Network Level Attacks and Mitigation

THE UNIVERSITY OF CHICAGO

Ben Zhao

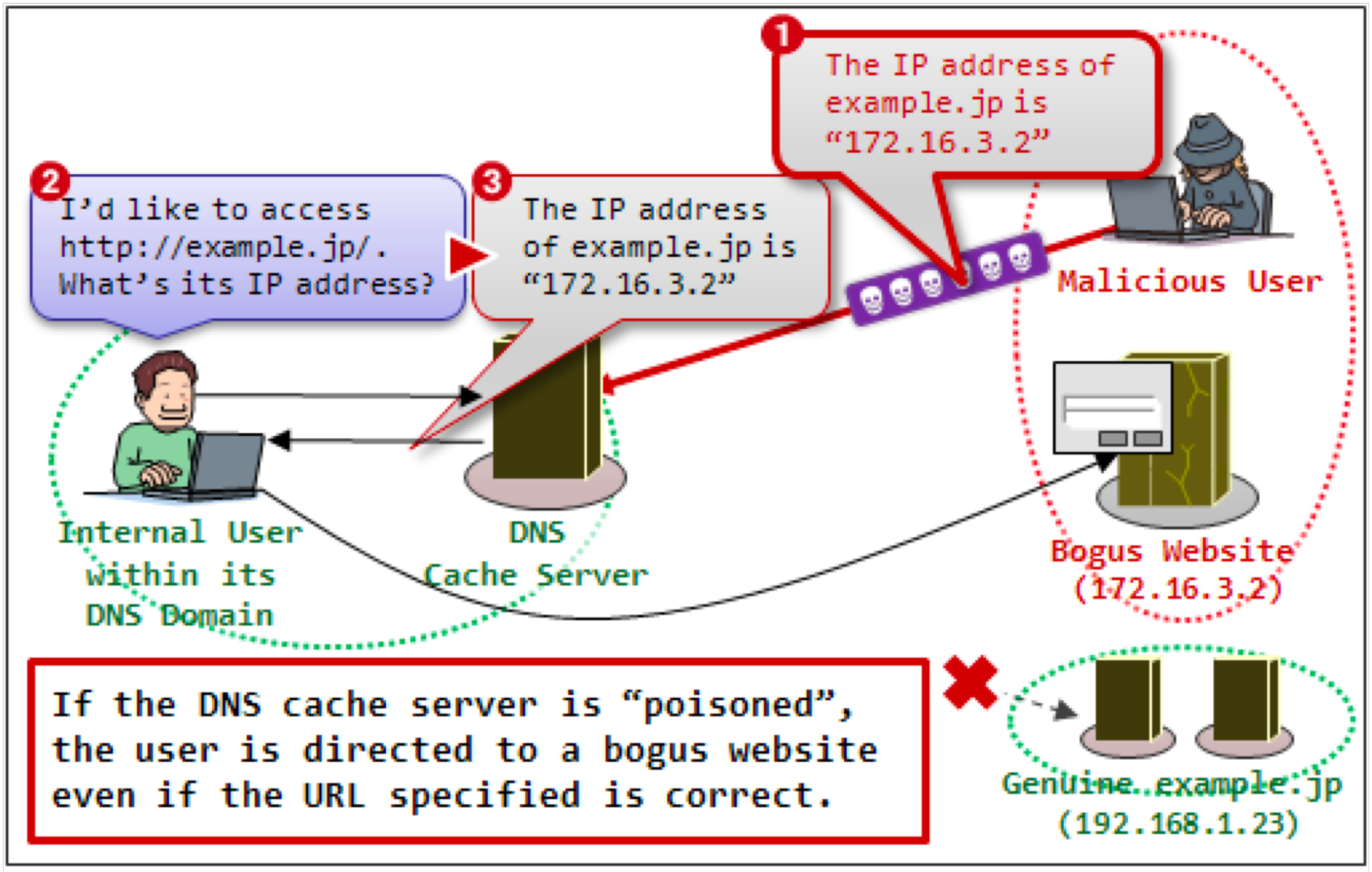
Oct 26, 2018

CS 232/332

Today

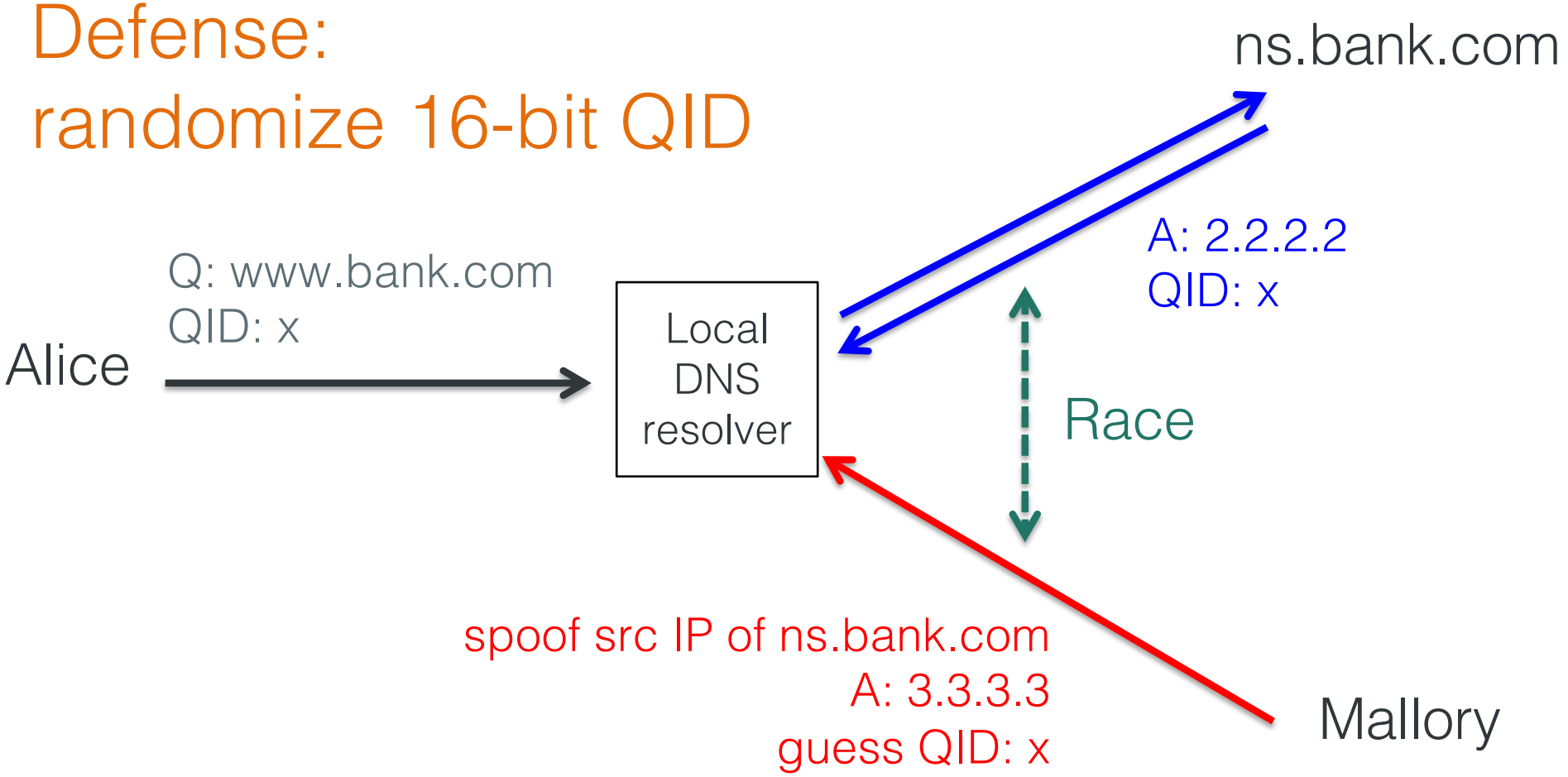
- Network level attacks
  - Attacks on DNS
  - Attacks against BGP
  - Denial of Service (DoS)
- Defenses
  - CDNs
  - Traceback

DNS Cache Poisoning

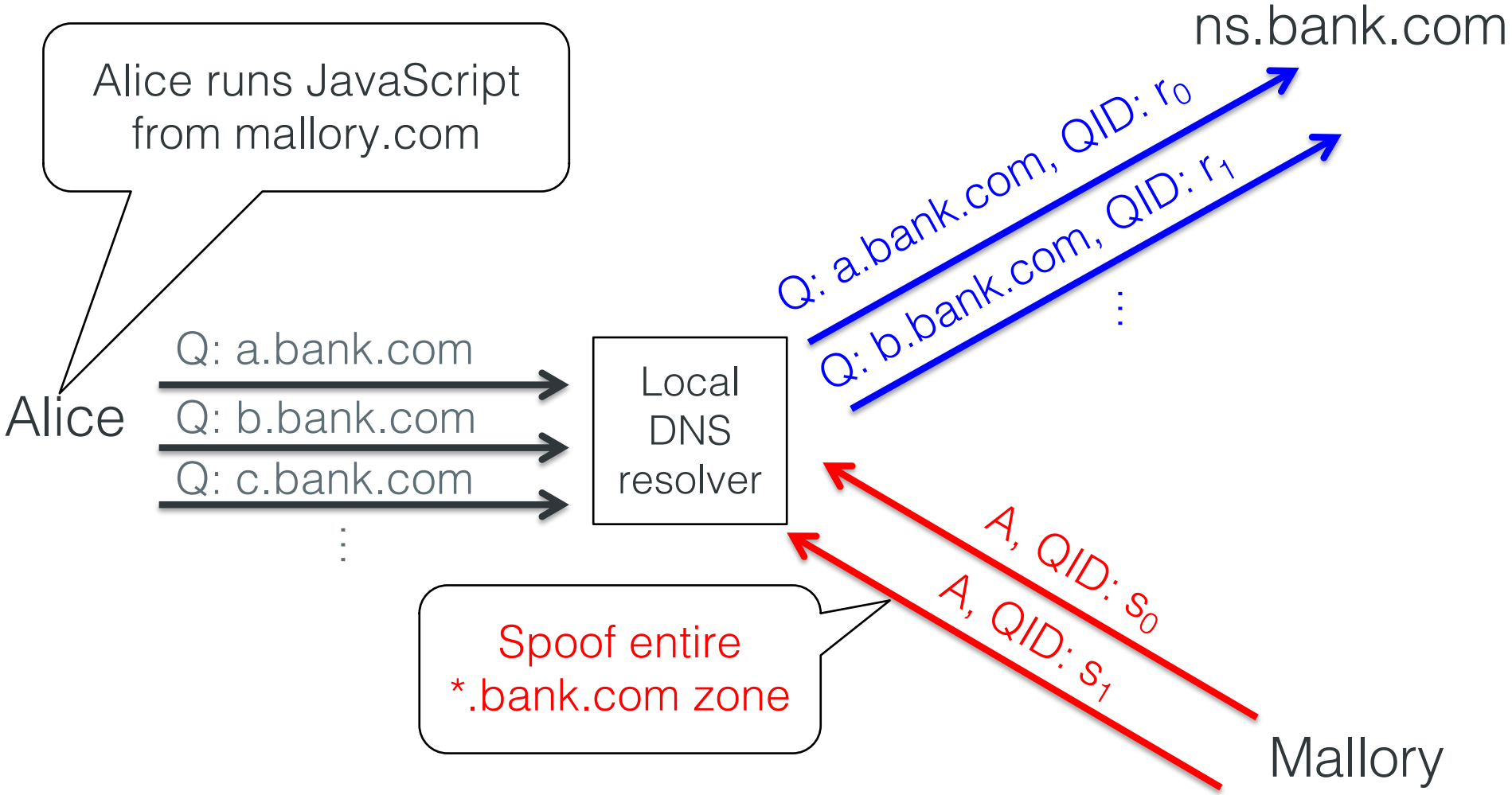


DNS Cache Poisoning (cont.)

Defense: randomize 16-bit QID



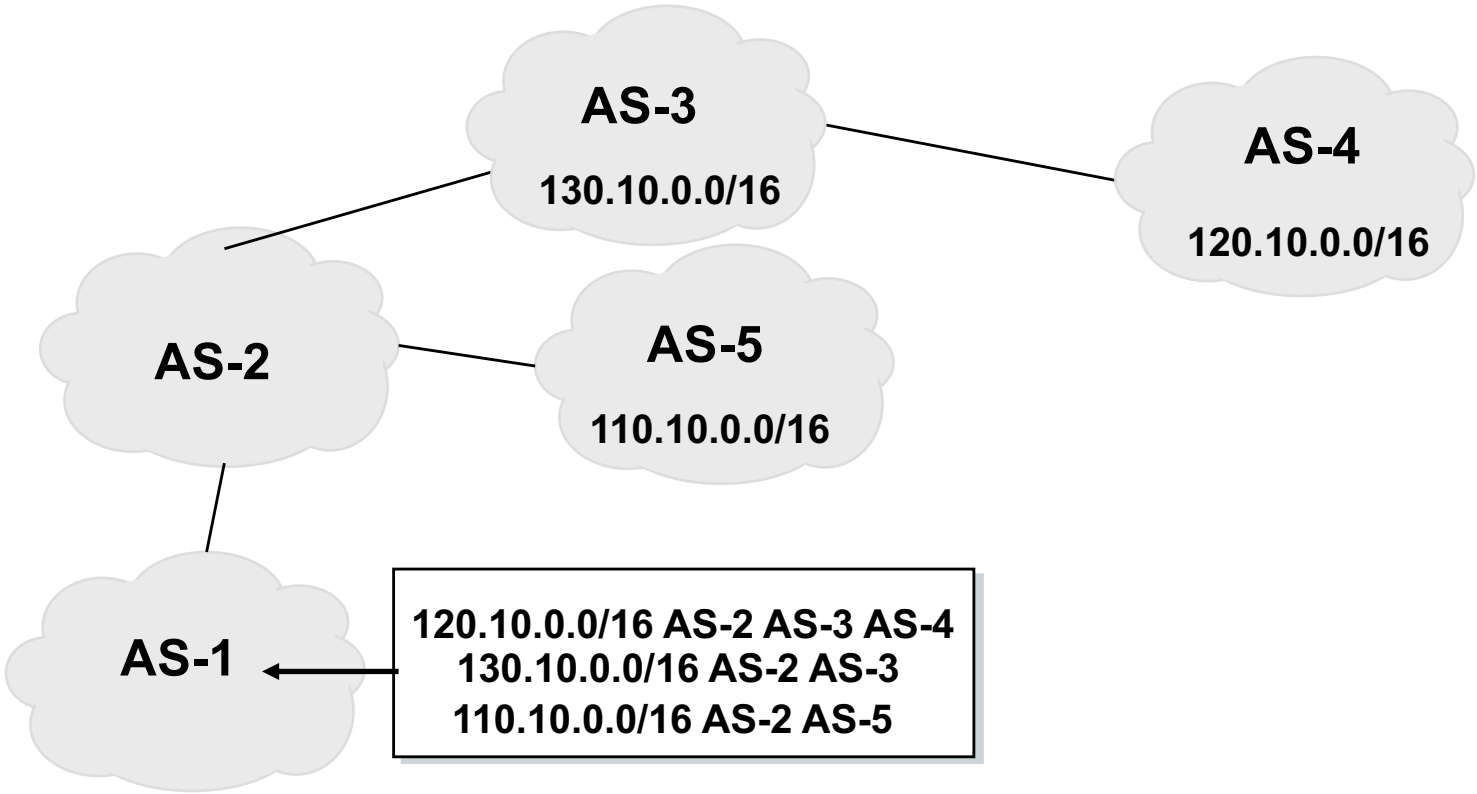
Kaminsky attack (2008)



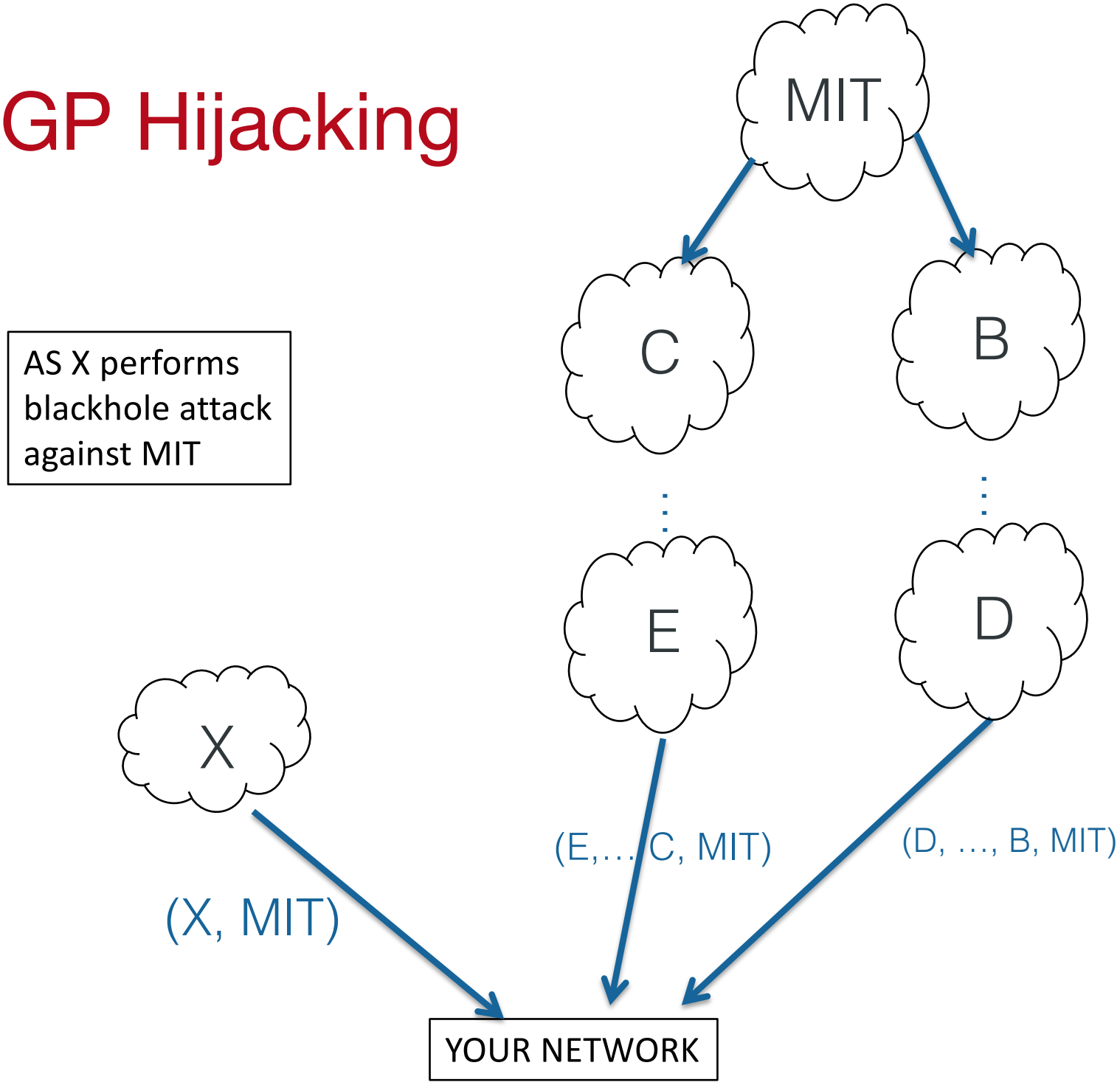
Mallory wins if any $r_i = s_j$

Recall: BGP: a Path-Vector Protocol

- An AS-path: sequence of AS's a route traverses
- Used for loop detection and to apply policy
- Default choice: route with fewest # of AS's



BGP Hijacking



Corrigendum- Most Urgent

GOVERNMENT OF PAKISTAN
PAKISTAN TELECOMMUNICATION AUTHORITY
ZONAL OFFICE PESHAWAR
Plot-11, Sector A-3, Phase-V, Hayatabad, Peshawar.
Ph: 091-9217279- 5829177 Fax: 091-9217254
www.pta.gov.pk

NWFP-33-16 (BW)/06/PTA February ,2008

Subject: **Blocking of Offensive Website**

Reference: This office letter of even number dated 22.02.2008.

I am directed to request all ISPs to immediately block access to the following website

URL: http://www.youtube.com/watch?v=o3s8jtvvg00

IPs: 208.65.153.238, 208.65.153.253, 208.65.153.251

Compliance report should reach this office through return fax or at email peshawar@pta.gov.pk today please.

Deputy Director
(Enforcement)

To:
1. M/s Comsats, Peshawar.
2. M/s GOL Internet Services, Peshawar.
3. M/s Cyber Internet, Peshawar.
4. M/s Cybersoft Technologies, Islamabad.
5. M/s Paknet, Limited, Islamabad
6. M/s Dancom, Peshawar.
7. M/s Supernet, Peshawar.

DNSSEC

DNS responses signed

Higher levels vouch for lower levels
— e.g., root vouches for .edu, .edu vouches for .uchicago, …

Root public key published

Problem?
Costly and slow adoption

S-BGP

IP prefix announcements signed

Routes signed
— previous hop authorizes next hop

Higher levels vouch for lower levels
— e.g., ICANN vouches for ARIN, ARIN vouches for AT&T, …

Root public key published

Problem?
Costly and slow adoption

Takeaway:

Internet protocol fossilization makes updating deployed protocols v hard.

The Coffeeshop Attack Scenario

- DNS servers bootstrapped by wireless AP
  - (default setting for WiFi)
- Attacker hosts AP w/ ID (O'Hare Free WiFi)
  - You connect w/ your laptop
  - Your DNS requests go through attacker DNS
  - www.bofa.com → evil bofa.com
  - Password sniffing, malware installs, …

- TLS/SSL certificates to the rescue!

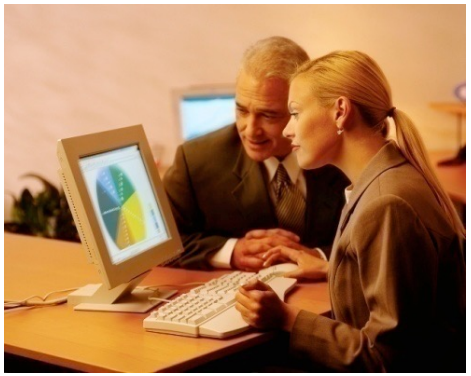
Recall: Man-in-the-middle Attack

- Alice sends to Bob her public key
- Carl intercepts the message and sends his own public key to Bob
- Bob sends to Alice his public key
- Carl intercepts the message and sends his own public key to Alice
- Alice sends to Bob a message encrypted with Carl's public key thinking she's encrypting with Bob's public key
- Carl intercepts the message, decrypts it with his own secret key, and re-encrypts it with Bob's public key
- Same for messages from Bob to Alice

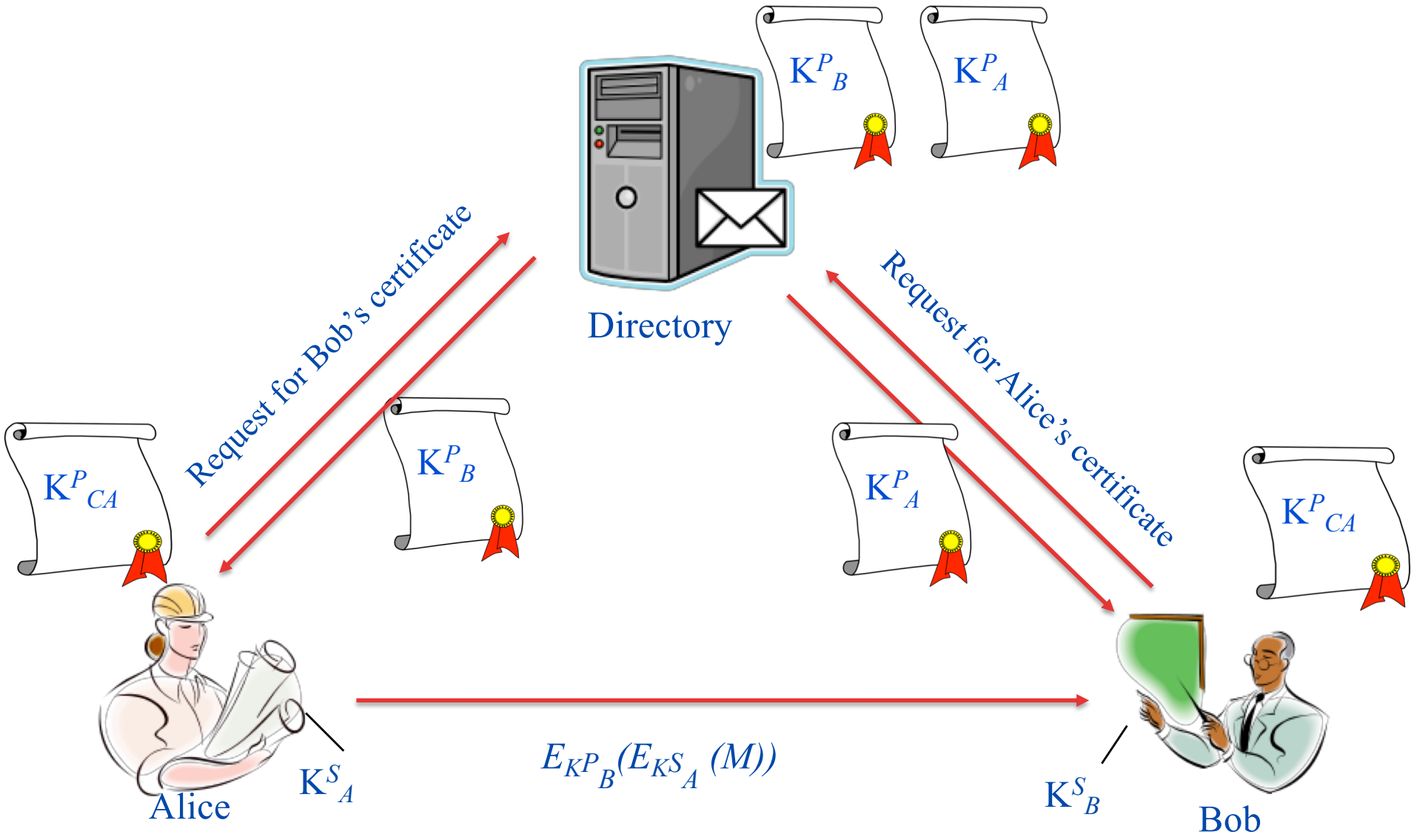
Bob

Carl

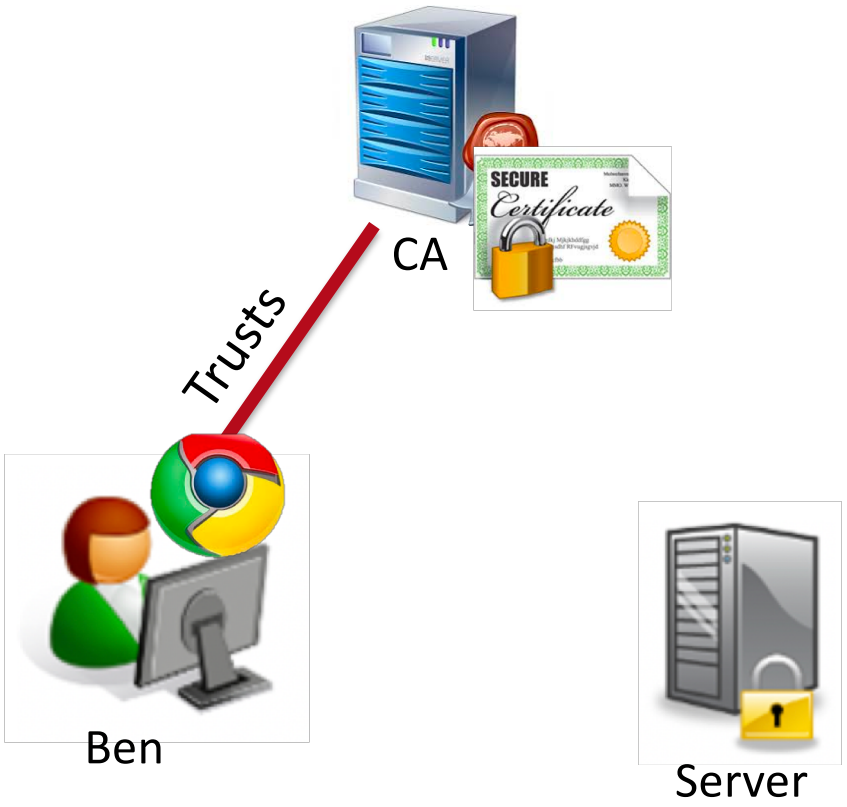
Alice



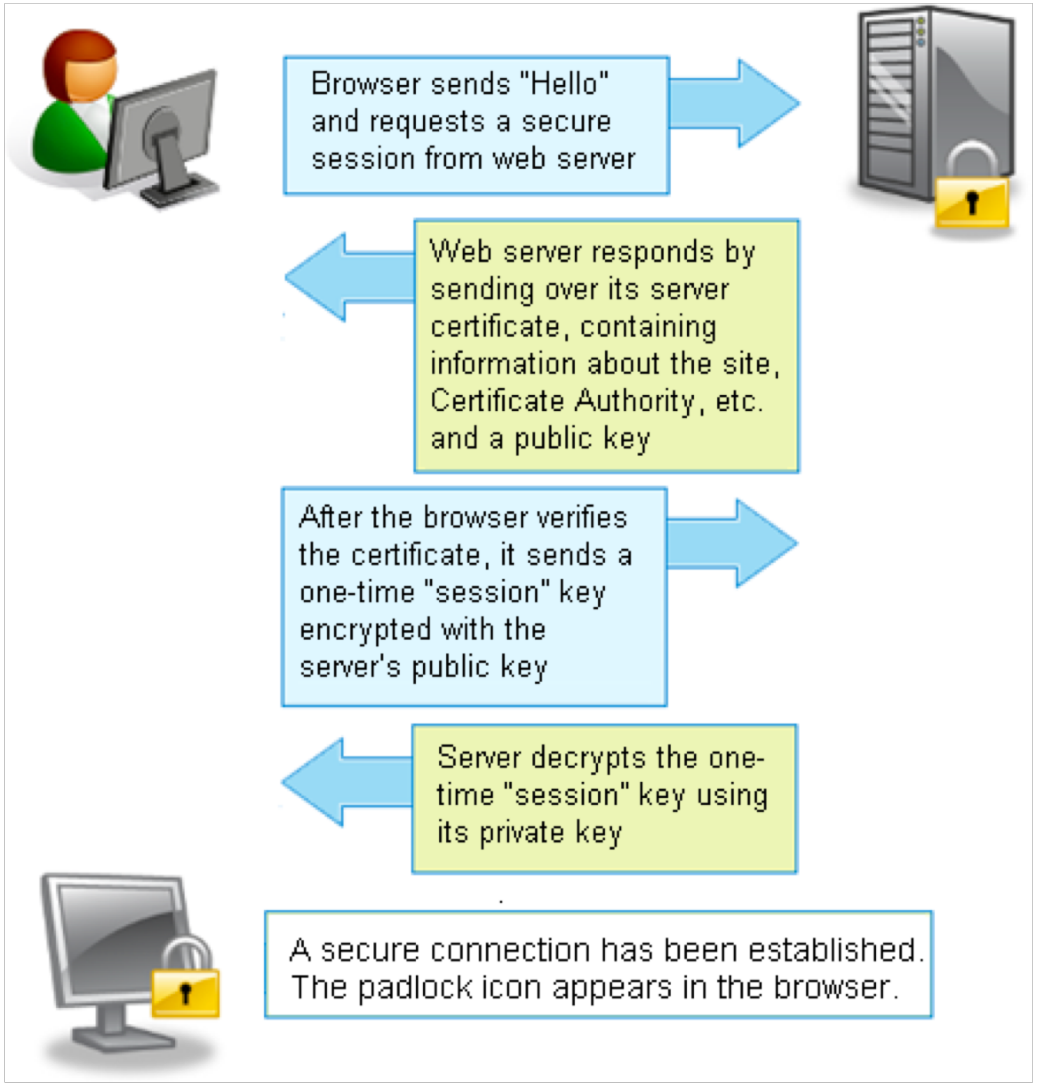
Using Public Key Certificates



SSL/TLS Server Certificates

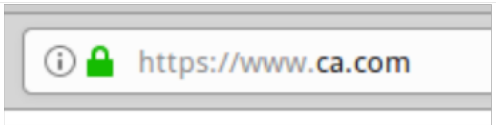


How do you know you can trust the CA?



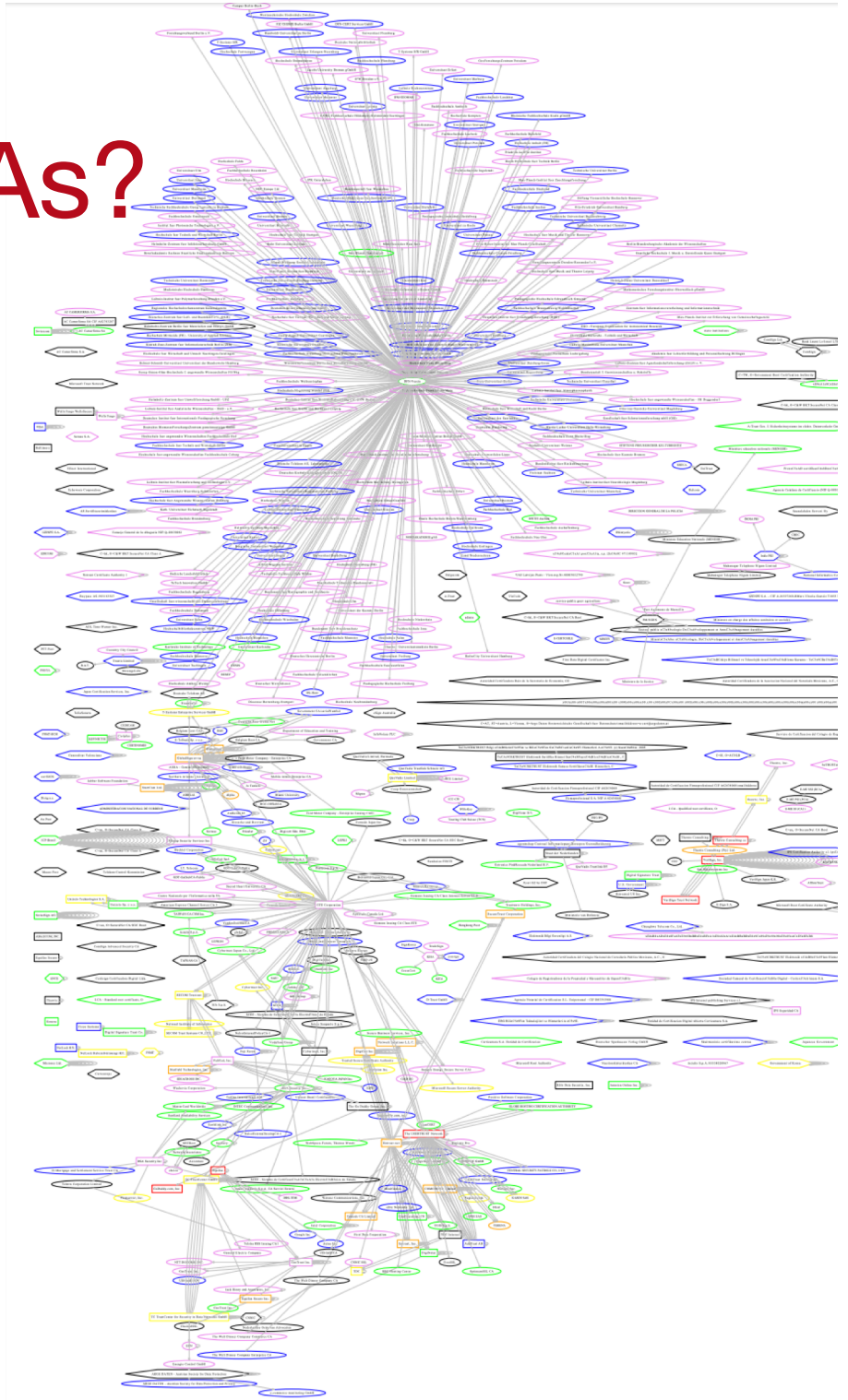
SSL/TLS Certificates & Weaknesses

- Corrupted browser
  - Trusts CA run by attacker
  - Or SSL library modified to return 1 on every certificate verification
- Manipulation by PC maker (Lenovo, Feb 2015)
  - Preinstalled its own fake CA in windows, and “signed” adware
- Long domain attack: www.bofa.com.blah.evil.com
  - Valid certificate for *.evil.com, url bar too short to show full URL
  - Extended validation (EV) certificates
- Homograph attacks: URL lookalikes: https://www.ca.com/



Can We Trust the CAs?

- EFF SSL observatory
  - 650+ CAs trusted by Mozilla or Microsoft
  - Any CA → any domain
  - Security of the weakest link
  - Misbehaving CAs known
- Compromised CAs
  - 2011, DigiNotar, Comodo, …
  - Certificate revocation (OCSP) (but OCSP can be blocked)
- Certificate pinning?
  - Only if your software is unaltered



Takeaway:

End to end security requires securing all components of long chain; weakest link prevails…

Denial of Service (DoS)

- Prevent users from being able to access a specific computer, service, or piece of data
- In essence, an attack on availability
- Possible vectors:
  - Exploit bugs that lead to crashes
  - Exhaust the resources of a target
- Often very easy to perform…
- … and fiendishly difficult to mitigate