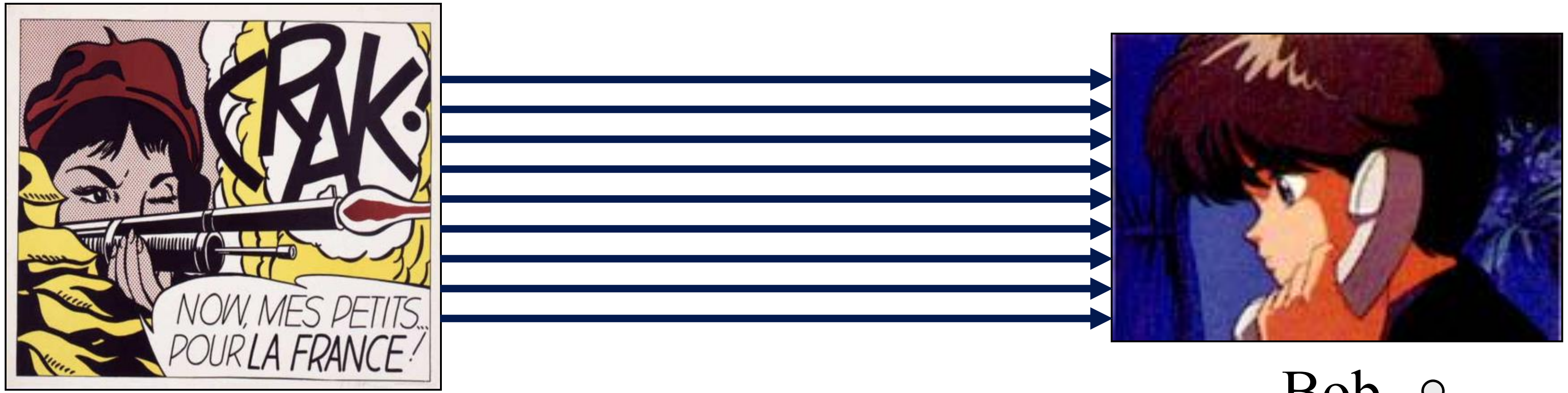
Introduction to Information Security
14-741/18-631 Fall 2021
Unit 4: Lecture 3:
Distributed Denial of Service Attacks

Limin Jia liminjia@andrew

This lecture's agenda

- **Outline**
  - DoS and DDoS overview
  - Walk through different types of DDoS attacks
  - Overview of possible defenses
- **Objective**
  - Gain exposure and understanding of one of the main families of security attacks
  - Understand its relationship with other types of attacks

Denial of Service (DoS) attack



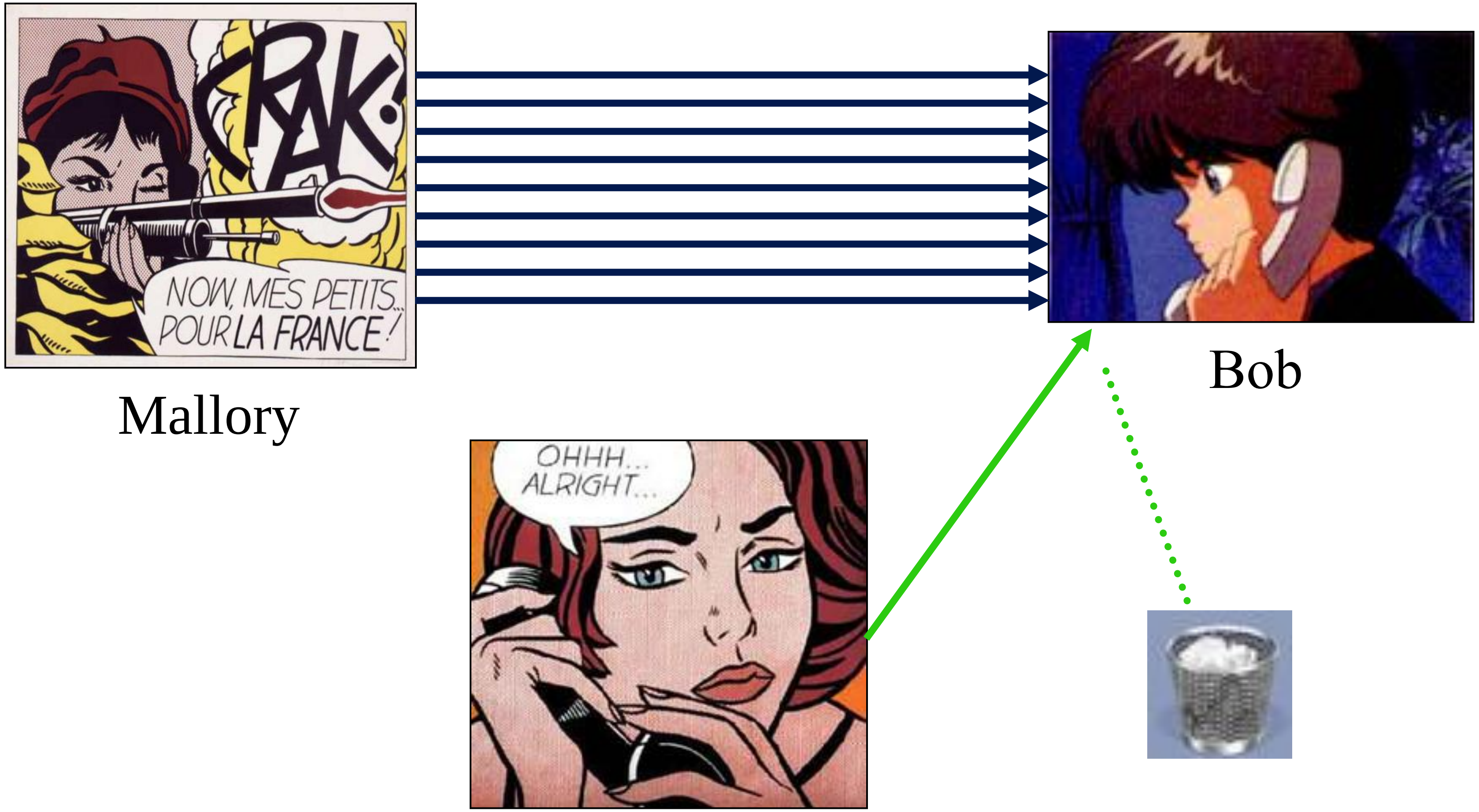
Mallory

Bob

Alice

Wow!
7.89×10^{26}
messages to
process!!

Denial of Service (DoS) attack

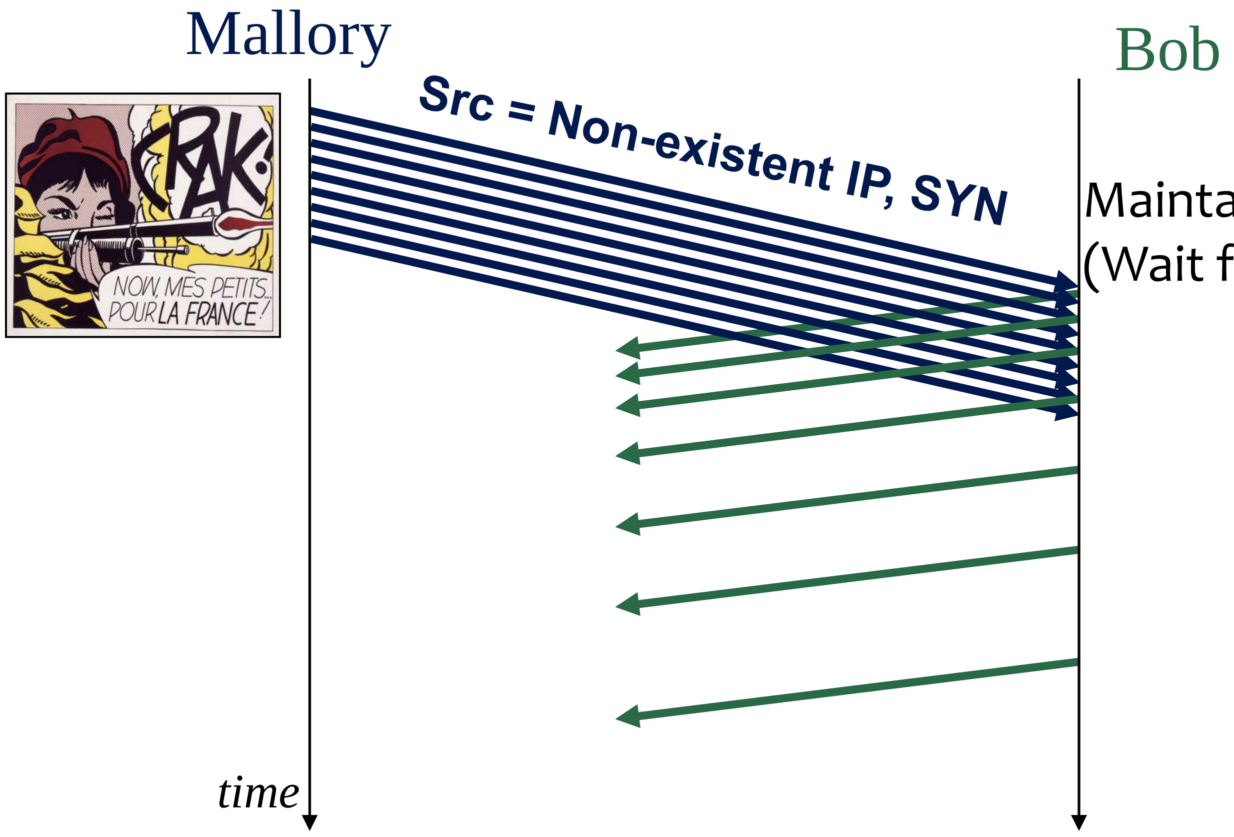


Mallory

Bob

Alice

DoS attack example: SYN flood



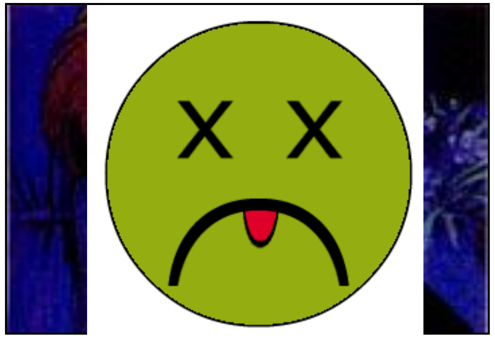
Mallory

Bob

Src = Non-existent IP, SYN

time

Maintain n connections half open
(Wait for n ACKs)



DoS: General definition

- **DoS is not access or theft of information or services**
- **Instead, goal is to stop the service from operating**
- **Deny service to legitimate users**
- **Usually a temporary effect that passes as soon as the attack stops**
- **Not necessarily a network attack!**
  - Crash the machine
  - Put it into an infinite loop
  - Use up a key machine resource
    - Try this C program for fun in your virtual machine

      ```
      #include <sys/types.h>
      #include <unistd.h>
      void main() { while (1) {fork();}}
      ```
  - Do you think the other users are very happy if you do this?

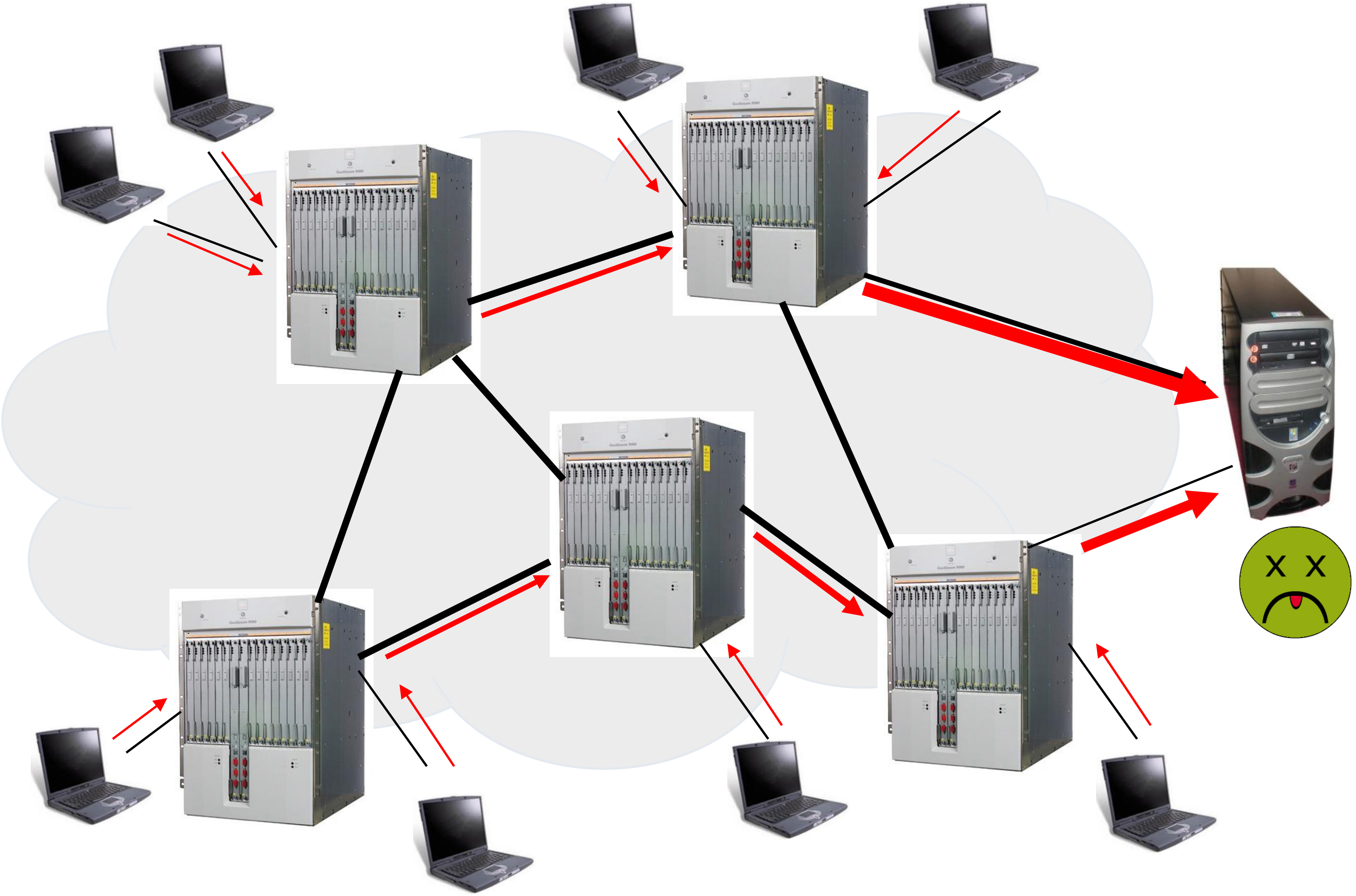
“Simple” DoS defenses

- **Ignore/quarantine attacker**
  - Ignore requests from attacker
  - Filter out traffic coming from attacker in case of a DoS over network
    - What if the source address is spoofed?
  - How do you detect attack?
    - Symptoms are generally themselves evidence of success
- **Overprovision system to be more powerful than most attackers**
  - Not necessarily feasible…
  - …and won’t help you in case of a DDoS

Distributed Denial of Service (DDoS)

- **Motivation (from attacker’s perspective)**
  - For simple DoS, attacker must be either more powerful than the target machine
- **Solution?**
  - Use as many machines as possible

The joys of distributed computing



DDoS in practice

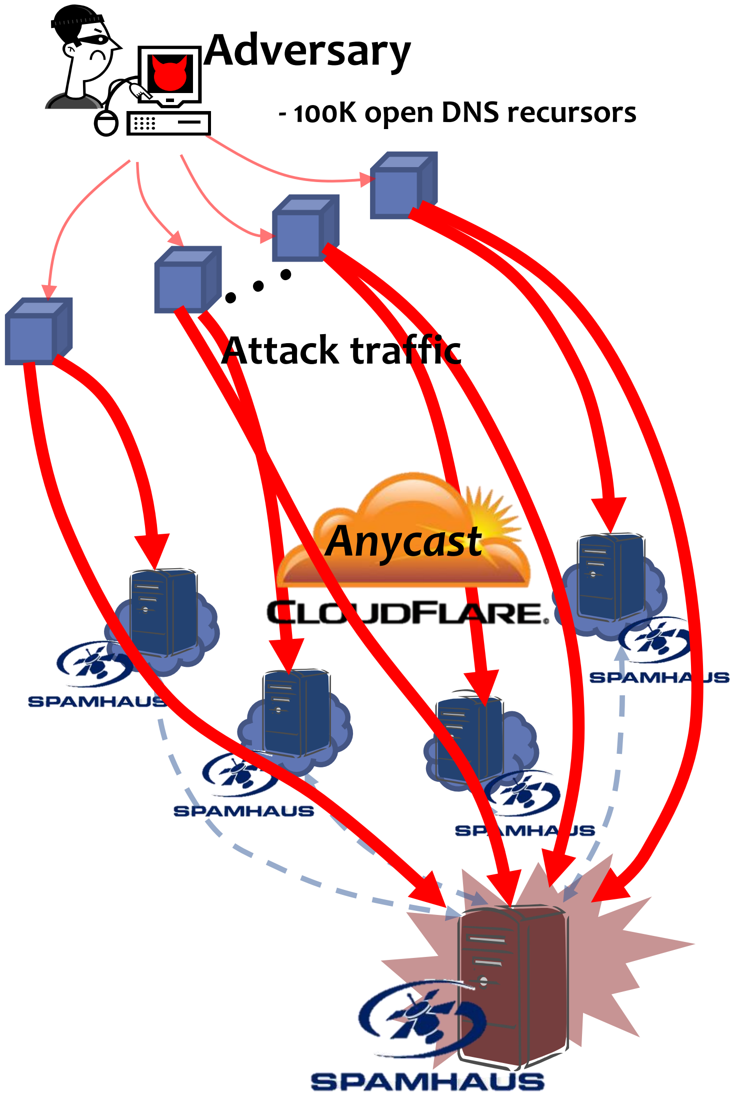
- Attacks happen every day (hundreds)
- On a wide variety of targets
- Tend to be highly successful
- Few good existing mechanisms to stop them
- Successful attacks on major commercial sites

Attack on Dyn (Mirai)

- October 21, 2016
- 100,000 infected devices (IoT) attacked Dyn servers
- Etsy, Github, Spotify and Twitter offline for a couple of hours, because Dyn was their DNS infrastructure

“Spamhaus” Attack (2013)

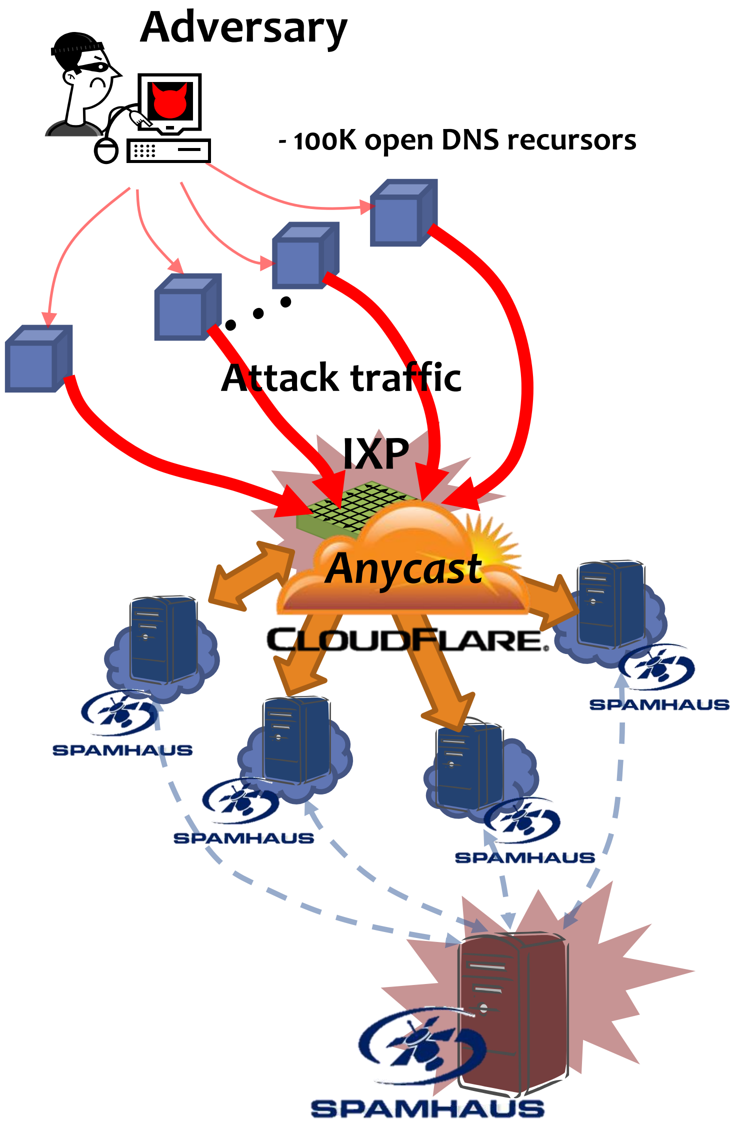
- Adversary: DDoS 1 Spamhaus Server 3/16 – 3/18: ~ 10 Gbps, persistent: ~ 2.5 days
- Spamhaus -> CloudFlare (3/19 – 3/22) 90-120 Gbps traffic is diffused over N > 20 servers in 4 hours



Slide courtesy Min Suk Kang

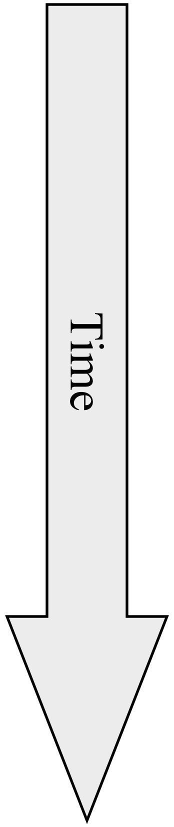
“Spamhaus” Attack (2013)

- **Adversary: DDoS -> 4 IXPs (3/23) non-persistent: attack detected, pushed back & legitimate traffic re-routed in ~ 1 - 1.5 hours**



Slide courtesy Min Suk Kang

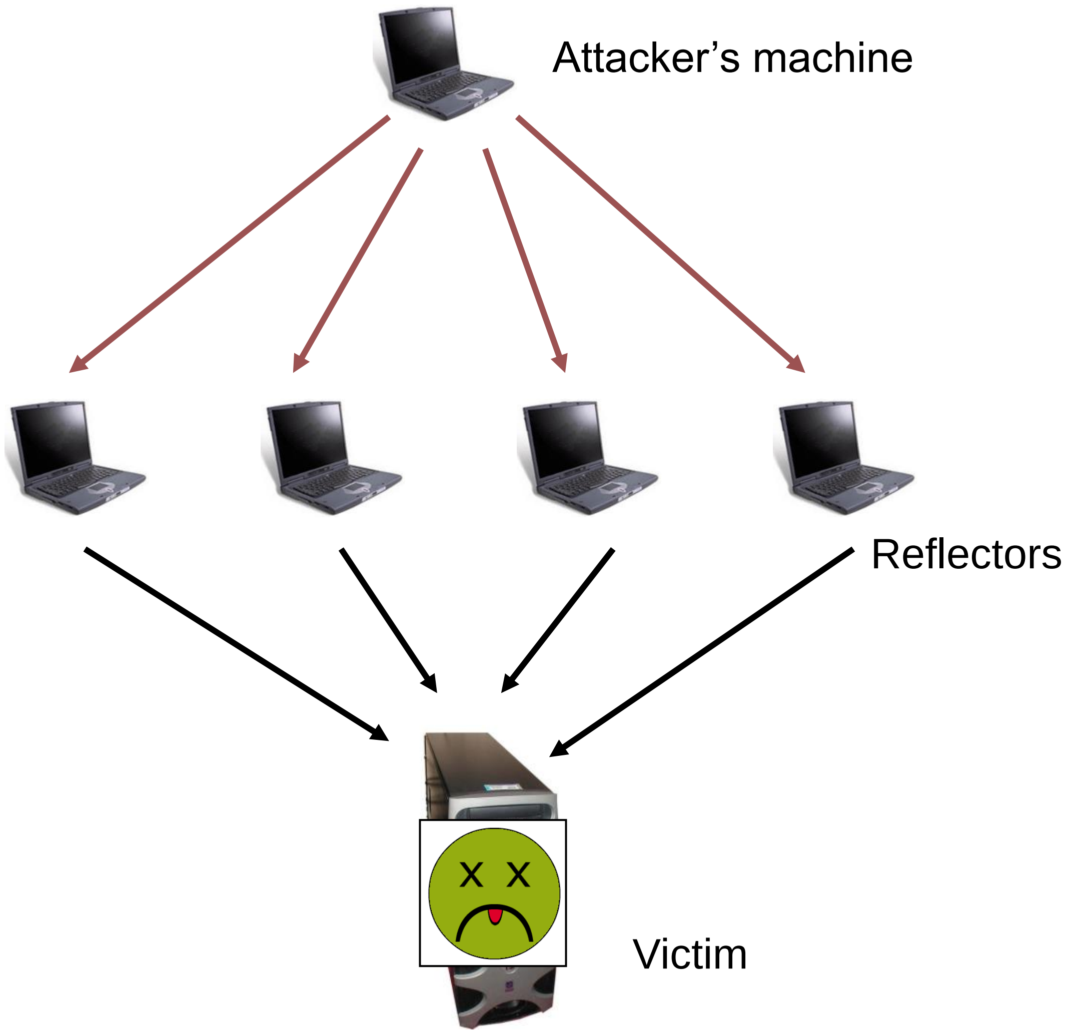
Evolution of (D)DoS in history



- Point-to-point DoS attacks
  - TCP SYN floods, Ping of death, etc..
- Smurf (reflection) attacks
- Coordinated DoS
- Multi-stage DDoS
- Amplification attacks (smurf returns)

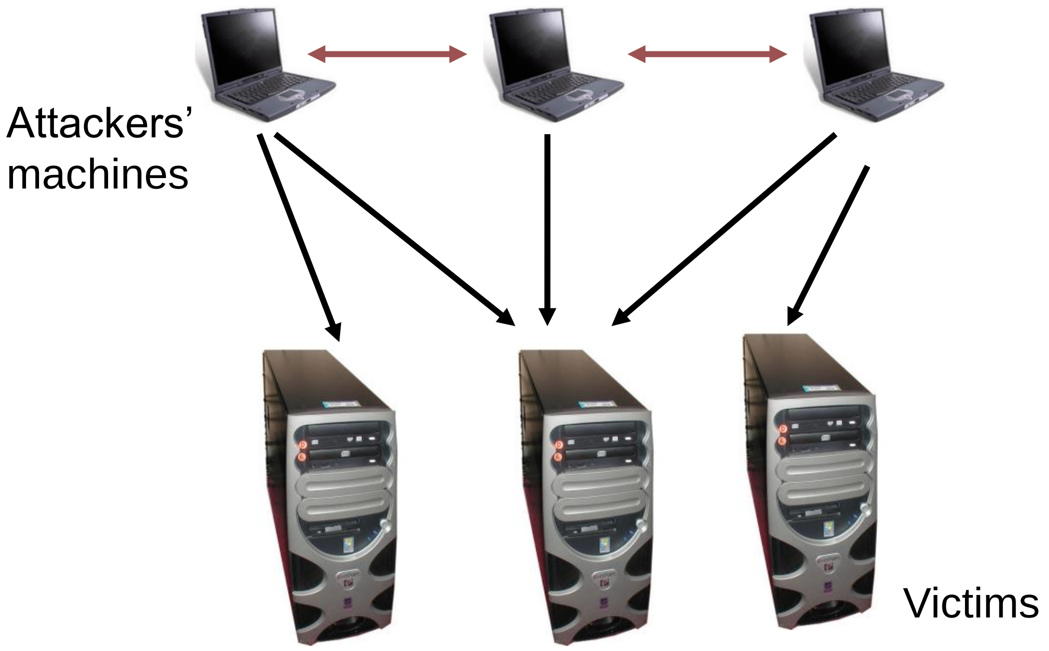
Smurf (reflection) attacks

1. **Attacker spoofs victim's IP address**
2. **Attacker sends error-generating packets w. spoofed IP addr. to reflectors**
3. **Reflectors all report errors to victim**
4. **Victim is killed by error messages**

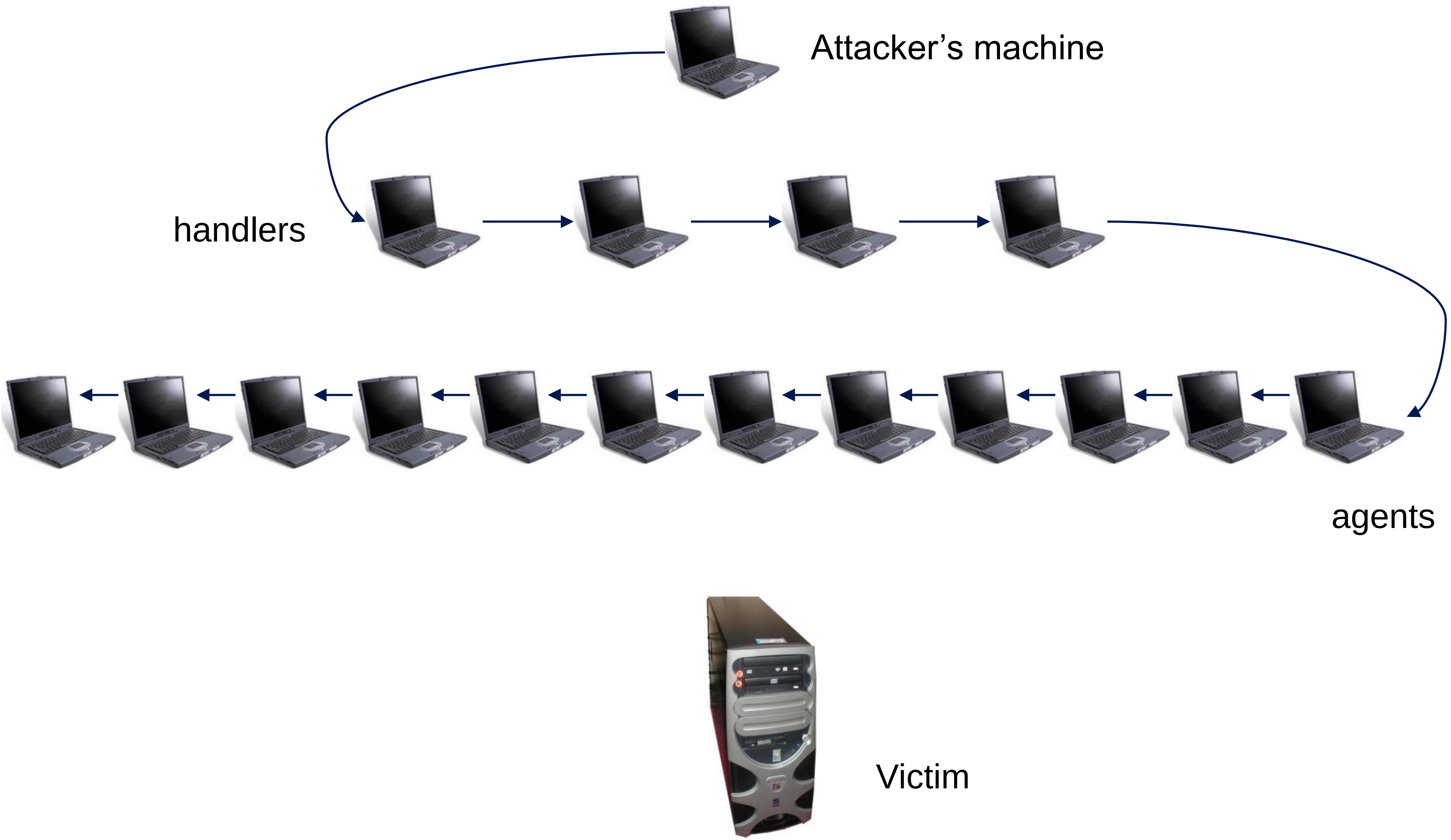


Coordinated DoS

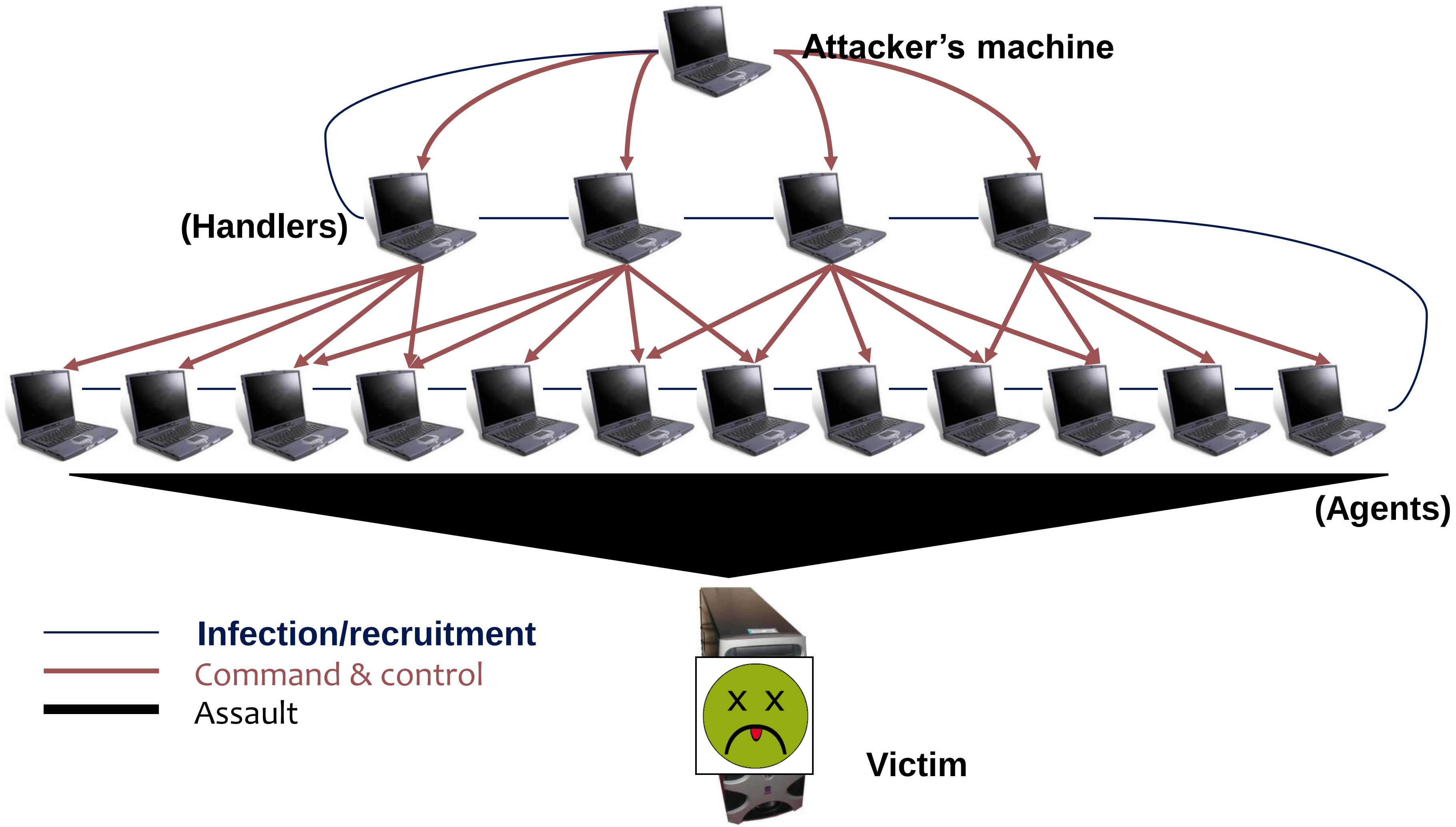
- **Simple extension of DoS**
- **Coordination between multiple parties**
  - Can be done off-band
  - IRC channels, email…



Typical DDoS setup



Typical DDoS setup circa 2005



Attacker’s machine

(Handlers)

(Agents)

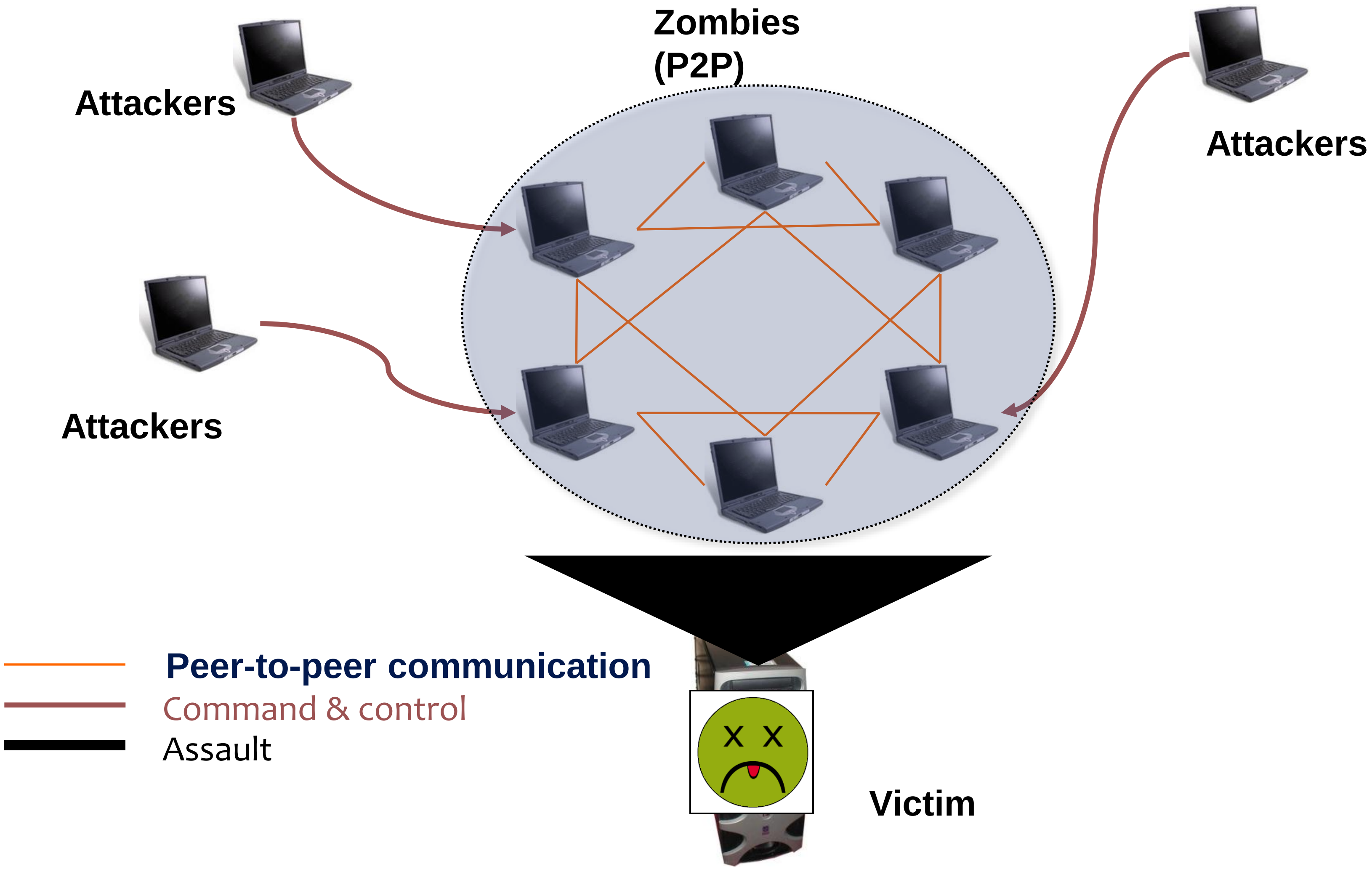
Victim

Infection/recruitment

Command & control

Assault

Modern Botnet setup



Attackers

Zombies
(P2P)

Attackers

Attackers

Victim

Peer-to-peer communication

Command & control

Assault

Amplication attacks example (DNS)

```
johnsmith@andrew $ dig hizbullah.me

; <<>> DiG 9.8.3-P1 <<>> hizbullah.me
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 20343
;; flags: qr rd ra; QUERY: 1, ANSWER: 242, AUTHORITY: 0,
ADDITIONAL: 0
```

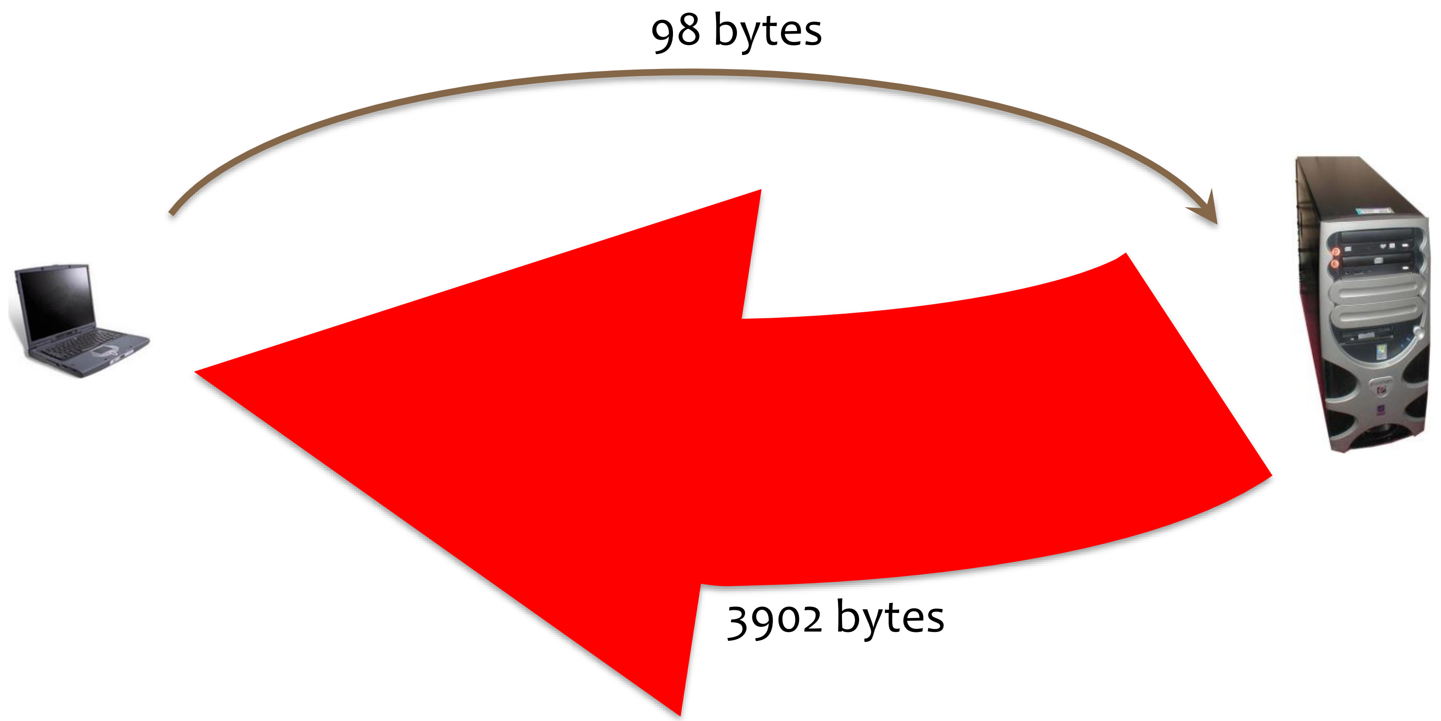
(lots of stuff omitted for brevity)

```
hizbullah.me.    1800   IN  A   204.46.43.113
hizbullah.me.    1800   IN  A   204.46.43.114
hizbullah.me.    1800   IN  A   204.46.43.115

;; Query time: 996 msec
;; SERVER: 192.168.2.1#53(192.168.2.1)
;; WHEN: Tue Feb  4 21:41:51 2014
;; MSG SIZE  rcvd: 3902
```

Amplification factors (DNS)

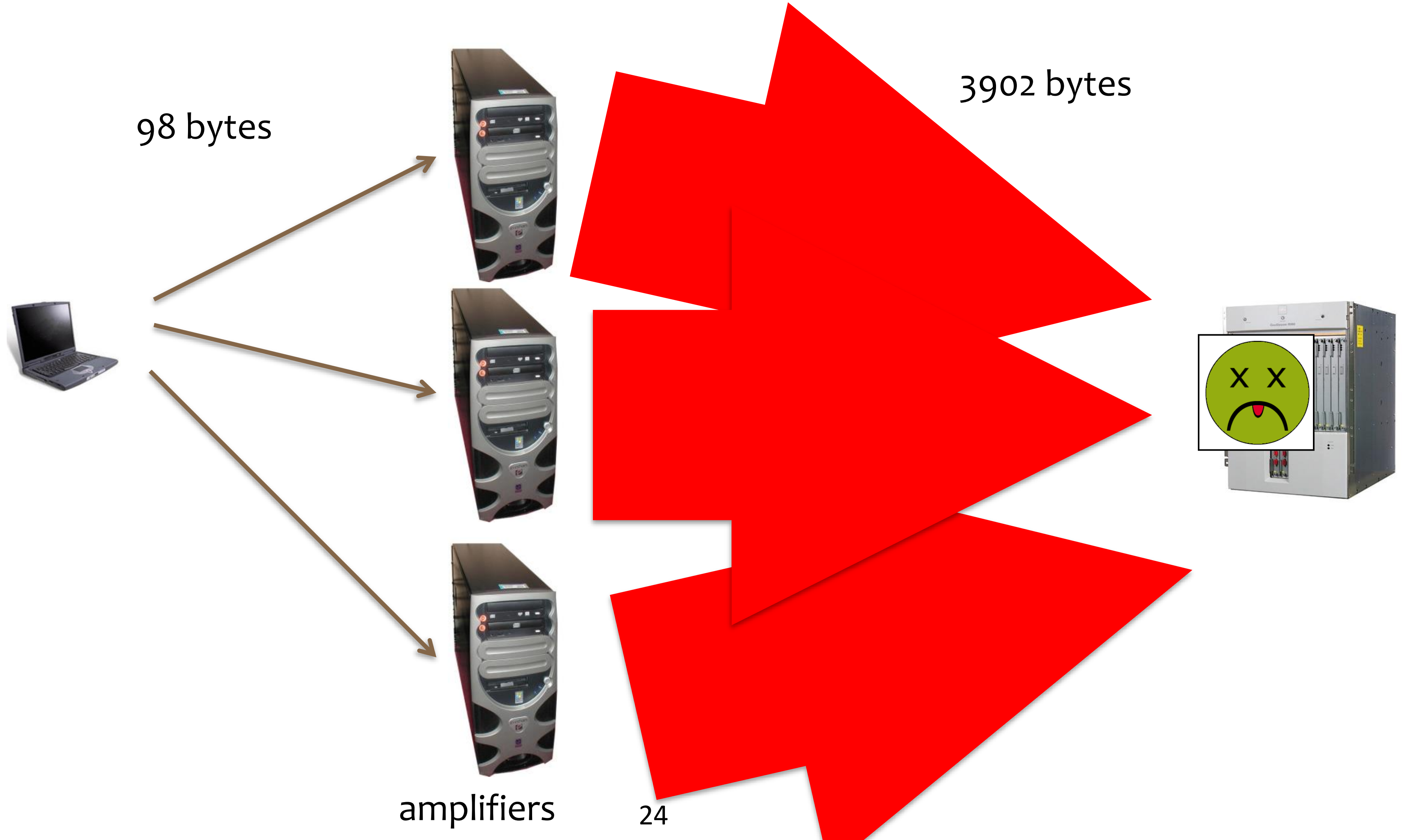
```
johnsmith@andrew $ dig hizbullah.me
```



39.81x amplification factor

Using amplification

```
johnsmith@andrew $ dig hizbullah.me
```



Attack on Krebs Security

- **8pm Eastern Sept 20, 2016**
- **Up to 620 Gbps of traffic!**
- **DNS reflection attack**
  - Small DNS queries create much larger response
  - Use “open recursive” DNS servers (bad configuration!)

Attack toolkits

- **Widely available on the net**
  - Easily downloaded along with source code
  - Easily deployed and used
- **Automated code for**
  - Scanning – detection of vulnerable machines
  - Exploit – breaking into the machine
  - Infection – placing the attack code
- **Rootkits**
  - Hide the attack code
  - Restart the attack code
  - Keep open backdoors for attacker access
- **DDoS attack code:**
  - Trin00, TFN(2K), Stacheldraht, Shaft, mstream, Trinity, LOIC, Zeus clients, etc…

Pitfalls and fallacies

- **Good host security protects against DDoS**
  - Unfortunately, it’s the others’ lousy security that is a vehicle for DDoS
- **Overprovisioning protects against DDoS**
  - You can’t be provisioned enough if 10,000+ machines attack you
- **Firewalls protect against DDoS**
  - One can target the firewall, and you lose your network access anyway, or the attacker can tunnel through the firewall

Any machine connected to the Internet is potentially vulnerable

Why DDoS is a hard problem

- **Simple form of attack**
  - No complex technique, just send a lot of traffic
  - Toolkits readily available
- **Prey on the Internet's strengths**
  - Simplicity of processing in routers
  - Total reachability
- **Attack machines readily available**
  - Easy to find 10,000's vulnerable machines of the Internet
- **Attack can look like normal traffic**
  - E.g., HTTP requests
- **Lack of Internet enforcement tools**
  - No traceability
- **Lack of cooperation between targets**
  - ISPs are competitive, and cooperation only at human timescales
- **Effective solutions hard to deploy**
  - We can't change the core of the Internet easily

Possible defenses I: Filtering

- **Filtering packets**
  - Difficult in general
  - False positives actually help the attack by denying legitimate traffic from reaching you
- **Egress filtering**
  - Filtering at the victim's firewall
  - Likely to be useless, firewall itself can be targeted
- **Ingress filtering**
  - Filtering at the attacker's firewall
    - Routers drop packets with an "invalid" source IP address field
  - Would need near universal deployment to be effective
    - Besides, does not prevent subnet spoofing
  - Economic incentives?

Possible defenses II: Pushback

- **Pushback: rate limit flows that compose large traffic aggregates to mitigate impact of DDoS**
- **Distributed solution: the whole network benefits**
- **Requires router modifications**
  - Deployment may take very long

Possible defenses III: Traceback

- **Traceback: Means of identifying source of attack even in the presence of IP spoofing**
  - Usually done by embedding some information in sample packets (by routers)
- **Very good for forensics if available**
  - Could be used to prosecute, etc.
- **Main problem: reaction time?**
  - Secondary problem: requires router modification, which itself limits deployment
- **Many research papers on the subject**

Take away slide

- **DDoS is the networked version of DoS**
- **DDoS attacks are a real threat**
  - Assessing the current number and dynamics of attacks is a worthy research question
- **Easy to carry out**
  - Toolkits readily available
- **Difficult to defend against**
  - Patching and securing one’s host is **not** enough
  - Principally due to the nature (default connected) of the Internet
  - Filtering can be as damaging as the attack
  - Prevention is difficult, due to the role other machines play
  - Legally very complicated (multiple jurisdictions, …)