Georgia Tech

CS 3251- Computer Networks 1:

Security Protocols (1)

Professor Patrick Traynor

4/19/11

Lecture 26

Announcements

- Homework 3 is now late.
  - If you have not submitted it, you can still do so with the standard lateness penalties assessed.
- Project 4
  - Due Thursday at 5pm

Last Time

- Trying to prove who you are simply by saying your name is an example of ...?
- How are MACs and Digital Signatures Different?
  - What algorithms used to implement them?
- Diffie-Hellman key exchanges are vulnerable to what kind of attack?

Chapter 8 roadmap

8.1 What is network security?

8.2 Principles of cryptography

8.3 Message Integrity

8.4 End point Authentication

8.5 Securing e-mail

8.6 Securing TCP connections: SSL

8.7 Network layer security: IPsec

8.8 Securing wireless LANs

8.9 Operational security: firewalls and IDS

Email Security

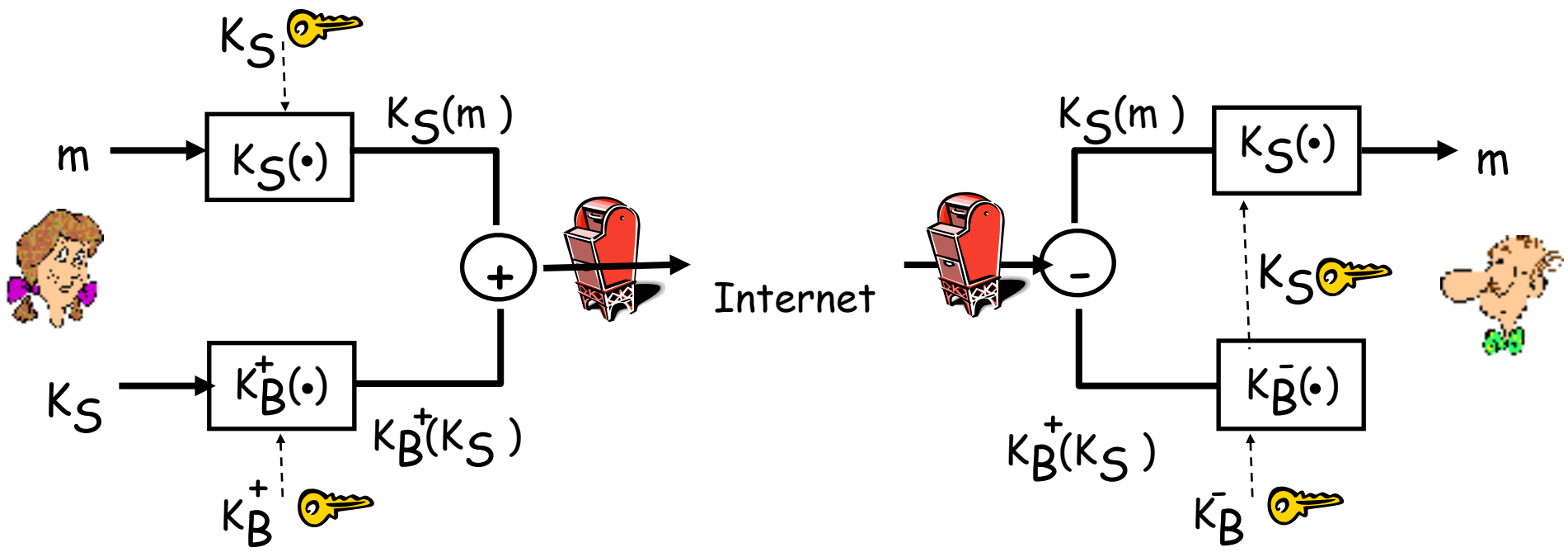
- Transmission is often not the only place crypto needs to be used to protect your email.

- Some system administrators, service providers and (if you're unlucky) law enforcement agencies read your email when it sits on the server.
  - e.g., GMail Advertisements

- How can you protect the confidentiality and integrity of your communications?

Secure e-mail

- Alice wants to send confidential e-mail, m, to Bob.

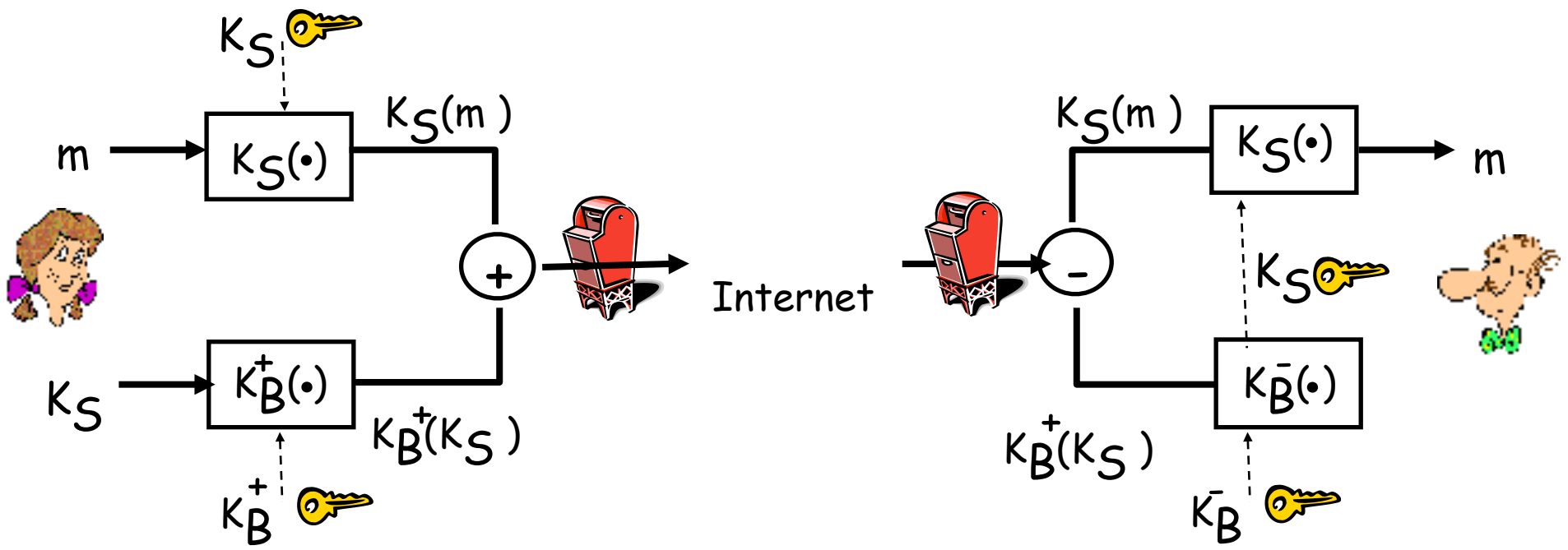


Alice:

- generates random symmetric private key, K_S.
- encrypts message with K_S (for efficiency)
- also encrypts K_S with Bob's public key.
- sends both $K_S(m)$ and $K_B(K_S)$ to Bob.

Secure e-mail

- Alice wants to send confidential e-mail, m, to Bob.

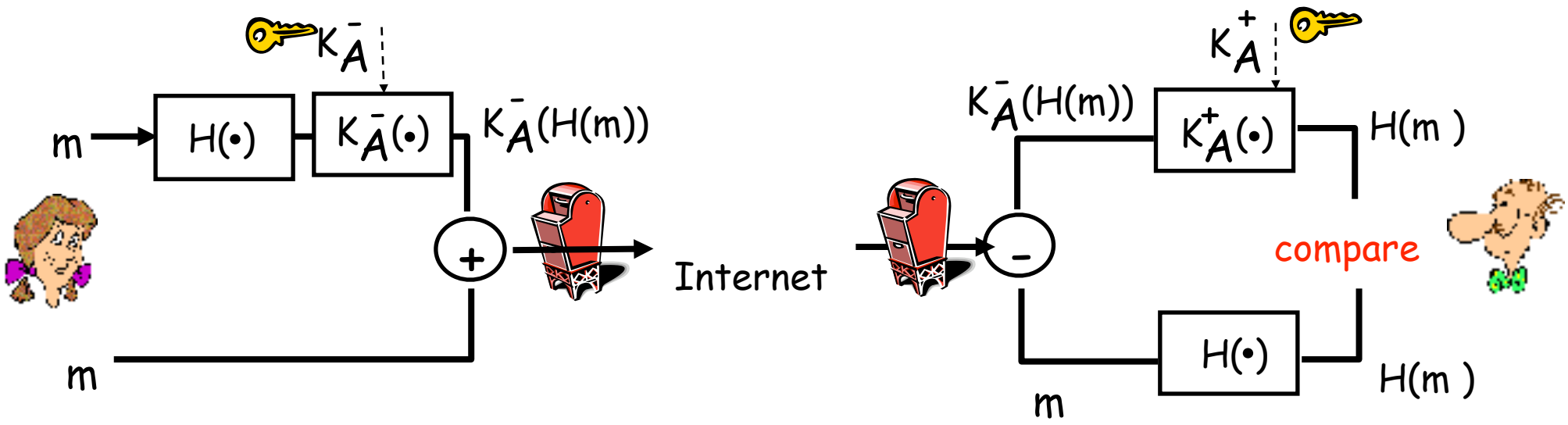


Bob:

- uses his private key to decrypt and recover K_S
- uses K_S to decrypt $K_S(m)$ to recover m

Secure e-mail (continued)

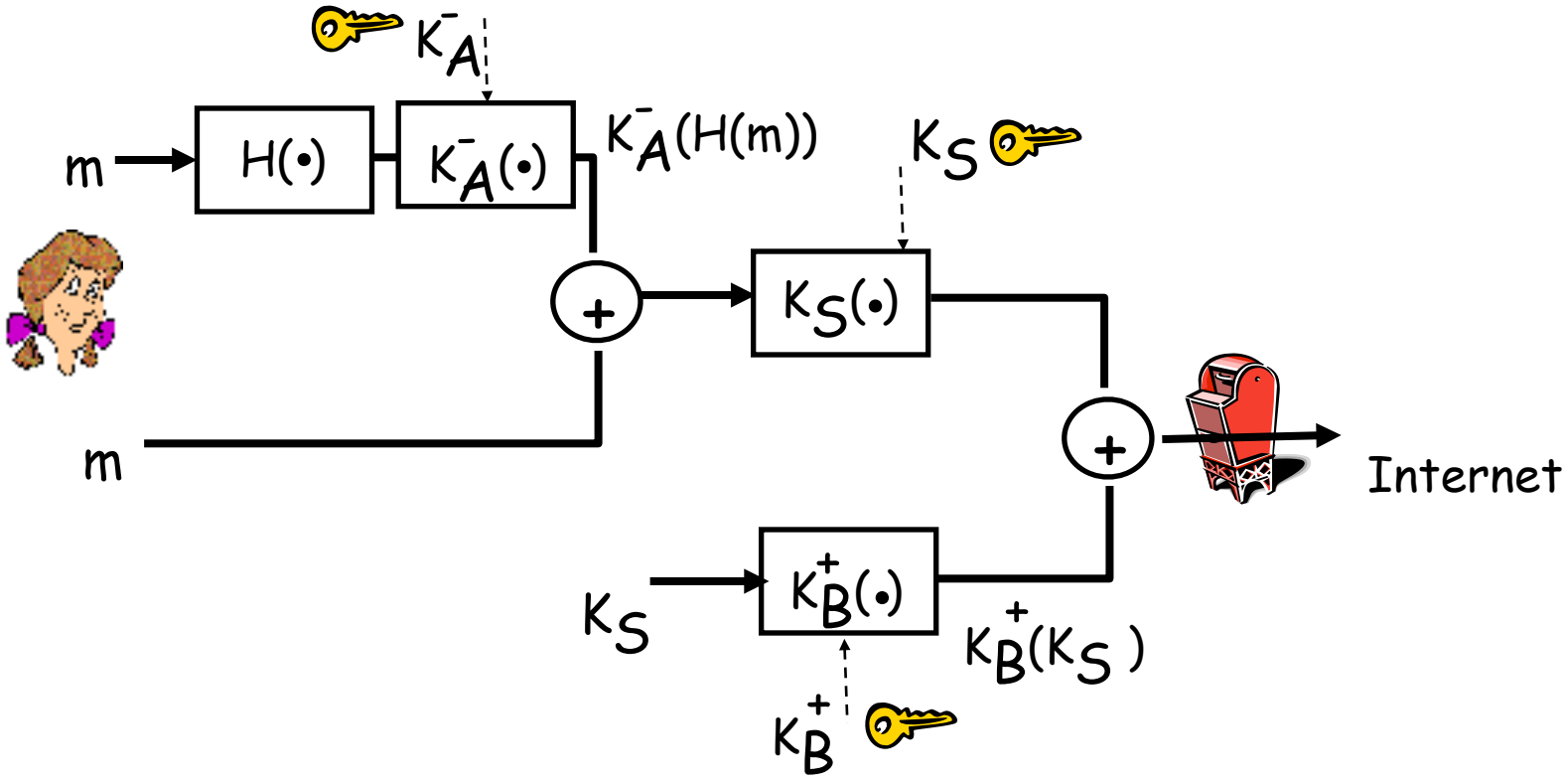
• Alice wants to provide sender authentication message integrity.



- Alice digitally signs message.
- sends both message (in the clear) and digital signature.

Secure e-mail (continued)

- Alice wants to provide secrecy, sender authentication, message integrity.



Alice uses three keys: her private key, Bob's public key, newly created symmetric key

Pretty good privacy (PGP)

- Internet e-mail encryption scheme, de-facto standard.
- uses symmetric key cryptography, public key cryptography, hash function, and digital signature as described.
- provides secrecy, sender authentication, integrity.
- inventor, Phil Zimmerman, was target of 3-year federal investigation.

A PGP signed message:

```
---BEGIN PGP SIGNED MESSAGE---
Hash: SHA1

Bob:My husband is out of town
    tonight.Passionately yours, Alice

---BEGIN PGP SIGNATURE---
Version: PGP 5.0
Charset: noconv
yhHJRHhGJGhgg/12EpJ
    +lo8gE4vB3mqJhFEvZP9t6n7G6m5Gw2
---END PGP SIGNATURE---
```

pgp.mit.edu

PGP: A Web of Trust

- Instead of relying on a CA, PGP uses social relationships to verify a key.
  - If you know a friend of mine and they signed my key (and you can verify their signature), you are more likely to believe the key belongs to me.

```
pub  1024D/4B675CEA 2006-10-19

uid Patrick Traynor <traynor@cc.gatech.edu>
sig  sig3  4B675CEA 2008-09-15 __________ __________ [selfsig]
sig  sig   291D61FD 2008-09-26 __________ __________ Frank Park <frank@gatech.edu>

uid Patrick Gerard Traynor <traynor@cse.psu.edu>
sig  sig3  4B675CEA 2006-10-19 __________ 2008-10-18 [selfsig]
sig  sig   E6A5C618 2006-10-19 __________ __________ William Enck <enck@cse.psu.edu>
sig  sig   2D18BAD7 2006-10-19 __________ __________ William Enck <wenck@psu.edu>
sig  sig   6076BF43 2006-10-19 __________ __________ Luke St.Clair <lstclair@cse.psu.edu>
sig  sig   3A4CC3BA 2007-03-26 __________ __________ Joshua Schiffman (Sycrim) <jschiffm@cse.psu.edu>
sig  sig   78075A3E 2007-06-26 __________ __________ Kevin Butler <butler@cse.psu.edu>
sig  sig   D44736F4 2007-10-30 __________ __________ yogesh raju sreenivasan (first gpg key) <sreeniva@cse.psu.edu>
sig  sig   D127450E 2007-10-30 __________ __________ Lisa Johansen <johansen@cse.psu.edu>
sig  sig   6C2900BD 2007-10-30 __________ __________ Stephen McLaughlin (.) <smclaugh@cse.psu.edu>
sig  sig   F7EE6984 2007-11-03 __________ __________ Sandra Rueda (Sandra Julieta Rueda Rodriguez) <ruedarod@cse.psu.edu>
sig  sig   33103478 2007-11-06 __________ __________ Boniface Hicks (monk, priest, computer science professor) <phicks@cse.psu.edu>
sig  sig   17F0F537 2008-05-06 __________ __________ Thomas Moyer <tmmoyer@cse.psu.edu>
sig  sig3  4B675CEA 2008-05-16 __________ __________ [selfsig]
sig  sig   039F0522 2008-09-26 __________ __________ Italo Dacosta <idacosta@gatech.edu>
sig  sig   039F0522 2008-09-26 __________ __________ Italo Dacosta <idacosta@gatech.edu>
sig  sig   4FB3AE73 2008-09-27 __________ __________ Chaitrali <to.chaitrali@gmail.com>
sig  sig   4FB3AE73 2008-09-27 __________ __________ Chaitrali <to.chaitrali@gmail.com>
sig  sig   0371D9B3 2008-10-01 __________ __________ Michael Hunter <mhunter@cc.gatech.edu>
sig  sig   0371D9B3 2008-10-01 __________ __________ Michael Hunter <mhunter@cc.gatech.edu>
sig  sig   9B952FFF 2009-01-30 __________ __________ Lalanthika Vasudevan <lalanthika.v@gatech.edu>

uid Patrick Gerard Traynor <traynor@cc.gatech.edu>
sig  sig3  4B675CEA 2008-07-08 __________ __________ [selfsig]
sig  sig   039F0522 2008-09-26 __________ __________ Italo Dacosta <idacosta@gatech.edu>
sig  sig   4FB3AE73 2008-09-27 __________ __________ Chaitrali <to.chaitrali@gmail.com>
sig  sig   0371D9B3 2008-10-01 __________ __________ Michael Hunter <mhunter@cc.gatech.edu>
sig  sig   9B952FFF 2009-01-30 __________ __________ Lalanthika Vasudevan <lalanthika.v@gatech.edu>

sub  2048g/C0999E7C 2006-10-19
```

Using PGP

- For Mac users, download MacGPG. Windows users should get GPG4win. Linux users can download GPG.
  - These are all free versions of PGP based on RFC4880.
- From the command-line:
  - gpg -c filename.txt (encrypt a file using a symmetric key generated from a passphrase)
  - gpg -e filename.txt (encrypt a file using the public key of the intended reader).

Public Key

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: SKS 1.1.0

mQGiBEU3fUwRBADkfQiDpTiW8KN/Leys4XUTrQDwBqtwqTXJXcHQCUlDV9mJ60PxDAuEguY5
lbjPwi/nVQ225tlNXCkaBzvyJq/8xIUwn7i+hsHHvlqglf7dSFSt7aqCaqCkNkuTrPwnB609
AlSSkYDA24Kt5TgsoDG3bMqvi6FNIGjZRdeaf7H6+wCg7w4YMtqio26Aa9Hs7lnVa7LQAPUD
+wQbK1pCoA217y5UFShQRtvF0PHwDxAIMUQjr34YmysTr5tVSwkckf9a0UoaNgF9H/K36riO
/eu8K43QOD8BIdm2npqk/Q/zckCaw2fLsihTFZivlqVT3ho3iQlNbdO6BaD5eQEJ7svR/5Ro
069N3NOBYS47erpDtCRruWh4Z+89A/4y7aAVlBDrVkQXYokjXdvT4yiN6RUNiCxJIpb1BebB
VPzx+FK94L/idT3zbwWbkALuGIJkN/IKNfwnpDMKgmP2aMr9G4AuRF0XGiFO0bVjkloEvqqQ
loZ5FFalSaImeCWydlevajHhb5PXFLzkRndH/6wG2SbWpn12FlfHRkpTBLQnUGF0cmljayBU
cmF5bm9yIDx0cmF5bm9yQGNjLmdhdGVjaC5lZHU+iEYEEBECAAYFAkjdQx4ACgkQCjNKhSkd
Yf0n4wCfeseyLBckAluqUiD6uvh3wQfRLQUAn0tmD42+Pl++xhdXQ6gP8dRVyd4/iGAEExEC
ACAFAkjOttwCGwMGCwkIBwMCBBUCCAMEFgIDAQIeAQIXgAAKCRD3JVd7S2dc6oTDAKCBXw+e
MoaU/T9uF5eJDBnP/FjMZQCgibbpCBQ2fEpUMUf8Rok2Lj9uovi0LFBhdHJpY2sgR2VyYXJk
IFRyYXlub3IgPHRyYXlub3JAY3NlLnBzdS5lZHU+iEYEEBECAAYFAkU3fzwACgkQGrKJXOal
xhioAgCffnuRbO/SZK7LdfZUjFj3F2oEJGcAoOERnKWB9/7994otrCM5xhqtutRqiEYEEBEC
AAYFAkU3f2wACgkQYI7uTi0YutcYMACeKQK2nPmXnFrc7eOwZWbX4GUMcJkAnjTOXRv5nvDg
Z5wORuIhTepZ4VTBiEYEEBECAAYFAkYIXNIACgkQr5A0jDpMw7ppWgCeMl2+IH1QpjhX7ZNL
8oj8NqgxwBIAnAzmz5qgApaeXc30hzvqWEE3t4jNiEYEEBECAAYFAkaBTLsACgkQnXLg9HgH
Wj592QCdGnRYZV6hZ2ayy+alUiZdL3w4+WgAoJTEAaqyAlWuPs9znfyPwJxm5q5liEYEEBEC
AAYFAkcnO24ACgkQtwxrN9RHNvRRWwCeINX9XHd7kkNAvCgkXXoTnH/AUHEAn33lbjjWYqyE
lr3x8aZ4qkb9NANciEYEEBECAAYFAkcnPS0ACgkQJ0tTE9EnRQ6WwwCffKP67MDZPwzRpd0L
wyUkkMjG0AMAnRywKK3yROY6FdHt2bvUWFa+NyEwiEYEEBECAAYFAkcnbgsACgkQIyPVYGwp
AL2CRACfcyjK+a8tikTBBWTJy4YxBTAJvecAn0K0OBTnMOzROXPzmmlYQwdaEA3biEYEEBEC
AAYFAkcs7ZUACgkQqSJqhPfuaYTsgQCgn3Kf4qZGSBHynDikwNxUtTfDwiYAn0/I304rCTEP
xzTqZ62AsToUBZcQiEYEEBECAAYFAkcv0nQACgkQIArE1zMQNHhULQCgts0t1ZoRQQU/LKL4
DMmrzDk3Y34AoMSMdfvOsSffp10a5MWY78RBSOFyiEYEEBECAAYFAkggm60ACgkQa7Yypxfw
9TfrDgCfRxfSEiGq9Mv9V/ybKVyYdQvfJvUAnRg2wMqvDJixS9bKaqUDQRz60BJGiEYEEBEC
AAYFAkjdTSoACgkQ/7xgkQOfBSJu3wCfR1fZkpF2n94mkJI+gfsyGNz5tR0An1XjljnntN8H
ttpJU7HrfrsXsx88iEYEEBECAAYFAkjdTTgACgkQ/7xgkQOfBSKqpQCghmCoKFunCD6n+5P8
ffsvzGCq/t8AnjesVVtaqCDbD2YYUUju3tHQ/kDLiEYEEBECAAYFAkjdib4ACgkQBLzC7k+z
rnP+AwCdFn0tsBDfbXMqFJSPb/j0B8ANaaQAnR/LD2hNz+7yI4BnPc8XbyDHR0jxiEYEEBEC
AAYFAkjdicYACgkQBLzC7k+zrnNlFgCePQmblHq/eftpUQk0yjBwUt4YuVMAoLdxDAIkehN7
dBPeTM0HHciewVVDiEYEEBECAAYFAkjjsNAACgkQ/547KQNx2bPD0ACcC+FlhVpLico2im0g
BtD3wdA+rTgAn1uHIdQTRWY0C0027GJT6HdA3usaiEYEEBECAAYFAkjjsNAACgkQ/547KQNx
2bPWcQCeL0oKn8MQ3lkaehWWgp8EO7v/X90An1sFCc7W9Zma+xcyT3OM5N79XanMiEYEEBEC
AAYFAkmDgOoACgkQSj2B0puVL/9EAQCgtHi8+lQoTqflToiblCv8A0kb8PgAoOnUH5FWP/B4
Dn7v/T+YdOvgGdyPiEkEEBECAAkFAkU3g5UCBwAACgkQwyk8VmB2v0PwiwCeN4aFN+fOEepz
8Pr3pG3Pcp5/SSkAn0LSXA0tLXheTny0RkAqSjbIjcyiiGAEExECACACGwMGCwkIBwMCBBUC
CAMEFgIDAQIeAQIXgAUCSC2ZWwAKCRD3JVd7S2dc6kTQAJwOHRTbgwq9V+nx4a1/43/+3tYt
qQCfTUb0qwf0U/tHr/PTxr8GC12w9ciIZgQTEQIAJgUCRTd9TAIbAwUJA8JnAAYLCQgHAwIE
FQIIAwQWAgMBAh4BAheAAAoJEPclV3tLZ1zqalgAoMKUbkH2qKkb83r+m5GKuI+Hs6YeAKDh
kHah0MioxXwc8Yge1BiQuOXwmrQuUGF0cmljayBHZXJhcmQgVHJheW5vciA8dHJheW5vckBj
Yy5nYXRlY2guZWRlPohGBBARAgAGBQJI3U0qAAoJEP+8YJEDnwUibt8An0dX2ZKRdp/eJpCS
PoH7Mhjc+bUdAJ9V45Y557TfB7baSVOx6367F7MfPIhGBBARAgAGBQJI3Ym+AAoJEAS8wu5P
s65z/gMAnRZ9LbAQ321zKhSUj2/49AfADWmkAJ0fyw9oTc/u8iOAZz3PF28gx0dI8YhGBBAR
AgAGBQJI47DQAAoJEP+eOykDcdmz1nEAni9KCp/DEN5ZGnoVloKfBDu7/1/dAJ9bBQnO1vWZ
mvsXMk9zjOTe/V2pzIhGBBARAgAGBQJJg4DlAAoJEEo9gdKblS//m34AoJ4af/wySOlXKjBH
lGe7U4BYNKlUAKDoapEiSfYzxuy2vaHQGoo4QmG/oYhgBBMRAgAgBQJIc+nwAhsDBgsJCAcD
AgQVAggDBBYCAwECHgECF4AACgkQ9yVXe0tnXOqgfACg7jJ71HKMVmHphkXVjH9LaKTBm+0A
mwROF1mKOFlUB5bvJg4e3qyACpE1uQINBEU3fY0QCADxjApA2rmjH4JuTrnEwP/GNp+UrYsV
0cyrXhNdnwtV4+L+M7tKmeTy+8SCfJRm8igQL8RNZrhtQenAVNGFEsQTyJPHOrKADxvX39G0
mx2cwQ9T4Bh4dfTNx2vmtWsGI0Al8ArlyRViifoTylLcmU787T6Rq9nEG6FyCiaPMUtYeEv1
hnyDoKtDLD63aMJj5b4aojZUDxO6A1gm96JT3fVPMqEa83sQ5f6f2zQ9kvhzrY9npOn0ySVa
vQx5NRRqn1jLP+j2lGI4QuR5696ING+upReXGJ3bBXuL/dr8vC9cUmzOj4zoWDN/WdwVIZWH
uvFX/3F0w9lmYzLM6pS7QW/LAAMFCADOLo+EgzYarRVa2IpaBTk9D4a8lcsp9+7vb9UmMhA/
6MHoPnKjdlkzmnY8Ki7j0hoU2F6i47PVzi2CNT2g2S2HwBGMMwmLtbpXUD3eqz7NuCuSiwc6
uEBnnNoFukjVKLn7WtpeGC0+jTtNz7gEIvh4xe1MP2GL9xslwjjN3///1Sq8OfYf7pwAzb3O
f1P0LSoQcCT3XrxtqaOCBHlVzpcgmWJw6Ze5I4zRbrG+jPTWd3STqUlcZmAl2ap/zsuigI4M
bk+vdL50QYG89bmxlbrnf+2Oh+pqf2nK3UJpcCs+OMbSb4HfWnfcxuUndpMqItRWHfdjlt2/
aBQQFp254jhWiEkEGBECAAkCGwwFAkgtmbUACgkQ9yVXe0tnXOpF2QCeLFSB74jvUbgjYXBj
MyKrjQdPf98AoLvsfjgPwqW5kEKNn73xBbSbEQxAiE8EGBECAA8FAkU3fY0CGwwFCQPCZwAA
CgkQ9yVXe0tnXOpa3QCgvqKU8ti9D0vmQAhpIS1+pP8bAkYAn1C/uXo90mGo5OouuEKsUf1F
e+e+
=6BWu
-----END PGP PUBLIC KEY BLOCK-----
```

Chapter 8 roadmap

8.1 What is network security?

8.2 Principles of cryptography

8.3 Message Integrity

8.4 End point Authentication

8.5 Securing e-mail

8.6 Securing TCP connections: SSL

8.7 Network layer security: IPsec

8.8 Securing wireless LANs

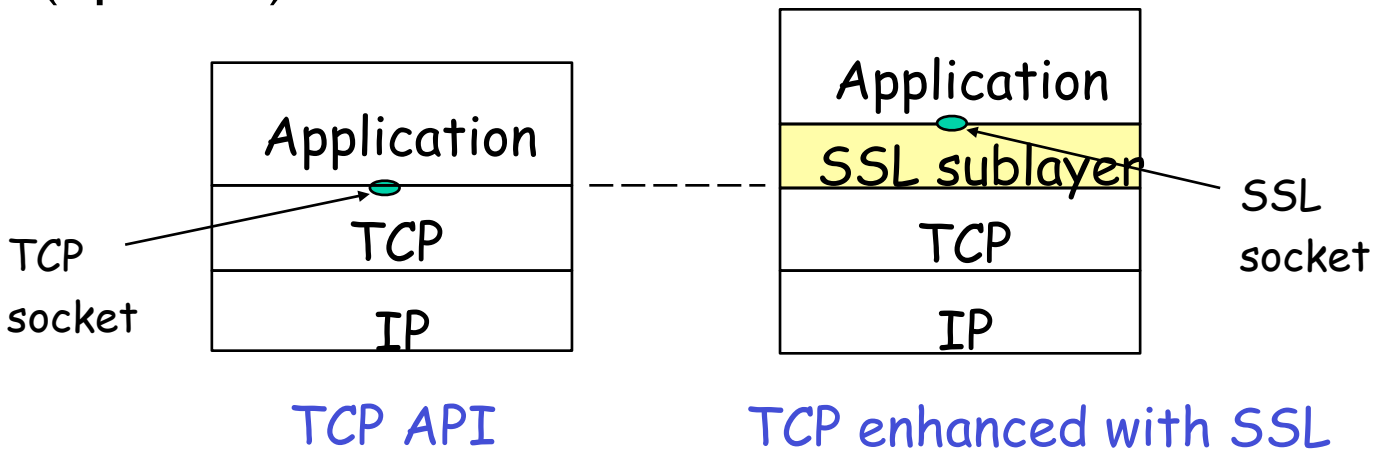
8.9 Operational security: firewalls and IDS

How do we get secure communications?

- We now have an idea of how cryptographic algorithms work (and what they try to guarantee).
- We also know how to ensure integrity of our communications.
- How do we actually use this stuff?
  - Are we using it on a daily basis?

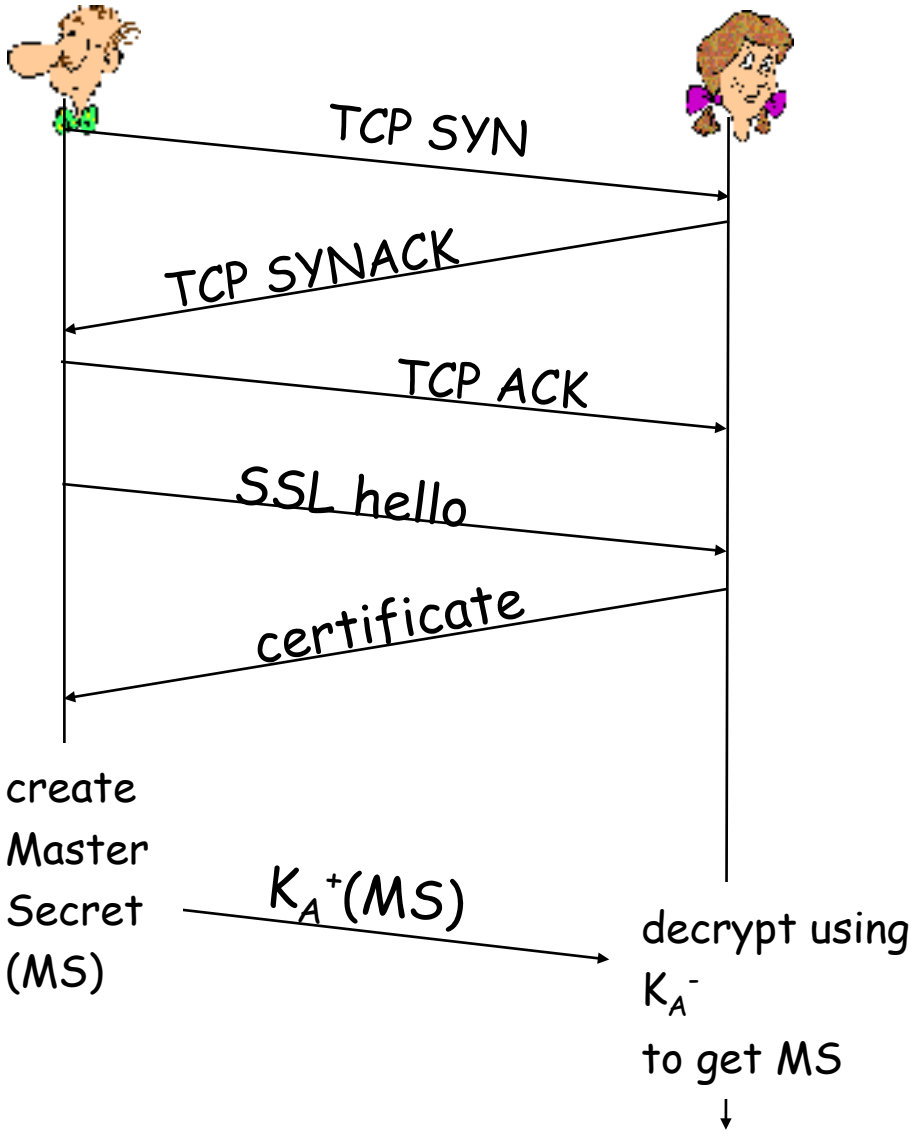
Secure Sockets Layer (SSL)

- Provides transport layer security to any TCP-based application using SSL services.
  - e.g., between Web browsers, servers for e-commerce (https)
- security services:
  - server authentication, data encryption, client authentication (optional)



SSL: Three Phases

- 1. Handshake:
  - Bob establishes TCP connection to Alice
  - authenticates Alice via CA signed certificate
  - creates, encrypts (using Alice's public key), sends master secret key to Alice
    - nonce exchange not shown

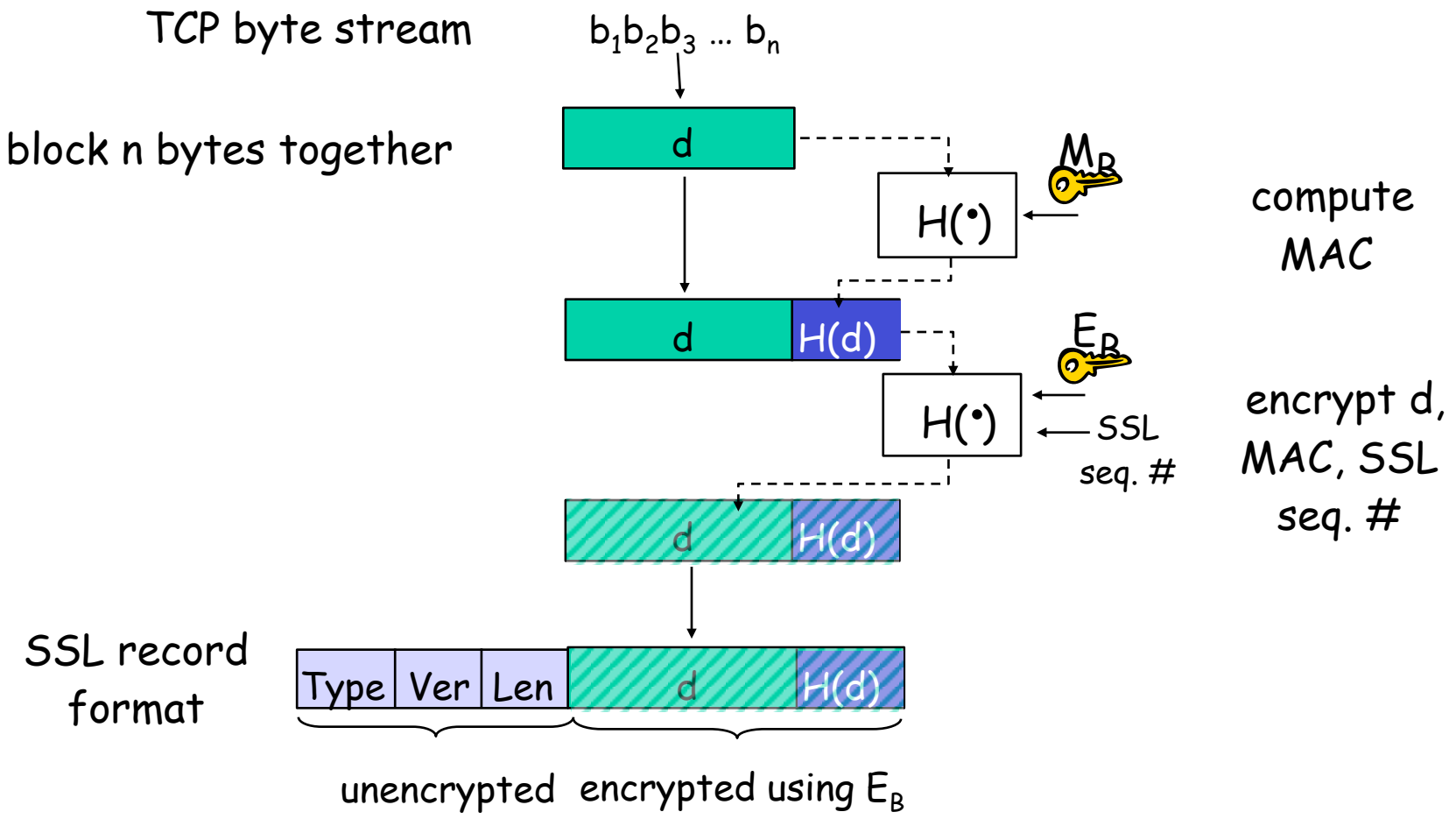


SSL: Three Phases

- 2. Key Derivation:
  - Alice, Bob use shared secret (MS) to generate 4 keys:
    - E_B: Bob->Alice data encryption key
    - E_A: Alice->Bob data encryption key
    - M_B: Bob->Alice MAC key
    - M_A: Alice->Bob MAC key
  - encryption and MAC algorithms negotiable between Bob, Alice
  - why 4 keys?

SSL: Three Phases

- 3. Data Transfer

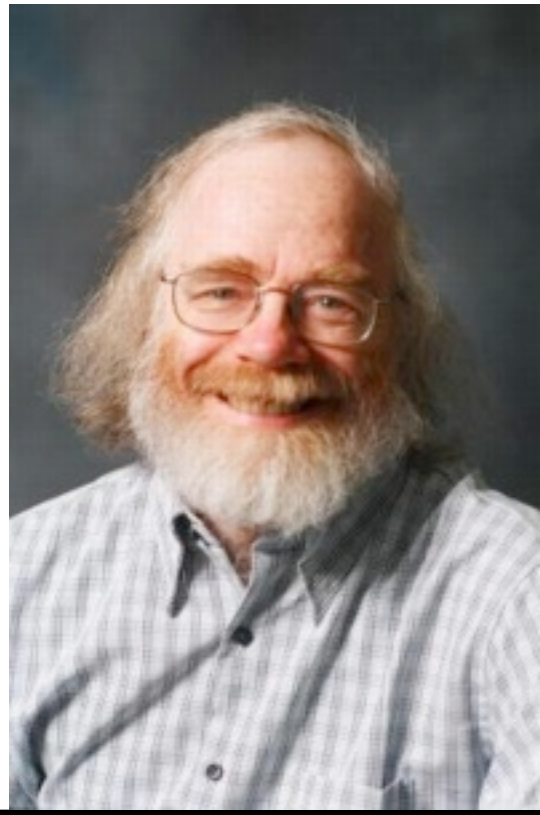


What does that little lock mean?

- What does this lock actually mean?
  - Are you secure?
- It really depends...
  - Some websites used negotiate the use of the "null cipher".
    - So even with the lock icon, no crypto was being used.
  - Attackers can launch SSL downgrade attacks against older browsers.
  - Commonly misspelled websites might make you think you are connected securely to the right page.

Steve Bellovin

- Long time researcher at AT&T Research/Bell Labs.
  - Member of the National Academy of Engineering
  - Professor at Columbia University
- Credited as one of the "Fathers of the firewall"
- One of the originators of USENET
  - The precursor to World Wide Web, allowed people to view and exchange content in newsgroups.



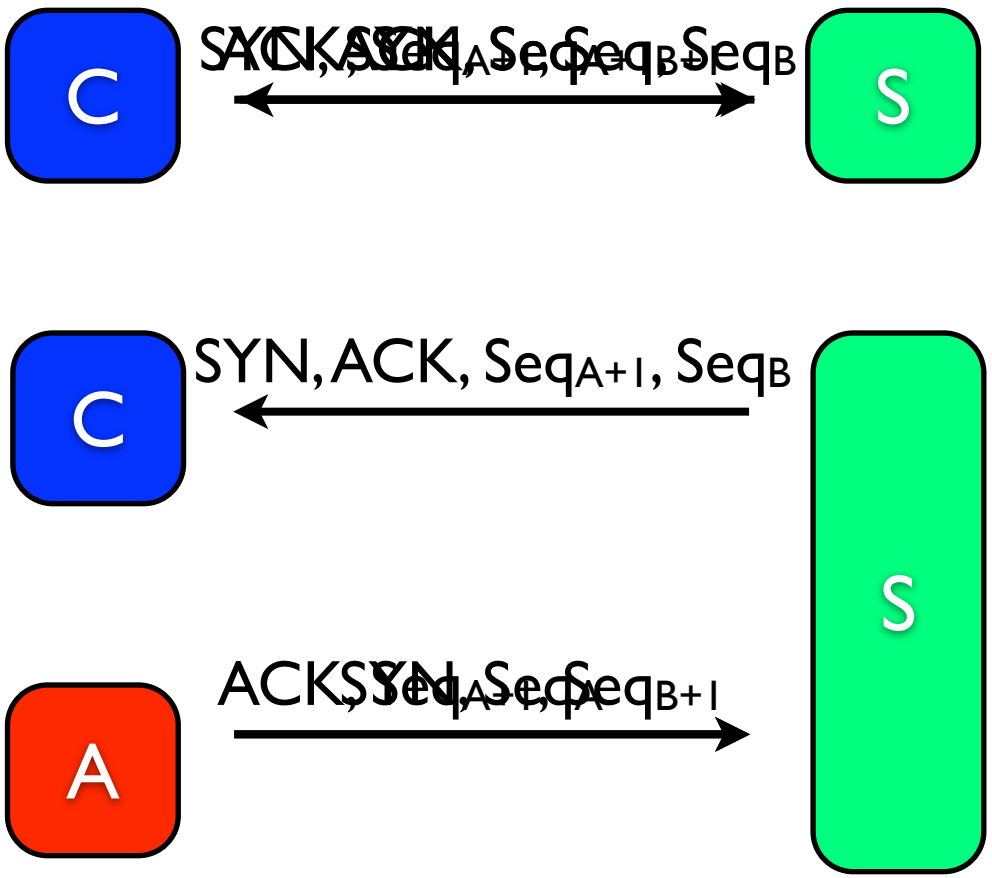
Security Problems in the TCP/IP Protocol Suite

- This is one of the classics of Network Security literature.
- Although written in 1989, many of the protocols discussed here are still widely used today.
- This is a nice overview of why security research is necessary.
  - It is hard to build secure systems when the infrastructure supporting them was never designed to consider security.
  - Attacks on specific implementations not discussed.
  - Three general attack categories: TCP/IP Attacks, Routing Attacks, and Abusing Common Protocols.

TCP/IP Sequence Number Guessing

- TCP connects are established by the 3-way handshake:
  - What do the three messages look like?
- Each client keeps a unique sequence number to order packets and prevent against loss.
- An attacker can spoof an IP address, but attempting to carry out a conversation when you don't know the correct responses is hard.
  - If you can guess the response, you can establish a connection.

How This Attack Works

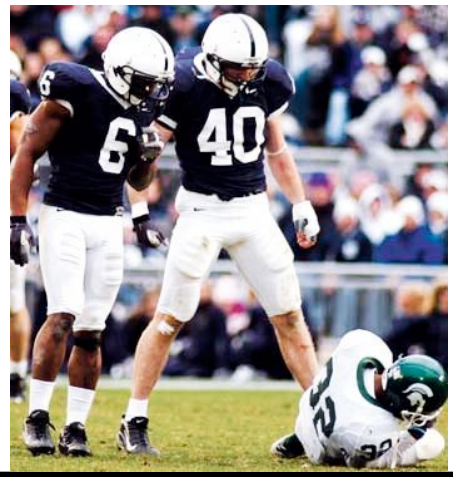


What Can You Do With This?

- On Christmas Day 1994, Kevin Mitnick used this attack to break into Tsuomo Shimamura's machine.
  - Claimed to be from a "trusted" IP address, added himself to rhosts file, gained full access.
- Unfortunately for Mitnick, Tsutomu Shimomura caught him in the act (saw the logs).
- Ultimately, this incident helped the FBI track down and arrest Mitnick in Raleigh, NC.

Defense Against SNG Attack

- Make the initial sequence number hard to guess.
  - Most systems now use a PRNG, but they're not great.
  - Most implementations of TCP will accept RST packets with a sequence number anywhere within their window.
  - For a 32Kb window, 2^{17} attempts is enough to get it right.
- Actively monitor your logs.
  - But you need to be on top of this as an attacker is likely to delete or modify them once they get access.



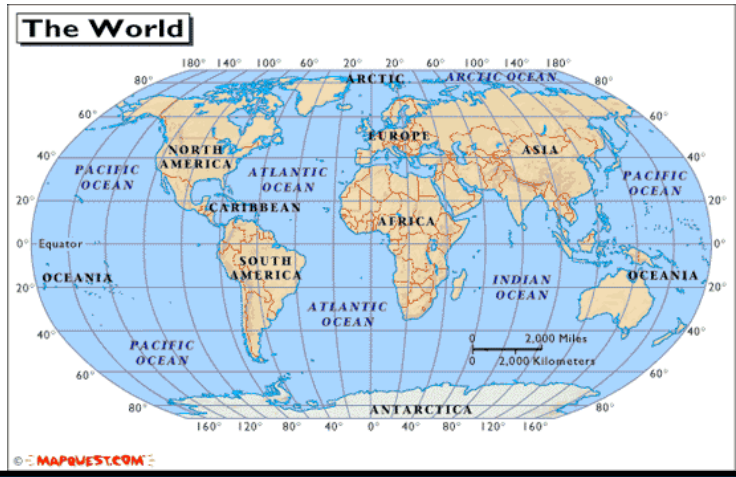
Class Exercise

- One way to make such attacks far more difficult is to make guessing an initial sequence number totally improbable to guess.

- Take 5 minutes and modify the 3-way handshake of TCP to make it more resistant to such an attack.
  - Can you incorporate a puzzle or something hard to calculate?

Real-World Routing Attacks

- AS7007 (1997)
- YouTube hijacked by Pakistan (2008)

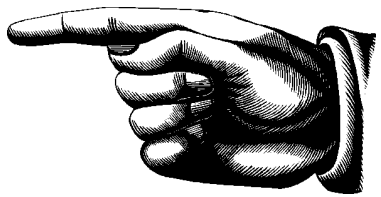


ICMP Attacks

- Examples
  - ICMP Redirect
  - ICMP Destination Unreachable
  - ICMP Time to Live Exceeded
- Defense
  - Filtering

Other Protocols

- Finger
  - Directory-like service.
  - Can this help with identity theft? Password cracking?
- Electronic Mail
  - We have already shown how to spoof email.
  - Until recently, even retrieving mail from your server used cleartext passwords.



Other Protocols (2)

- DNS
  - Sequence number guessing and response spoofing thought to be potentially serious attacks in 1989.
  - These are major issues today... why?
- ARP
  - A local attacker could similarly siphon off all your traffic.

General Defenses

- Authentication
  - Authentication by assertion repeatedly gets us into trouble.
  - Why do we still do it?
- Encryption
  - End-to-End
  - Link-layer

Conclusions

- IP addresses are meaningless as an authentication token.
- Use random numbers whenever knowledge of that number may open your system to attack.
- The core of the network is based on algorithms that fall over pretty easily, making the Internet very fragile.

Next Time

- Read Chapter 8.7 - 8.9

- Project 4 is looming...
  - Remember, not being able to get it to work the night before it is due is a problem of bad time management.