ROYAL INSTITUTE
OF TECHNOLOGY

(Distributed) Denial of Service Attacks

aka

(D)DoS Attacks

Panos Papadimitatos

Networked Systems Security Group

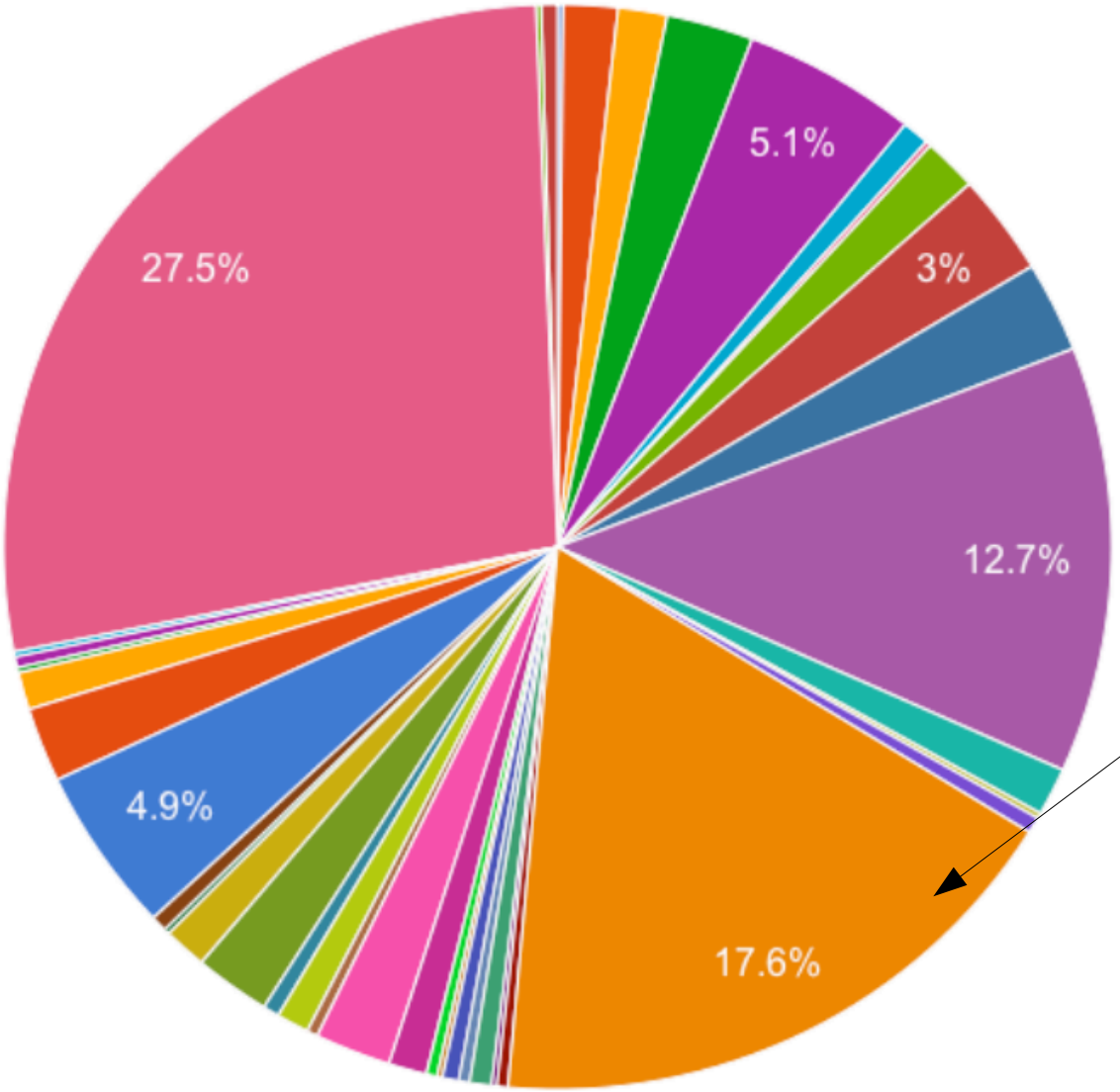
www.kth.se/nss

ROYAL INSTITUTE OF TECHNOLOGY

Outline

- Introduction
    - A Denial of Service Attack?
    - A Distributed Denial of Service Attack?
- BotNets, BotNet Architectures, Bot Recruitment
- Transport Layer DoS Attacks
    - TCP attacks
- Network Layer and Overlay Attacks
    - Smurf Attacks, P2P based DDoS
- Operation #PayBack
- Research on DoS and DDoS
    - Tracing back the source of DDoS traffic

Introduction



- Approximately 20% of attacks targeting web sites are DoS based
- Things get worse in case of DDoS attacks

Web Hacking Incident Database

ROYAL INSTITUTE OF TECHNOLOGY

Introduction (cont'd)

(Recall: Introduction lecture - revise)

DoS and DDoS are common attack methods targeting:

Introduction (cont'd)

Companies

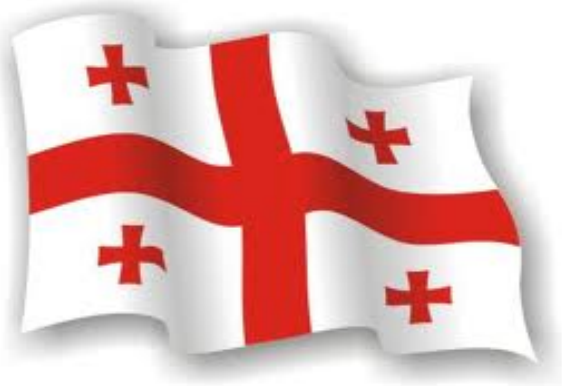
Introduction (cont'd)

Authorities

ROYAL INSTITUTE OF TECHNOLOGY

Introduction (cont'd)

Or even Nations...



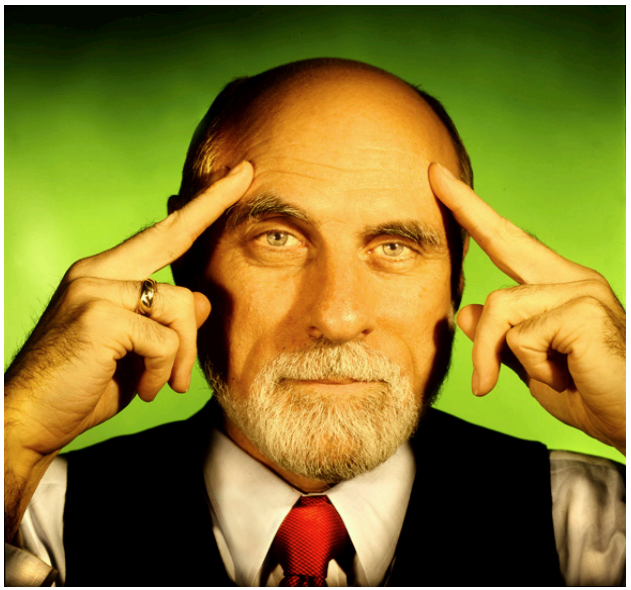
ROYAL INSTITUTE OF TECHNOLOGY

Introduction (cont'd)

Defending against them is really hard...

Because when these DDoS attacks swamp access lines, then filtering at the other end does not help

Vinton Cerf



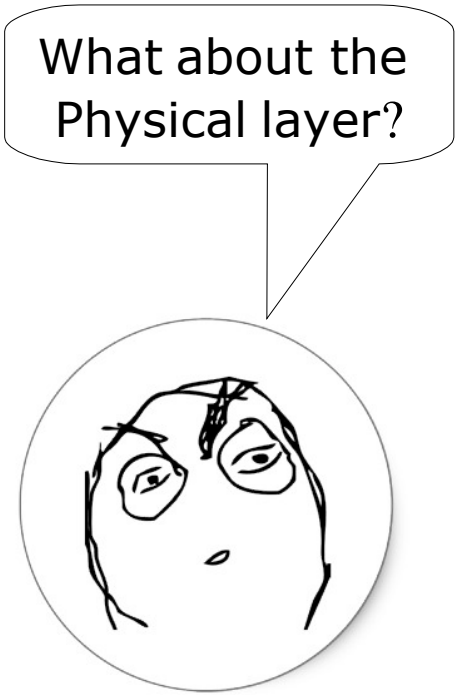
DoS Attacks

- Denial of Service (DoS) Attacks target system availability
- They do not require a lot of computing work and resources
- They take advantage of
  - Security-agnostic design
  - Design problems
  - System defects, bugs

DoS attacks (cont'd)

- Can be launched on all OSI layers:
  - 802.11b bug: Link Layer DoS
  - Apache Killer: Application Layer DoS

Jamming is a DoS attack too
- *Recall previous lecture*



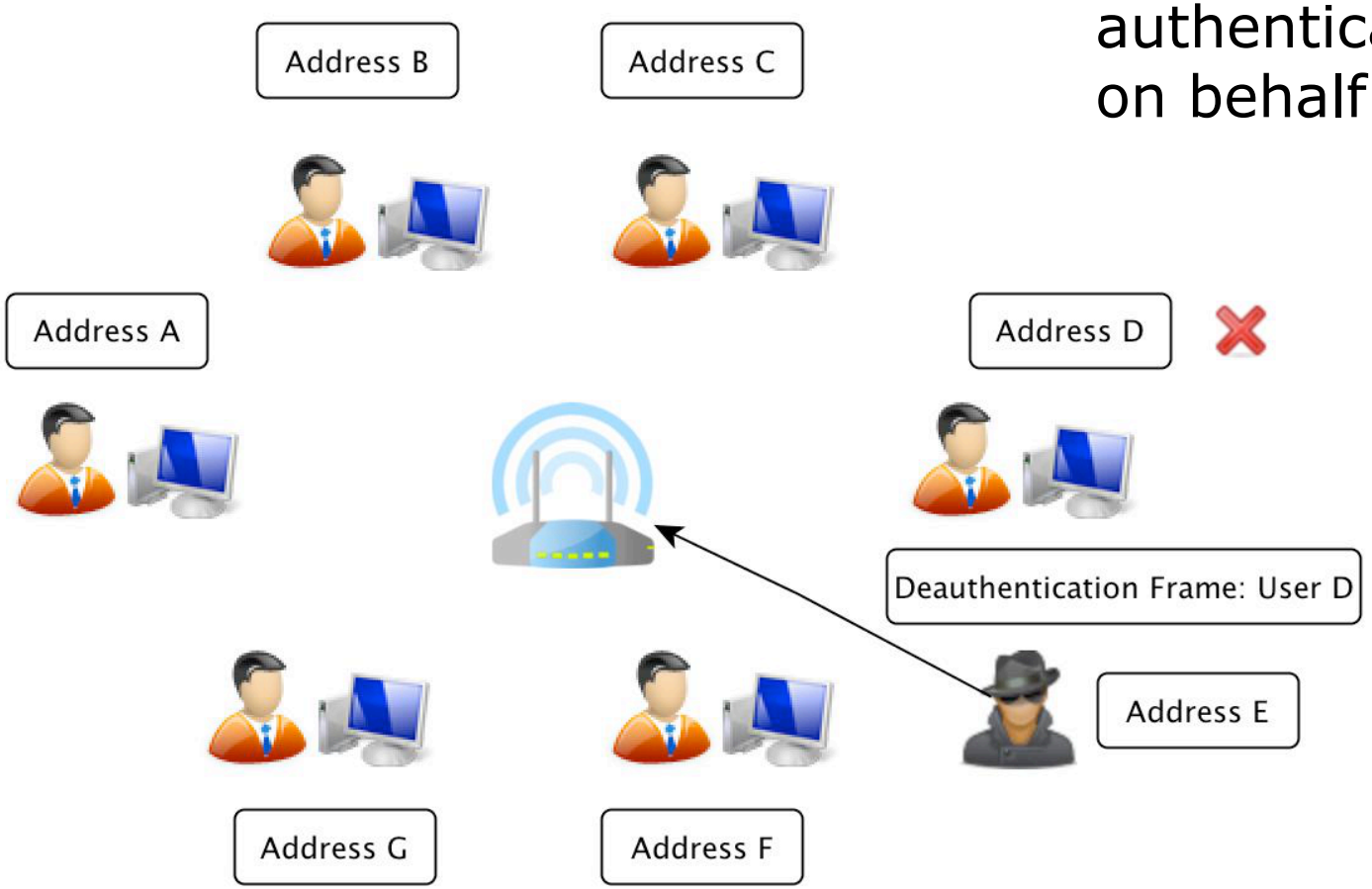
DoS attacks: 802.11b De-authentication

- All users are connected to the AP in a 802.11b network

DoS attacks: 802.11b De-authentication (cont'd)

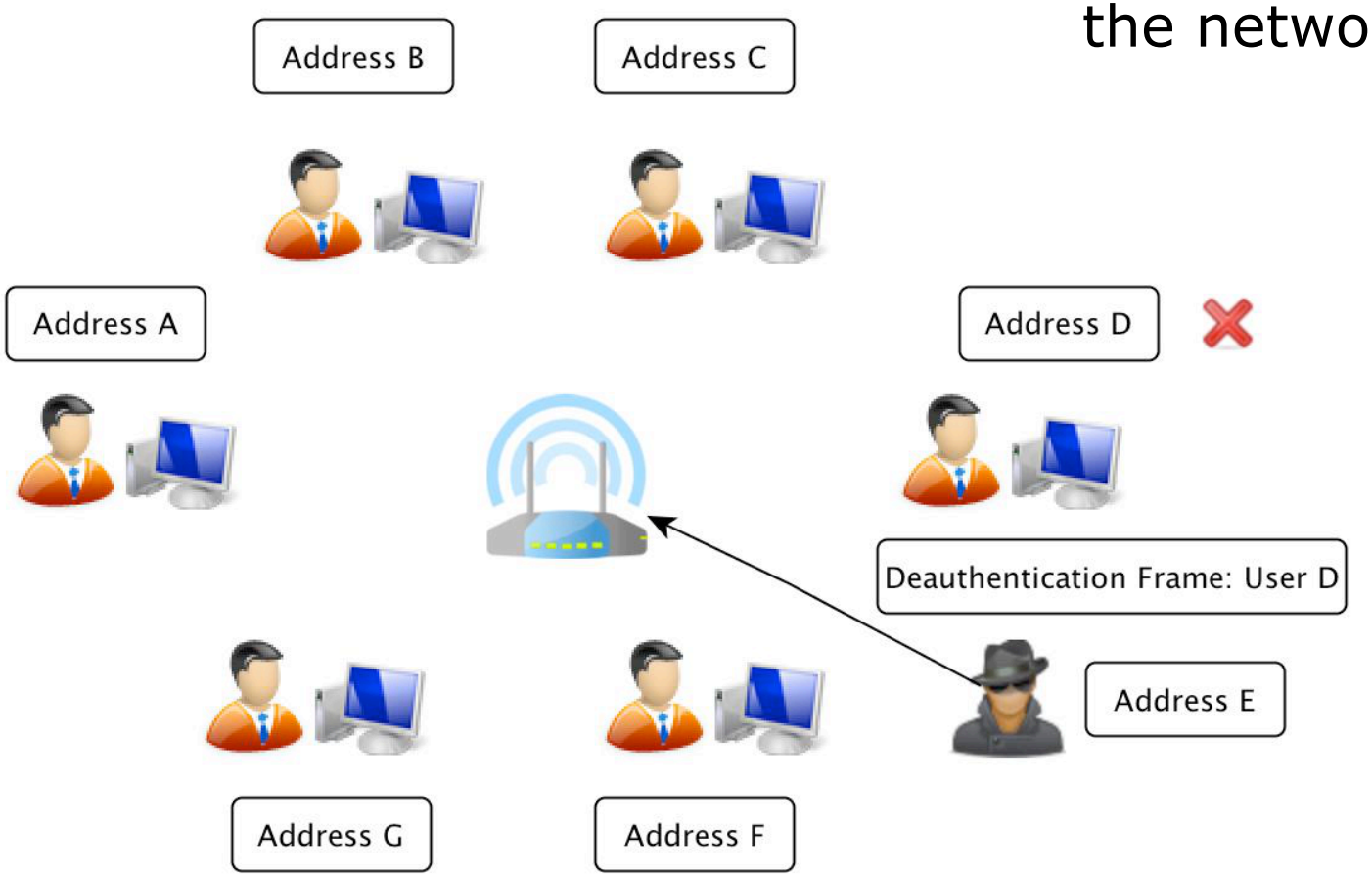
The 802.11b De-authentication:

- The attacker sends a de-authentication frame to the AP on behalf of user D

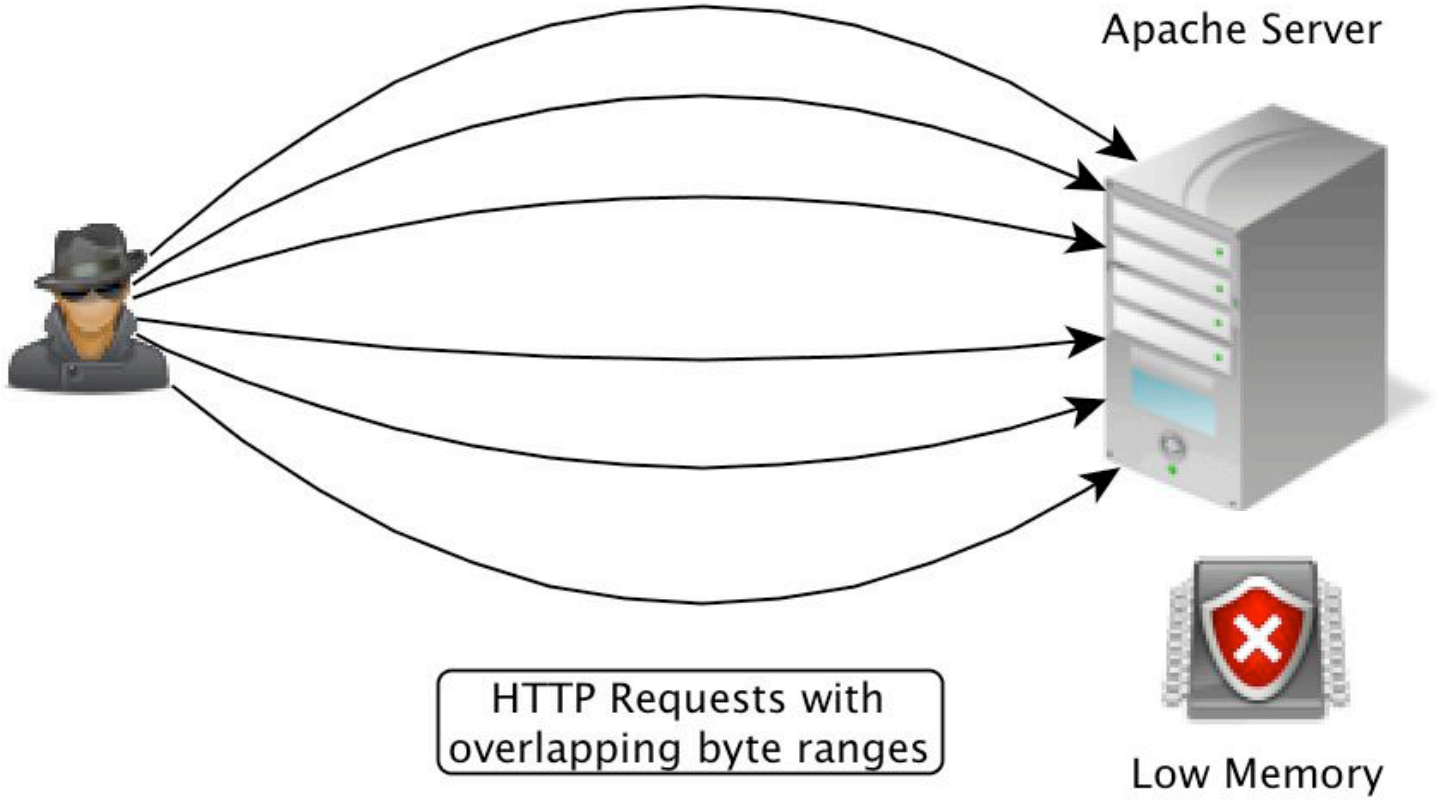


DoS attacks: 802.11b De-authentication (cont'd)

- User D gets disconnected from the network



DoS attacks: The Apache Killer Bug



ROYAL INSTITUTE OF TECHNOLOGY

DoS attacks (cont'd)

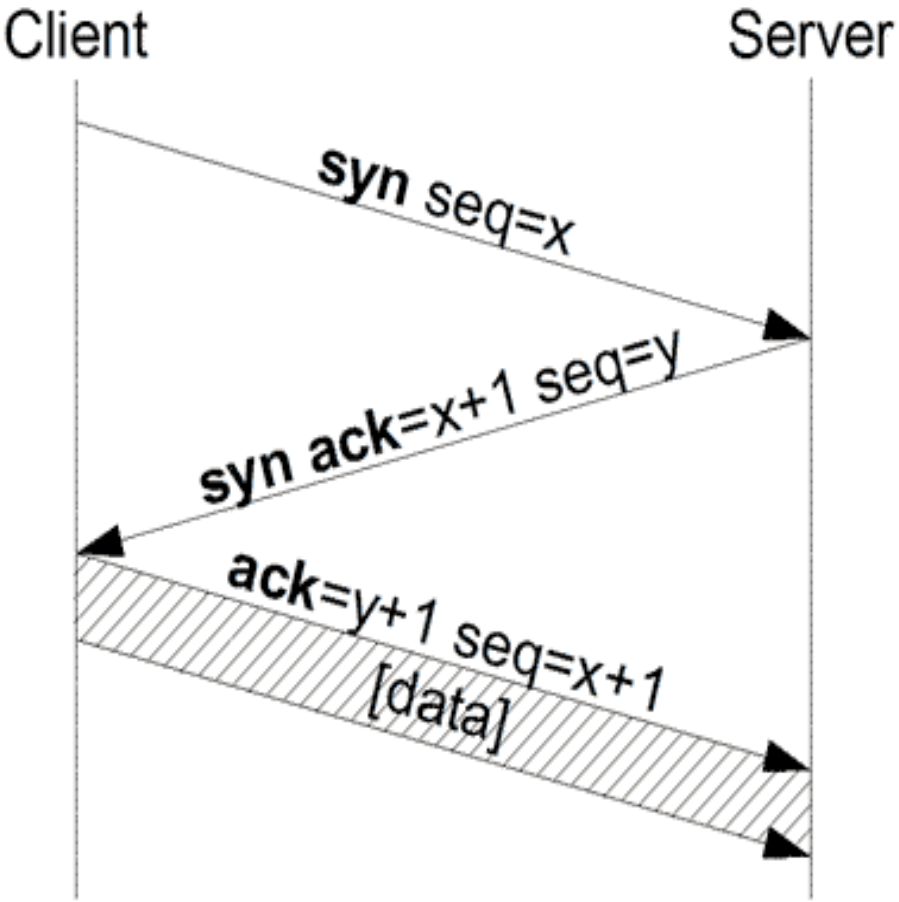
- Feasible when there is a **mismatch** between
  - Client resources to issue a request
  - Server resources respond to the request

  E.g.,
  - SSL/TLS Handshake RSA verification
  - HTTP request of large files

* Flash forward: **Every** technique used to launch a DoS attack can be used as part of a Distributed DoS (DDoS) attack...

SYN Flooding (1)

Transport Layer Attacks (SYN Flooding)

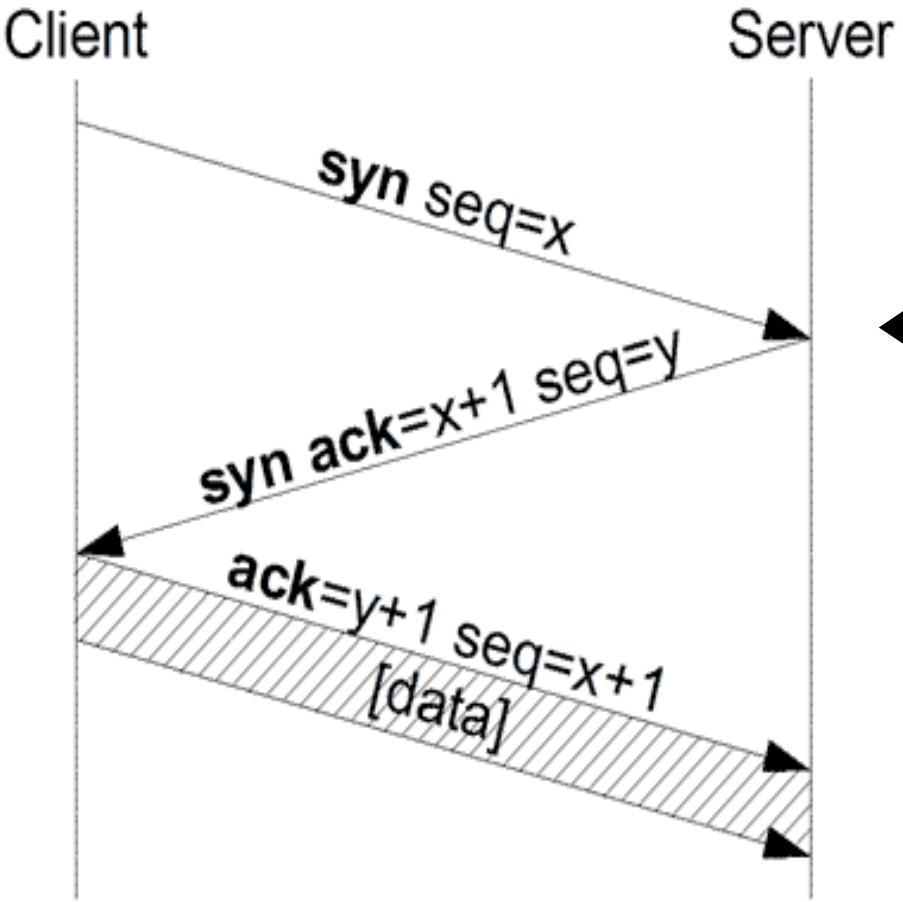


A TCP connection is established with a 3-way handshake

- SYN message
- SYN-ACK message
- ACK message

SYN Flooding (2)

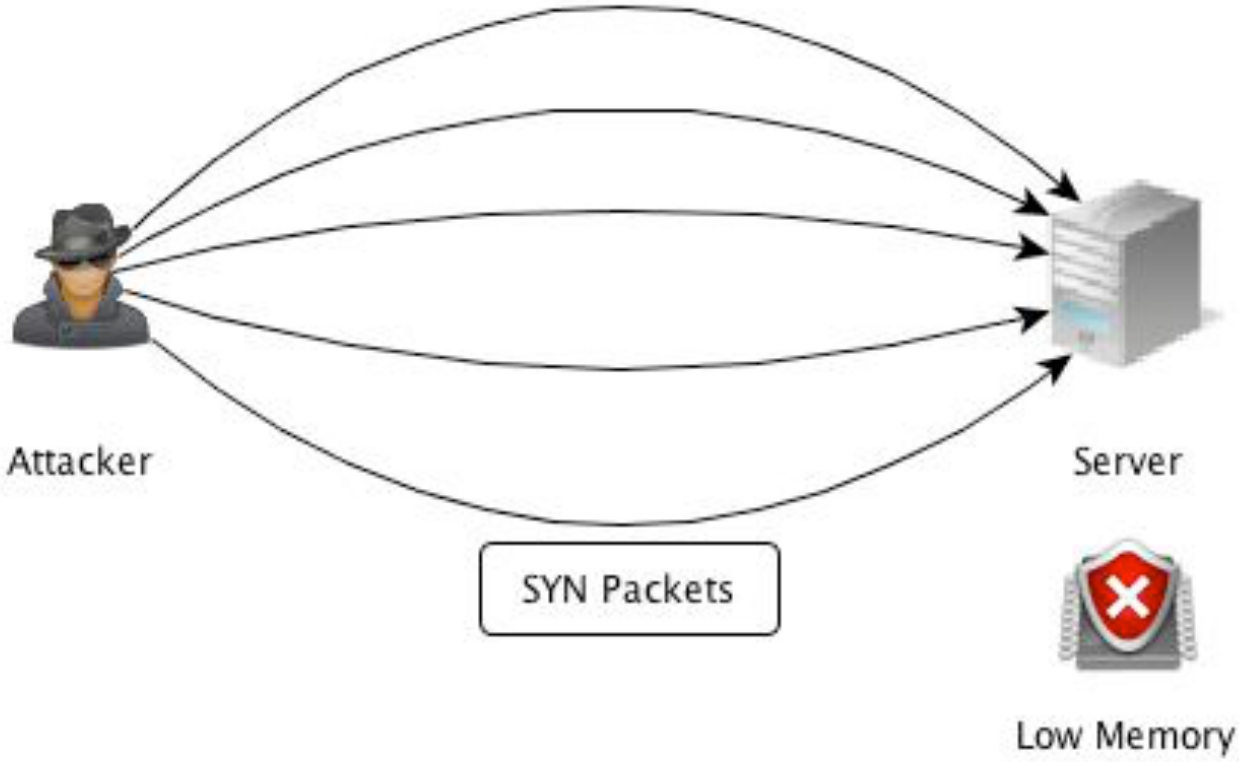
Transport Layer Attacks (SYN Flooding)



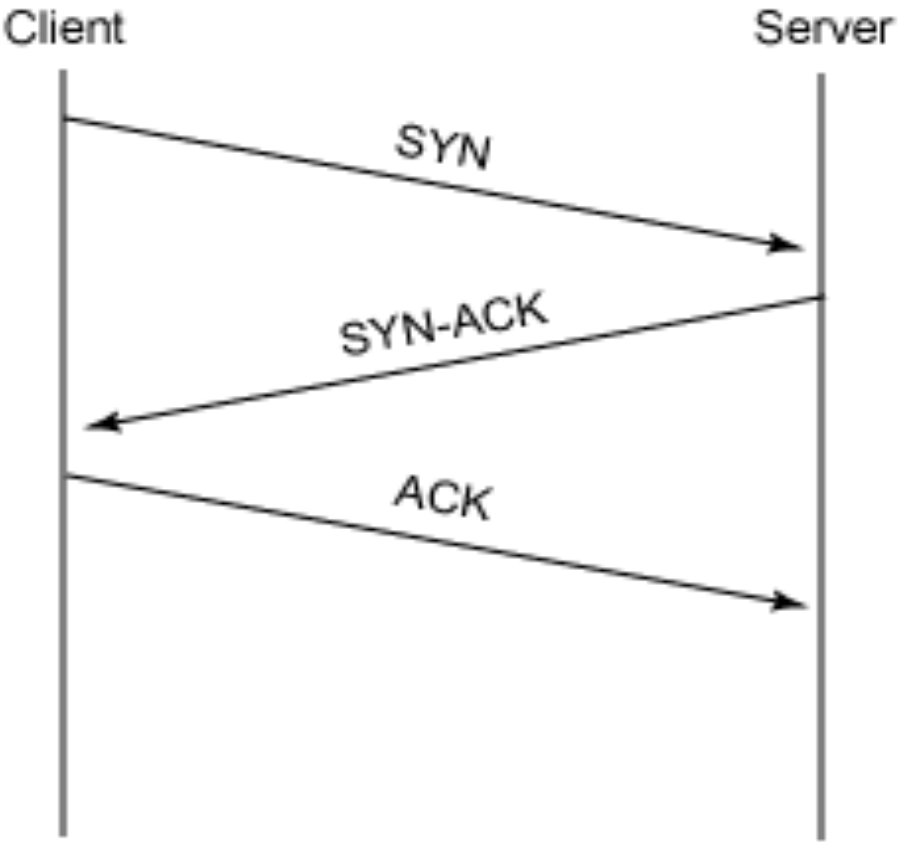
At this point the server keeps state and as a result consumes resources

SYN Flooding (3)

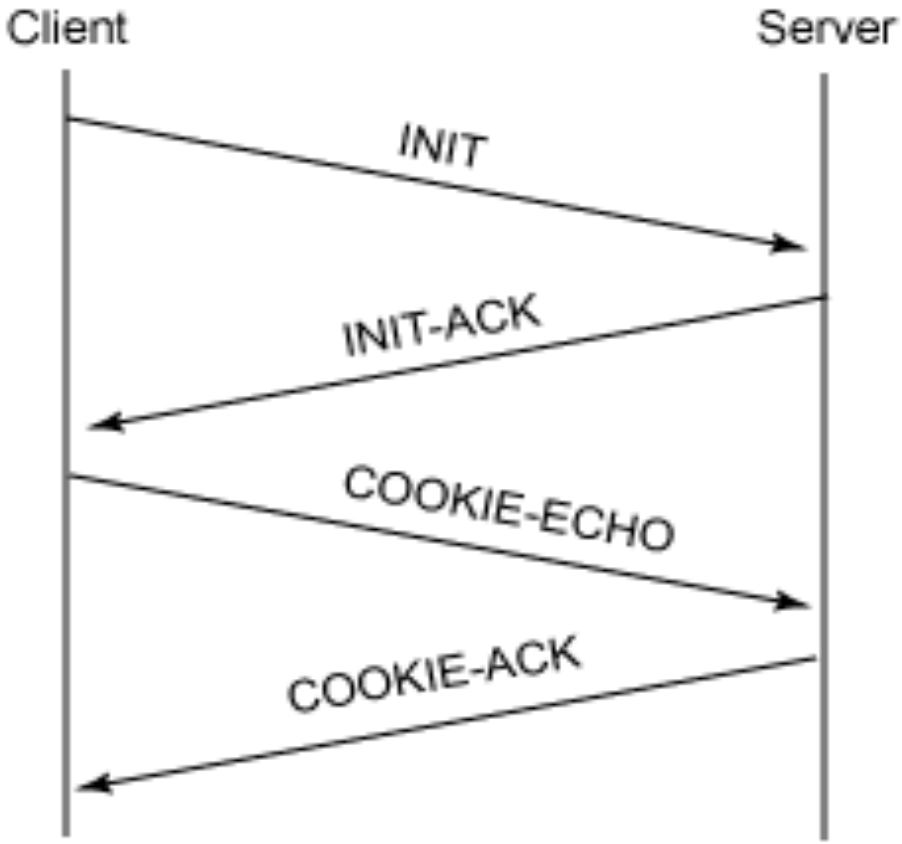
Transport Layer Attacks (SYN Flooding)



Protecting Against SYN-Flooding: The SCTP Protocol



TCP 3-way handshake



SCTP 4-way handshake

Protecting Against SYN-Flooding: The SCTP Protocol

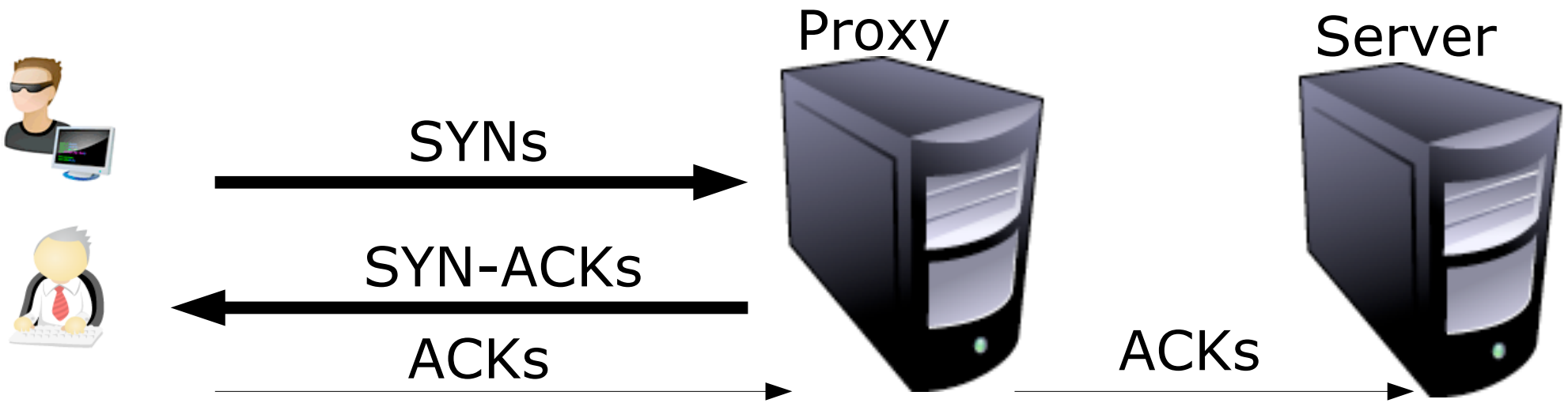
- Use of SCTP transport protocol:

  - The server sends a **cookie** to the initiator of the SCTP connection **(INIT- ACK)**
  - If the client did not use a spoofed IP address, then she receives the cookie and replays it back to the server
  - The server calculates the cookie in the **INIT-ACK** message and does not save it (no state kept)
  - Rather, it expects the **COOKIE-ECHO** within a (short) "validity" period. If so, it saves the state and proceeds

Protecting Against SYN-Flooding: Proxies

Preventing SYN Flooding:

- Use of Proxies

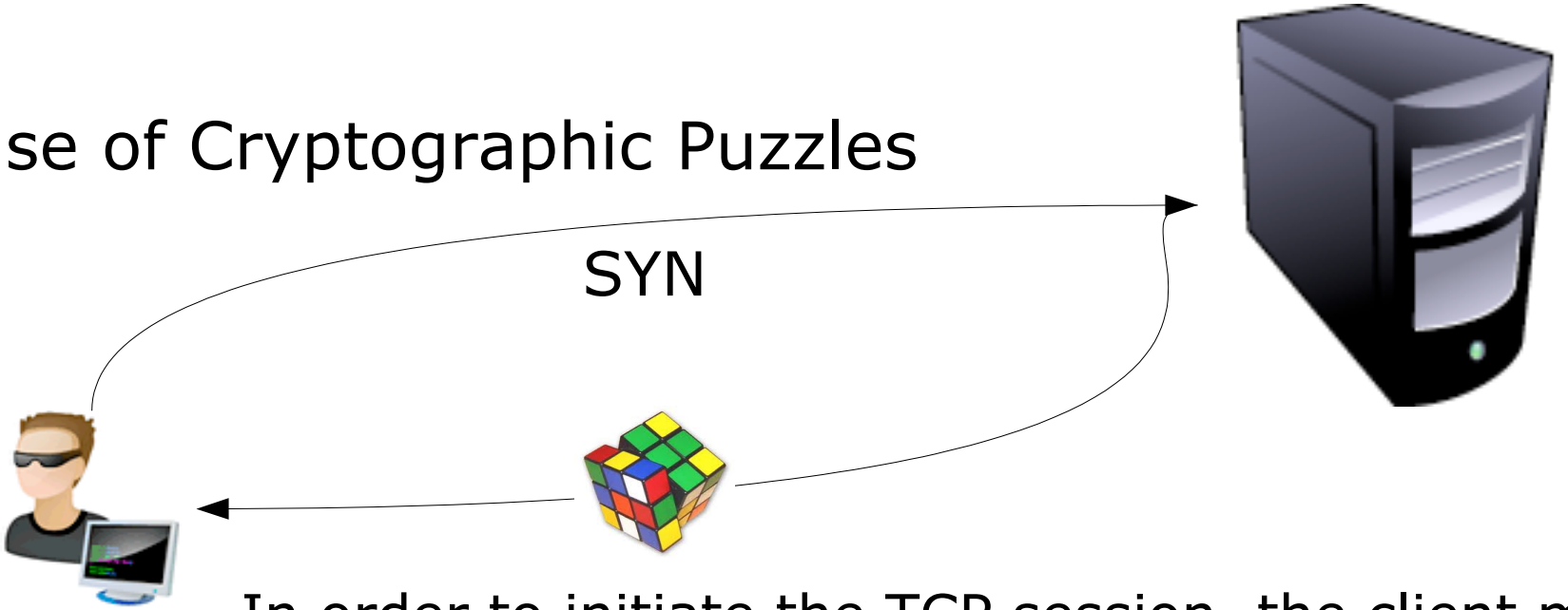


Protecting Against SYN-Flooding: Cryptographic Puzzles

Transport Layer Attacks (SYN Flooding)

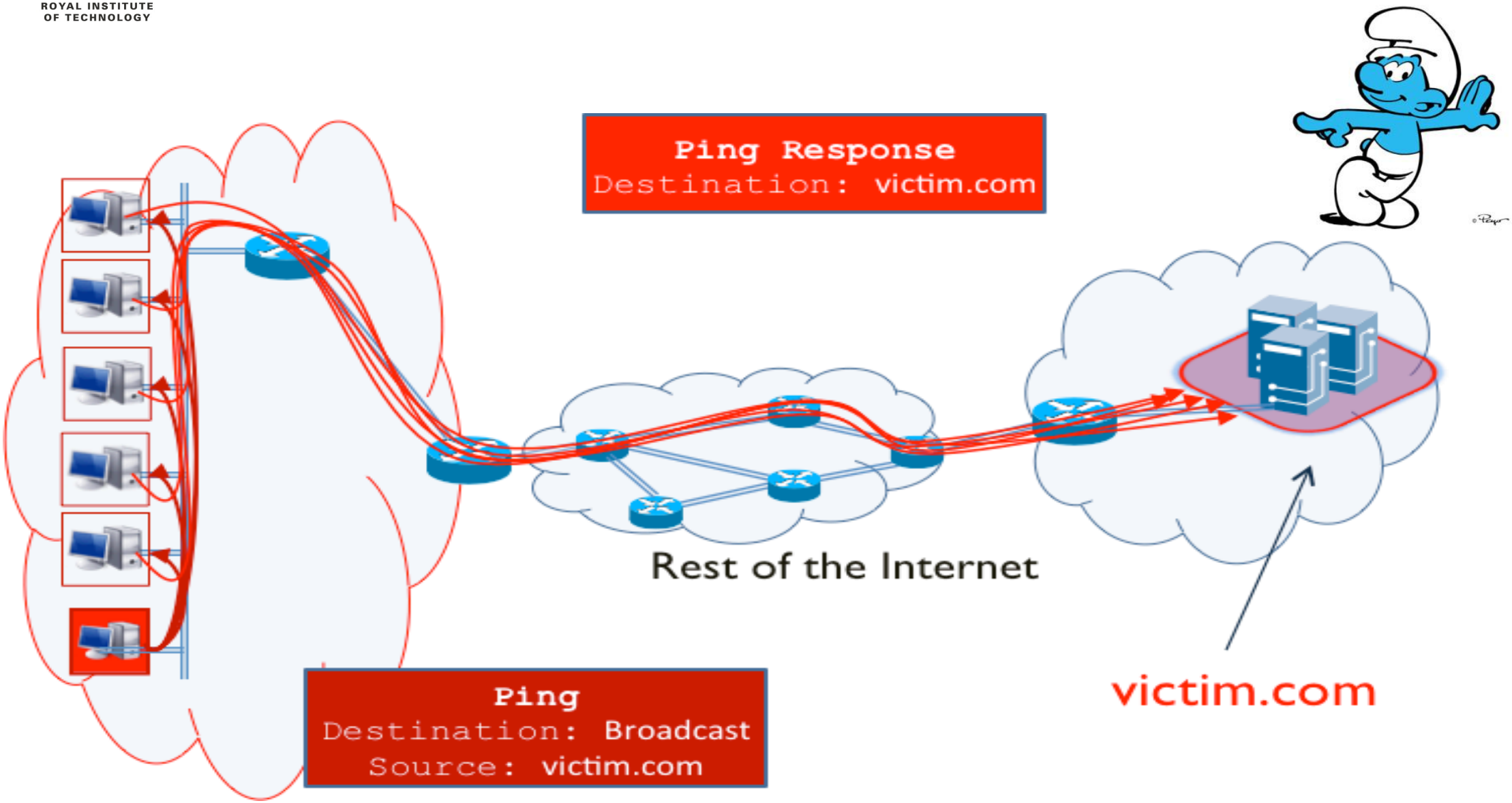
Preventing SYN Flooding:

- Use of Cryptographic Puzzles



In order to initiate the TCP session, the client must solve a (cryptographic) puzzle.

Smurf Attacks



Preventing Smurf Attacks

- Ingress Filtering must prevent the forwarding of Directed Broadcast Traffic

- Use Access Control to define which hosts (subnets) can trigger directed Broadcast traffic (CISCO Guide)

Distributed Denial of Service (DDoS) Attacks

DoS vs DDoS

Hollywood version of a **BotNet**

Vs

[Agent Smith, aka Hugo Weaving; "The Matrix" (motion picture)]

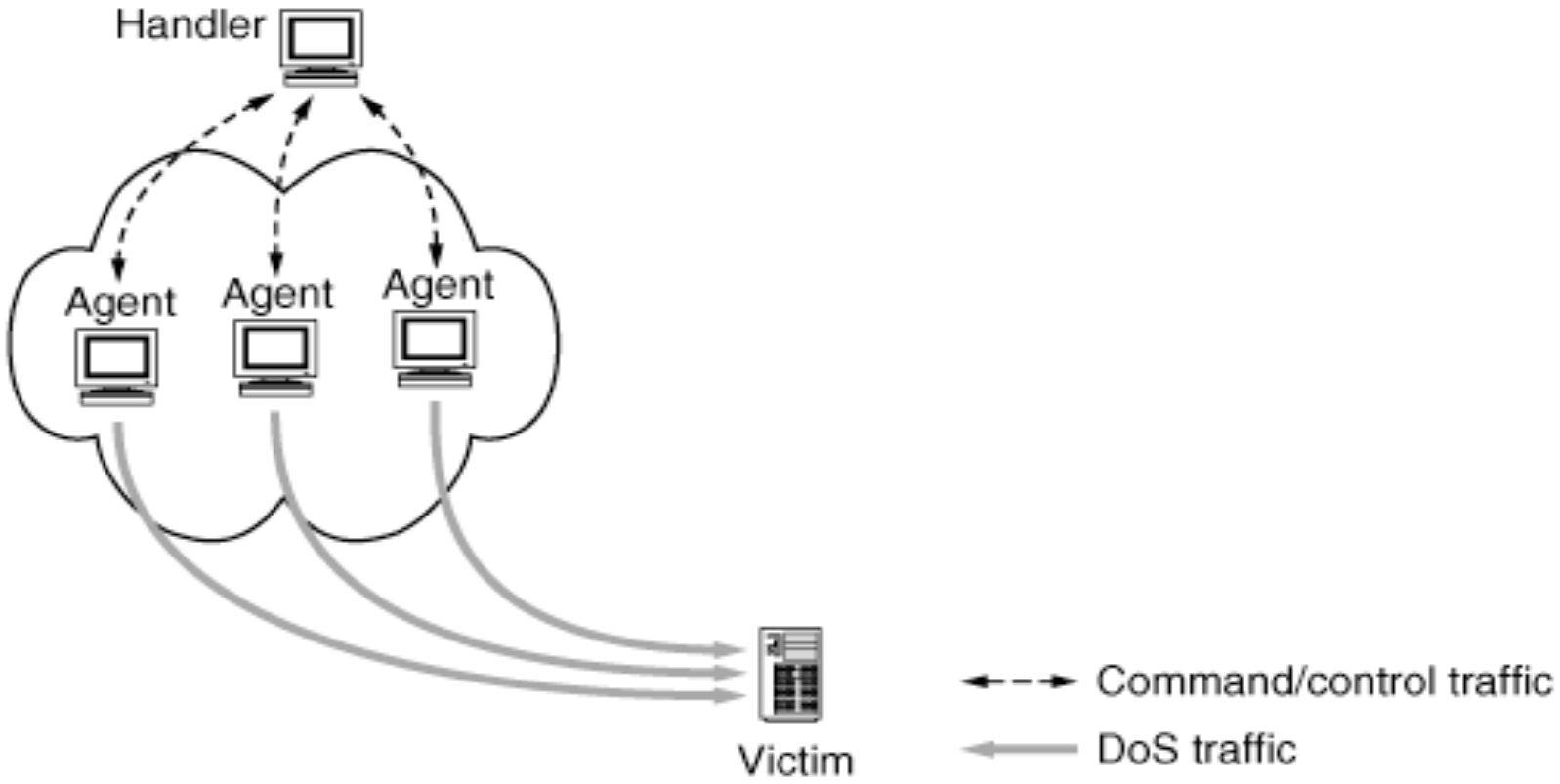
ROYAL INSTITUTE OF TECHNOLOGY

Basic BotNet Architectures

BotNet: A large number of compromised computers

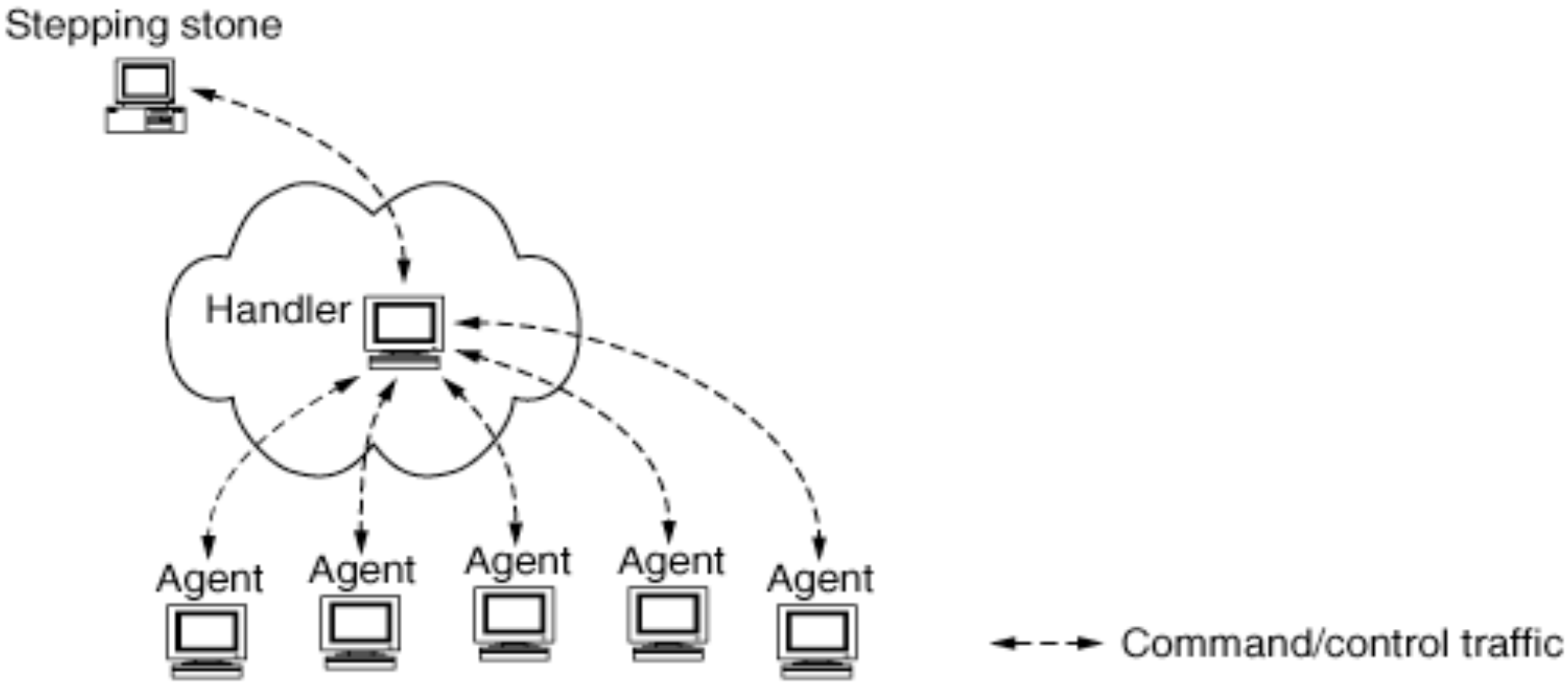
- Controlled by one or more Bot-Masters
- Computers are 'recruited' with the use of Malicious Code (Trojan, viruses, backdoors ...)
- BotNets are used for various malicious purposes:
  - DDoS
  - Spam
  - Attacking on-line communities
  - ...

Basic BotNet Architectures (1)



Internet Denial of Service: Attack and Defense Mechanisms

Basic BotNet Architectures (2)



Internet Denial of Service: Attack and Defense Mechanisms

Basic BotNet Architectures (3)

- Stepping Stone machines
  - Bot-Masters communicate with Handlers going through Stepping Stones
  - Stepping Stones are, in essence, an additional layer of hierarchy in the BotNet architecture
  - Their purpose: to prevent tracing of the Bot-Masters

ROYAL INSTITUTE OF TECHNOLOGY

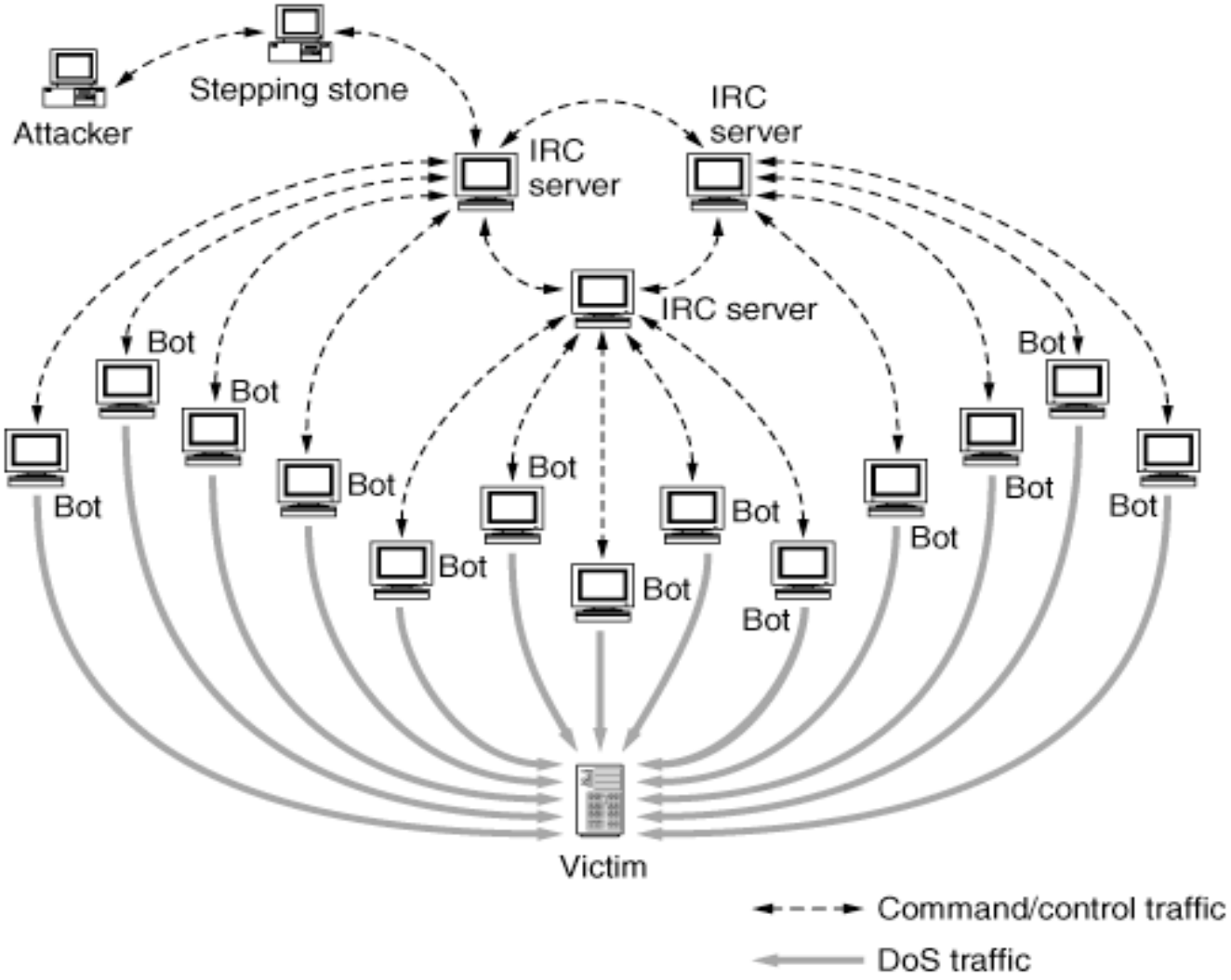
Basic BotNet Architectures (4)

- A Handler machine controls the bots of the BotNet
- Control Traffic between the Handler and the Bots
- Attack DDoS Traffic: sent by the bots to the targeted victim server

Basic BotNet Architectures (5)

- But, still, direct communication between the Handler and the Bot-Master is easily traceable
- Further obscurity is required so that Bot-Masters are not traceable

IRC controlled BotNets



ROYAL INSTITUTE OF TECHNOLOGY

IRC controlled BotNets (2)

The most common DDoS Architecture

- For historical reasons
- For obscurity (thousands of channels)
- Maintainability (IRC Channels are maintained by IRC communities)

BotNet Recruitment

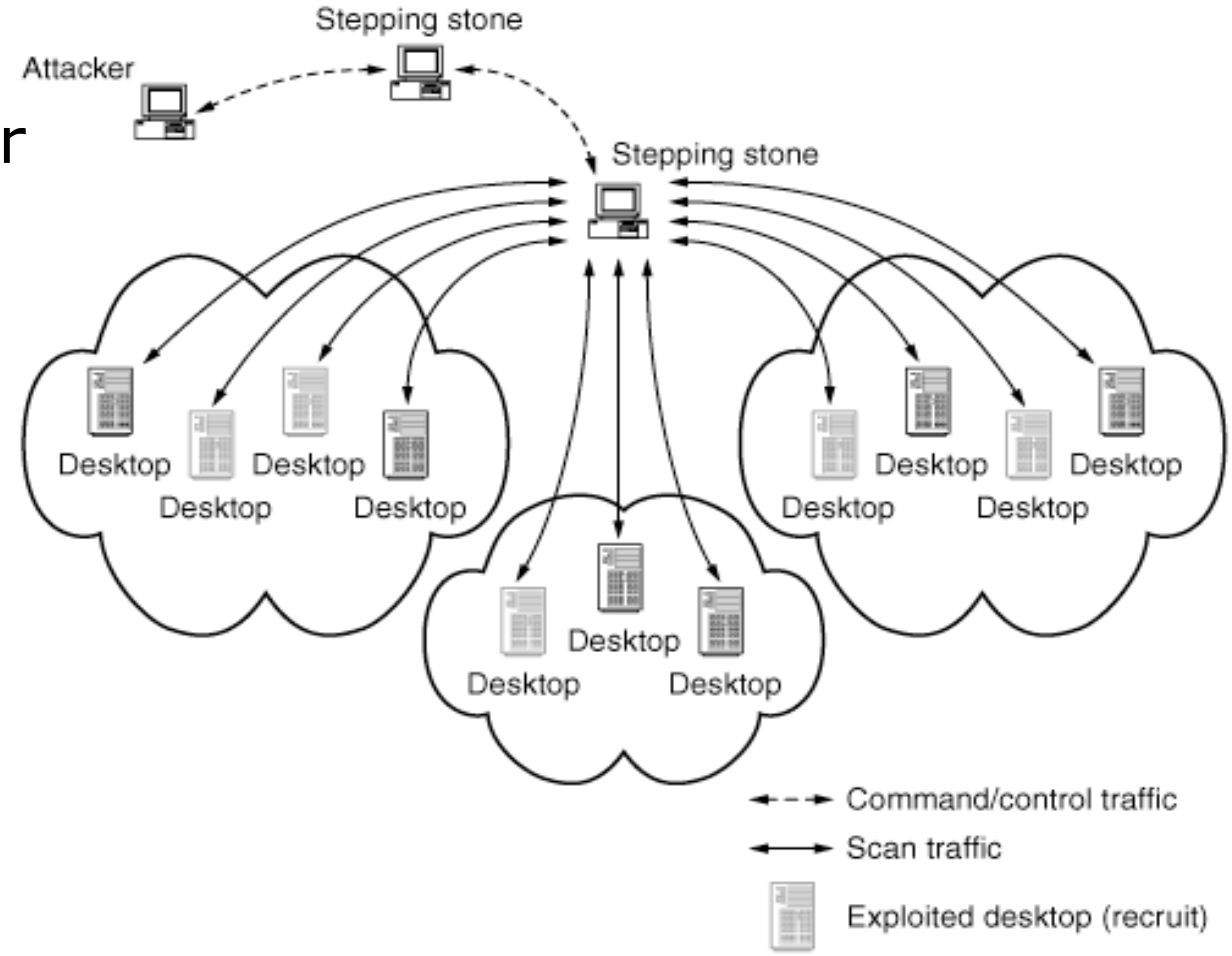
BotNet Recruitment (1)

Scanning for vulnerable machines to 'recruit' for a BotNet:

- Random: Brute-force the IP address space
- Random IP range: Scan randomly, a specific range of the IP space
- Intelligent scan: Look for specific type of machines like Windows boxes
- Step-by-step scanning: Once a machine is compromised, check for other machines it is associated with

BotNet Recruitment (2)

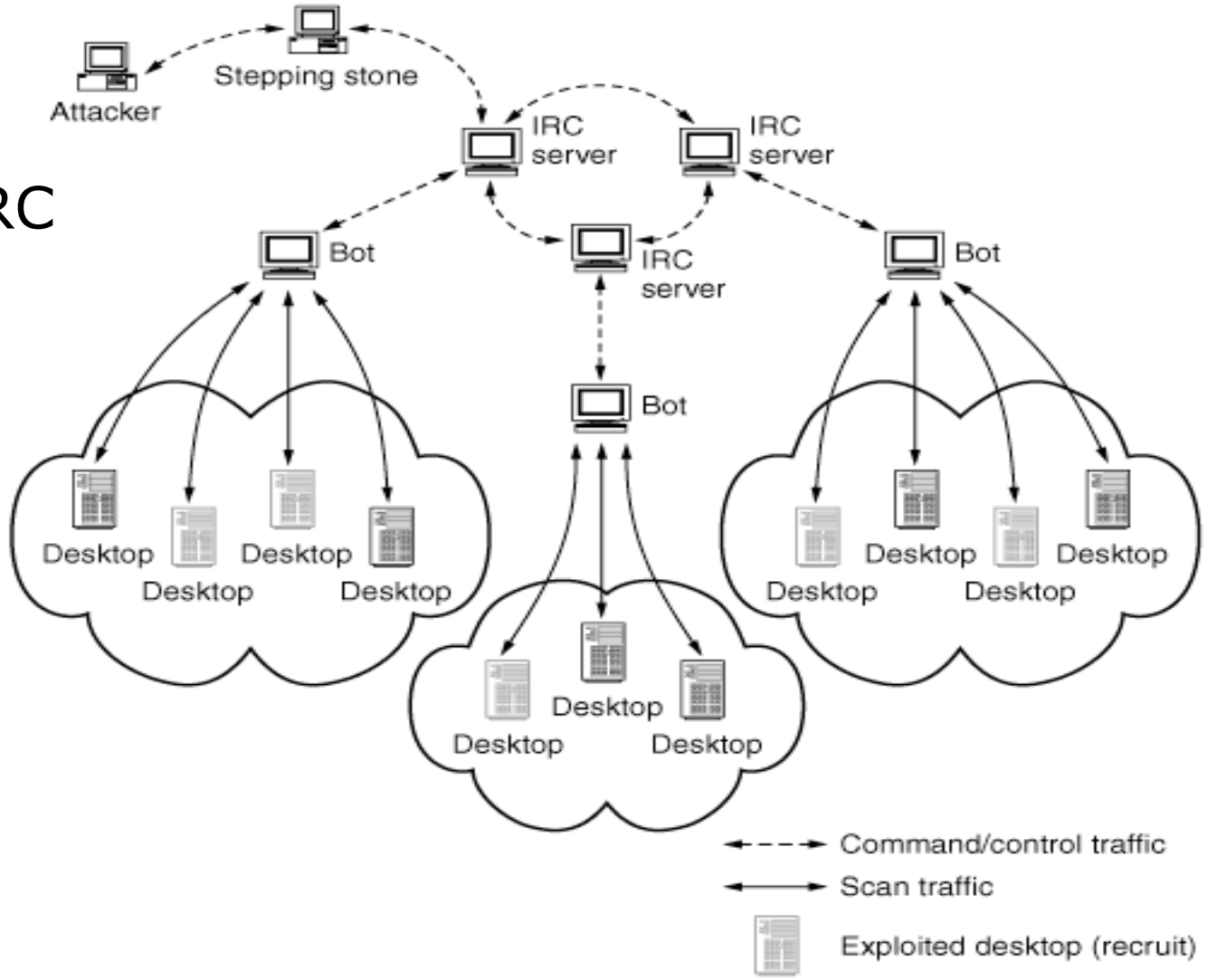
Stepping Stones looking for vulnerable machines



Internet Denial of Service: Attack and Defense Mechanisms

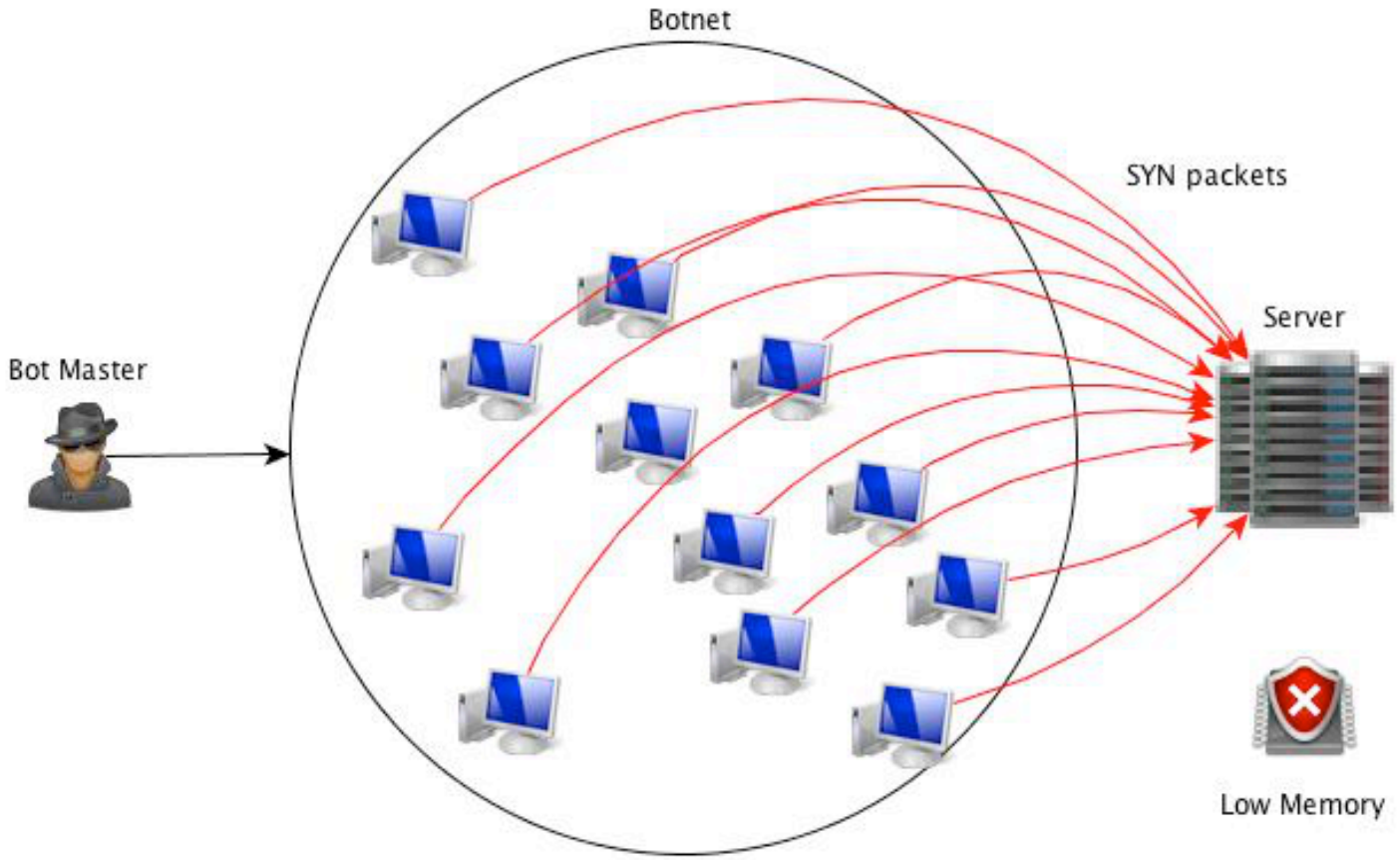
BotNet Recruitment (3)

Looking for vulnerable machines within the IRC network



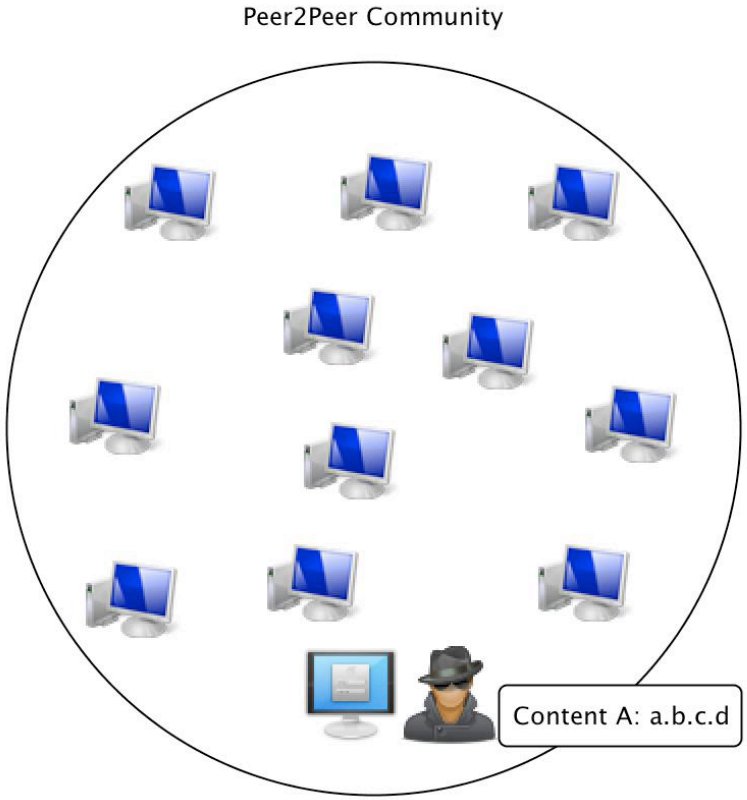
Internet Denial of Service: Attack and Defense Mechanisms

Distributed SYN flooding



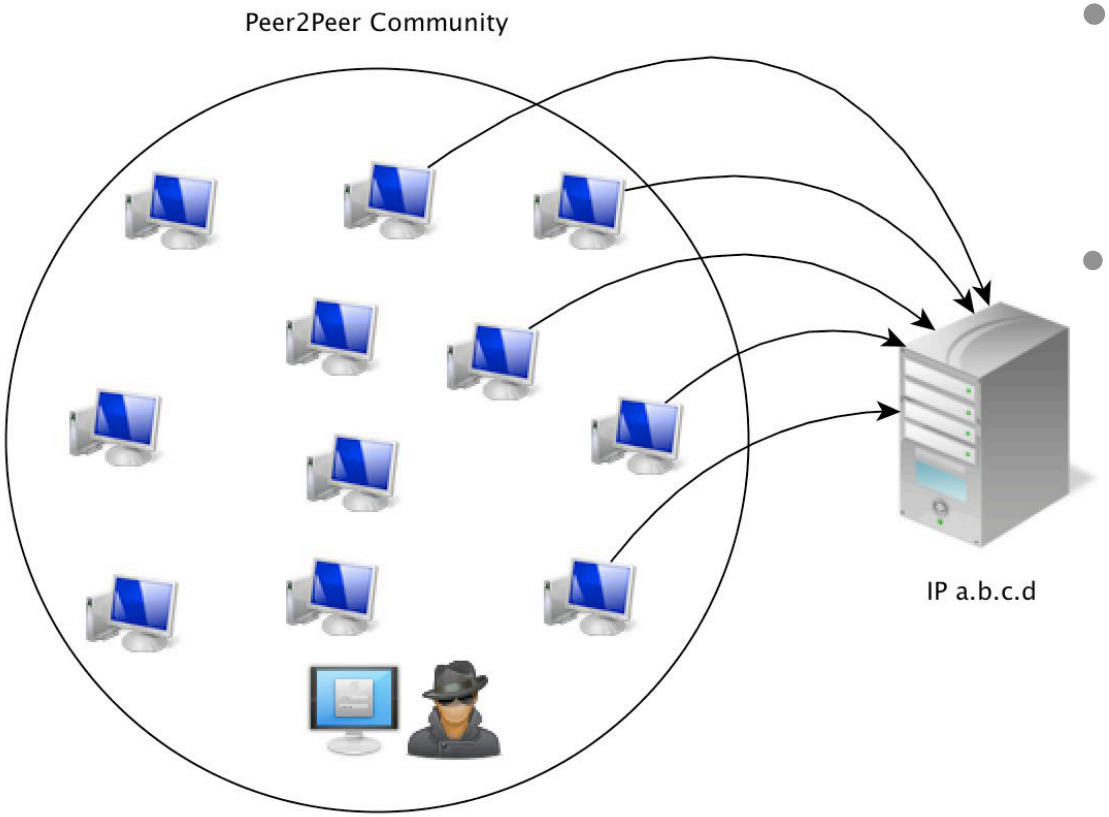
- The same idea like the simple DoS version of TCP flooding
- Much more effective due to the use of a BotNet
- Server has to keep state for thousands semi-open TCP sessions.

P2P based DDoS Attacks



- A large number of hosts have joined a P2P Community for content exchange purposes

P2P based DDoS Attacks (2)



- The server is overwhelmed with requests for content it does not possess
- Most of the time, the connections that the hosts try to establish to the server are TCP connections

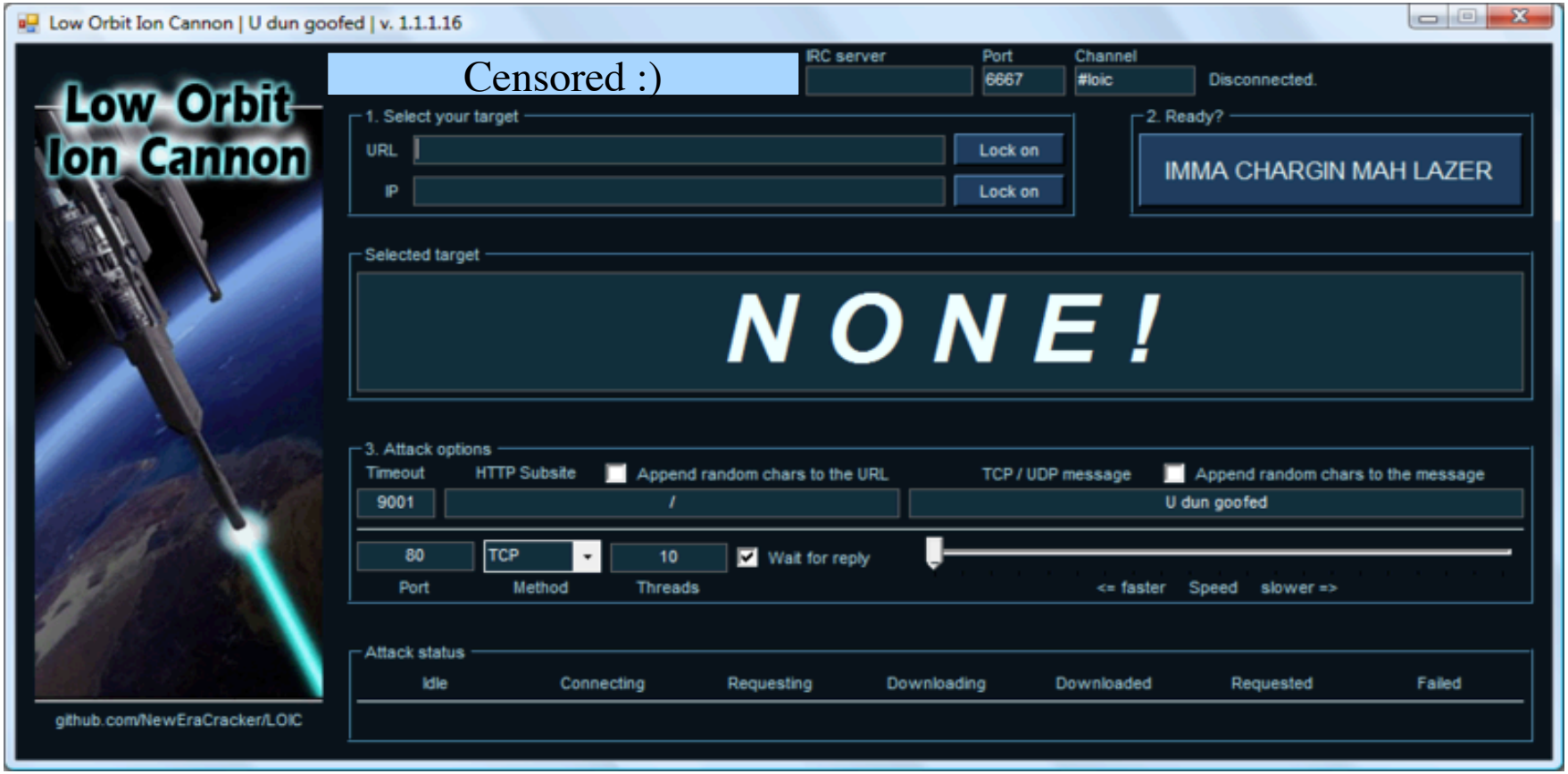
Operation #PayBack

Social DDoS

- Social BotNets
- Normal users joining willingly a DDoS attack against major websites (paypal, mastercard, visa, ...)

Operation #PayBack (2)

Social DDoS



http://en.wikipedia.org/wiki/LOIC

Operation #PayBack (3)

Social DDoS

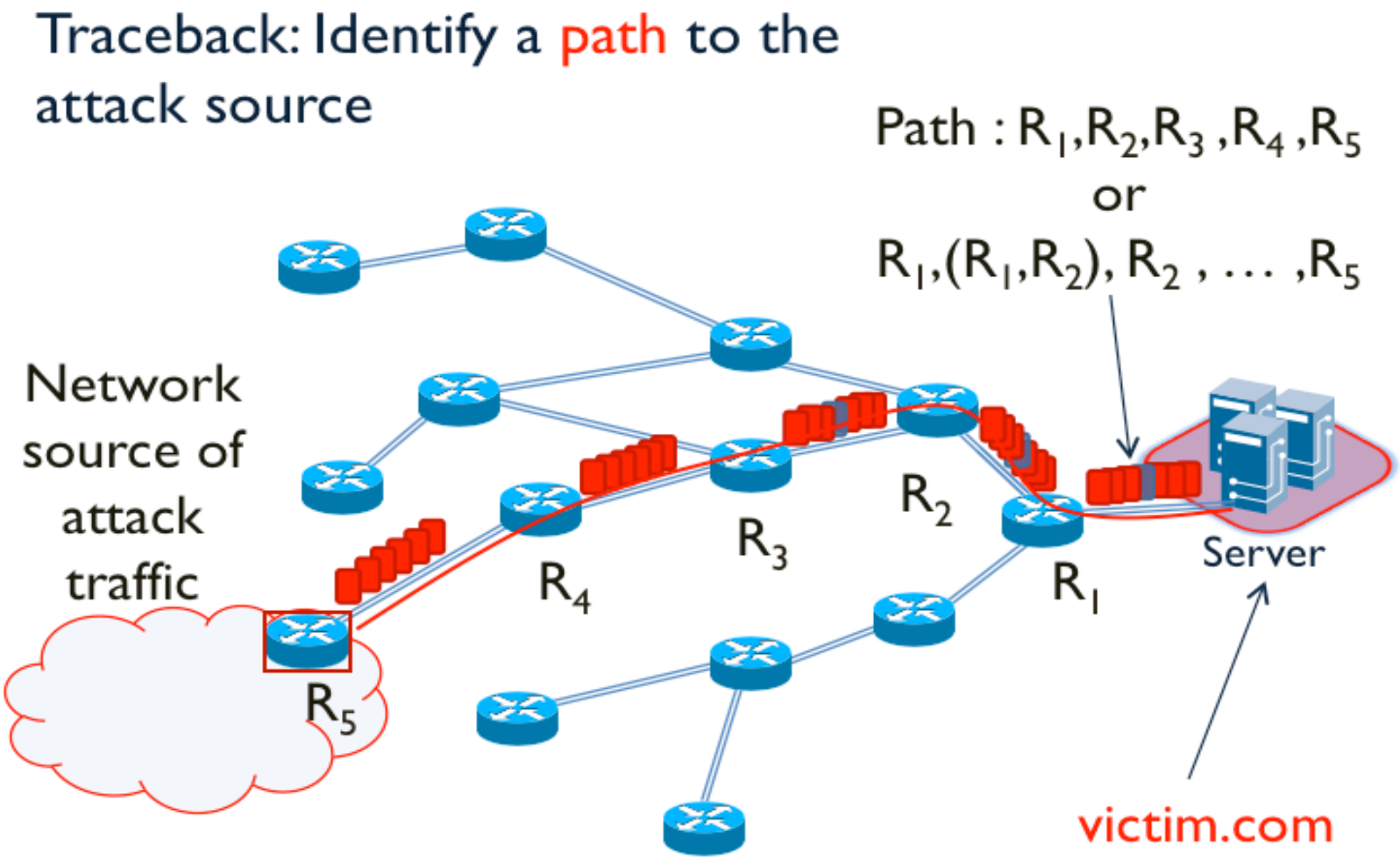
Operation Payback @Anon_payback 8 Dec 10

CURRENT TARGET: WWW.VISA.COM :: WEAPONS

http://bit.ly/e6iR3X ::: SET YOUR LOIC TO --> irc.anonops.net &

FIRE FIRE FIRE!!! #WIKILEAKS #DDOS

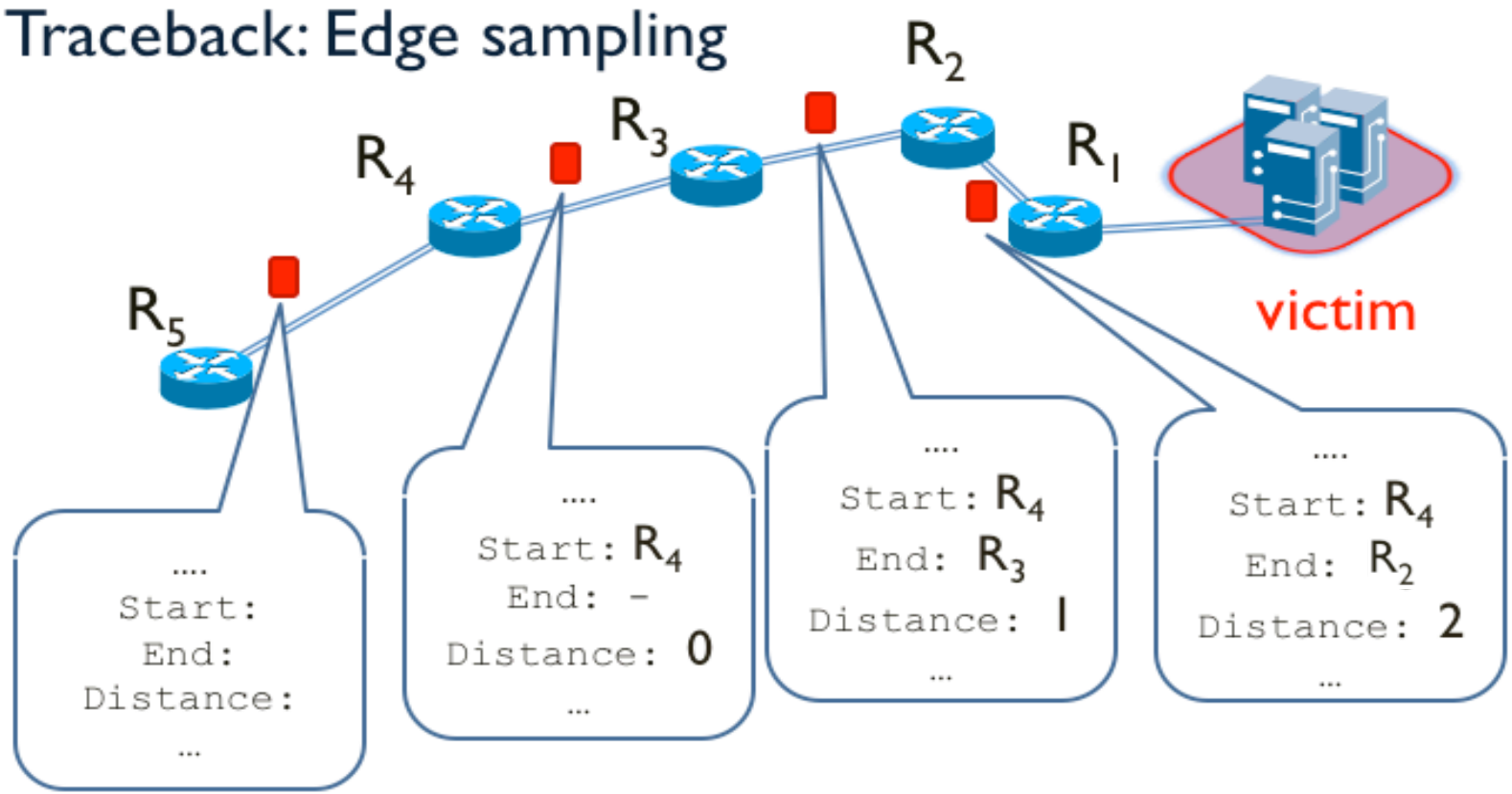
Research on DoS and DDoS



[S. Savage, D. Wetherall, A. Karlin and T. Anderson, "Practical Network Support for IP Traceback," ACM SIGCOMM 2000]

13

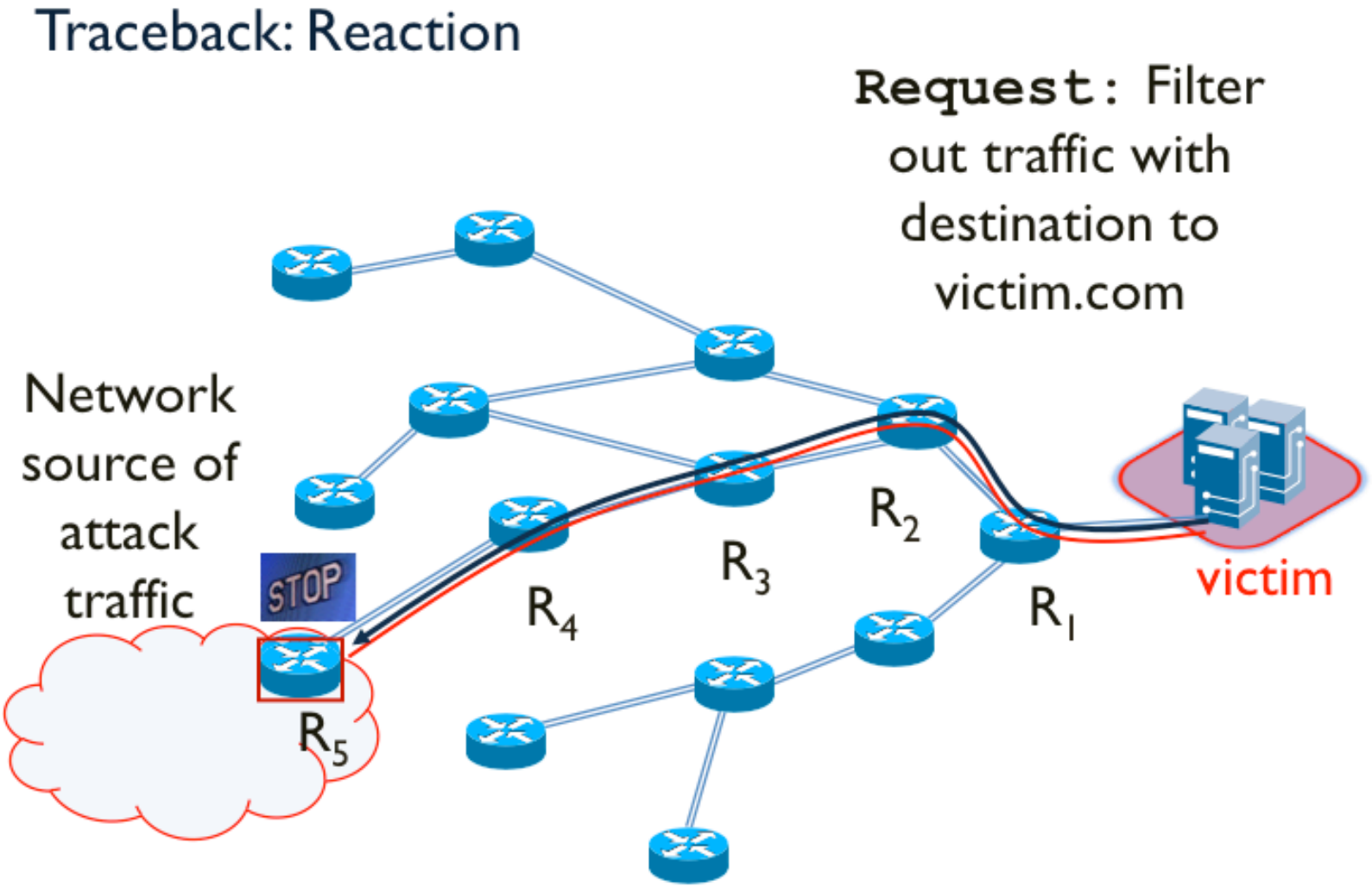
Research on DoS and DDoS



- Victim:
  - Gets (R_i,R_j,d) from each *attack* packet
  - Adds it to the 'picture' if it fits in

14

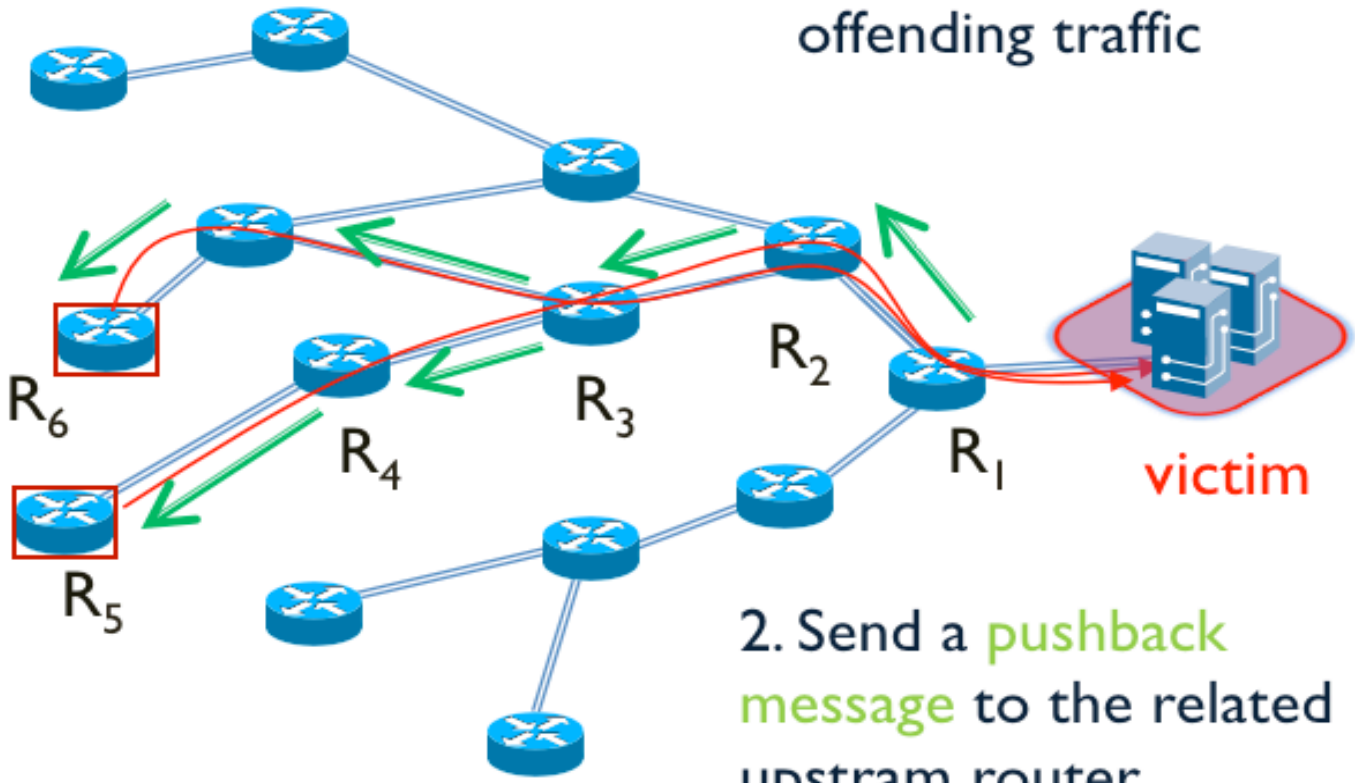
Research on DoS and DDoS (2)



Research on DoS and DDoS (3)

Pushback: Deal with congestion one hop at a time

1. Detect an aggregate of offending traffic



2. Send a pushback message to the related upstram router

[R. Mahajan, S. Bellovin, S. Floyd, J. Ioannidis, V. Paxson, and S. Shenker, "Controlling High Bandwidth Aggregates in the Network," ACM CCR 2002]

18

ROYAL INSTITUTE OF TECHNOLOGY

Conclusions

- DoS and DDoS target the availability of a system/service
- Attackers can take advantage of system defects to launch a DoS/DDoS attack
- DoS attacks do not require many resources from the attacker.
- Any DDoS attack can be launched as a Distributed attack
- These attacks require the use of large collections of infected computers (Botnets)
  - Botnets need to be created, organized and managed
- Different attack traffic can be used by the Botnets to overwhelm a targeted server.
- The countermeasures available depend on the type of the attack
- But still it is and probably will remain a hard problem to solve...
  - Many vulnerable machines out there are willing to join a Botnet