Communication Networks (0368-3030) / Spring 2011

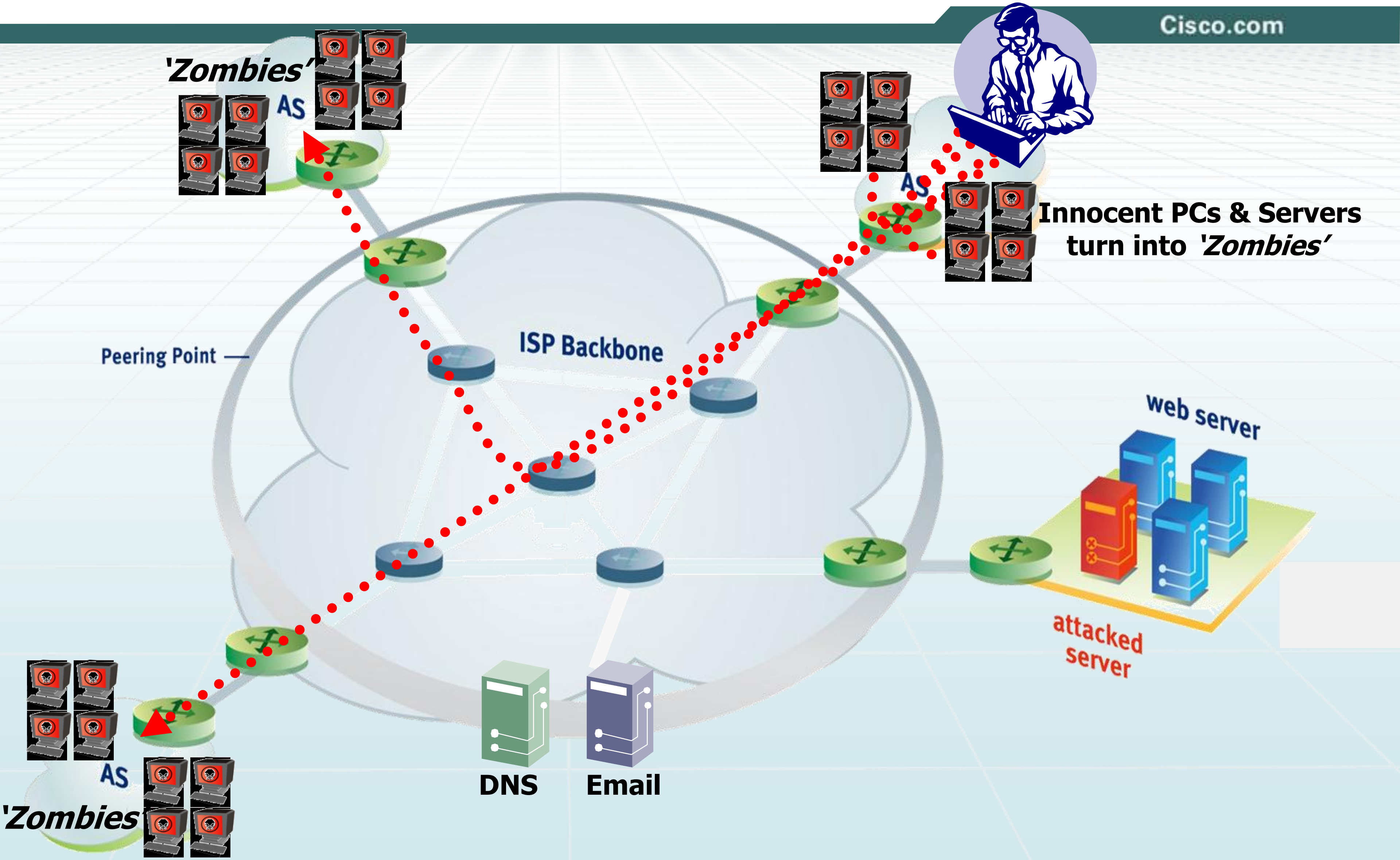
The Blavatnik School of Computer Science, Tel-Aviv University

Allon Wagner

DDoS and Related Attacks

Several slides adapted from a presentation made by Dan Touitou on behalf of Cisco.

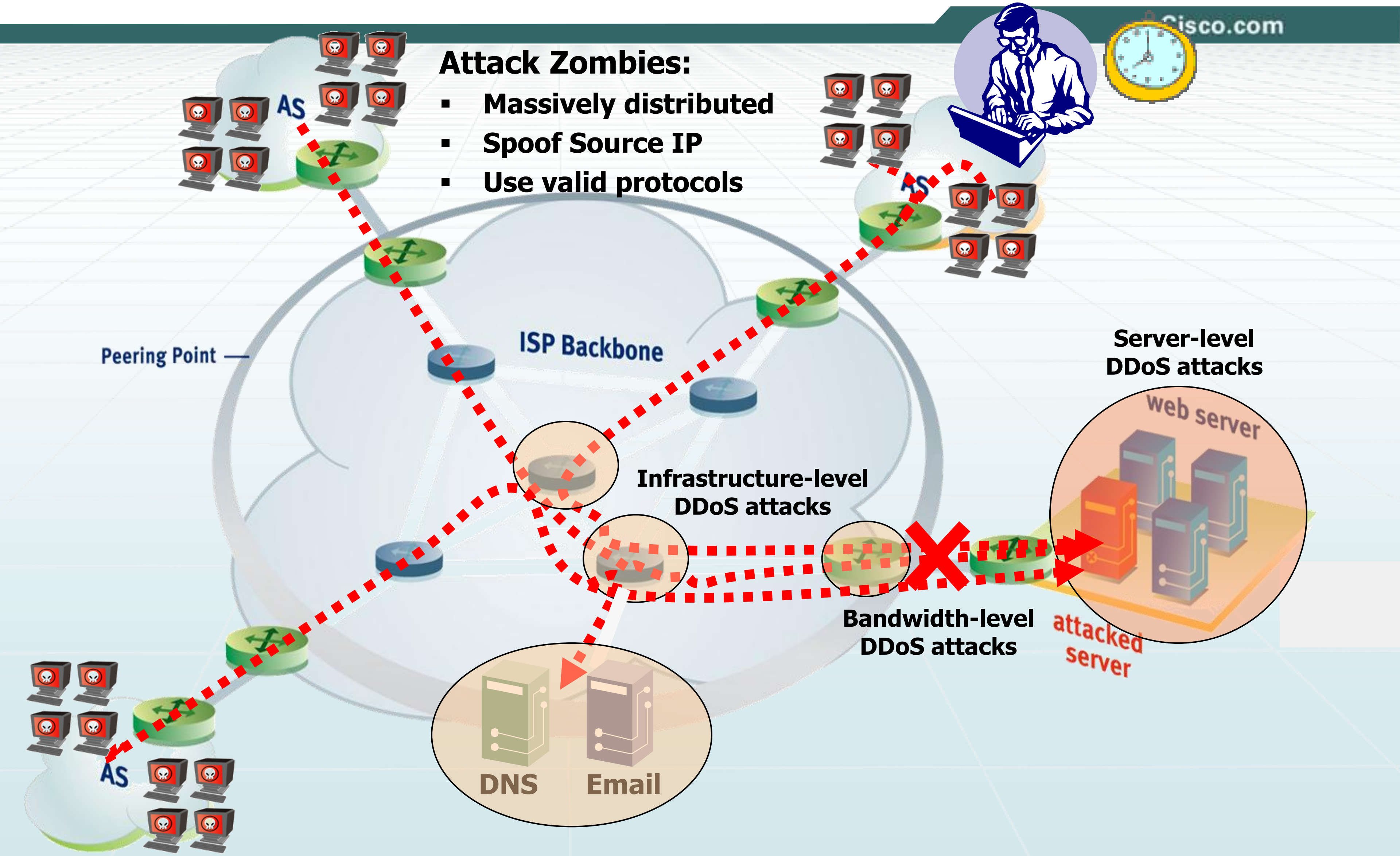
How do DDoS Attacks Start ?



The Effects of DDoS Attacks

Attack Zombies:

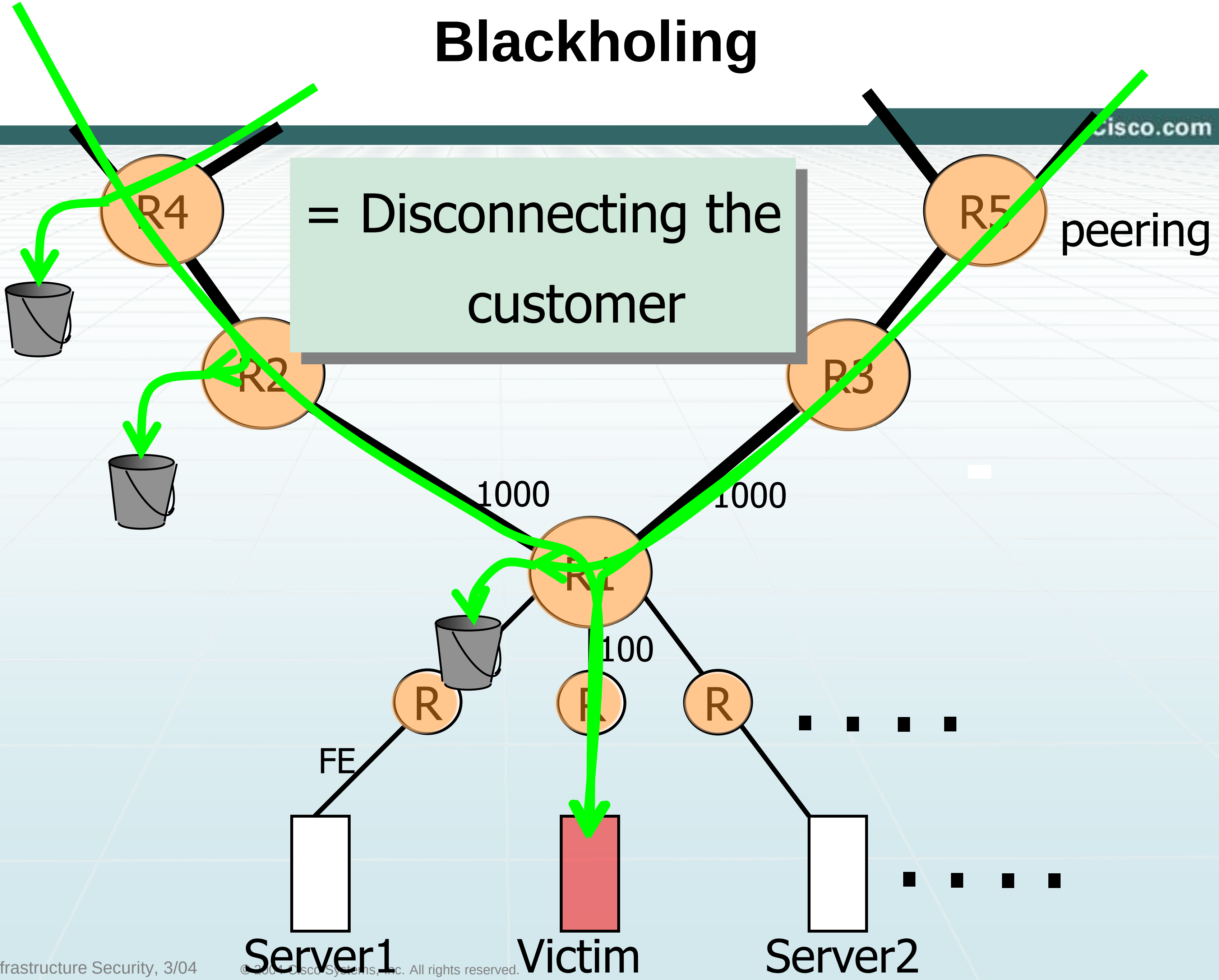
- Massively distributed
- Spoof Source IP
- Use valid protocols



Motivation to attack

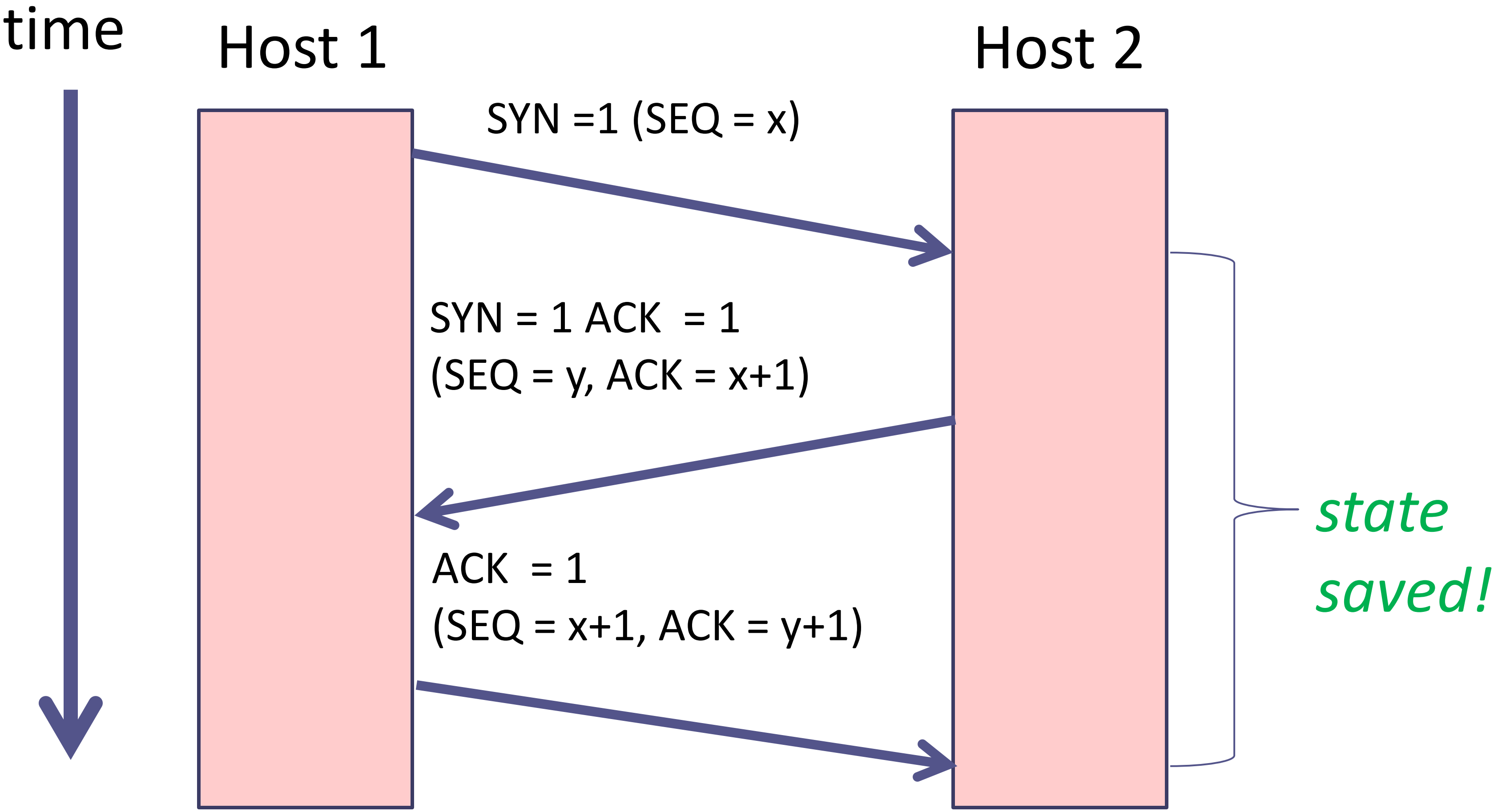
- Economically driven
  - Extortion
  - Zombie armies for hire
- Cyber-vandalism
- Cyber-terrorism / Cyber-war
- Backdrop for a more sophisticated attack
  - For example, an attacker brings a target down, and can then hijack its identity

Blackholing



= Disconnecting the customer

Three-way handshake & SYN-Flood attacks



time

Host 1

Host 2

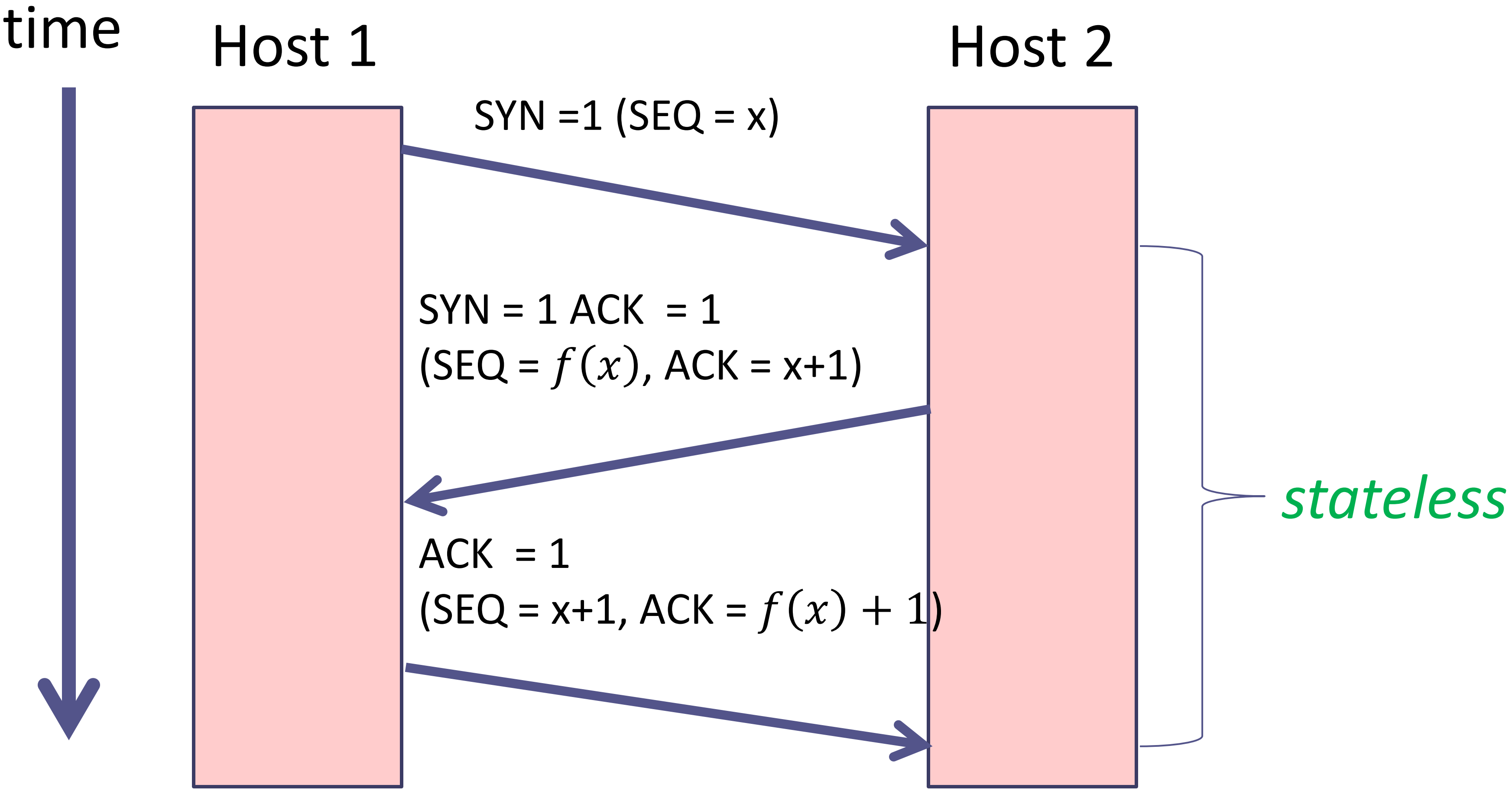
SYN =1 (SEQ = x)

SYN = 1 ACK = 1
(SEQ = y, ACK = x+1)

ACK = 1
(SEQ = x+1, ACK = y+1)

state saved!

SYN Cookies – the idea



SYN Cookies (somewhat simplified)

- A client sends a SYN packet.
- The server does not choose a random SEQ for its reply. Instead, it calculates a $H(x)$ - a cryptographic hash of:
    - t – a slowly increasing time function (e.g increases every 64 seconds)
    - Server's IP and port
    - Client's IP and port
    - s - a secret
- The SEQ returned in the SYN+ACK packet is a concatenation $(t, H(x))$.

SYN Cookies (somewhat simplified)

- When a new client sends an ACK with ACK=y, the server decreases 1 and obtains:
  - ▫ t – allows it to ensure this is a recent request
  - ▫ the supposed hash result $H'(x)$
- It can recompute $H(x)$
- If $H(x) = H'(x)$ the client is legitimate and a TCP connection is opened

Anti-spoofing

- Spoofing – masquerading as a different network user
  - IP spoofing
  - DNS spoofing
  - ARP spoofing
  - …
- Malicious clients spoof IP addresses in order to mount DoS attacks.
- An idea to prevent (or at least hinder) spoofing: respond to the client in a way that forces it to reply.

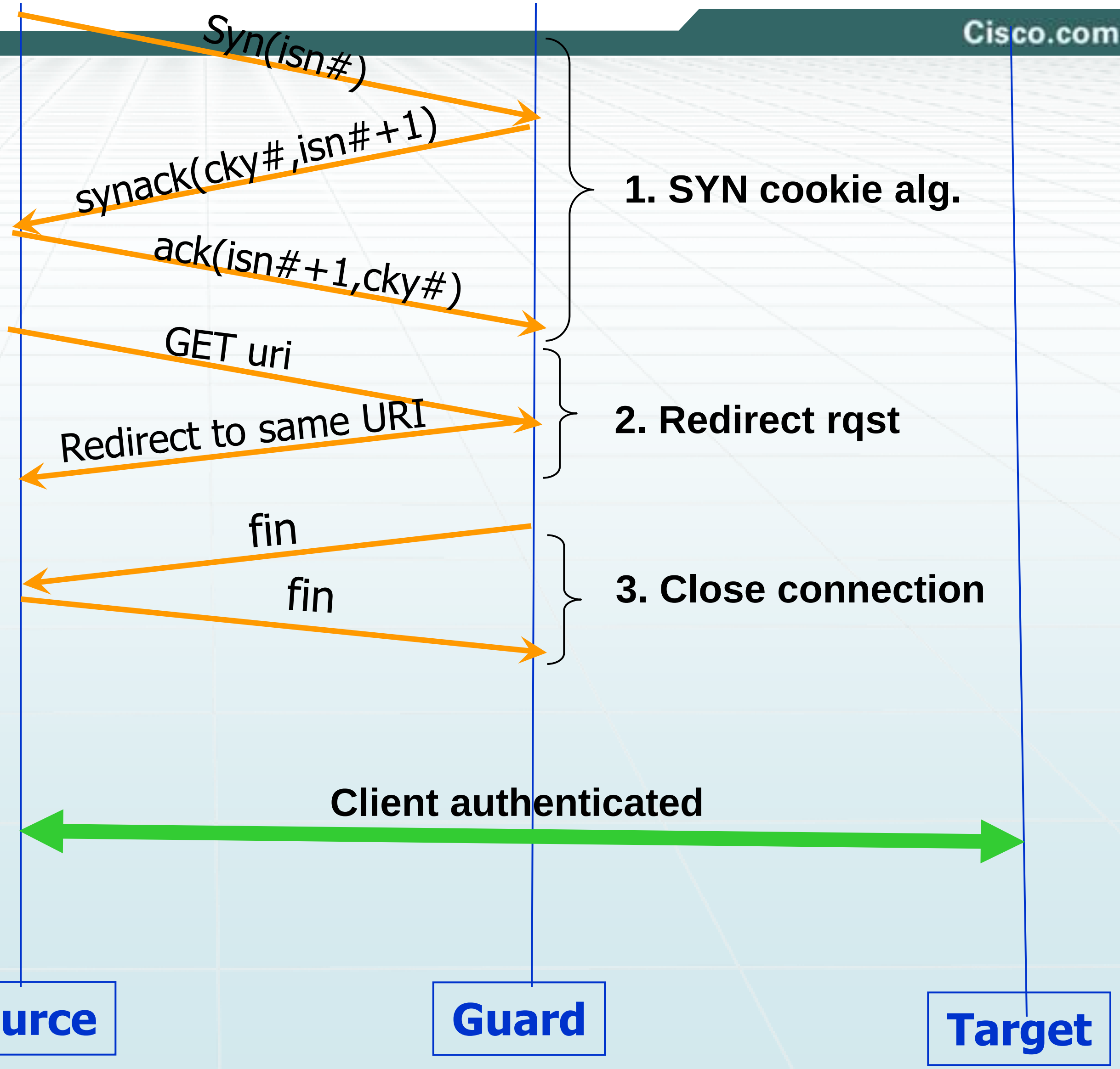
Anti-Spoofing Defense

- One example: HTTP

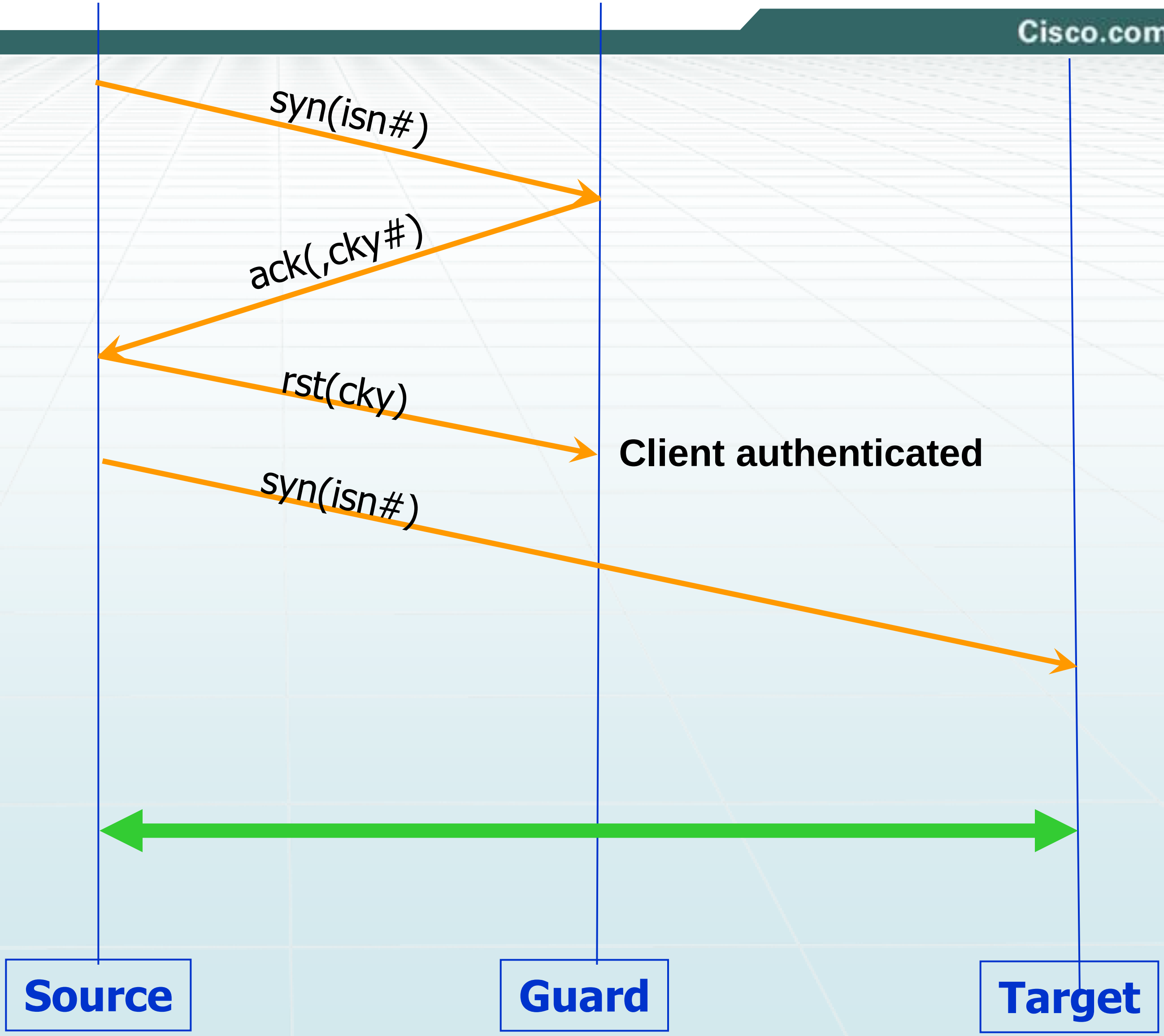
Antispoofing only when under attack

- Authenticate source on initial query

- Subsequent queries verified



RST cookies – how it works



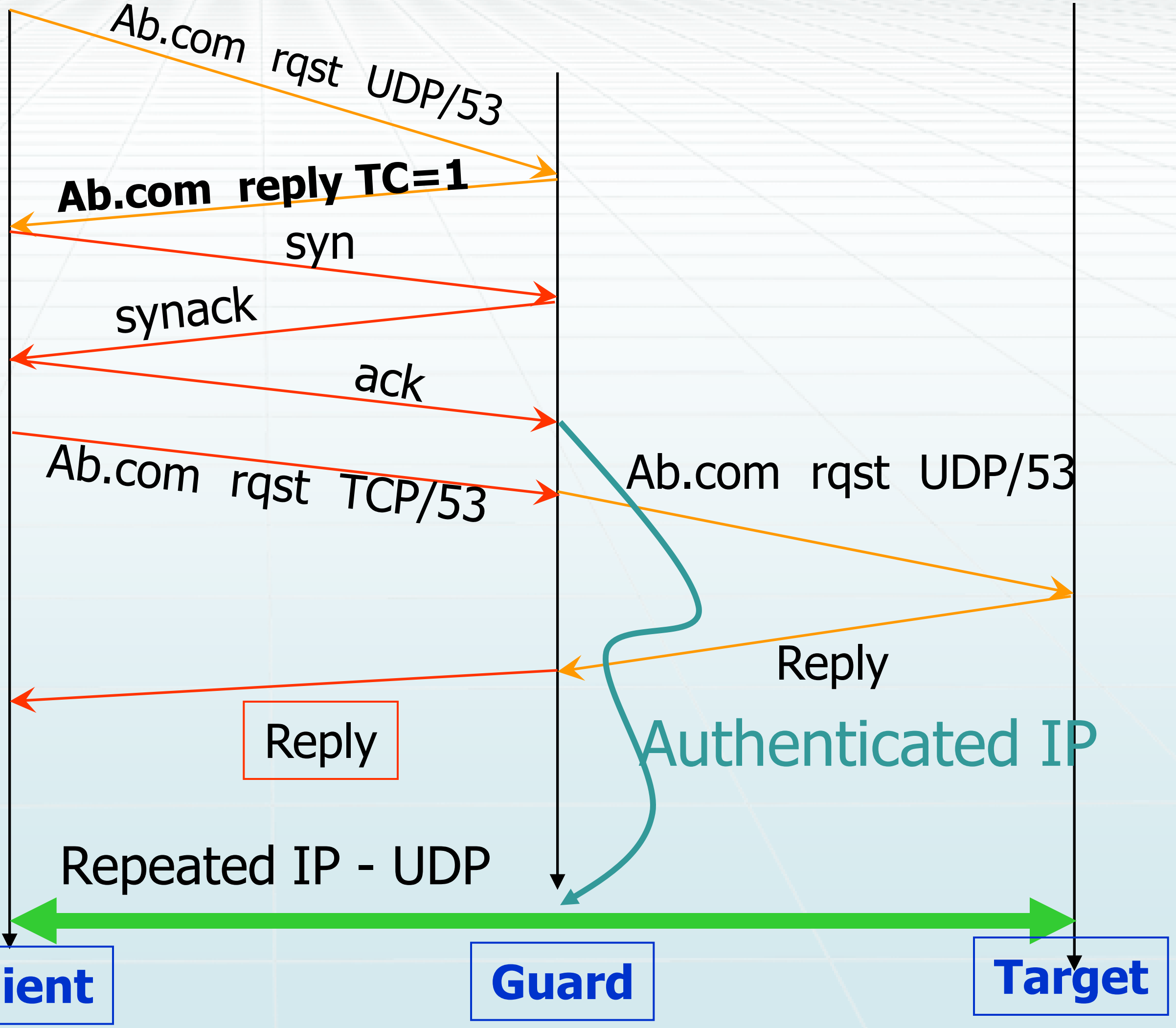
Anti-Spoofing Defense

- One example: DNS Client-Resolver (over UDP)

Antispoofing only when under attack

- Authenticate source on initial query

- Subsequent queries verified


Ab.com rqst UDP/53
Ab.com reply TC=1
syn
synack
ack
Ab.com rqst TCP/53
Ab.com rqst UDP/53
Reply
Reply
Authenticated IP
Repeated IP - UDP
Client
Guard
Target