Lecture 19 – Denial of Service:

October 30, 2018

Dr. Dan Massey

Read Computer Security: Principle and Practices Chapter 7

Denial of Service

Denial-of-Service (DoS) Attack

The NIST Computer Security Incident Handling Guide defines a DoS attack as:

"An action that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources such as central processing units (CPU), memory, bandwidth, and disk space."

Denial-of-Service (DoS)

- A form of attack on the availability of some service
- Categories of resources that could be attacked are:

Network bandwidth

Relates to the capacity of the network links connecting a server to the Internet

For most organizations this is their connection to their Internet Service Provider (ISP)

System resources

Aims to overload or crash the network handling software

Application resources

Typically involves a number of valid requests, each of which consumes significant resources, thus limiting the ability of the server to respond to requests from other users

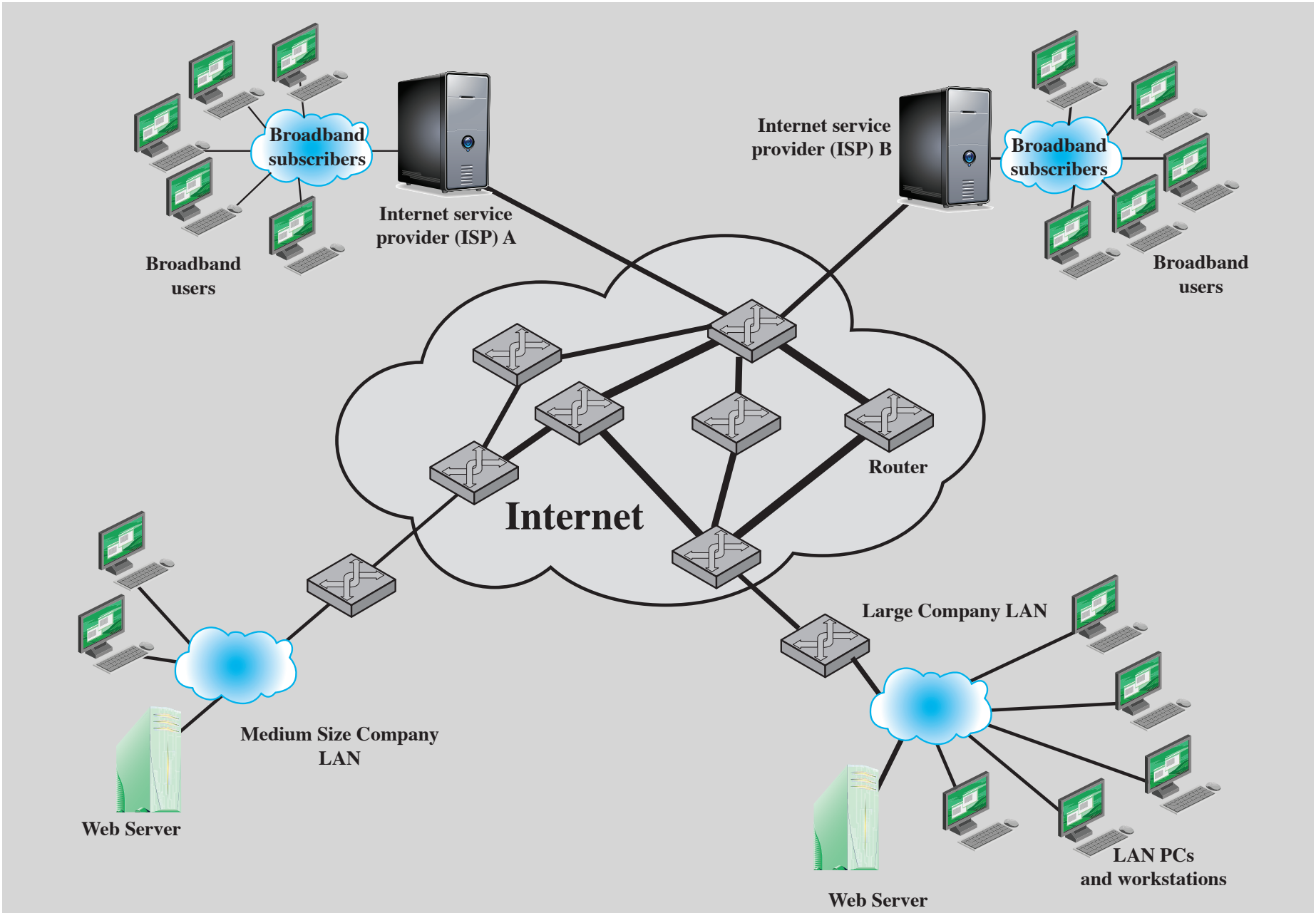


Figure 7.1 Example Network to Illustrate DoS Attacks

Classic DoS Attacks

- Flooding ping command
  - Aim of this attack is to overwhelm the capacity of the network connection to the target organization
  - Traffic can be handled by higher capacity links on the path, but packets are discarded as capacity decreases
  - Source of the attack is clearly identified unless a spoofed address is used
  - Network performance is noticeably affected

Source Address Spoofing

- Use forged source addresses
  - Usually via the raw socket interface on operating systems
  - Makes attacking systems harder to identify
- Attacker generates large volumes of packets that have the target system as the destination address
- Congestion would result in the router connected to the final, lower capacity link
- Requires network engineers to specifically query flow information from their routers
- *Backscatter traffic*
  - Advertise routes to unused IP addresses to monitor attack traffic

Source Address Validation

- **Existing Standards Make Attacks More Difficult and Attribution Easier**
  - Techniques such as ***Best Current Practice 38 (BCP38)*** block spoofing
  - Essentially check the packets leaving your network have your address
    - E.G. Packets leaving DHS network have DHS return addresses (source address)
  - Spoofed packets used in a variety of attacks
    - Computer at DHS reports its source is an NSF computer so others reply to NSF
    - Computer at DHS reports its source is NSF so others think NSF (not DHS) is attacking them
  - **Identify and Overcome technological road blocks to deployment**
  - **Tragedy Of The Commons Challenge**
- **Measurement and Deployment Needed**
  - **Systems for active measurement and reporting**

BCP38

- Read BCP 38

https://tools.ietf.org/html/bcp38

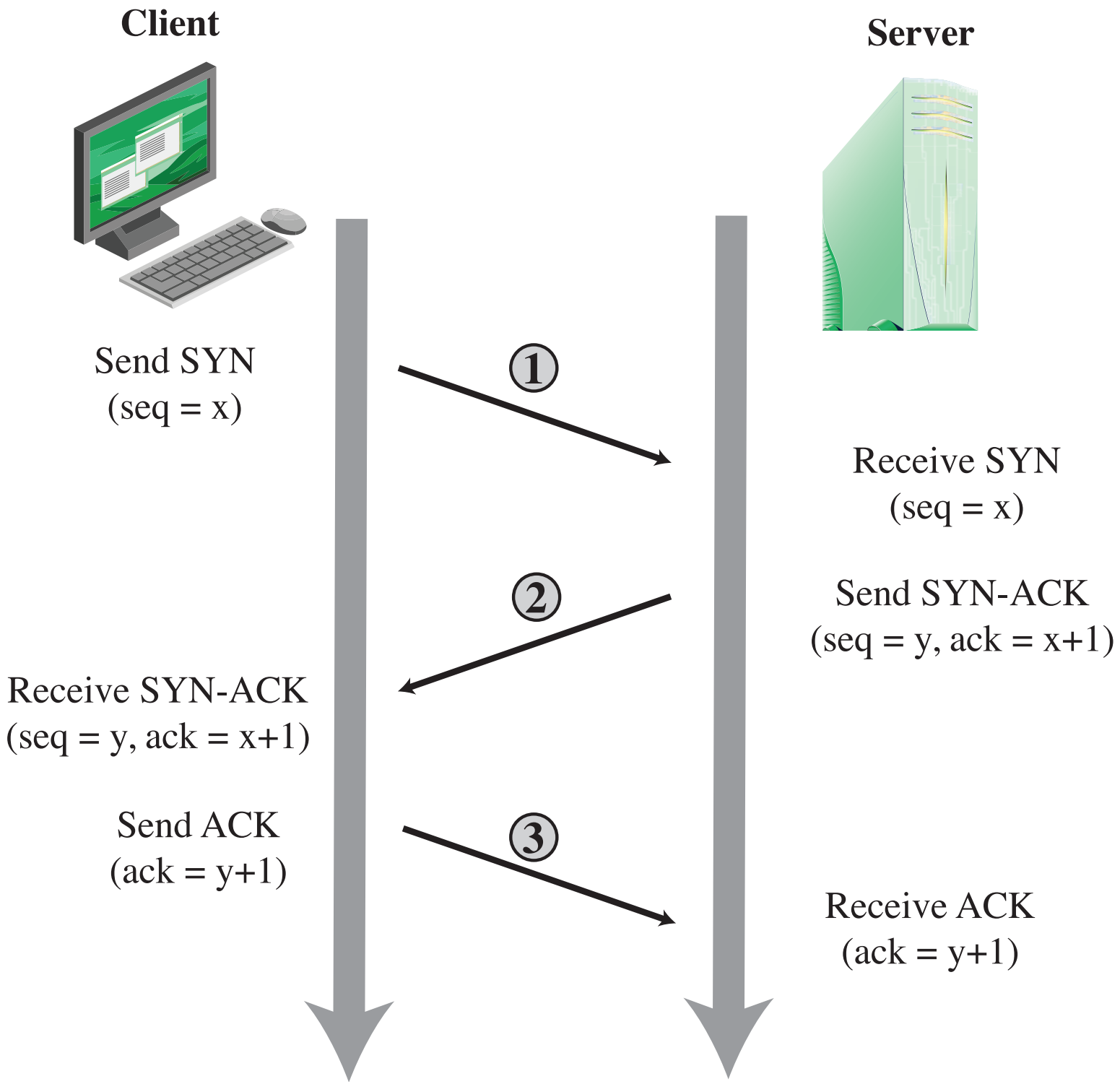
- Watch the Spoofer Video at:

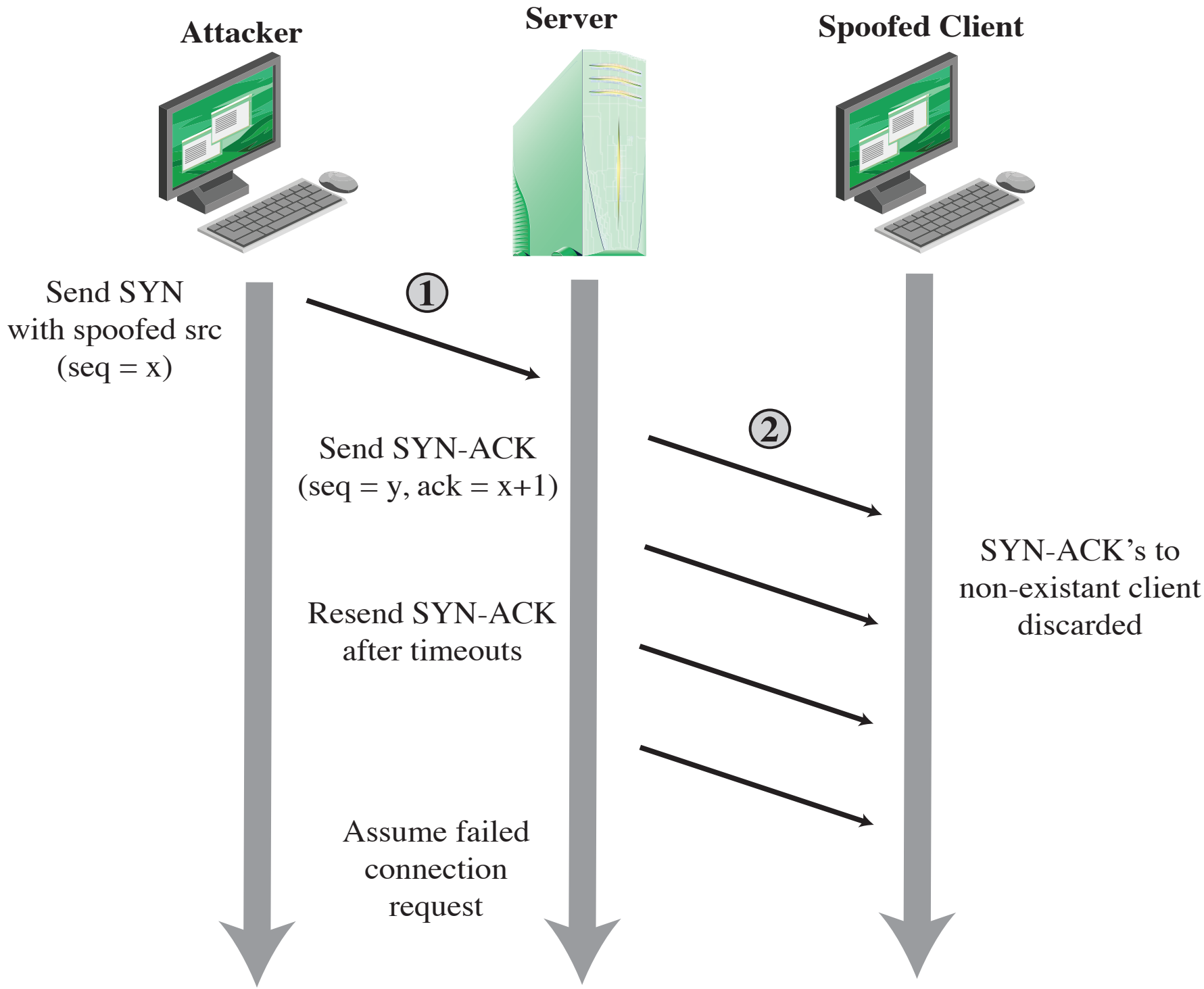
https://www.caida.org/projects/spoofer/

9

SYN Spoofing

- Common DoS attack
- Attacks the ability of a server to respond to future connection requests by overflowing the tables used to manage them
- Thus legitimate users are denied access to the server
- Hence an attack on system resources, specifically the network handling code in the operating system


Client
Server
Send SYN
(seq = x)
1
Receive SYN
(seq = x)
2
Send SYN-ACK
(seq = y, ack = x+1)
Receive SYN-ACK
(seq = y, ack = x+1)
Send ACK
(ack = y+1)
3
Receive ACK
(ack = y+1)


Attacker
Server
Spoofed Client
Send SYN
with spoofed src
(seq = x)
1
Send SYN-ACK
(seq = y, ack = x+1)
2
SYN-ACK's to
non-existant client
discarded
Resend SYN-ACK
after timeouts
Assume failed
connection
request

Flooding Attacks

- Classified based on network protocol used
- Intent is to overload the network capacity on some link to a server
- Virtually any type of network packet can be used

ICMP flood	• Ping flood using ICMP echo request packets • Traditionally network administrators allow such packets into their networks because ping is a useful network diagnostic tool
UDP flood	• Uses UDP packets directed to some port number on the target system
TCP SYN flood	• Sends TCP packets to the target system • Total volume of packets is the aim of the attack rather than the system code

Distributed Denial of Service (DDoS) Attacks

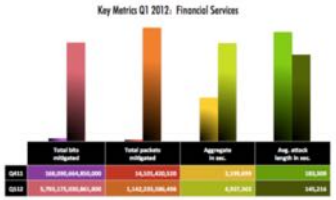
Use of multiple systems to generate attacks

Attacker uses a flaw in operating system or in a common application to gain access and installs their program on it (zombie)

Large collections of such systems under the control of one attacker's control can be created, forming a botnet

Distributed Denial Of Service

Distributed Denial of Service attacks render key systems and resources unavailable, effectively denying users access to the service



USA Today: *Why DDoS attacks continue to bedevil financial firms … adversaries may potentially be nation states …*

NY Times: *Attacks used the internet against itself to clog traffic Attack traffic exceeds 400 Gbps!*

eWeek: *DHS, FBI Warn of Denial-of-Service Attacks on Emergency Telephone Systems*

Current Advantage Favors Attackers:

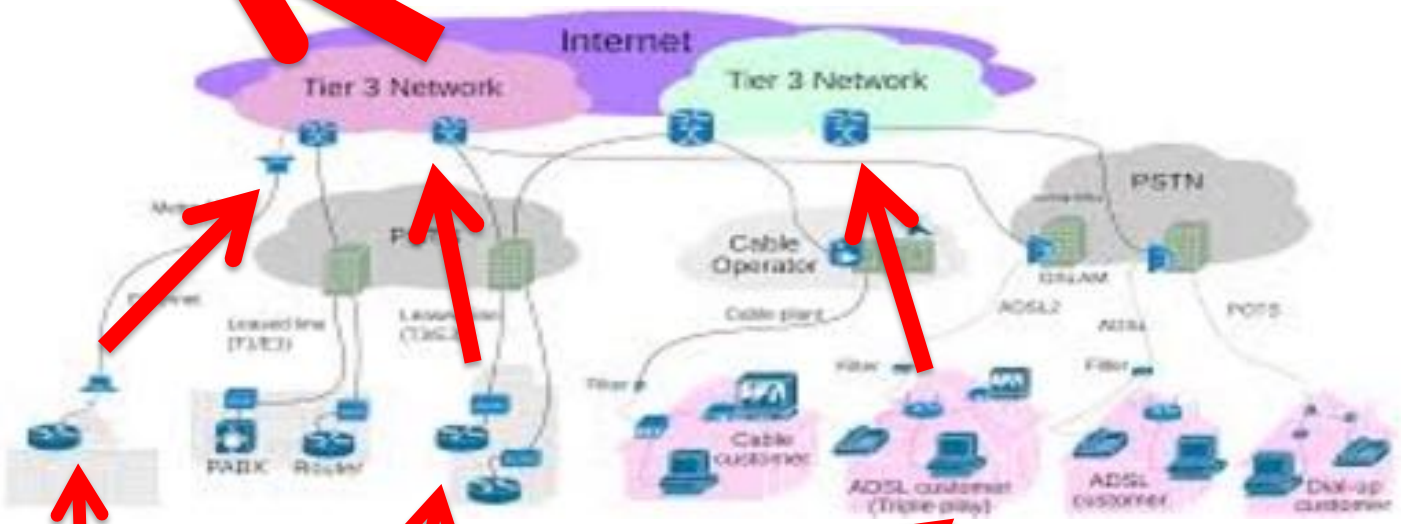
- *Attack resources are cheap compromised machines while defense requires provisioning*
- *Attackers easily cross boundaries while defense requires cross-organization collaboration*

Challenge: shift advantage in DDoS events toward defense

Problem: DDoS Attacks 101

Victim is overwhelmed. Examples include:
- 400 Gbps traffic to 10 Gbps access link
- Millions of requests to server designed for thousands
- Thousands 911 calls to system designed for hundreds

Both brute force and clever ways to overwhelm the target



Attack traffic originated from multiple locations throughout the Internet

Control Over Vast Number of Compromised Devices: Desktops, laptops, and even refrigerators!
http://thehackernews.com/2014/01/100000-refrigerators-and-other-home.html

Command and Control:
Nation State, Criminal Organization, Hactivist groups, etc.

Problem: Advantage Favors Attacks

Resources Costs Favor Attackers

- Attacks use large numbers of machines (millions) and send vast amounts of traffics (400 Gbps)
- Defense relies on marshaling more powerful systems that withstand attacks
- Attacker does not pay for computation or bandwidth while defenders purchase and deploy systems
- Known best practices can mitigate attacks but require multi-organizational actions and lack leadership

The ZeroAccess botnet, which is likely to have more than 1.9 million slave computers at its disposal….
http://news.cnet.com/8301-1009_3-57605411-83/symantec-takes-on-one-of-largest-botnets-in-history/

Distributed Nature Favor Attackers

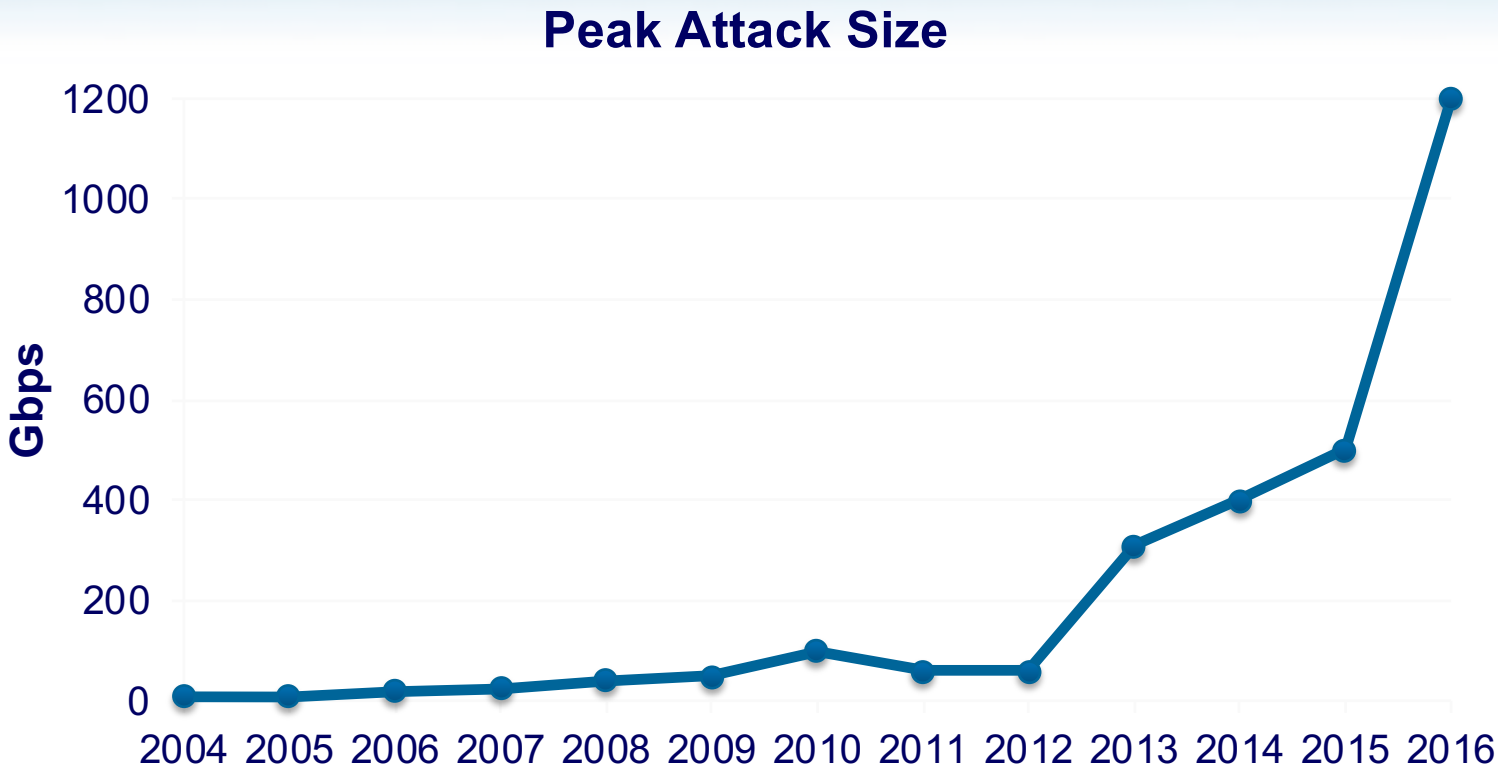
- Attacks use large numbers of systems, ***ignoring multiple organizational policies***
- Filtering at victim requires resources that can be overwhelmed by distributed attacks
- Lack of tools, collaboration mechanisms, and ***requirement to respect multiple polices*** make cross organization response difficult

Increased demand and new applications provide attackers with a target rich environment

- Attacks can succeed by disabling any key element, and defense must protect all elements
- Attacks will exploit future trends in mobile devices, emergency response systems, sensors, and so forth.
  http://www.eweek.com/security/dhs-fbi-warn-of-denial-of-service-attacks-on-emergency-telephone-systems/
- Defense is almost entirely reactive with little proactive research on next targets

17

Distributed Denial of Service (DDoS) Attacks Grow Size and Number



Source data: Arbor Networks Worldwide Infrastructure Security Report, and recent media reports

125% increase in DDoSD attacks year over year

Source data: Akamai's Q1 2016 State of the Internet

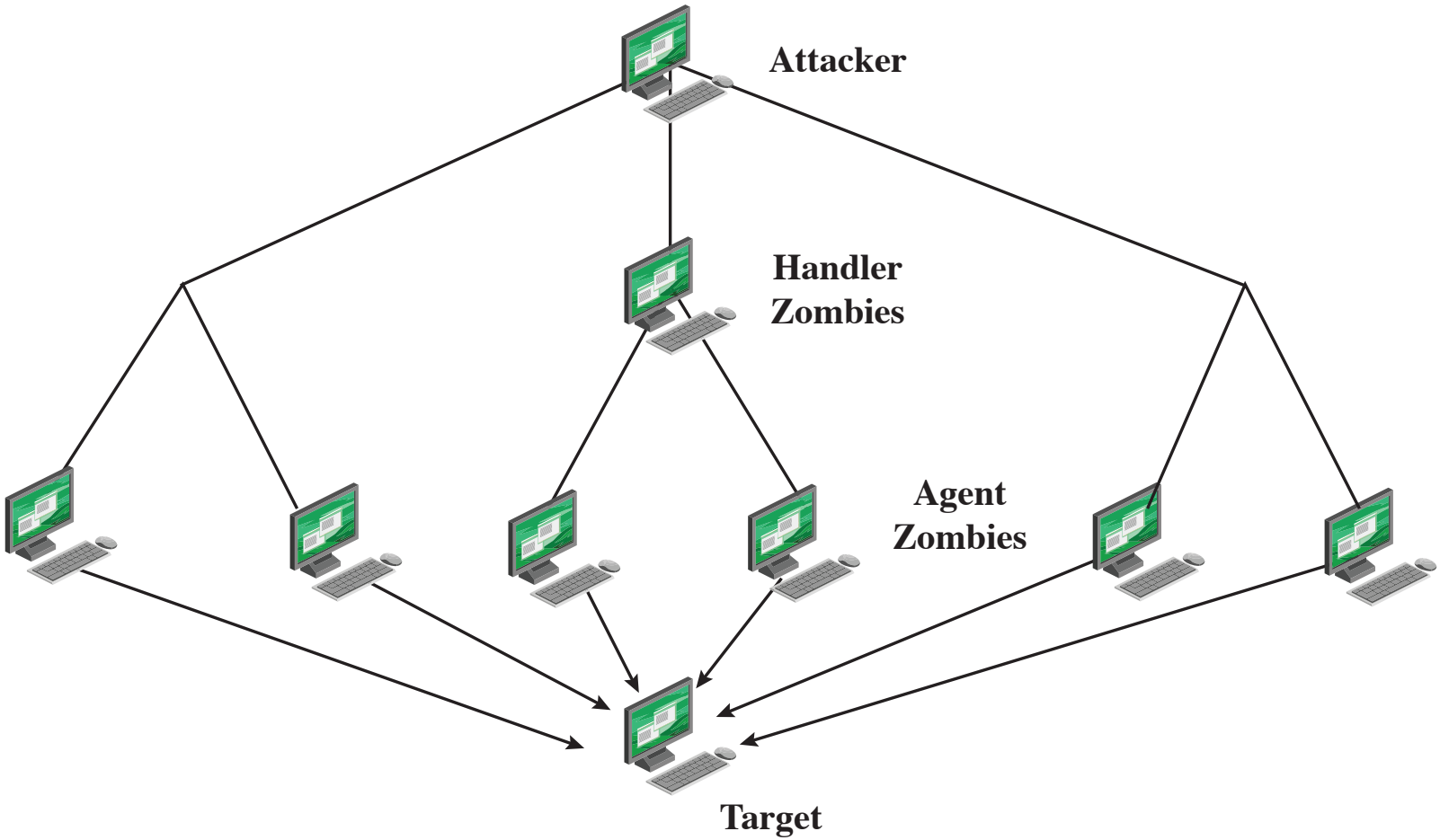


Figure 7.4 DDoS Attack Architecture

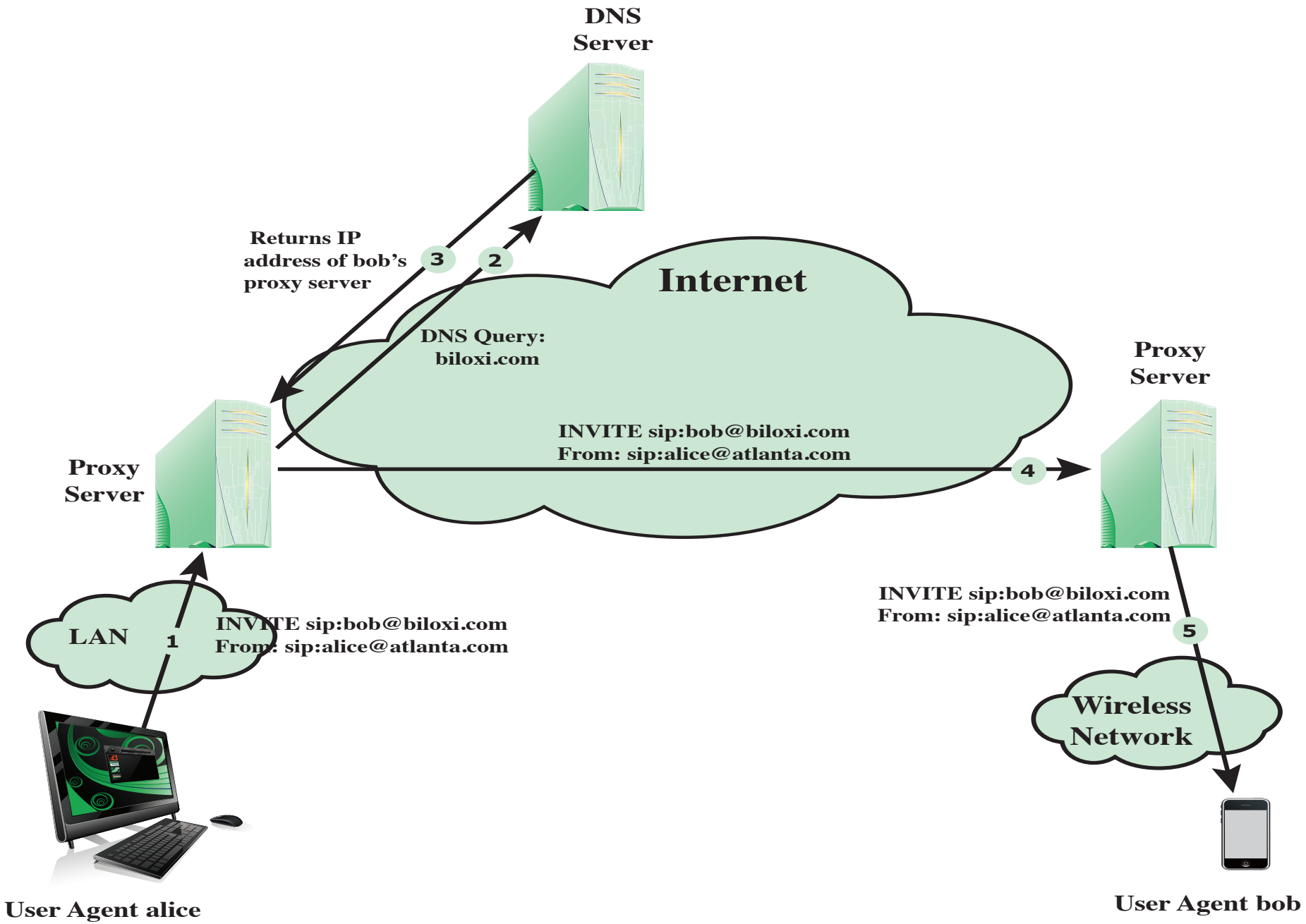


Figure 7.5 SIP INVITE Scenario

Hypertext Transfer Protocol (HTTP) Based Attacks

HTTP flood

- Attack that bombards Web servers with HTTP requests
- Consumes considerable resources
- Spidering
  - Bots starting from a given HTTP link and following all links on the provided Web site in a recursive way

Slowloris

- Attempts to monopolize by sending HTTP requests that never complete
- Eventually consumes Web server's connection capacity
- Utilizes legitimate HTTP traffic
- Existing intrusion detection and prevention solutions that rely on signatures to detect attacks will generally not recognize Slowloris

Reflection Attacks

- Attacker sends packets to a known service on the intermediary with a spoofed source address of the actual target system
- When intermediary responds, the response is sent to the target
- “Reflects” the attack off the intermediary (reflector)
- Goal is to generate enough volumes of packets to flood the link to the target system without alerting the intermediary
- The basic defense against these attacks is blocking spoofed-source packets

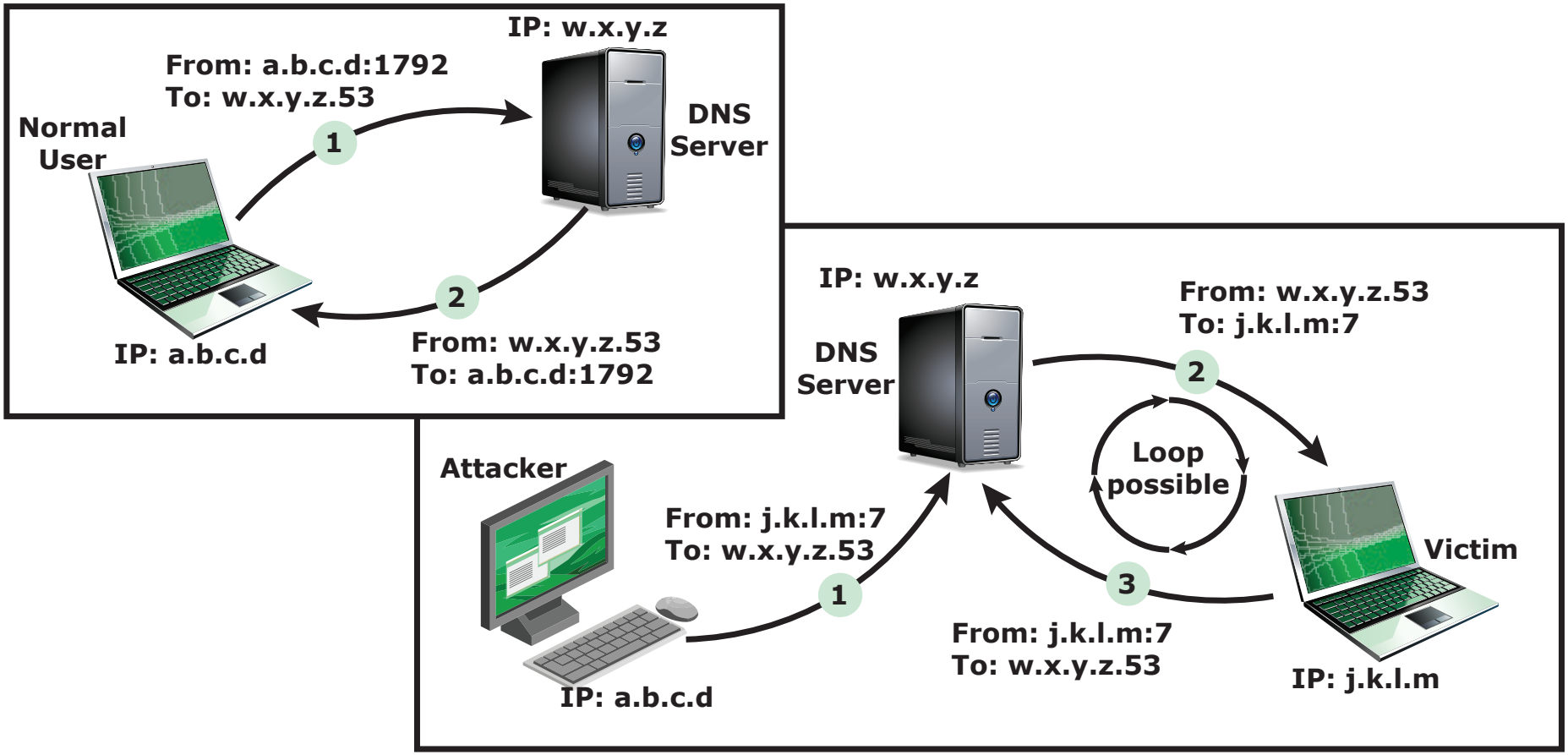


Figure 7.6 DNS Reflection Attack

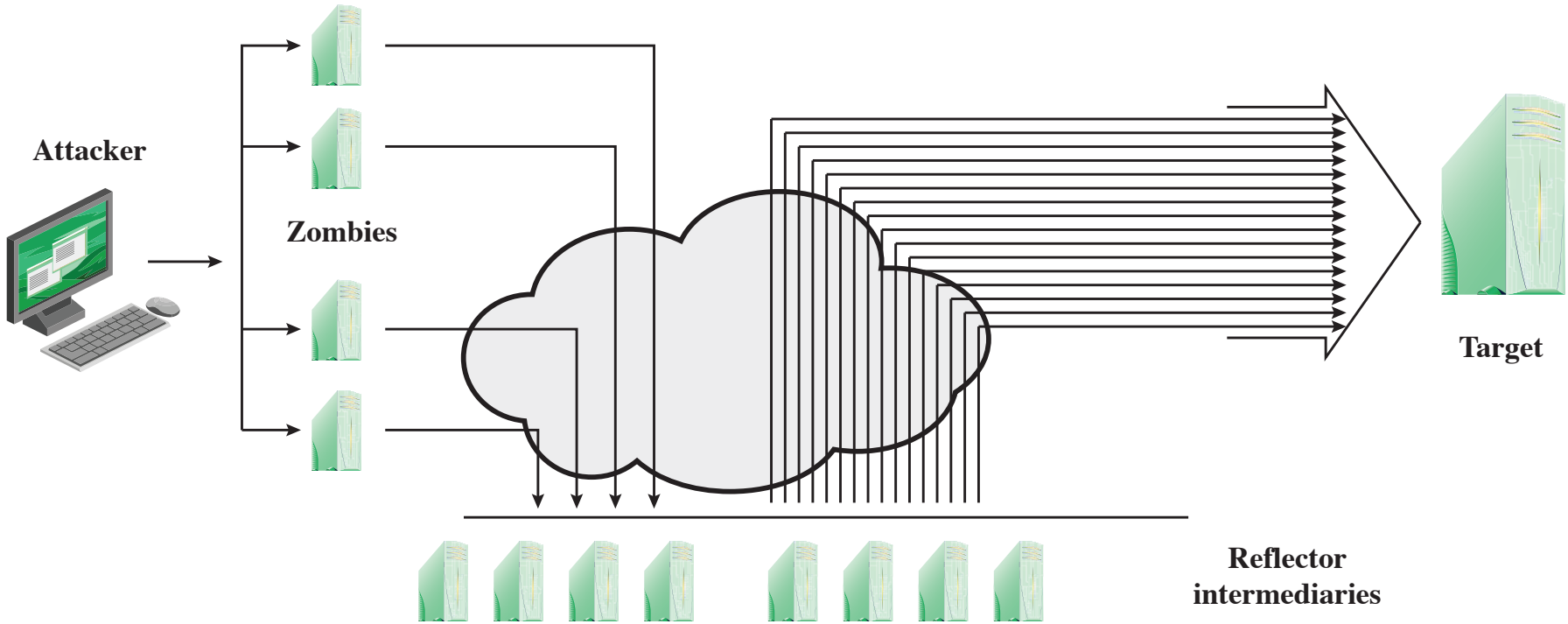
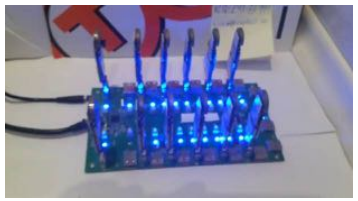


Figure 7.7 Amplification Attack

DNS Amplification Attacks

- Use packets directed at a legitimate DNS server as the intermediary system
- Attacker creates a series of DNS requests containing the spoofed source address of the target system
- Exploit DNS behavior to convert a small request to a much larger response (amplification)
- Target is flooded with responses
- Basic defense against this attack is to prevent the use of spoofed source addresses

TDoS Threat – Disable 911



Public Voice Network

TDM/SIP Trunks

Internet

Internet Connection

Firewall
IDS/IPS
DDoS Mitigation

UC Servers

CM VM CC Admin

Gate way DB TFTP DHCP DNS

TDM Phones

Modem

Fax

Voice VLAN

IP Phones

Data VLAN

UC Clients

Servers/PCs

911 Statistics

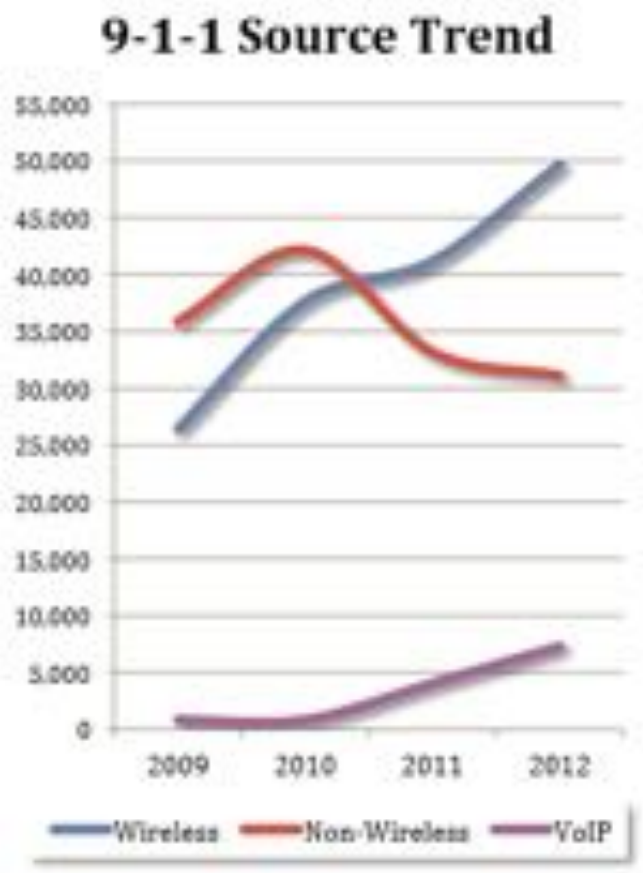
- There are **240 Million** calls to 9-1-1 each year, in some communities, 50% of those calls are made from a mobile device – NENA

2012 Annual Statistics

Telephone Statistics

Group	Incoming	Outgoing	Total Calls
911 – EMS	37,396	0	37,396
911 – Fire	7,691	0	7,691
911 – Law	49,315	0	49,315
Admin	41,531	9,7902	139,433
Business – EMS	20,805	26	20,831
Business – Fire	23,179	716	23,895
Business – Law	51,161	47	51,208
Emergency – EMS	21,514	1,172	22,686
Emergency – Fire	33,631	236	33,867
Emergency – Law	96,237	46	96,283
Microwave	8,957	17,687	26,644
Miscellaneous	10,659	8	10,667
Totals	**402,076**	**117,840**	**519,916**

Source: Overview of the San Mateo County Office of Public Safety Communications. 2012.



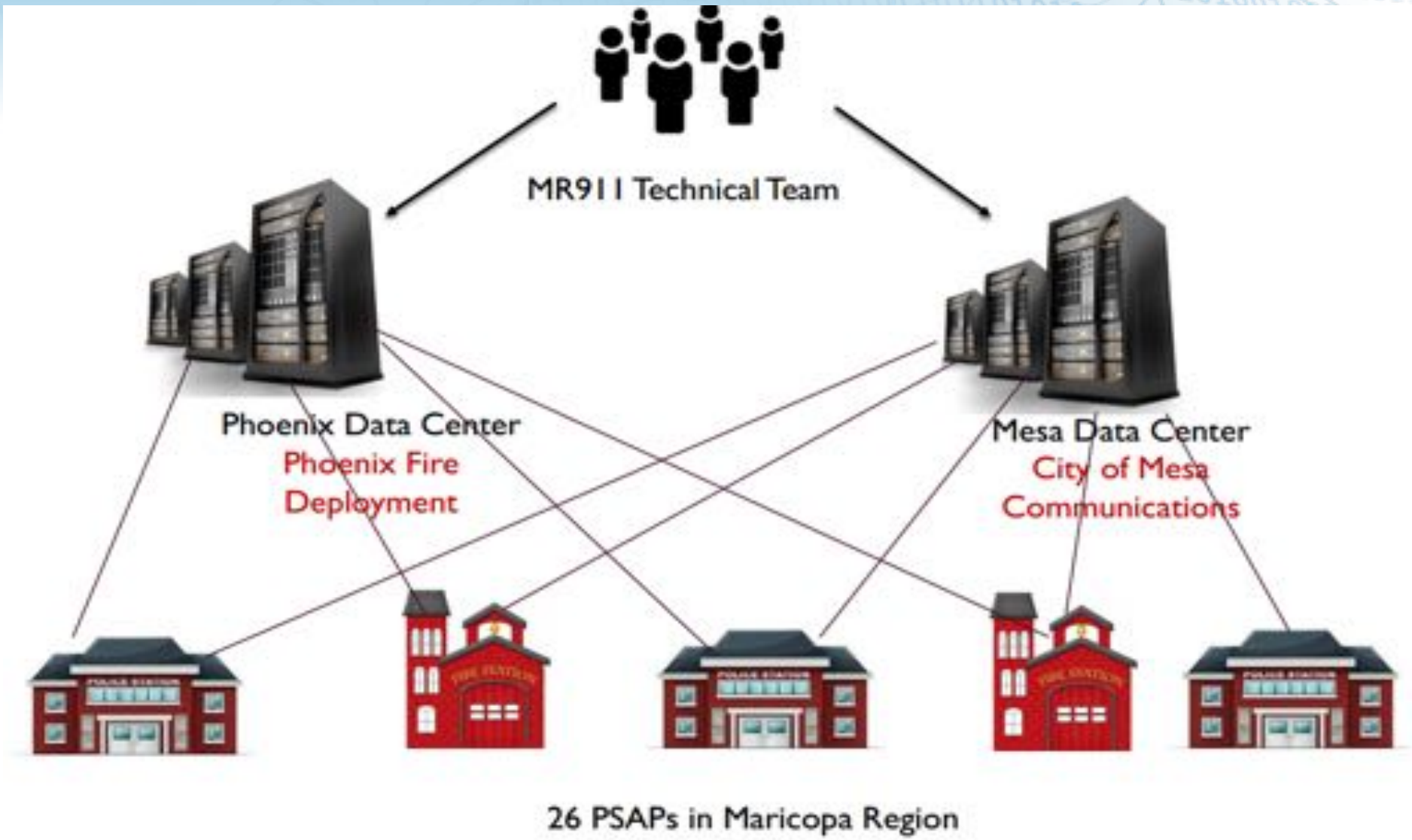
Current State of the Art from FCC

- *In 38 states, no money was spent in 2015 on cyber security for 9-1-1 centers.*
- *420 out of 6,500 9-1-1 centers had implemented a cyber security program.*

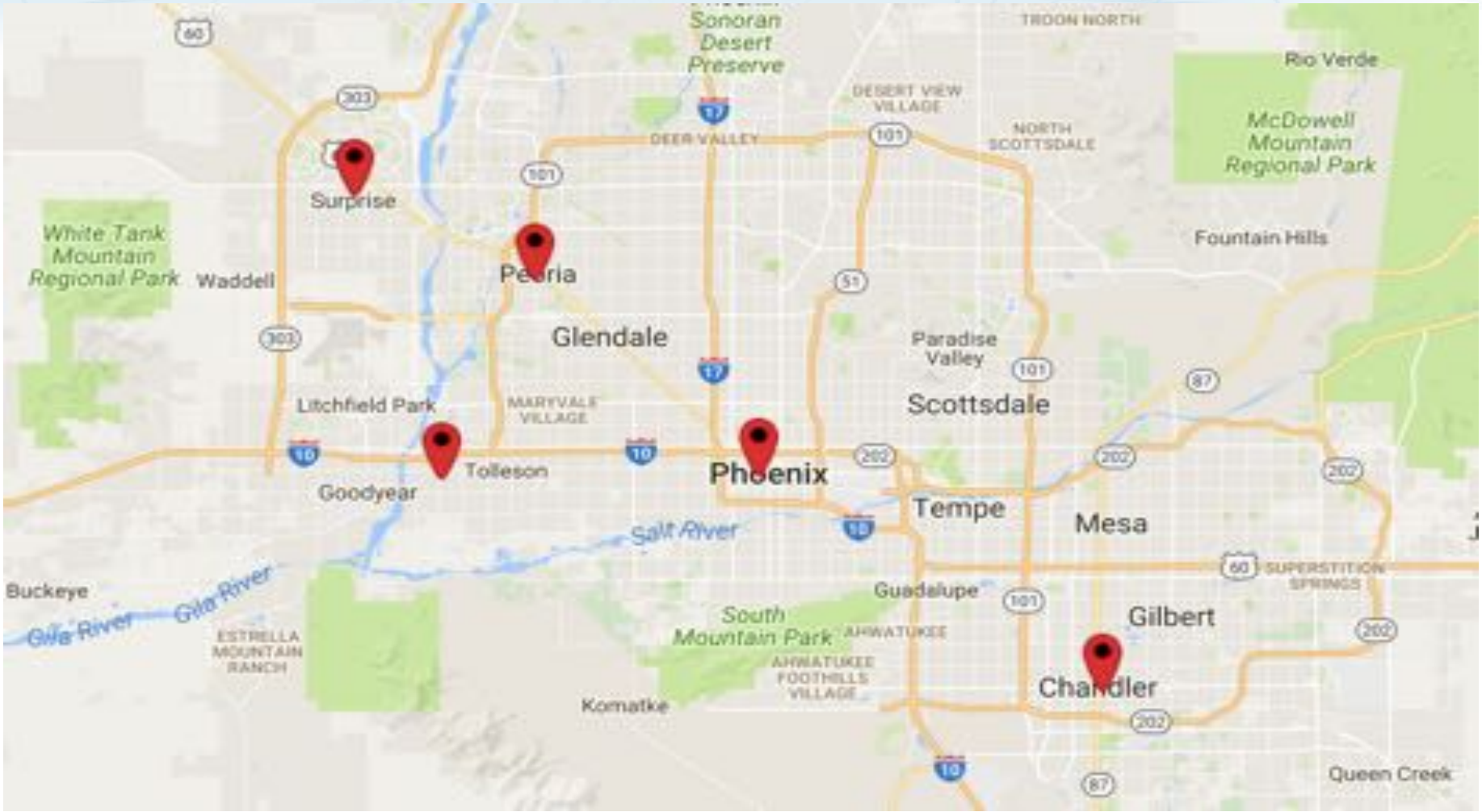
A Multi-State TDoS Attack on 9-1-1

- **INCIDENT:** *TDoS attack against PSAPS in multiple states.*
- **CAUSES:** *The attack was distributed/propagated through a Twitter mobile application.*
- **AFFECTED STATES:** *PSAPs in many states including Arizona, Texas, California, Florida, Washington State, Minnesota.*
- **DURATION:** *Approximately 10:00 p.m. on* ***October 25, 2016*** *– 2:00 a.m.* ***on October 26, 2016*** *local incident time.*

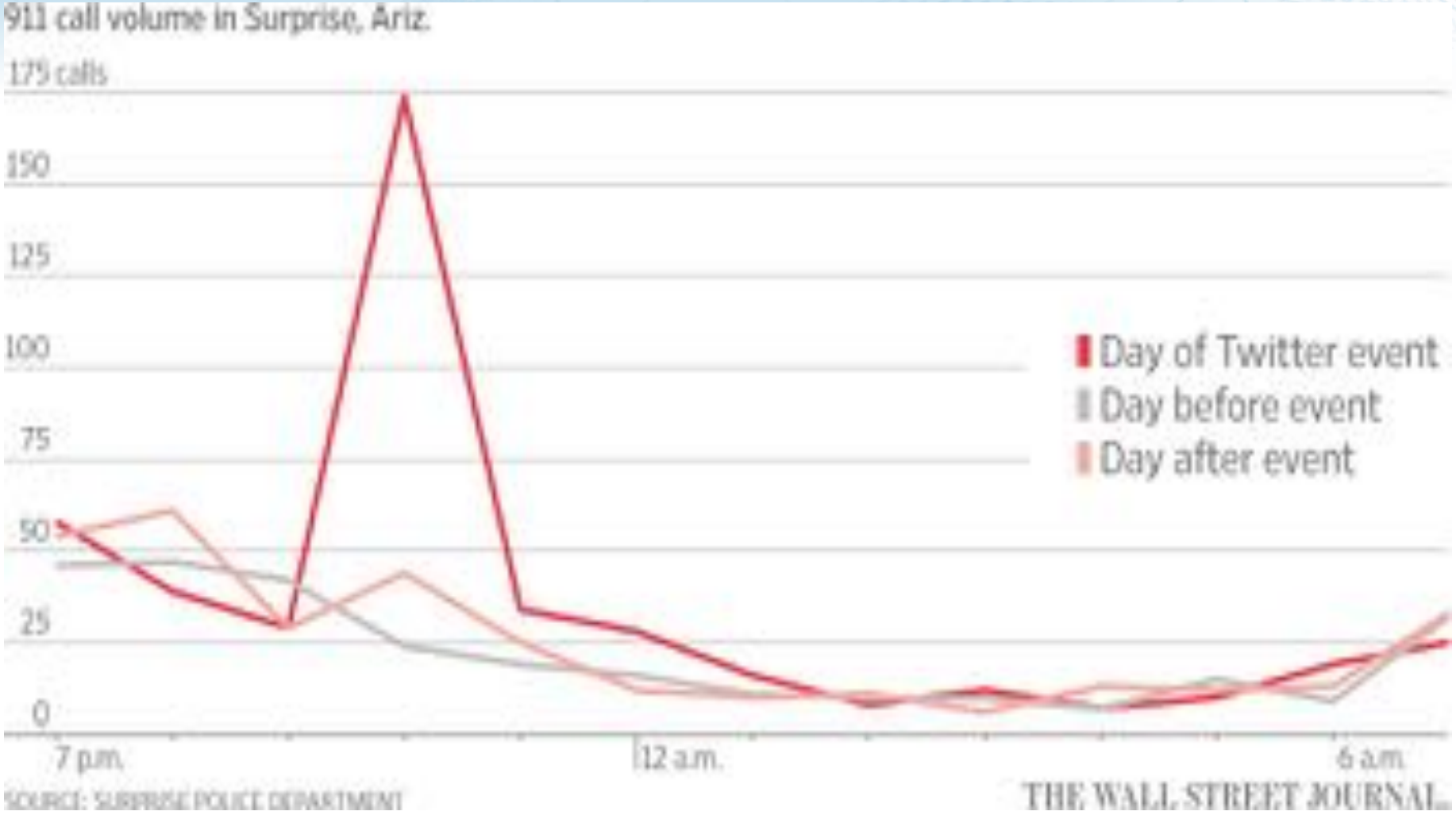
Maricopa Regional 9-1-1 Infrastructure



PSAPs in Maricopa Affected by the Oct TDoS Attack



Example Call Volume - Surprise, Ariz



The Oct 2016 Malware

- The TDoS malware exploits an iOS WebView auto dialer bug.
  - After clicking, the malware blocks the phone's UI.
  - It causes iOS to open a second application while the phone is dialing the given number.
  - User has no control to cancel the call.
- The bug was first discovered in 2008 by Collin Mulliner.
- It affects all iOS apps that embed WebView.
- The malware is written using Java script.

The Oct 2016 Attacker

- The code was first posted online by a teenage in *Phoenix*, *Arizona*.
- The original version was described in a Youtube video "Freak out your friends" without using 9-1-1 as the target phone number.
- The teenage made a 9-1-1 version, posted it online, and sent the link to the person who made the video.
- The link was added to the video's caption. The Youtube channel has 250K followers.
- Retweeted link including account with over 400K followers.

The Investigation

- Investigator confirmed identity of the teenage from screenshot of Internet speed test posted on social media website.

- The test records longitude and latitude information.

The picture on the right side is not the original one.

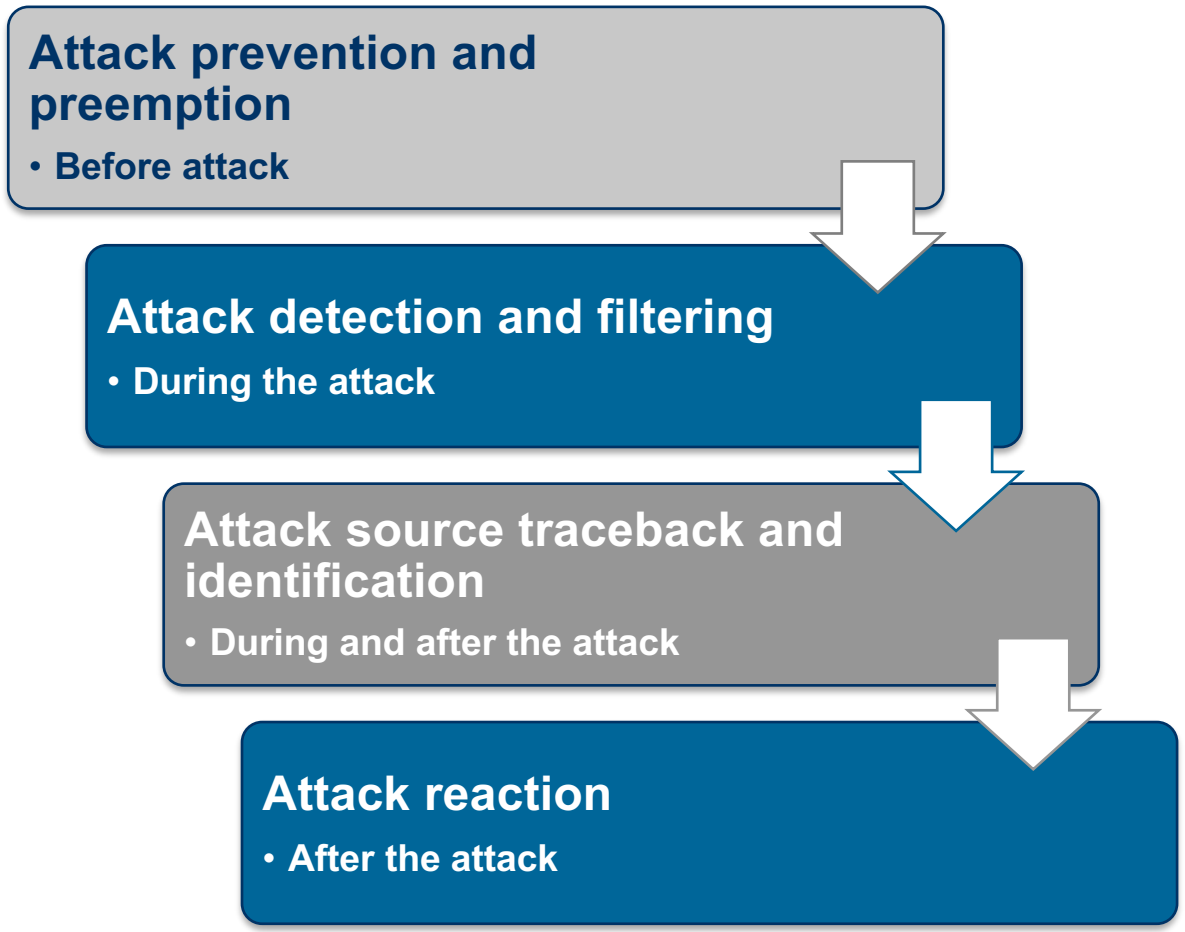
Lessons Learned

- TDoS caused by **mobile malware** poses a real threat.
- **Social media** can accelerate spread of the attack.
- The consequence could have be **much worse** if not from a teenage hacktivist.
- Similar attack could happen again in future.

DoS Attack Defenses

- These attacks cannot be prevented entirely
- High traffic volumes may be legitimate
  - High publicity about a specific site
  - Activity on a very popular site
  - Described as *slashdotted, flash crowd, or flash event*

Four lines of defense against DDoS attacks



Mitigating The DDoS Threat

(1) Measurement and Analysis to Promote Best Current Practices

Slow the growth in DDoS attacks by adopting best practices

(2) Tools for Communication and Collaboration

Provide existing targets more effective tools and techniques for response and mitigation.

(3) Novel DDoS Attack Mitigation and Defense Techniques

Anticipate new types of attacks before they occur and apply novel new approaches to mitigation.

DoS Attack Prevention

- Block spoofed source addresses
  - On routers as close to source as possible
- Filters may be used to ensure path back to the claimed source address is the one being used by the current packet
  - Filters must be applied to traffic before it leaves the ISP's network or at the point of entry to their network
- Use modified TCP connection handling code
  - Cryptographically encode critical information in a cookie that is sent as the server's initial sequence number
    - Legitimate client responds with an ACK packet containing the incremented sequence number cookie
  - Drop an entry for an incomplete connection from the TCP connections table when it overflows

DoS Attack Prevention

- Block IP directed broadcasts
- Block suspicious services and combinations
- Manage application attacks with a form of graphical puzzle (captcha) to distinguish legitimate human requests
- Good general system security practices
- Use mirrored and replicated servers when high-performance and reliability is required

Responding to DoS Attacks

Good Incident Response Plan

- Details on how to contact technical personal for ISP
- Needed to impose traffic filtering upstream
- Details of how to respond to the attack

- Antispoofing, directed broadcast, and rate limiting filters should have been implemented
- Ideally have network monitors and IDS to detect and notify abnormal traffic patterns

Responding to DoS Attacks

- Identify type of attack
  - Capture and analyze packets
  - Design filters to block attack traffic upstream
  - Or identify and correct system/application bug
- Have ISP trace packet flow back to source
  - May be difficult and time consuming
  - Necessary if planning legal action
- Implement contingency plan
  - Switch to alternate backup servers
  - Commission new servers at a new site with new addresses
- Update incident response plan
  - Analyze the attack and the response for future handling

Summary

- Denial-of-service attacks
  - The nature of denial-of-service attacks
  - Classic denial-of-service attacks
  - Source address spoofing
  - SYN spoofing
- Flooding attacks
  - ICMP flood
  - UDP flood
  - TCP SYN flood
- Defenses against denial-of-service attacks
- Responding to a denial-of-service attack
- Distributed denial-of-service attacks
- Application-based bandwidth attacks
  - SIP flood
  - HTTP-based attacks
- Reflector and amplifier attacks
  - Reflection attacks
  - Amplification attacks
  - DNS amplification attacks

Heilmeier Questions

- What are you trying to do? Articulate your objectives using absolutely no jargon.
- How is it done today, and what are the limits of current practice?
- What is new in your approach and why do you think it will be successful?
- Who cares? If you succeed, what difference will it make?
- What are the risks?
- How much will it cost?
- How long will it take?
- What are the mid-term and final “exams” to check for success?