CMPE 209 Network Security

Denial-of-Service Attacks (Chapter 7)

Dr. Younghee Park

SAN JOSÉ STATE UNIVERSITY

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

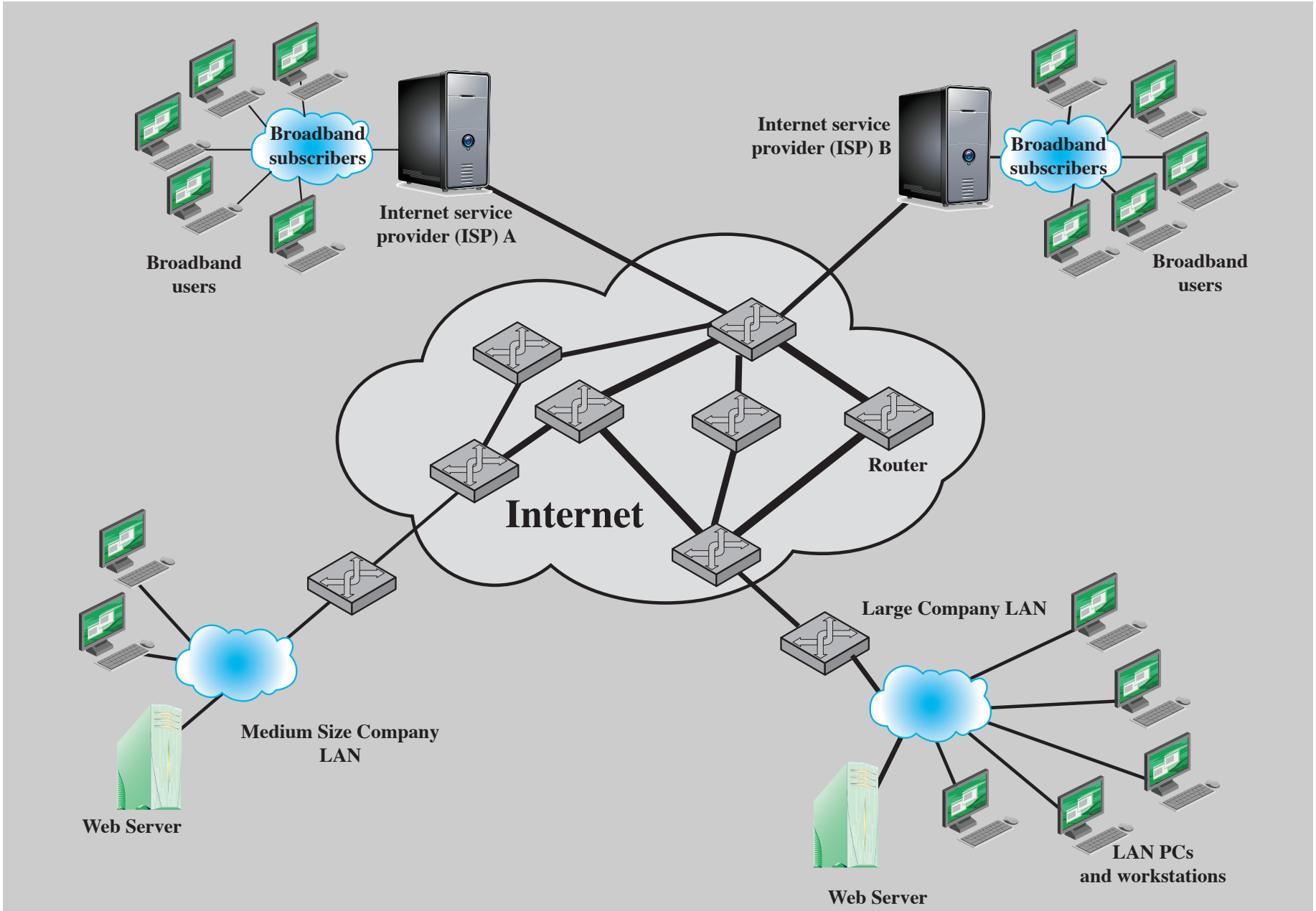
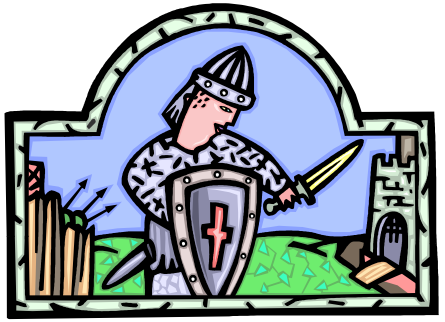


Figure 7.1 Example Network to Illustrate DoS Attacks

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

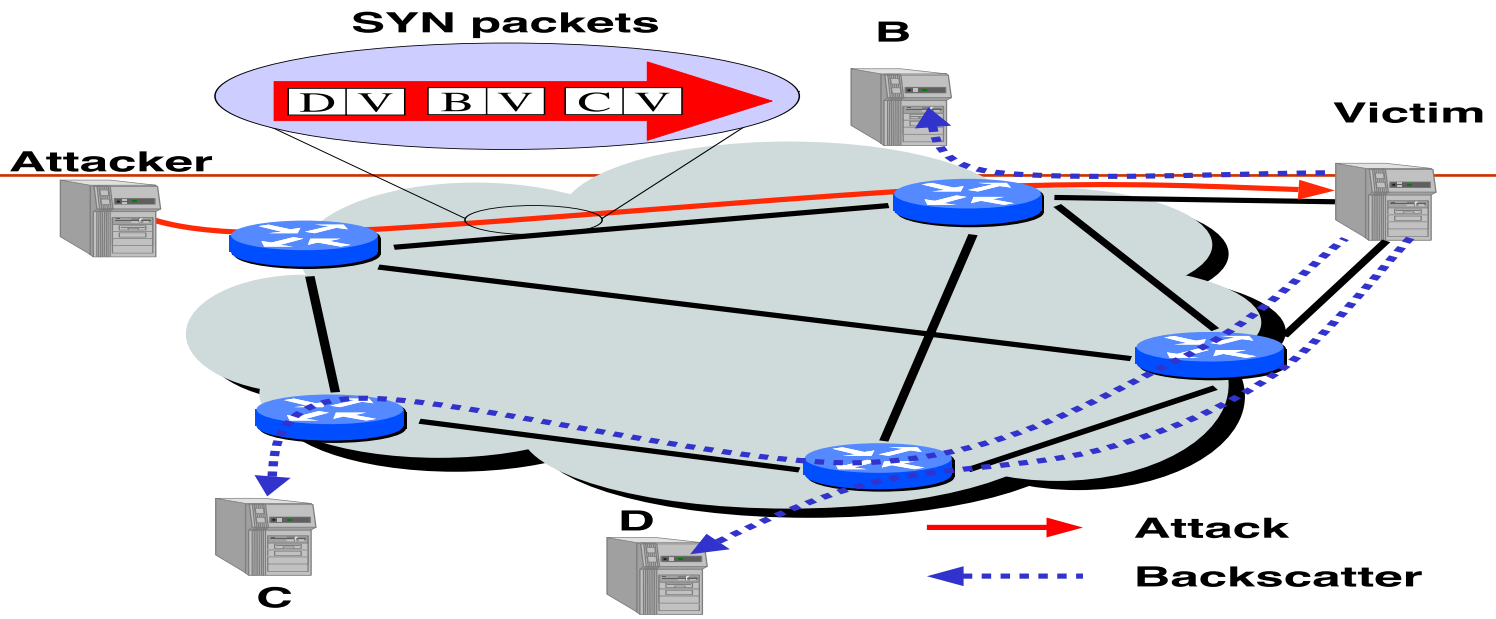


Figure 1: An illustration of backscatter in action. Here the attacker sends a series of SYN packets towards the victim V, using a series of random spoofed source addresses: named C, B, and D. Upon receiving these packets the victim responds by sending SYN/ACKs to each of spoofed hosts.

Backscatter is a term coined by Vern Paxson to describe Internet background noise resulting from a DDoS attack using multiple spoofed addresses.This backscatter noise is used by network telescopes to indirectly observe large scale attacks in real time.

Vern Paxson's paper: Inferring Internet Denial-of-Service Activity

SYN Flooding using 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

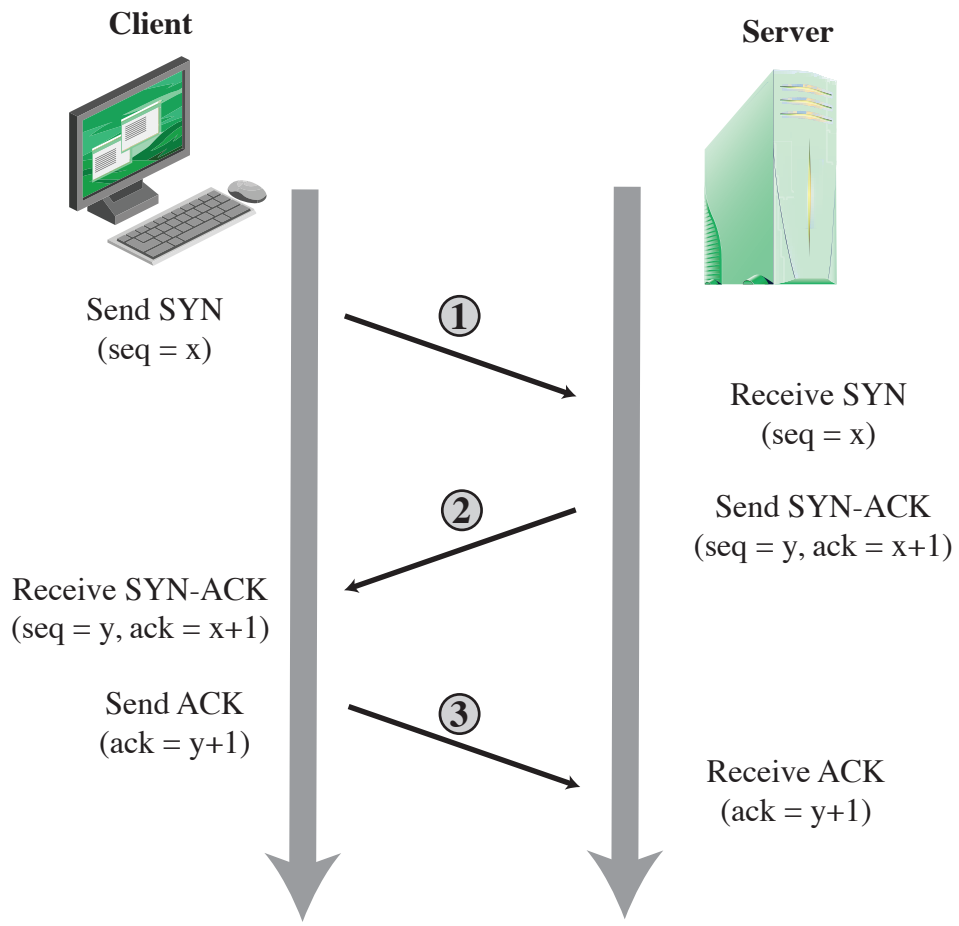


Figure 7.2 TCP Three-Way Connection Handshake

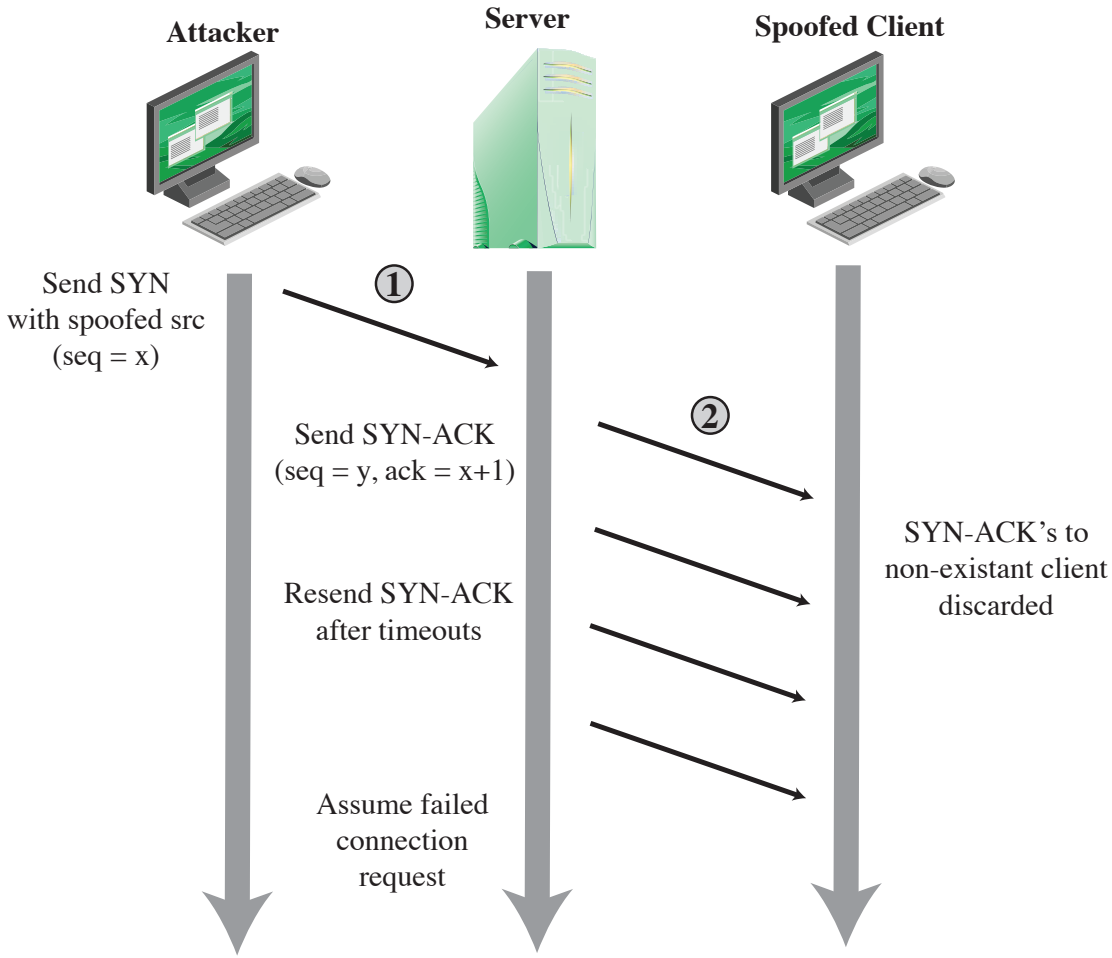


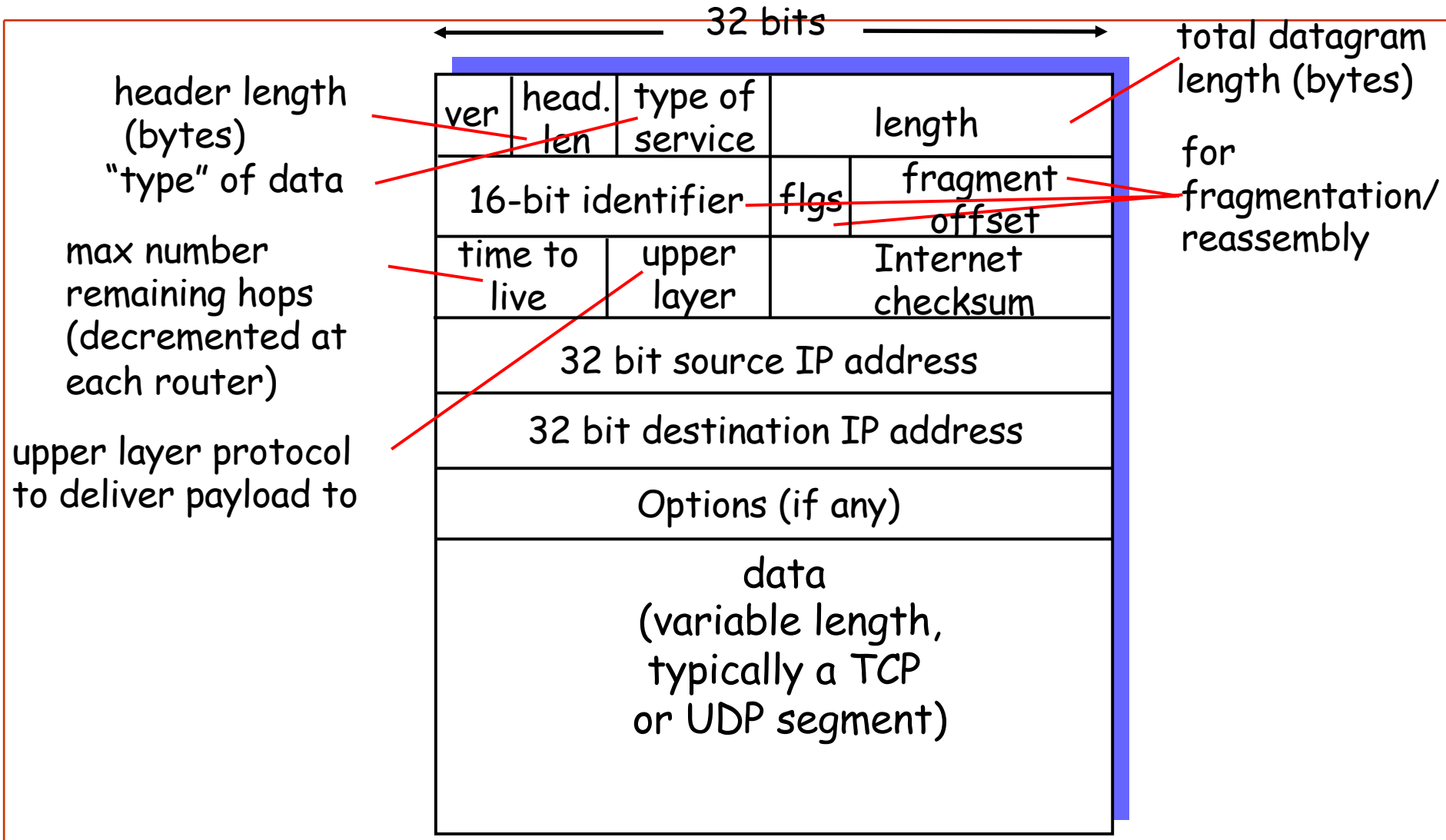
Figure7.3 TCP SYN Spoofing Attack

IP spoofing with TCP?

- Can an attacker make a TCP connection to server with a spoofed IP address?
- SYN/ACK and any subsequent packets sent to spoofed address.
- If attacker can guess initial sequence number, can attempt to send commands
  - Send ACK with spoofed IP and correct seq #, say, one second after SYN
- But TCP uses random initial sequence numbers.
- Demo: https://www.youtube.com/watch?v=P_y9MdFTgv0

```
$ sudo iptables -t nat -A POSTROUTING -j SNAT --to-source 1.1.1.1
```

Interlude: IP datagram format



Ping of Death

- ICMP Echo Request (Ping) is 56 bytes
- If a ping message is more than 65536 bytes (max for IP packet), this can cause some machines to crash
- Older windows systems

Solution: patch OS, filter out ICMP packets

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

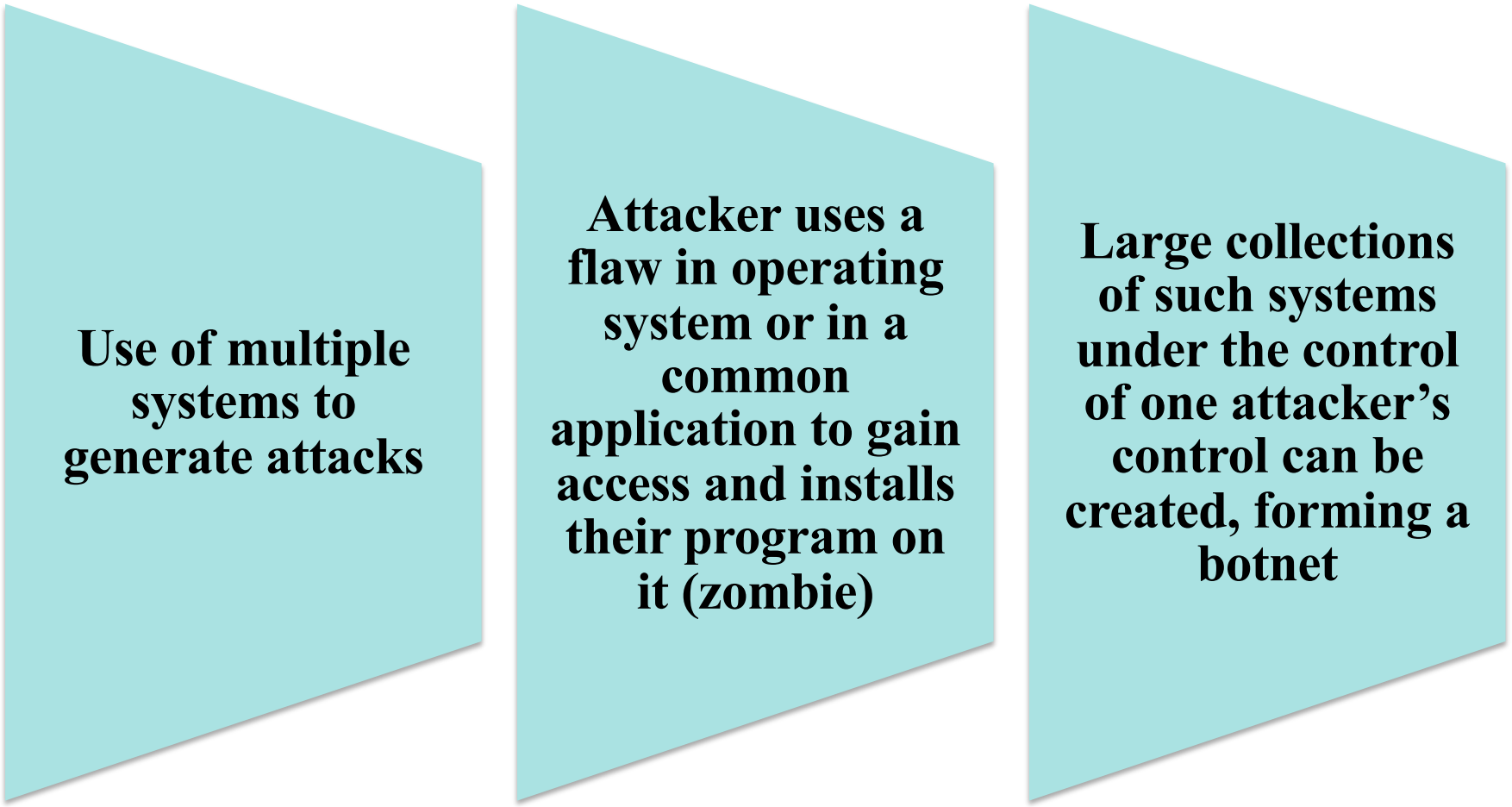
UDP flood

- 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



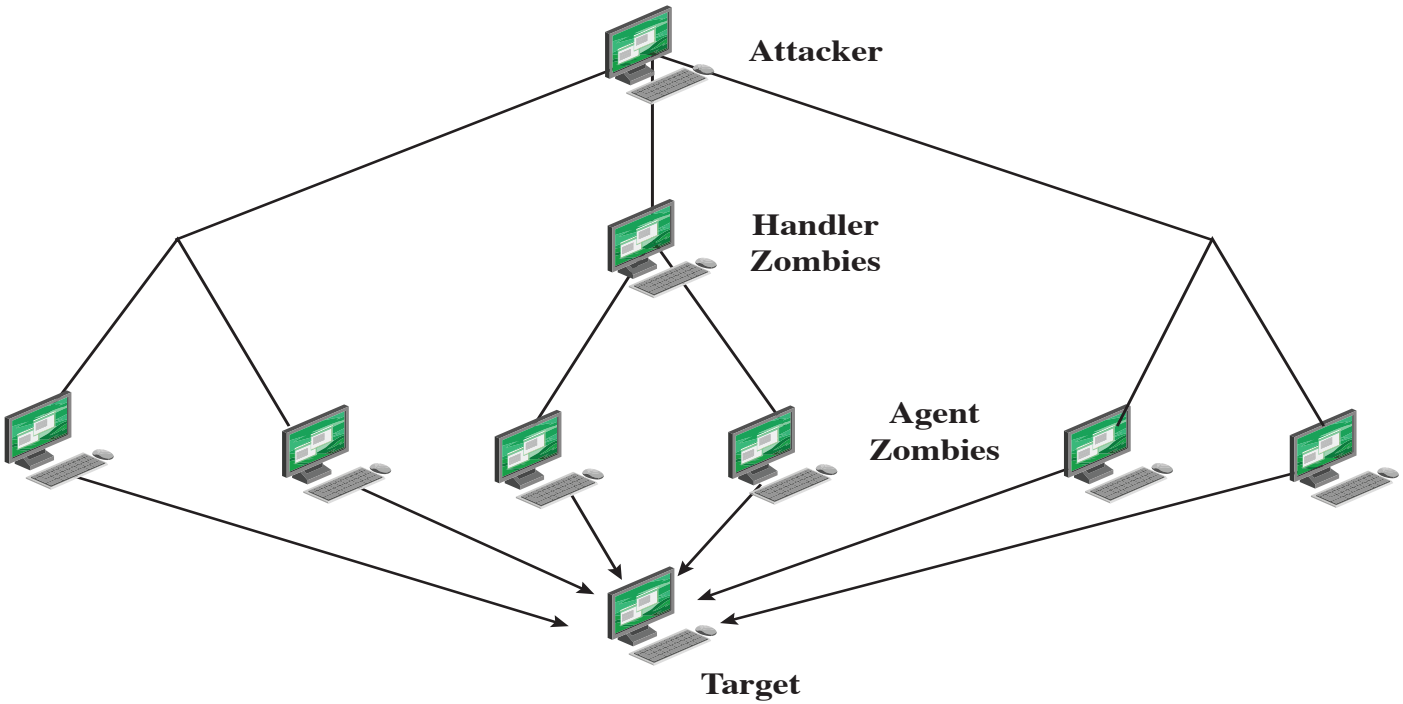
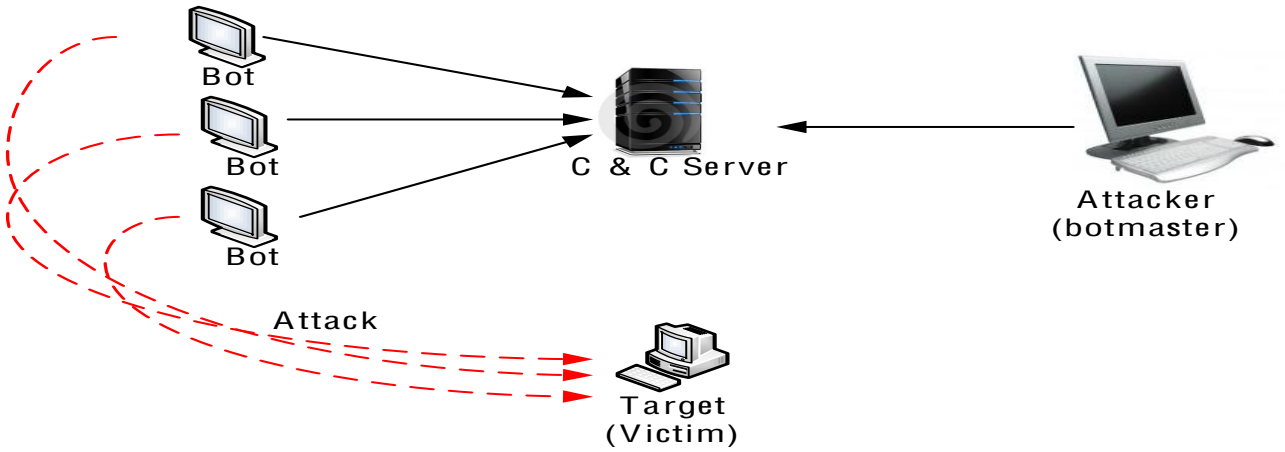


Figure 7.4 DDoS Attack Architecture

Botnets

- A network of compromised hosts (i.e. bots), pose serious threats to the Internet.
  - Botmaster/Bot commands/Bots
  - DDoS, Spam, identify theft, phishing, etc.
  - IRC-based, P2P-based, HTTP-based botnets



An example of bot command in IRC

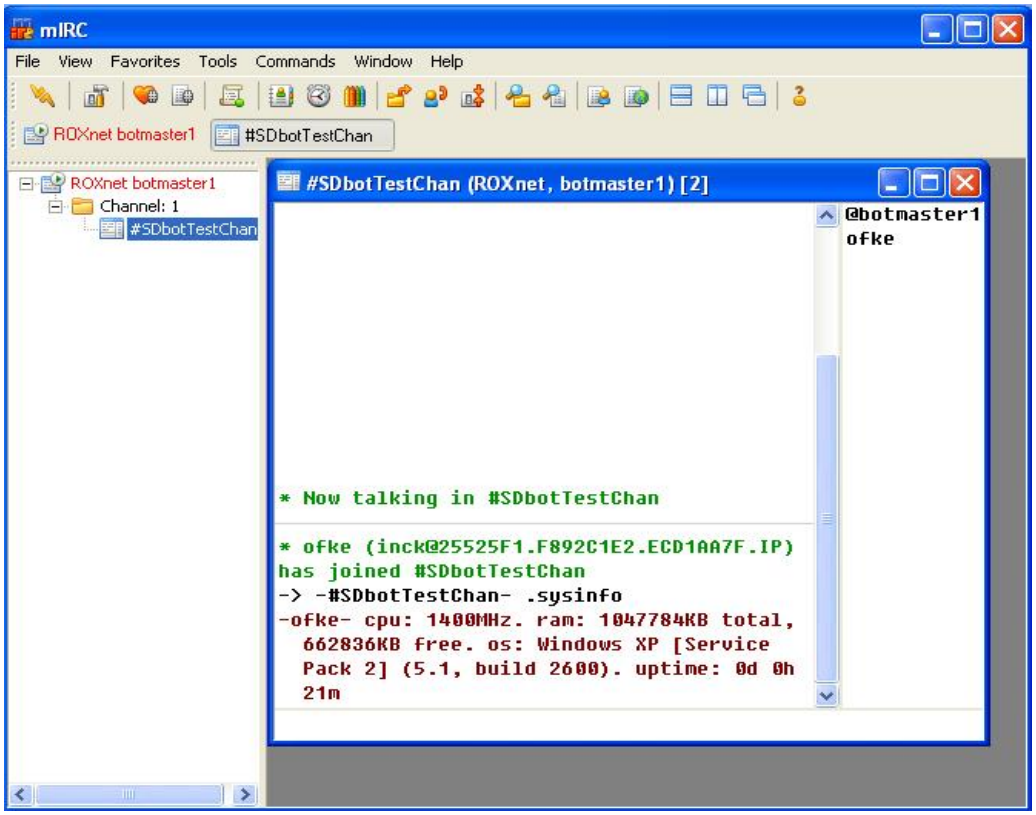


Figure 1.2: An example of the execution of a bot command ("sysinfo") for SDBot in IRC-based Botnets

Bot Commands

Table 4.1: Classification for bot commands

General Commands	Host Control Commands
login/logout, reconnect, id alias, action, join, part privmsg, mode, cmdlist about/version, disconnect nick, rndnick, status, quit	remove/die, clone, open, delete sysinfo, shutdown, listprocess passwords, killthread, killprocess execute, sendkey/getcdkey keylogger, threads, opencmd
Network Control Commands	**Attack Commands**
server, netinfo, download, update, dns redirect, httpd/httpserver scan, visit	synflood, updflood httpflood, pingflood email

Botnet Defenses

- Traceback to Botmaster
- Bot Command Detection
- Bot Detection
- Botnet Protocol/Phenomena Understanding
- C&C Channel Detection
- Various mitigation methods against botnet-driven threats

Hypertext Transfer Protocol (HTTP) Based Attacks

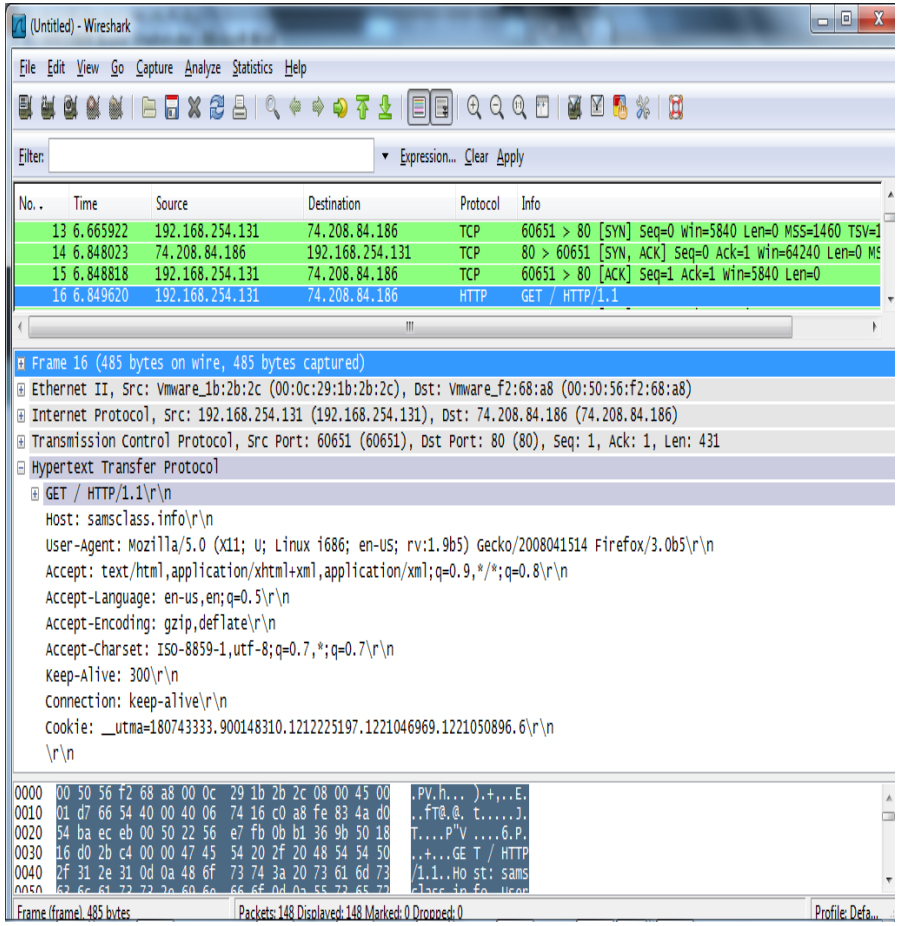
HTTP Flood

- 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
- https://www.youtube.com/watch?v=BzgsT-_GC4Q

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
- https://www.youtube.com/watch?v=XRi_xf53QU0

Slowloris



In http protocol, a blank line after the header's is used to represent the completion of the header.

Slowloris tool takes advantage of this in implementing its attack. It does not send a finishing blank line, which indicates the end of the http header.

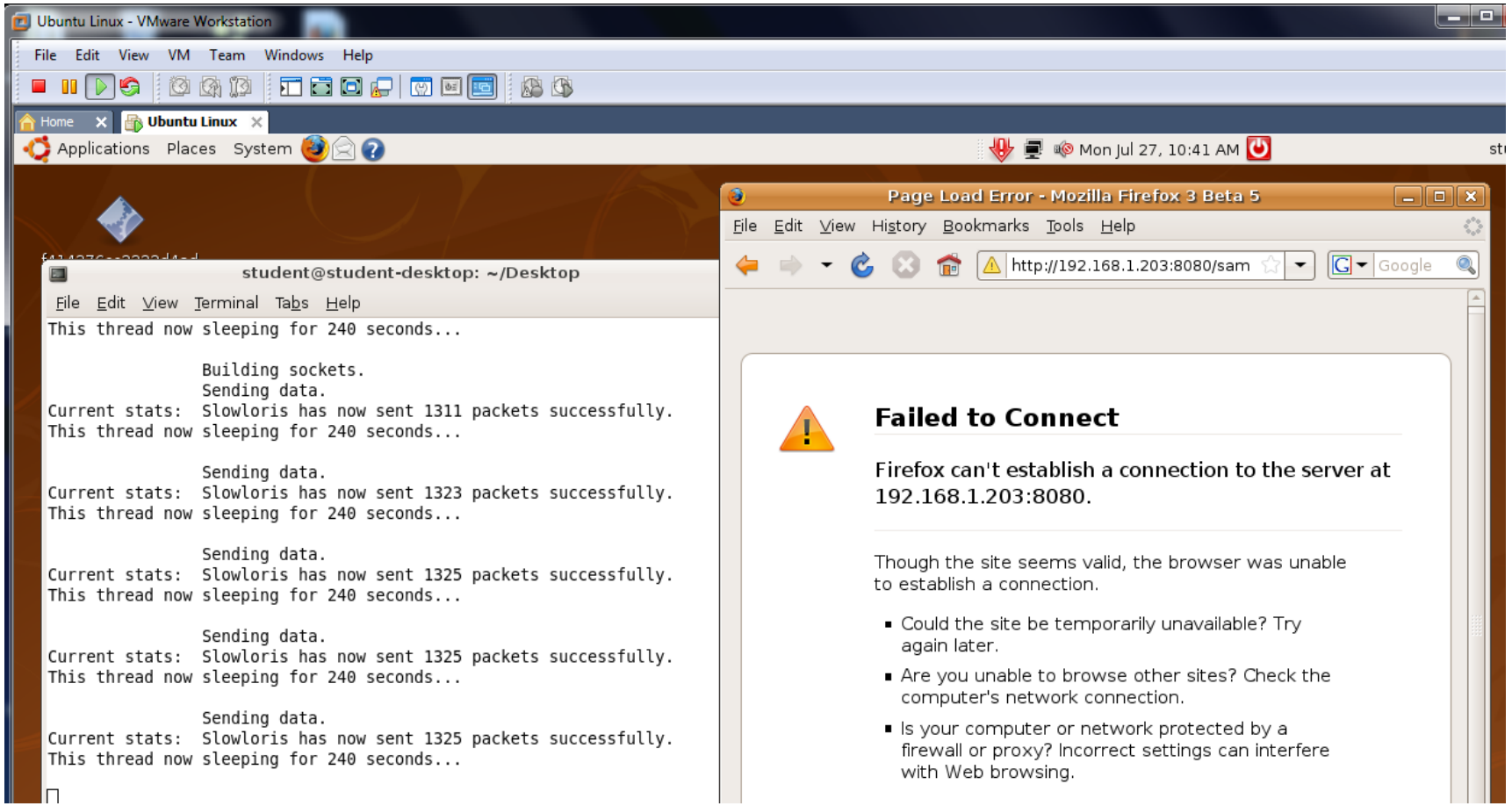
Slowloris

- A piece of software written by Robert "RSnake" Hansen which allows a single machine to take down another machine's web server with minimal bandwidth and side effects on unrelated services and ports
- Send incomplete HTTP requests
  - Apache has a queue of approx. 256 requests
  - Each one waits approx. 400 seconds by default for the request to complete
  - So less than one packet per second is enough to occupy them all
  - Low-bandwidth DoS--no collateral damage!
- Extra reading: https://en.wikipedia.org/wiki/Slowloris_(computer_security)

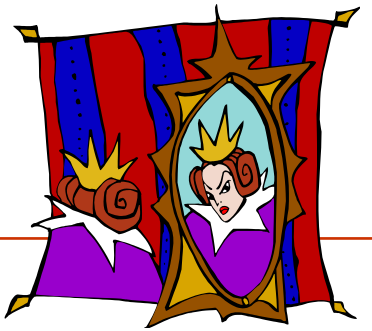
Slowloris

OSI Model	DoS Attack
7 Application	Slowloris – Incomplete HTTP Requests
6 Presentation	
5 Session	
4 Transport	SYN Flood – Incomplete TCP Handshakes
3 Network	
2 Data Link	
1 Physical	Cut a cable

Slowloris (Demo)



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

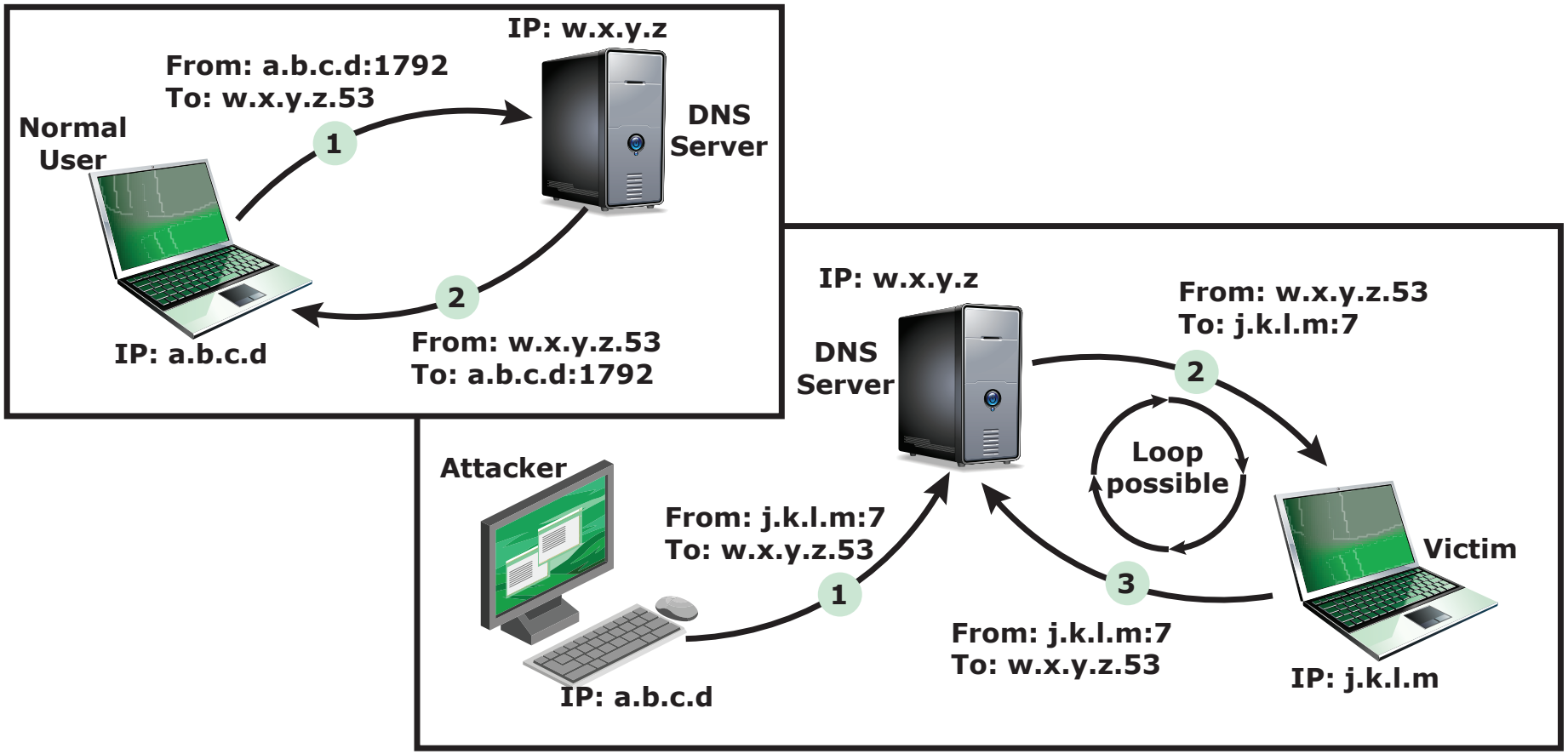
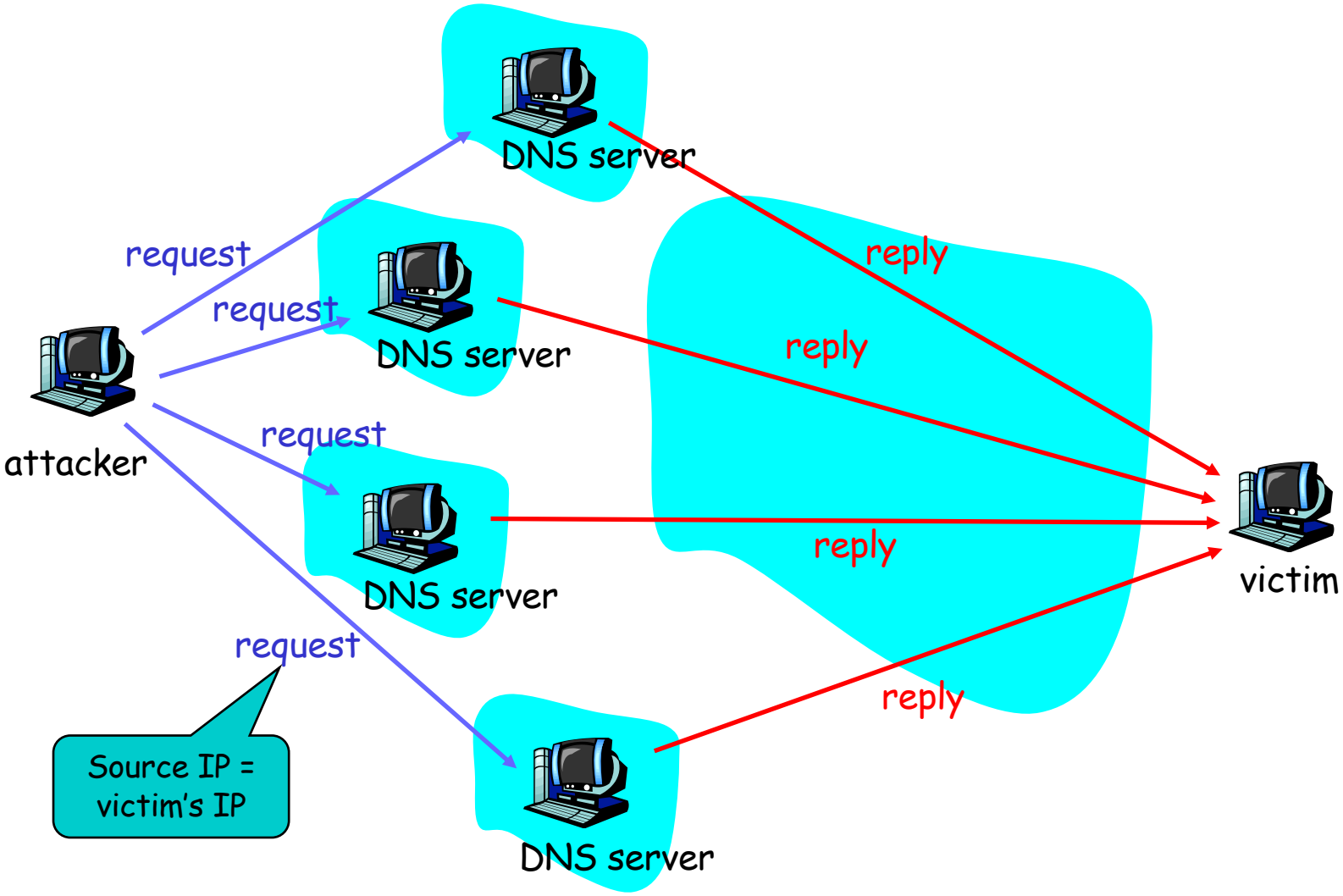


Figure 7.6 DNS Reflection Attack

DDoS: Reflection attack



- Amplification attacks are a **variant of reflector attacks** and also involve sending a packet with a spoofed source address for the target system to intermediaries.
- Generate multiple response packets for each original packet sent. This can be achieved by directing the original request to the broadcast address for some network.

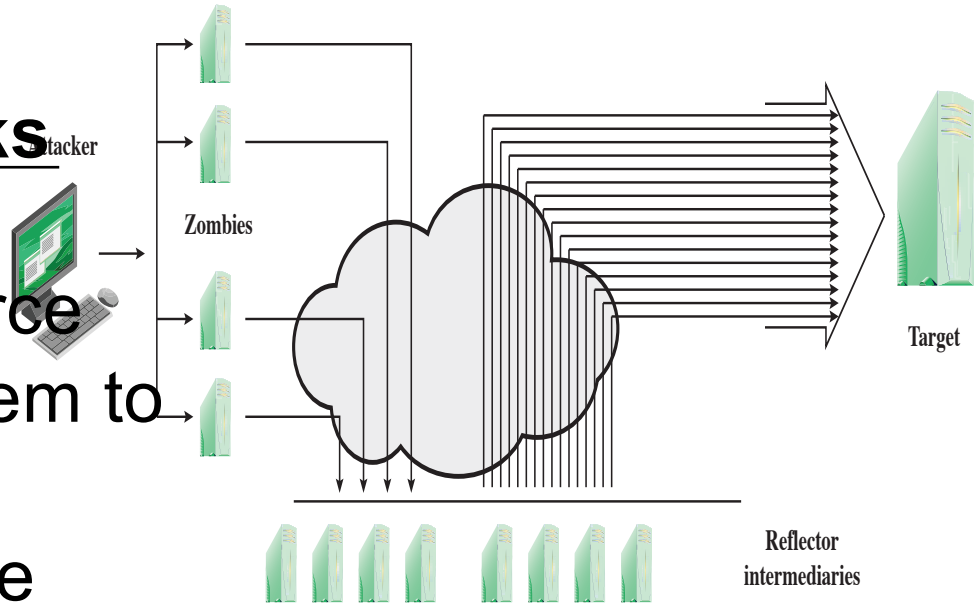


Figure 7.7 Amplification Attack

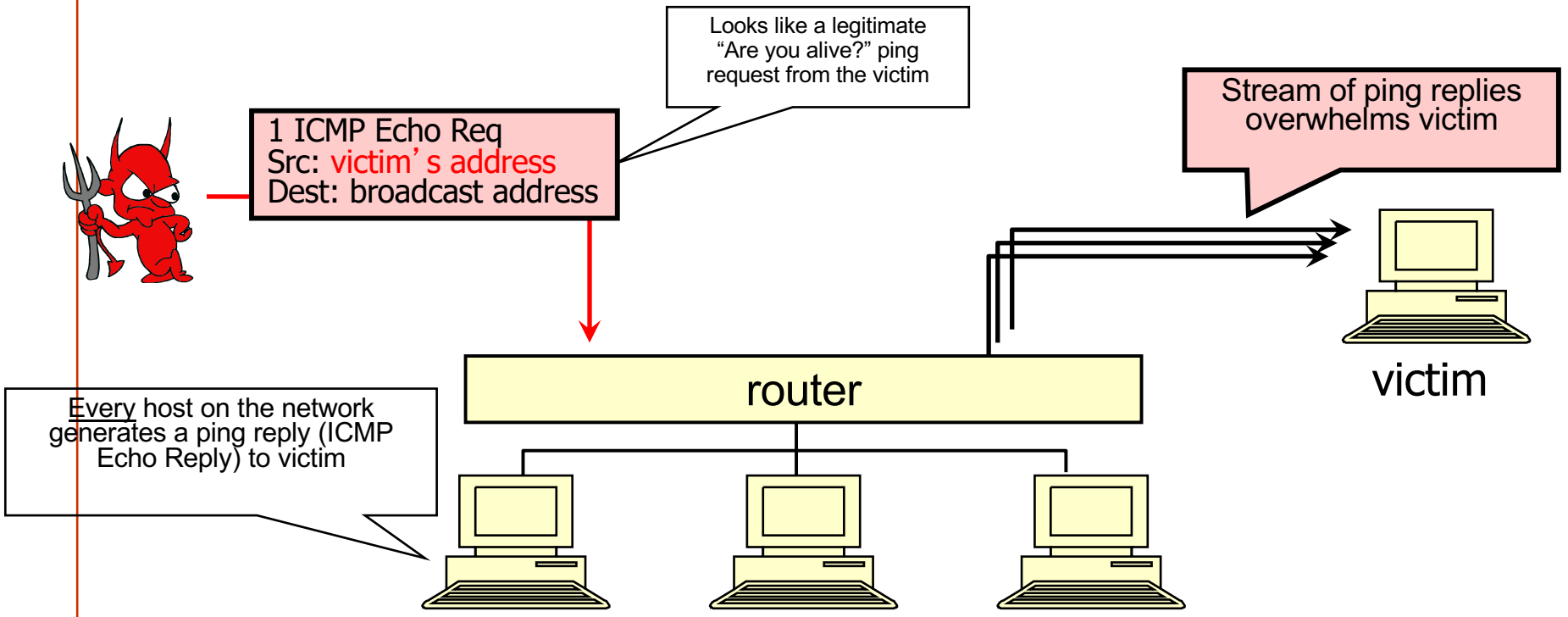
Reflection attack

- Spoof source IP address = victim's IP
- Goal: generate lengthy or numerous replies for short requests: amplification
  - Without amplification: would it make sense?
- January 2001 attack:
  - requests for large DNS record
  - generated 60-90 Mbps of traffic
- Reflection attack can be also be done with Web and other services

DNS Amplification Attacks

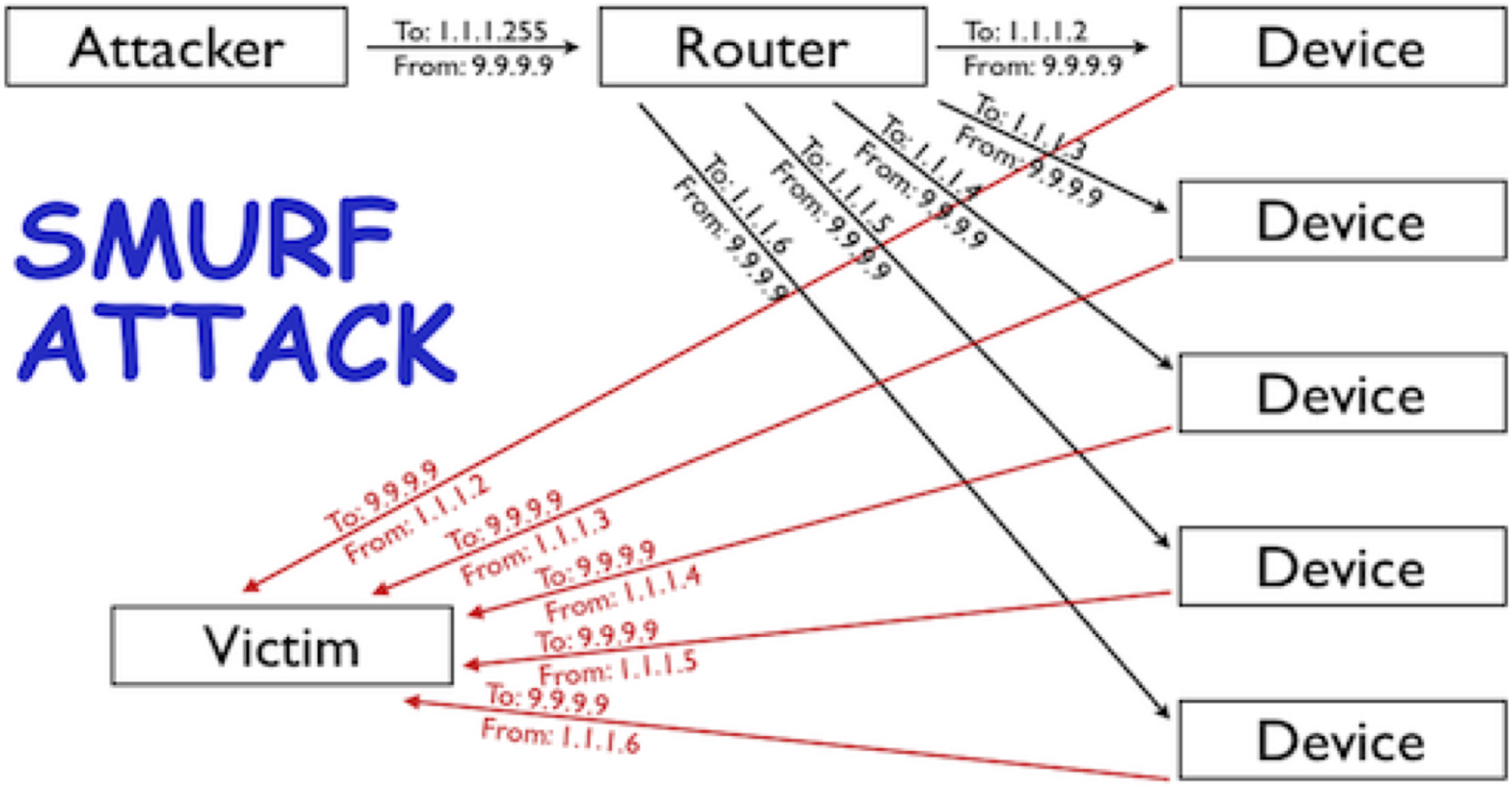
- Use packets directed at a legitimate DNS server as the intermediary system
- Attacker creates a series of DNS requests containing the spoofed source address of the target system
- Exploit DNS behavior to convert a small request to a much larger response (amplification)
- Target is flooded with responses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

"Smurf" Attack



Solution: reject external packets to broadcast addresses

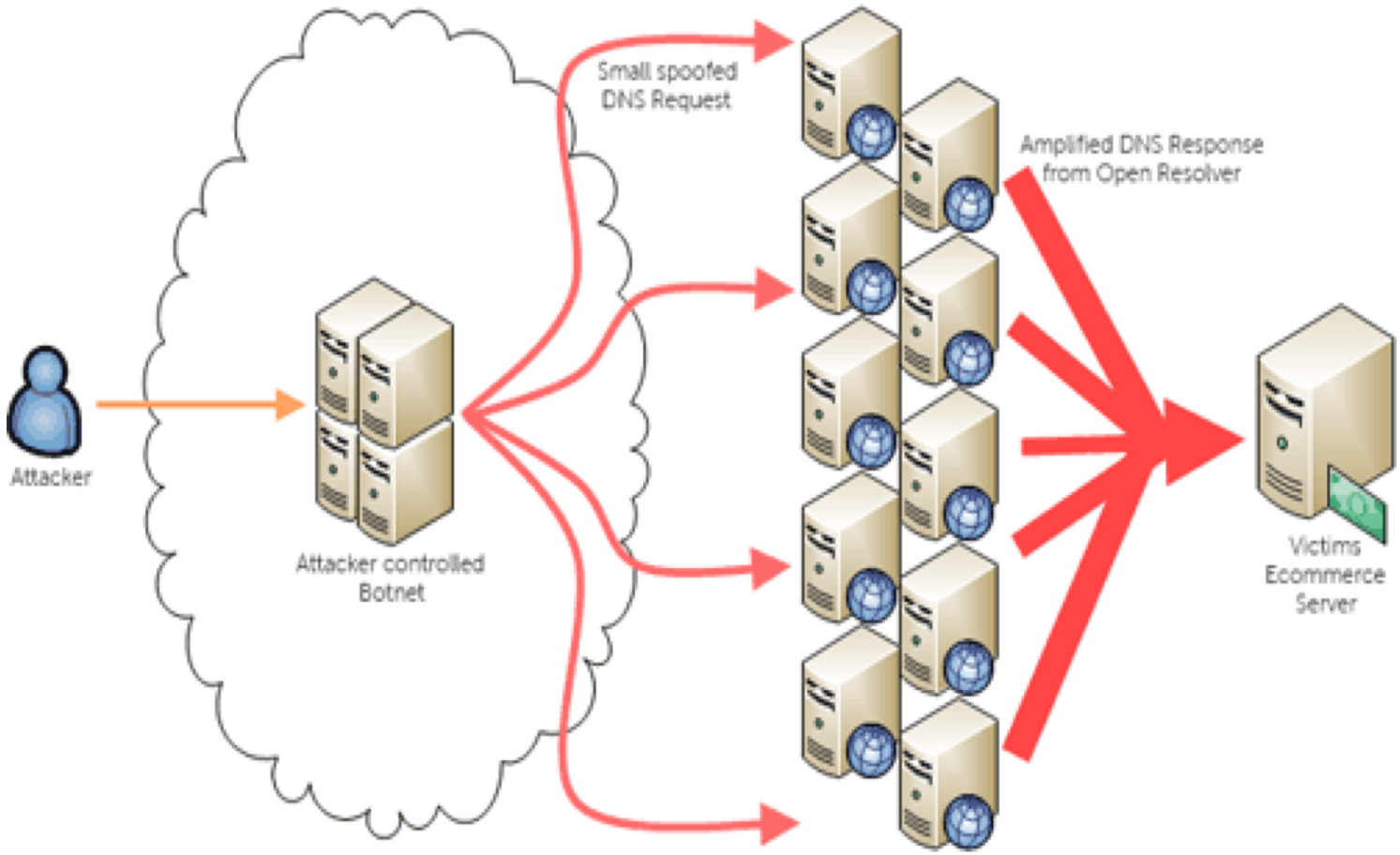
Smurf Attack Example



DNS Amplification Case

- dig ANY isc.org @x.x.x.x
  - a 64 byte query
  - resulted in a 3,223 byte response
  - https://blog.cloudflare.com/deep-inside-a-dns-amplification-ddos-attack/

DNS amplification attack using a botnet



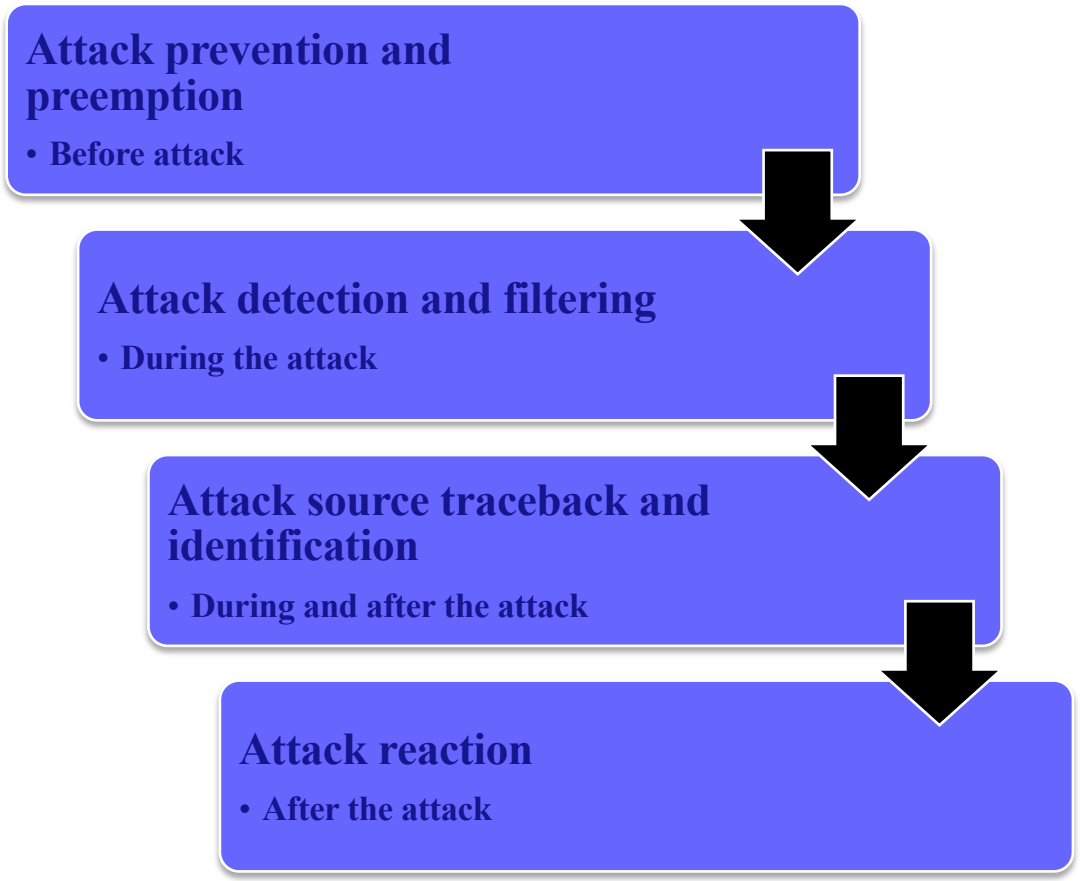
DoS and DDoS

- DoS:
  - source of attack small # of nodes
  - source IP typically spoofed
- DDoS
  - From thousands of nodes
  - IP addresses often not spoofed

DoS Attack Defenses

Four lines of defense against DDoS attacks

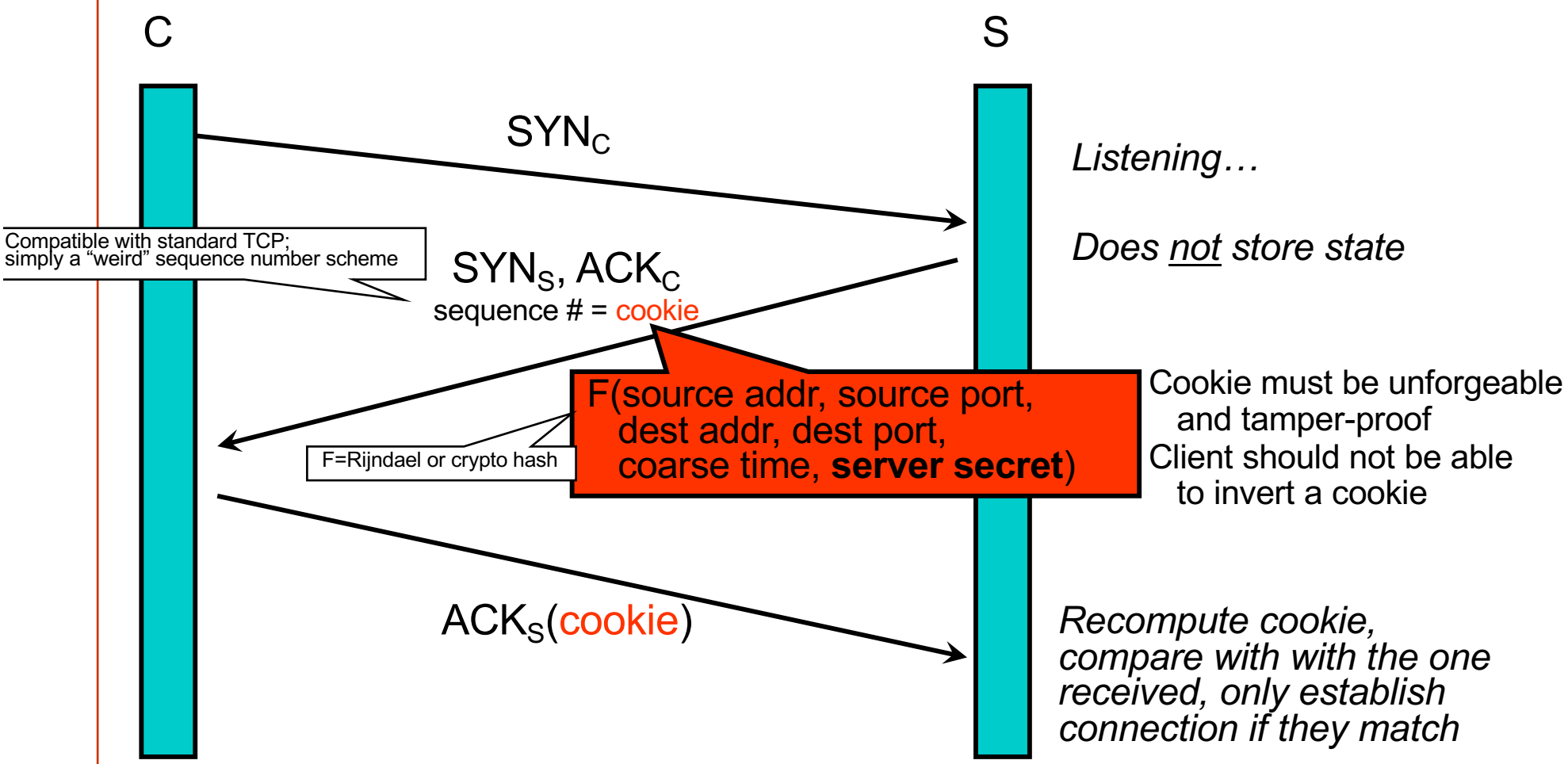
- These attacks cannot be prevented entirely
- High traffic volumes may be legitimate
  - High publicity about a specific site
  - Activity on a very popular site



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

SYN Cookies



More info: http://cr.yp.to/syncookies.html

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

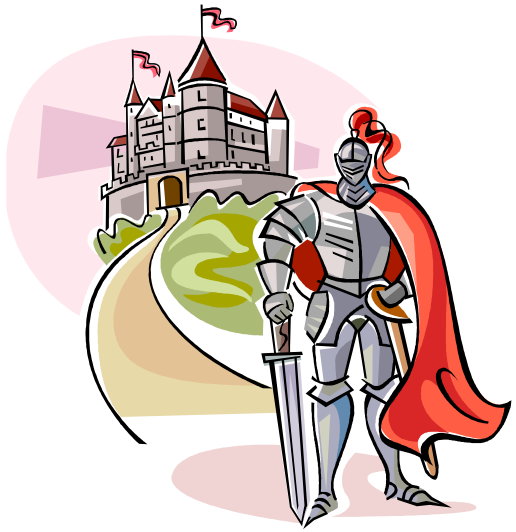
Good Incident Response Plan

- 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

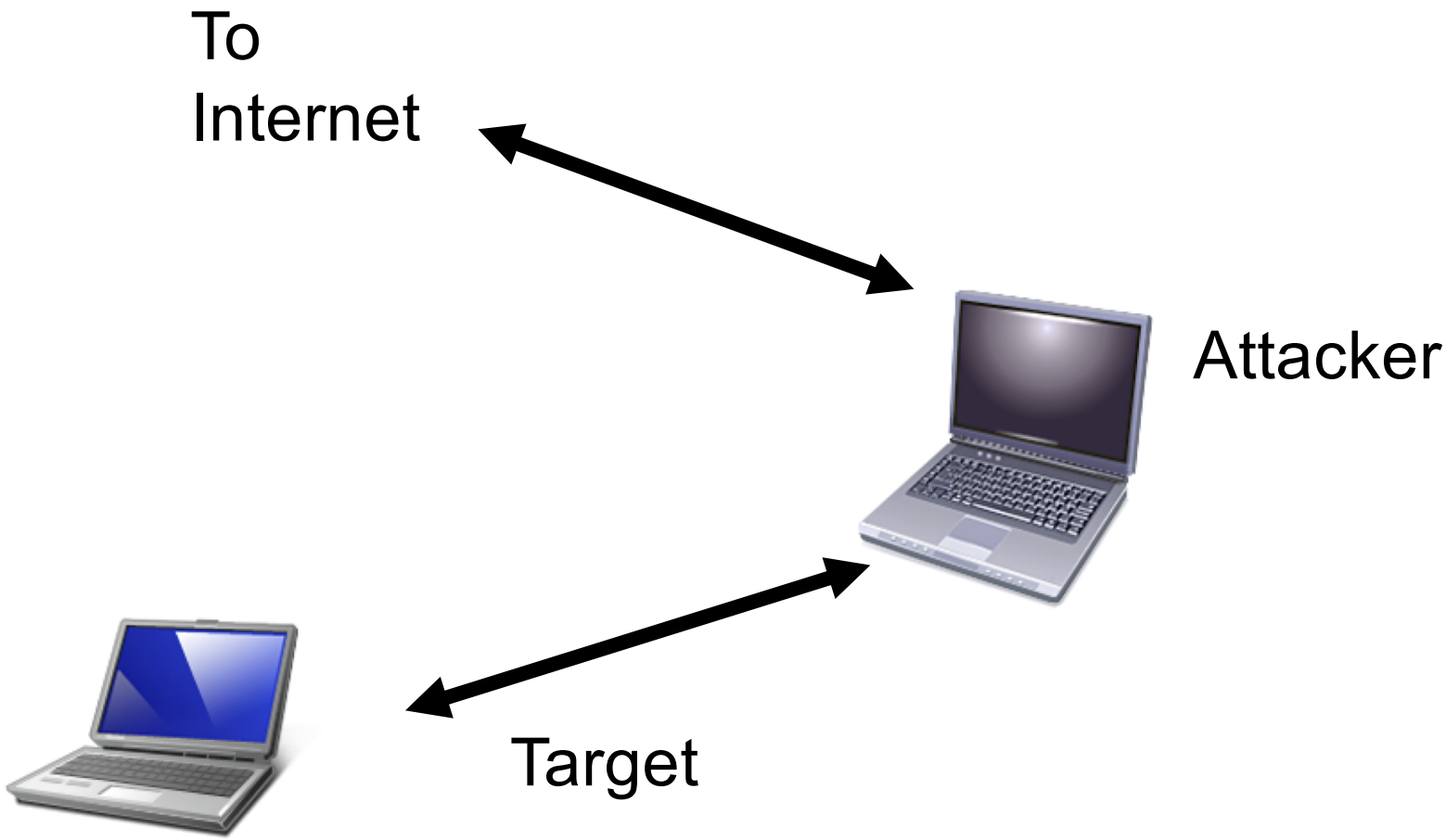


DDoS Defenses

- Don't let your systems become bots
  - Keep systems patched up
  - Employ egress anti-spoof filtering on external router.
- Filter dangerous packets
  - Vulnerability attacks
  - Intrusion prevention systems
- Over-provisioning of resources
  - Abundant bandwidth
  - Large pool of servers
  - ISP needs abundant bandwidth too.
  - Multiple ISPs
- Signature and anomaly detection and filtering
  - Upstream hopefully
- Rate limiting
  - Limit # of packets sent from source to dest

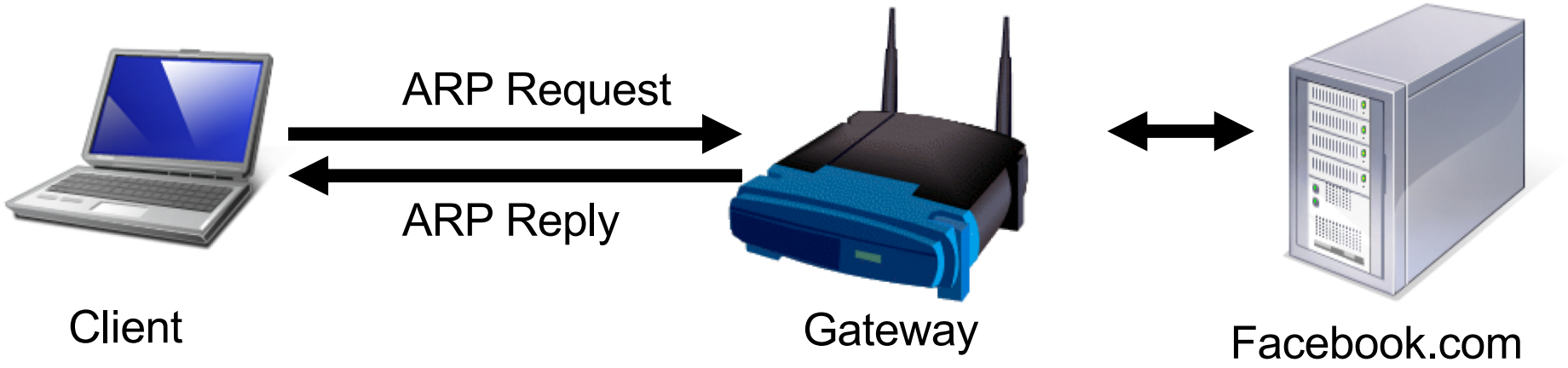
ARP Poisoning

- Physical Insertion in a Wired Network



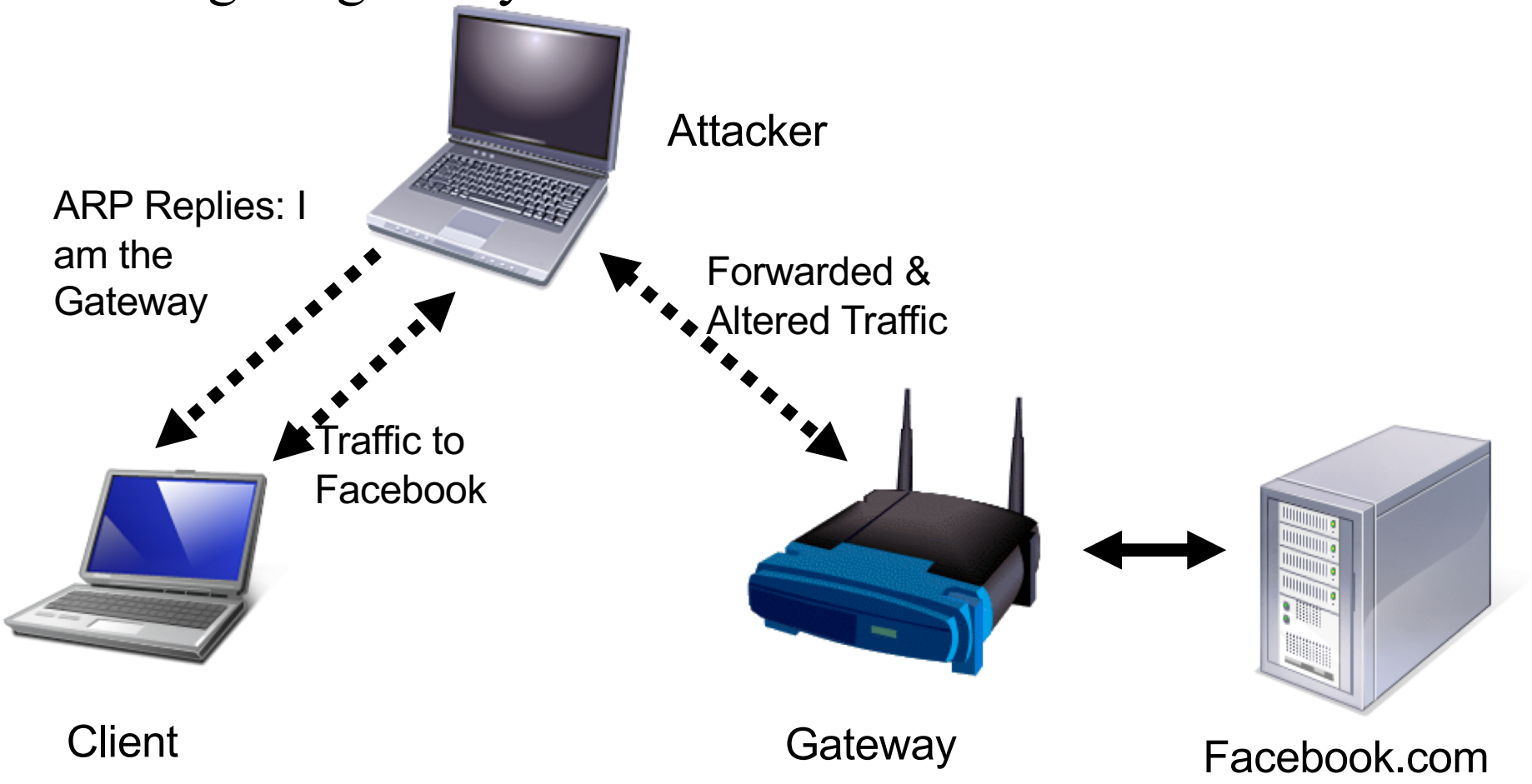
ARP Request and Reply

- Client wants to find Gateway
- ARP Request: Who has 192.168.2.1?
- ARP Reply:
  - MAC: 00-30-bd-02-ed-7b has 192.168.2.1



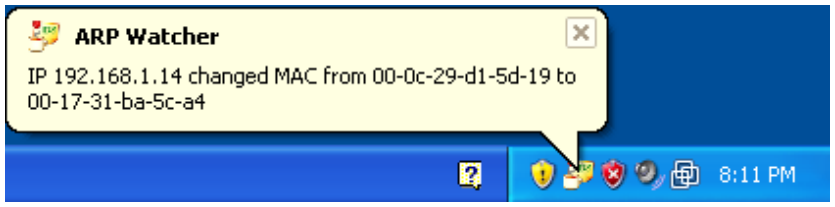
ARP Poisoning

- Configuring Proxy Server in the Browser



ARP Poisoning

- Redirects Traffic at Layer 2
- Sends a lot of false ARP packets on the LAN
- Can be easily detected by DeCaffienateID by IronGeek
  - http://k78.sl.pt



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