L24: Secure channels

Nickolai Zeldovich
6.033 Spring 2012
Subject evaluation

• Help us improve 6.033 for future years

• http://web.mit.edu/subjectevaluation

• Please fill out before the beginning of finals week
• We read every one of your comments
Network insecurity

# tcpdump -A -s 2272 -i mon0
11:53:41.281771 2462 MHz 11g -26dB signal antenna 15 [bit 14] 
   CF +QoS IP 128.31.33.180.41899 > 74.125.226.180.80: Flags 
   [P.], seq 490544447:490545563, ack 2165662404, win 501, 
   options [nop,nop,TS val 701636 ecr 3105280684], length 1116 
...
GET /search?hl=en&source=hp&q=mit+150&... HTTP/1.1 
Host: www.google.com 
Connection: keep-alive 
Referer: http://www.google.com/ 
User-Agent: Mozilla/5.0 (X11; CrOS i686 0.0.0) ... 
Cookie: NID=45=0N-XmK6HCc6gbx-DAQCh2-IBwUK8JV-79rK3iFzK08pL...
...

Diffie-Hellman key exchange

Common parameters: prime $p$, generator $g$
Diffie-Hellman key exchange

Alice

Bob

random \( a \)

\( g^a \mod p \)

Common parameters: prime \( p \), generator \( g \)
Diffie-Hellman key exchange

Common parameters: prime $p$, generator $g$
Diffie-Hellman key exchange

Common parameters: prime $p$, generator $g$

Alice

- random $a$
- $k = (g^b)^a = g^{ba} \mod p$

Bob

- random $b$
- $k = (g^a)^b = g^{ab} \mod p$

$g^a \mod p$ from Alice to Bob

$g^b \mod p$ from Bob to Alice

Encrypt($k, m$) from Bob to Alice
Man-in-the-middle (MITM) attack

Common parameters: prime $p$, generator $g$
Diffie-Hellman with signatures

SKalice; random $a$

$\{ g^a \mod p \}_{SKalice}$

SKbob; random $b$

$\{ g^b \mod p \}_{SKbob}$
Diffie-Hellman with signatures

Alice
SKalice; random $a$

{ $g^a \mod p$ }$_{SKalice}$

Bob
SKbob; random $b$

{ $g^b \mod p$ }$_{SKbob}$

Need PKbob to verify
Need PKalice to verify
Certificate authority mistakes

- 2001: Verisign cert for Microsoft Corp.
- 2011: Comodo certs for mail.google.com, etc
- 2011: DigiNotar cert for *.google.com
Summary

- Network adversary: secure channel abstraction
- Primitives: Encrypt/Decrypt, MAC, Sign/Verify
- Key exchange requires knowing public keys
- Certificates