorized access to another machine. Activist groups, like the Zapatistas, electro-hippies, or Anonymous, have multiple users run attack software voluntarily from their own machines. These attacks do not require compromised computer nodes for attack.

Most DDoS attacks, such as those using botnets and worms, use compromised machines. Unfortunately, compromising third party machines is not difficult. There are many theories as to why individual computers are insecure. Ross Anderson of Cambridge University maintains that computers are vulnerable because of economics. Computer manufacturers do not lose money when user machines are compromised. Engineering secure machines and testing their products would cost manufacturers money [3].

Annual costs to the USA of insecure software has been conservatively estimated to be $180 billion and market surveys indicate the 75% of the computers on the Internet have been infected by botnets [41]. Unfortunately, there is no penalty for producing insecure machines, since current laws shield computer manufacturers from the legal liability that other manufacturers have when they market defective, insecure products [41]. These facts are particularly salient, when we consider that software engineering often concentrates on maintaining a positive cash flow [7].

In spite of these economic externalities, many professionals feel user behavior is largely to blame for security failures. Most machine infections (94%) in 2020 relied on user email as the attack vector [15]. Many professionals blame user's being naive for these infections. But the sheer volume, and the prevalence of these attacks across industries, would imply that individual users are not the real vulnerability.

The economics of computer insecurity is aggravated by how interdependent the marketplace has become. Poorly secured Internet of things (IoT) devices are increasingly vulnerable to attack. Hardware level attacks are currently used mainly by advanced nation states, but as exploits become known they will be used by less advanced actors. Similarly, companies are being infected by contractors whose compromised machines connect to their internal networks. Developer software tools suffer from supply chain attacks, where an infected tool that is used anywhere in the software supply chain can compromise every program after that point. For example, a widely used disk cleaning utility (Crap Cleaner) was used by a software developer whose programs were

[19]LAND attacks forge packets so that both packet source and destination addresses point at the victim. The victim ends up generating attack traffic against itself.

used by ASUS. Later in the supply chain, this inserted malware into properly signed operating system updates for ASUS laptops. Any software written using those laptops would also spread the infection. The industry previously believed that individual machines and individual users needed to maintain their own security. This concept of having an *attack surface* is no longer viable. The entire ecosystem is poorly maintained and vulnerable [8].

CONCLUSION

The DDoS exploitation tools and approaches presented in this paper can be seen as proofs of concept for flaws in Internet design. Unwittingly, design decisions created system bottlenecks and other flaws for attackers to exploit. Exploited flaws include:

- The Internet's open design[20] allows network access for any and all. First, individual pranksters, like mafiaboy, planted attack bots on machines and overwhelmed the network. Seeing the effects of these pranks, activist communities distributed tools to like-minded users whose coordinated activities overwhelmed networks even more effectively. This succes by pranksters and activists, gave ideas to bad actors who used botnets and the Internet of things to access even more machines to more effectively overwhelm victims.
- Distributed management makes it difficult to counter DDoS. Since individual bots, stressers, are usually located in different ISP's and the traffic generated by the few local devices are not terribly significant. The traffic is harmful when it converges at the victim. The victim ISPs have no incentive to invest time, effort, and resources into tracking down those individual bots.
- Eventually, large commercial infrastructure emerged that was just as highly distributed as any attacker could be. *Content delivery networks*[21], like Cloudflare, and cloud providers (AWS, Azure, Google Cloud) are largely impervious to flooding attacks, but expensive. In which case, DDoS attackers starve victims by consuming users of money, instead of bandwidth directly [27].[22]
- The use of DDoS for Internet deprivation, by governments inverted the original DDoS vulnerability. Instead of having a system that is open to any and all, network infrastructure is used to block user access to outside information sources. Once again, a bottleneck is found to stop the flow of traffic. This time denial of service is perpetrated by whoever controls network infrastructure, instead of rogue individuals [52].
- Open services like DNS, which are core parts of the Internet design, are exploited by amplification attacks. Since network responses can be much larger than requests, these increase the volume of network attack traffic [42].
- Header information is in clear text and easily forged [38]. This lets users hide their real location, redirect query responses to victims, black-hole attacks, etc.

While none of these flaws were obvious during Internet creation, they are now consistently used to hinder proper network use. Changing the Internet's design now would be painful and expensive. these changes may eventually be unavoidable.

It would have been possible to build networks using radically different approaches than the current Internet design. The current design simply forwards packets from source to destination with minimal flow management within the network. All of the system intelligence is at the network's end points. Making the network core intelligent could possibly remove the current flaws, but it is easy to imagine that shared management resources, more complex routing logic, or data

[20]In other contexts, the open design is a strength.

[21]Content delivery networks, or content distribution networks (CDNs) are geographically distributed networks that can maintain cached versions of data. This allows remote machines to quickly respond to data requests using the local versions of the data. Large CDNs can reduce response latency for users and bandwidth consumption for data providers. If the CDN is large with adequate computational and network bandwidth, it can absorb DDoS attacks.

[22]Some actors, including Equalit.ie and Team Cymru, provide low cost CDN protection to NGOs that face this threat [47].

caching would provide a larger attack surface for malicious exploitation.

The success of the Internet, including its dominance over alternative technologies that existed at the time: X.25, DECNet, token ring, etc. indicates that there were many advantages to the Internet's design at the time. The increasing popularity of shared infrastructure, like cloud computing and content delivery networks, may indicate that user needs and societal risks have evolved to the point where changes are needed.

DDoS attacks have been exploited for fun, profit, and political gain. Over time attackers have included pranksters, artists, blackmailers, protesters, and nation-states. These attacks primarily exploit the facts that there is no access control for the global Internet, and that packets are not inspected for correctness. Removing these vulnerabilities would require drastic changes to Internet infrastructure, which is unlikely. DDoS attacks are likely to endure. They are becoming increasingly potent and difficult to trace back to the attacker. Costs of renting a DDoS botnet are falling at about 5% annually [32]. DDoS traffic volume has been measured at over 1500 Gbps [45], [21]. In addition to being used in warfare between nation-states, DDoS and Internet blackouts are tools for censorship and oppression by local governments [35], [52]. These attacks are almost certain to continue and evolve. Their history provides insights into how Internet infrastructure has been, and is still, used and abused by DDoS.

REFERENCES

1. Bin Laden: Steganography Master?, Feb. 7, 2001, http://www.wired.com/news/politics/0,1283,41658,00.html?tw=wn_story_page_prev2.
2. http://dewy.fem.tu-ilmenau.de/CCC/CCCamp07/video/m4v/cccamp07-en-2050-Estonia_and_information_warfare.m4v.
3. Ross Anderson. *Security engineering*. John Wiley & Sons, 2008.
4. L. Cavallaro B. Gilbert M. Szydlowski R. Kemmerer C. Kruegel B. Stone-Gross, M. Cova and G. Vigna. Your botnet is my botnet: Analysis of a botnet takeover. In *Proceedings of the ACM CCS*. ACM, 2010.
5. H. Berghel. Malware Month. *Communications of the ACM*, 46:15–19, 2003.
6. Judith Bessant. Democracy denied, youth participation and criminalizing digital dissent. *Journal of Youth Studies*, 19(7):921–937, 2016.
7. Stefan Biffl, Aybuke Aurum, Barry Boehm, Hakan Erdogmus, and Paul Grünbacher. *Value-based software engineering*. Springer Science & Business Media, 2006.
8. R. R. Brooks. The evolving attack surface https://www.youtube.com/watch?v=SWz2bir_grU, (last visited 11/2020), 2019.
9. Richard R Brooks. *Introduction to computer and network security: navigating shades of gray*. CRC Press, 2013.
10. J. Brunner. *The Shockwave Rider*. Ballantine Books, NY, 1975.
11. Robert E. Calem. New york's panix service is crippled by hacker attack, https://archive.nytimes.com/www.nytimes.com/library/cyber/week/0914panix.html (last visited 12/18).
12. William R Cheswick, Steven M Bellovin, and Aviel D Rubin. *Firewalls and Internet security: repelling the wily hacker*. Addison-Wesley Longman Publishing Co., Inc., 2003.
13. Ronald J Deibert, Rafal Rohozinski, and Masashi Crete-Nishihata. Cyclones in cyberspace: Information shaping and denial in the 2008 russia–georgia war. *Security Dialogue*, 43(1):3–24, 2012.
14. Wesley Eddy. Tcp syn flooding attacks and common mitigations. Technical report, 2007.
15. Josh Fruhlinger. Top cybersecurity facts, figures and statistics for 2020 https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html, (last visited 11/2020), 2020.
16. Gary Genosko. The case of 'mafiaboy'and the rhetorical limits of hacktivism. *The fibreculture J.*, (9), 2006.
17. Andy Greenberg. *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. Doubleday, 2019.
18. Nazrul Hoque, Dhruba K Bhattacharyya, and Jugal K Kalita. Botnet in ddos attacks: Trends and challenges. *IEEE Communications Surveys and Tutorials*, 17(4):2242–2270, 2015.
19. Mattijs Jonker, Alistair King, Johannes Krupp, Christian Rossow, Anna Sperotto, and Alberto Dainotti. Millions of targets under attack: a macroscopic characterization of the dos ecosystem. In *Proceedings of the 2017 Internet Measurement Conference*, pages 100–113, 2017.
20. Stephen W Korns and Joshua E Kastenberg. Georgia's cyber left hook. Technical report, ARMY WAR COL-

LEGE CARLISLE BARRACKS PA STRATEGIC STUDIES INSTITUTE, 2009.

21. Brian Krebs. Dutchman arrested in spamhaus ddos. *Krebs on Security*, 26, 2013.
22. John Kuhn, 2014.
23. L0pht, 1998.
24. Colin Lecher. Massive attack: How a weapon against war became a weapon against the web, the verge, https://www.theverge.com/2017/4/14/15293538/electronic_disturbance_theater_zapatista_tactical_floodnet_sit_in (last visited 12/18).
25. Robert M Lee, Michael J Assante, and Tim Conway. Ics cp/pe (cyber-to-physical or process effects) case study paper–media report of the baku-tbilisi-ceyhan (btc) pipeline cyber attack. sans institute, 2014.
26. Denis Makrushin. The cost of launching a ddos attack, https://securelist.com/the-cost-of-launching-a-ddos-attack/77784/, 2017.
27. Steve Mansfield-Devine. Ddos: threats and mitigation. *Network Security*, 2011(12):5–12, 2011.
28. John Markoff. Before the gunfire, cyberattacks. *New York Times*, 12:27–28, 2008.
29. Niall McKay. Pentagon deflects web assault, wired, https://www.wired.com/1998/09/pentagon-deflects-web-assault/ (last visited 12/18).
30. Graham Meikle. Electronic civil disobedience and symbolic power. 2008.
31. Joseph Menn. *Cult of the Dead Cow: How the Original Hacking Supergroup Might Just Save the World*. PublicAffairs, 2019.
32. David Monahan. The cost of a ddos attack on the darknet, https://blog.radware.com/security/2017/03/cost-of-ddos-attack-darknet/ (last visited 02/2019), 2017.
33. D. Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford, and N. Weaver. Inside the Slammer Worm. *IEEE Security and Privacy*, 1(4), 2003.
34. Jose Nazario. Estonian ddos attack - a summary to date. Website (last visited September 2012), May 2007.
35. Jose Nazario. Politically motivated denial of service attacks. *The Virtual Battlefield: Perspectives on Cyber Warfare*, pages 163–181, 2009.
36. The Parliament of the Commmonwealth of Australia. *Hackers, Fraudsters and Botnets: Tackling the Problem of Cyber Crime, The Report of the Inquiry into Cyber Crime*. Commonwealth of Australia, 2010.
37. CNN Online. "Computer worm grounds flights, blocks ATMs," http://www.cnn.com/2003/TECH/internet/01/25/internet.attack/.
38. İlker Özçelik and Richard Brooks. *Distributed Denial of Service Attacks: Real-world Detection and Mitigation*. CRC Press, 2020.
39. Donn B. Parker. The Dark Side of Computing: SRI International and the Study of Computer Crime. *IEEE Annals of the History of Computing*, pages 3–15, 2007.
40. Rita Raley. *Tactical media*, volume 28. U of Minnesota Press, 2009.
41. David Rice. *Geekonomics: The Real Cost of Insecure Software (paperback)*. Pearson Education, 2007.
42. Christian Rossow. Amplification hell: Revisiting network protocols for ddos abuse. In *NDSS*, 2014.
43. Molly Sauter. *The coming swarm: DDOS actions, hacktivism, and civil disobedience on the Internet*. Bloomsbury Publishing USA, 2014.
44. Paulo Shakarian. The 2008 russian cyber campaign against georgia. *Military review*, 91(6):63, 2011.
45. Ars Technica. When spammers go to war: Behind the spamhaus ddos, 2013.
46. H.F. Tipton and M. Krause. *Information Security Handbook*. CRC Press, Boca Raton, FL, 2003.
47. Seamus Tuoy and Equalit.ie. Botnet attack analysis of deflect protected website blacklivesmatter.com https://equalit.ie/deflect-labs-report-3/ (last visited 02/2019), 2016.
48. Martin van Creveld. *Command in War*. Harvard University Press, Cambridge, MA, 1985.
49. Martin Van Creveld. *Supplying war: logistics from Wallenstein to Patton*. Cambridge University Press, 2004.
50. McKenzie Wark. A hacker manifesto [version 4.0]. *Subsol, Available at: http://subsol. c3. hu/subsol_2/contributors0/warktext. html (accessed 18 Apr. 2004)*, 2004.
51. K. Wong. The hackers and computer crime. In *Securicom 1986, Paris France*, pages 11–26. SEDEP, 1986.
52. Ethan Zuckerman, Hal Roberts, Ryan McGrady, Jillian York, and John Palfrey. Distributed denial of service attacks against independent media and human rights sites. *The Berkman Center*, 2010.

Acknowledgment

This material is based upon work supported by, or in part by,the National Science foundation grants CNS-1049765, OAC-1547245, CNS-1544910, OAC-1642143, Republic of Turkey Ministry of National Education and The Scientific and Technological Research Council of Turkey (TUBITAK).

The U.S. Government and the Turkish Government are authorized to reproduce and distribute reprints for Governmental purposes

notwithstanding any copyright notation thereon. The authors gratefully acknowledge this support and take responsibility for the contents of this report.

The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied,of the National Science Foundation, The Scientific and Technological Research Council of Turkey, Republic of Turkey Ministry of National Education, the Turkish Government or the U.S. Government.

The authors also gratefully acknowledge use of the services and facilities of the SimCenter, Center of Excellence in Applied Computational Science and Engineering at the University of Tennessee at Chattanooga. The authors would also like to give a heartfelt thanks to the Director of the SimCenter, Dr. Antony Skjellum.

R. R. Brooks is a Professor in the Holcombe Department of Electrical and Computer Engineering at Clemson University and CTO of Danaides NGO. He is part of the Africtivistes NGO. He received a PhD in Computer Science from LSU and a B.A. in Mathematical Sciences from Johns Hopkins. He is fluent in German and French. He was Head of the Distributed Systems Department of the Penn State Applied Research Laboratory for 7 years. Dr. Brooks' research on computer and network security has been sponsored by US DoD, NIST, Dept. of State, NSF, and BMW. His security research works to advance freedom of expression and protect vulnerable civilian populations. Contact him at rrb@acm.org.

Lu Yu received the B.S. degree in information engineering and the M.S. degree in control theory from Xi'an Jiaotong University, Xi'an, China, and the Ph.D. degree in electrical engineering from Clemson University, Clemson, South Carolina. She is currently a research assistant professor with the Holcombe Department of Electrical and Computer Engineering, Clemson University. Her research interests include cyber security and user privacy and anonymity.

Ilker Ozcelik eceived the MS degree in Electrical Engineering from Syracuse University in 2010, and the PhD degree in Electrical Engineering from the Holcombe Department of Electrical and Computer Engineering, Clemson University, Clemson, South Carolina in 2015. He is currently an assistant professor with the Department of Computer Engineering, Recep Tayyip Erdoğan University, Rize, Turkey. He is a member of IEEE and ACM. His research interests include network traffic analysis, network security, software defined networking, blockchain, security and privacy in intelligent systems. Contact him at ozcelikilker@ieee.org.

Jon Oakley received the B.S. degree in electrical engineering from Clemson University in 2016 and the Ph.D. Degree in computer engineering from the Holcombe Department of Electrical and Computer Engineering in 2020. His research interests include protocol mimicry, network traffic analysis, cryptocurrencies, and Markov processes.

Nathan Tusing received the B.S. degree in engineering from Bob Jones University, Greenville, South Carolina. He is currently pursuing the Ph.D. Degree in computer engineering from Clemson University, Clemson, South Carolina with the Holcombe Department of Electrical and Computer Engineering. His research interests include software defined networking, steganography, and network traffic analysis.