

Security I: 8.1 to 8.4

Smith College, CSC 249
April 15, 2008

slides mostly from J.F Kurose and K.W. Ross,
copyright 1996-2007

Chapter 8: Network Security

Chapter goals:

- understand principles of network security:
 - ❖ cryptography and its *many* uses beyond "confidentiality"
 - ❖ message integrity
 - ❖ authentication
 - ❖ Securing each layer
- security in practice:
 - ❖ firewalls
 - ❖ security in application, transport, network, link layers

2

Introduction: NPR Series

- **Cyber Unit Pivotal in Solving Crime Online and Off, Jan 6, 2008**

<http://www.npr.org/templates/story/story.php?storyId=17850966>

- ❖ Listen to about 3 minutes

- **Criminals Find New Ways to Attack on the Internet, Oct. 9, 2006**

<http://www.npr.org/templates/story/story.php?storyId=6223908>

- **Cyber Sleuths Zero In as Web Fraud Takes Toll, Jan 20, 2008**

<http://www.npr.org/templates/story/story.php?storyId=18117120>

3

CyberSecurity? - Line Breaks

- Accidental Fiber-Optic Line Break Cuts Internet Service in the Middle East And Southeast Asia, Feb, 2008
- It wasn't sabotage that cut a high-capacity fiber-optic line in the Mideast but the anchor of a ship forced to port by a powerful storm off the Egyptian coast, according to cybersecurity experts.
- The cut caused Internet service to be disrupted across the United Arab Emirates, Saudi Arabia, Qatar, India, Pakistan and Bangladesh.
- There were not enough nearby lines with adequate capacity to reroute the Internet traffic.
- While this failure was accidental, Internet security experts point out that this underlines the vulnerability of single points of failure. "If this is what happens during a series of coincidences, think what intentional activity could do,"
- Lines are cut every day in the U.S. through accidental activity such as a backhoe cutting a landline. Usually, service can be rerouted through another line or provider so that no disruption in service occurs.
- There are, however, some vulnerable fat pipes where given a little research and malevolent motivation, enormous disruptions could occur through a few specific line cuts, according to cybersecurity experts.

4

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

5

What is network security?

Confidentiality: only sender, intended receiver should "understand" message contents

- ❖ sender encrypts message
- ❖ receiver decrypts message

Authentication: sender, receiver want to confirm identity of each other

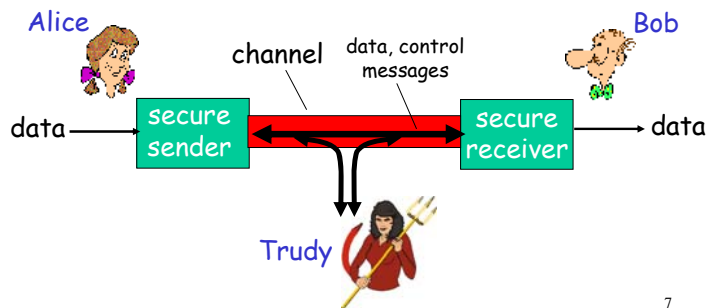
Data Integrity: sender, receiver want to ensure message not altered (in transit, or afterwards) without detection

Access and Availability: services must be accessible and available to users

6

Friends and enemies: Alice, Bob, Trudy

- ❑ well-known in network security world
- ❑ Bob and Alice want to communicate "securely"
- ❑ Trudy (intruder) may intercept, delete, add and/or alter messages



7

Who might Bob, Alice be?

- ❑ Human application users, or...
- ❑ Web browser/server for electronic transactions (e.g., on-line purchases)
- ❑ on-line banking client/server
- ❑ DNS servers
- ❑ routers exchanging routing table updates
- ❑ etc...

8

Types of security breaches

Possible actions

- ❖ *eavesdrop*: intercept messages
- ❖ actively *insert* messages into connection
- ❖ *impersonation*: can fake (spoof) source address in packet (or any field in packet)
- ❖ *hijacking*: "take over" ongoing connection by removing sender or receiver, inserting himself in place
- ❖ *denial of service*: prevent service from being used by others (e.g., by overloading resources)

9

Uses for cryptography

- Provide **confidentiality**
 - ❖ privacy, secrecy
 - ❖ ensures data can be read by authorized persons only
- Ensure **message/data integrity**
 - ❖ prevents unauthorized people from altering a message
- Provide **authentication**
- Provide **nonrepudiation**

11

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

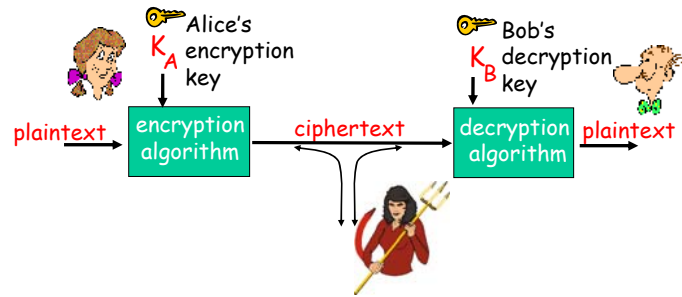
10

Discussion Question

- Difference between authentication and non-repudiation?
 - ❖ Non-repudiation provides evidence that can be shown to an adjudicator about the identity of the author
 - ❖ Authentication only assures that the recipient is convinced of the identity of the author

12

The language of cryptography

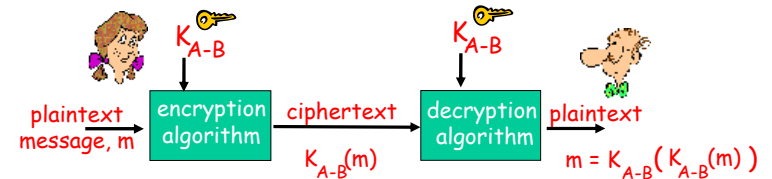


symmetric key cryptography: sender & receiver keys are *identical* and *secret* (but known by 2 parties)

public-key cryptography: the encryption key is *public*, the decryption key *secret*, and known only by one party

13

Symmetric key cryptography



symmetric key cryptography: Bob and Alice share/know the ~~same~~ (symmetric) key: K

- e.g., key is knowing substitution pattern in mono-alphabetic substitution cipher
- **Q:** how do Bob and Alice agree on key value?

14

Public Key Cryptography

symmetric key cryptography

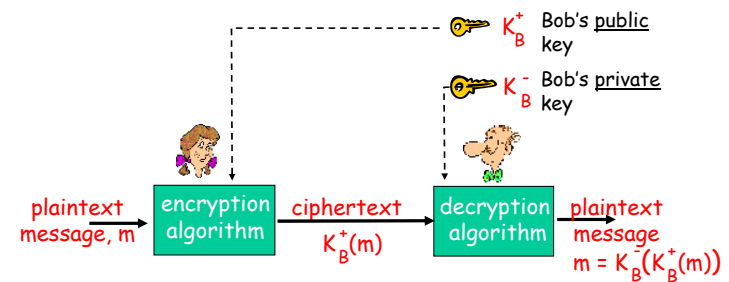
- requires sender & receiver to know shared secret key
- **Q:** how to agree on key in first place (particularly if they have never "met")?

public key cryptography

- radically different approach
- sender, receiver do *not* share secret key
- *public* encryption key known to *all*
- *private* decryption key known only to receiver

15

Public key cryptography



16

Public key encryption algorithms

Requirements:

- ① need $K_B^+(\cdot)$ and $K_B^-(\cdot)$ such that

$$K_B^-(K_B^+(m)) = m$$

- ② given public key K_B^+ , it should be impossible to compute private key K_B^-

RSA: Rivest, Shamir, Adelson algorithm

17

RSA: Choosing keys

1. Choose two large prime numbers p, q .
(e.g., 1024 bits each)
2. Compute $n = pq, z = (p-1)(q-1)$
3. Choose e (with $e < n$) that has no common factors with z . (e, z are "relatively prime").
4. Choose d such that $ed-1$ is exactly divisible by z .
(in other words: $ed \bmod z = 1$).
5. Public key is (n, e) . Private key is (n, d) .
 $\underbrace{\hspace{1cm}}_{K_B^+} \quad \underbrace{\hspace{1cm}}_{K_B^-}$

18

RSA: Encryption, decryption

0. Given (n, e) and (n, d) as computed above
1. To encrypt bit pattern, m , compute
 $c = m^e \bmod n$ (i.e., remainder when m^e is divided by n)
2. To decrypt received bit pattern, c , compute
 $m = c^d \bmod n$ (i.e., remainder when c^d is divided by n)

Number
theory
result

$$m = (\underbrace{m^e \bmod n}_c)^d \bmod n$$

19

RSA example:

Bob chooses $p = 5, q = 7$. Then $n = 35, z = 24$.
 $e = 5$ (so e, z relatively prime).
 $d = 29$ (so $ed-1$ exactly divisible by z)

encrypt:	<u>letter</u>	<u>m</u>	<u>m^e</u>	<u>$c = m^e \bmod n$</u>
	I	12		
decrypt:	<u>c</u>	<u>c^d</u>		<u>$m = c^d \bmod n$</u> <u>letter</u>

20

Activity

- Using RSA, choose $p = 3$, $q = 11$. Encode a word of your choice and send it to a different host to decode.
- Suggestion for e ? ... choose
- Then $(p-1)(q-1) =$
- Also choose $d =$
 - ❖ so $e*d =$
 - ❖ $e*d-1 = \epsilon$
- Thus $n =$

21

Public Key Cryptography Concerns?

- It must be *very* difficult to discover or determine private keys
- Since encryption keys are public, entities can *claim* to be someone else when sending a message
 - ❖ Need more than just public key cryptography
 - ❖ ... Need to bind the message to a sender

23

RSA: another important property

The following property will be *very* useful later:

$$\underbrace{K_B^-(K_B^+(m))}_{\text{use public key first, followed by private key}} = m = \underbrace{K_B^+(K_B^-(m))}_{\text{use private key first, followed by public key}}$$

22

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

24

Message Integrity

Bob receives msg from Alice, wants to ensure:

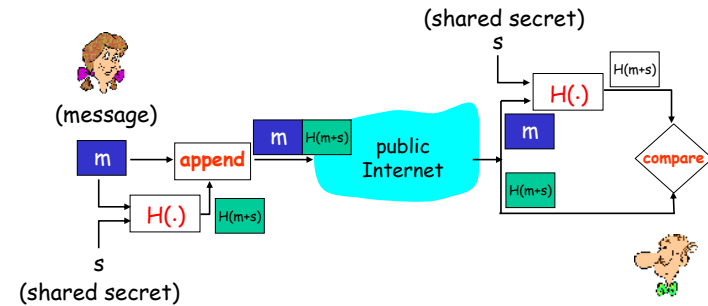
- message originally came from Alice
- message not changed since sent by Alice

Cryptographic Hash:

- takes input m , produces fixed length value, $H(m)$
 - ❖ e.g., as in Internet checksum, CRC
- computationally infeasible to find two different messages, x, y such that $H(x) = H(y)$
 - ❖ equivalently: given $m = H(x)$, (x unknown), can not determine x .
 - ❖ note: Internet checksum *fails* this requirement!

25

Message Authentication Code: $H(m+s)$



Issue...?

How to distribute the shared authentication key, s

26

Digital Signatures

Cryptographic technique analogous to hand-written signatures.

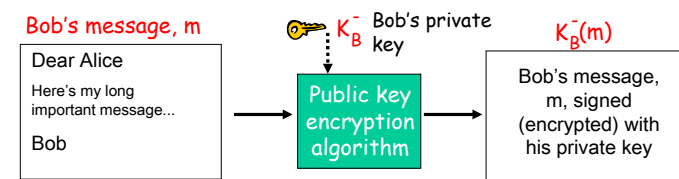
- sender (Bob) digitally signs document, establishing he is document owner/creator.
- verifiable, nonforgeable: recipient (Alice) can prove to someone that Bob, and no one else (including Alice), must have signed document

27

Digital Signatures: Application for Public Key Cryptography

Simple digital signature for message m :

- Bob signs m by encrypting with his private key K_B^- , creating "signed" message, $K_B^-(m)$



28

Digital Signatures (more)

- Suppose Alice receives msg m , digital signature $K_B^-(m)$
- Alice verifies m signed by Bob by applying Bob's public key K_B^+ to $K_B^-(m)$ then checks $K_B^+(K_B^-(m)) = m$.
- If $K_B^+(K_B^-(m)) = m$, whoever signed m must have used Bob's private key.

Alice thus verifies that:

- Bob signed m .
- No one else signed m .
- Bob signed m and not m' .

Non-repudiation:

- Alice can take m , and signature $K_B^-(m)$ to court and prove that Bob signed m .

29

Public Key Certification

public key problem:

- When Alice obtains Bob's public key (from web site, e-mail, diskette), how does she *know* it is Bob's public key, not Trudy's?

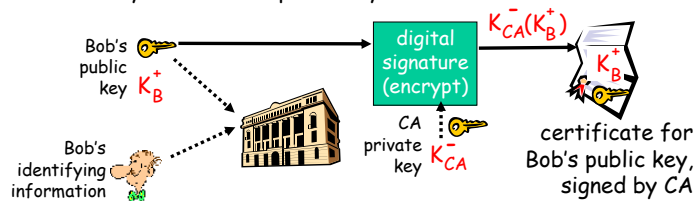
solution:

- trusted certification authority (CA)

30

Certification Authorities

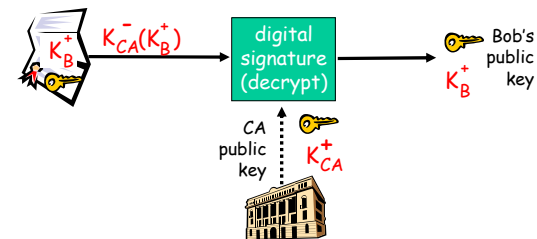
- Certification Authority (CA):** binds public key to particular entity, E.
- E registers its public key with CA.
 - E provides "proof of identity" to CA.
 - CA creates certificate binding E to its public key.
 - certificate containing E's public key digitally signed by CA: CA says "This is E's public key."



31

Certification Authorities

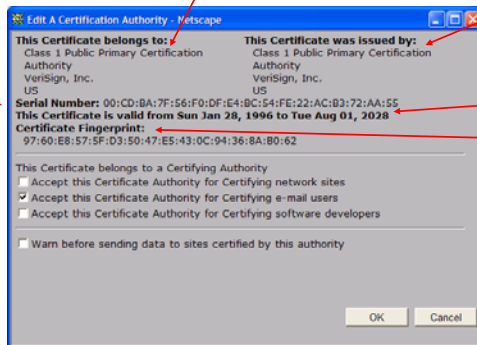
- when Alice wants Bob's public key:
 - gets Bob's certificate (Bob or elsewhere).
 - apply CA's public key to Bob's certificate, get Bob's public key



32

A certificate contains:

- ❑ Serial number (unique to issuer)
- ❑ info about certificate owner, including algorithm and key value itself (not shown)



- ❑ info about certificate issuer
- ❑ valid dates
- ❑ digital signature by issuer

33

Discussion Question

- ❑ If a Certification Authority goes down, what is the impact on the ability of parties to communicate securely. Who can and cannot communicate?

34

Cyber Attacks: Estonia

- ❑ The **Guardian** reports that the attacks began in late April, 2007, coinciding with Estonia's decision to move a Soviet World War II memorial from a central location in the Baltic nation's capital.
- ❑ The crisis unleashed a wave of so-called DDoS, or Distributed Denial of Service, attacks, where websites are suddenly swamped by tens of thousands of visits, jamming and disabling them by overcrowding the bandwidths for the servers running the sites.
- ❑ Estonian officials and computer security experts say that, particularly in the early phase, some attackers were identified by their internet addresses - many of which were Russian, and some of which were from Russian state institutions. ...
- ❑ The **Guardian** notes that Estonia is a pioneer of "e-government" and one of the most wired countries in Europe, making it that much more vulnerable to cyberattacks. In order to stop the attacks, Estonia has shut down foreign access to the sites under siege.

35

NPR Series con't

- ❑ **Defense Contractors May Be Chink in Cyber Security, Dec. 13, 2005**

<http://www.npr.org/templates/story/story.php?storyId=5050285>

- ❑ **Cyber Crime Transforms Legal Landscape, Jan 13, 2008**

<http://www.npr.org/templates/story/story.php?storyId=17937934>

❖ About 3 minutes – up to Wikipedia

36

Chapter 8 Part 1 Summary

- Defining network security
 - ❖ confidentiality, authentication, integrity, nonrepudiation (access control)
- Cryptography
 - ❖ Symmetric, public and mixed
- Integrity
 - ❖ Message digest
 - ❖ Digital signature
- Certification Authority