CprE 450/550X
Distributed Systems and Middleware

Security

Yong Guan
3216 Coover
Tel: (515) 294-8378
Email: guan@ee.iastate.edu

April 15 & 22, 2003

Announcement

- Term paper and the second course project will due this Friday (April 25th), 5:00pm.
- Please schedule a time (from Monday to Wednesday next week) to show your project demo.

- Final take-home exam will be distributed to the students next Thursday (May 1) and will due on Wednesday (May 7, 11:59am).

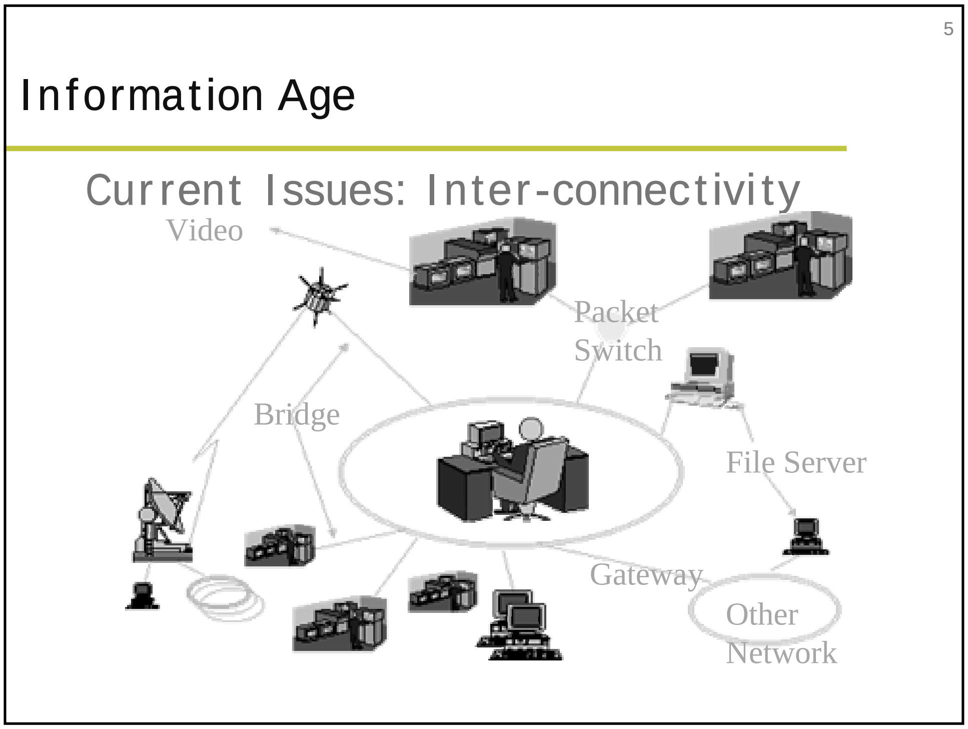
- You will give a 6-minute presentation on Friday (May 9, 12:00-2:00pm). Please send me the powerpoint file with two or three slide to me before May 8, 11:59pm). I will post a slide template on the course page tonight.

Readings for Today's Lecture

- References
  - Chapter 8 of "Distributed Systems: Principles and Paradigms"
  - Ross Anderson, "Security Engineering"

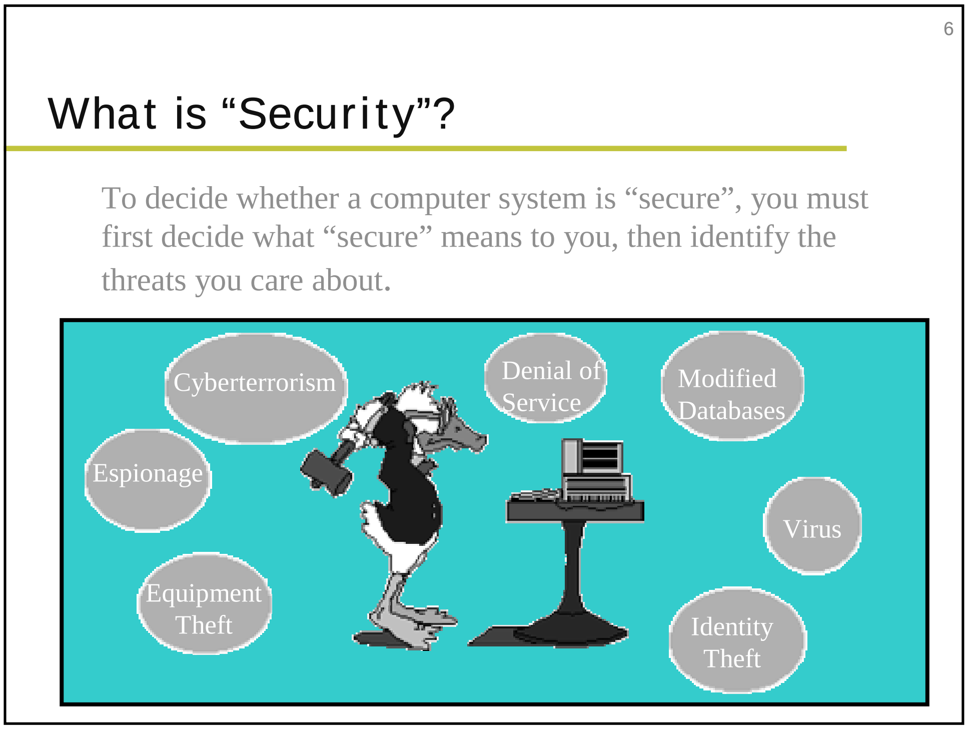
The Questions Are:

- What is Information Technology Security?
- Why should you care?
- Who is responsible?
- How do you get there?



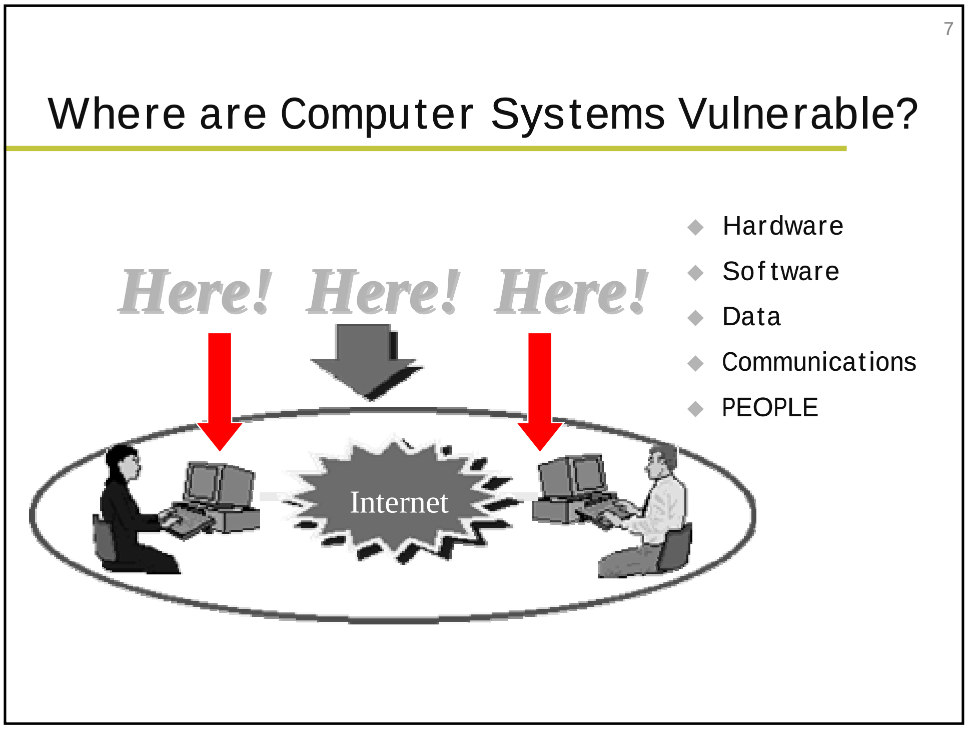
Information Age

Current Issues: Inter-connectivity



What is “Security”?

To decide whether a computer system is “secure”, you must first decide what “secure” means to you, then identify the threats you care about.

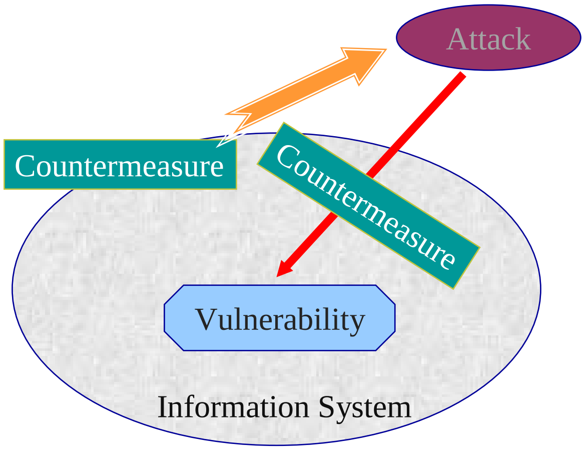


Where are Computer Systems Vulnerable?

- Hardware
- Software
- Data
- Communications
- PEOPLE

Who Is The Threat? I Just Didn't Know

Security Vulnerability, Attack, and Countermeasure



Attack

Countermeasure

Countermeasure

Vulnerability

Information System

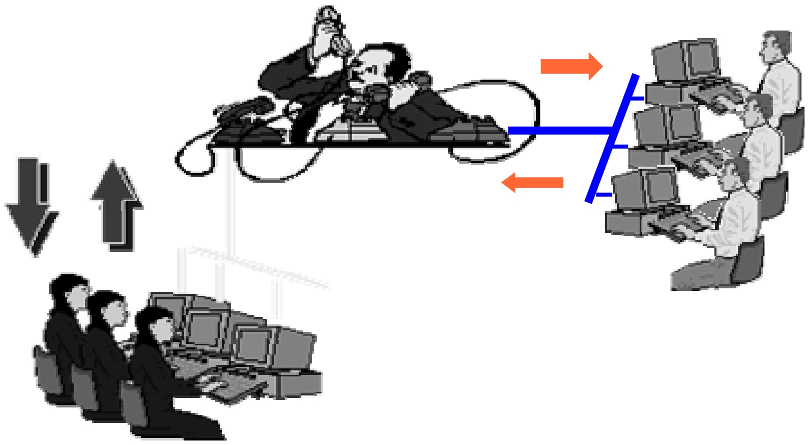
Security Vulnerability

- Physical security weakness
- Software or hardware flaws
- Poor system management

Security Attacks

- Active Attacks: The adversary actively changes the protected object and often shows some anomalous behavior.
  - File: be destroyed or subtly altered
  - Messages: be altered, deleted, inserted, mis-rerouted
  - Trap doors: be set up
  - Authorization status: be altered
  - Availability of service: be denied
- Passive Attacks: The adversary never changes the protected object, but listens, and does not show anomalous behavior.
  - Shoulder Surfing
  - Tapping
    - Telephone tapping, Analog car phone (spectrum scanning), Facsimile
  - Traffic Analysis
    - Knowledge about traffic information who called whom when, how often, for how long, from where

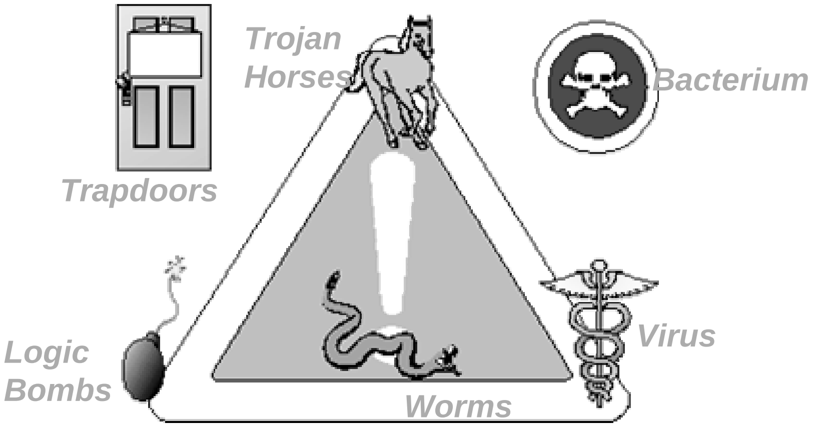
Eavesdropping



13

Malicious Code

(Program and System Threats)

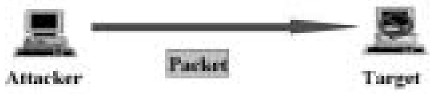


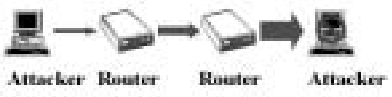
14

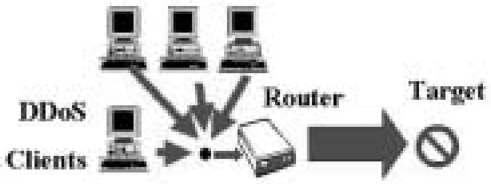
Availability

(From Single DOS to DDOS)

See source: www.hackernews.com/bufferoverflow/00/dosattack/dosattack.html

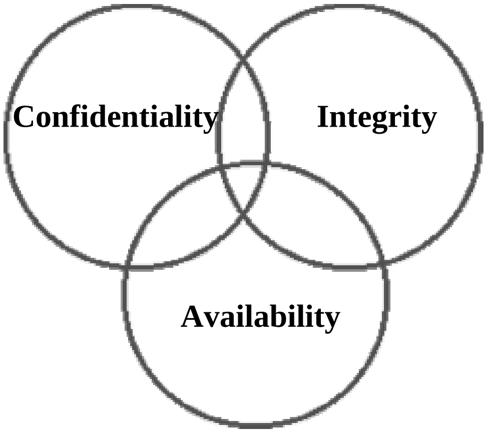






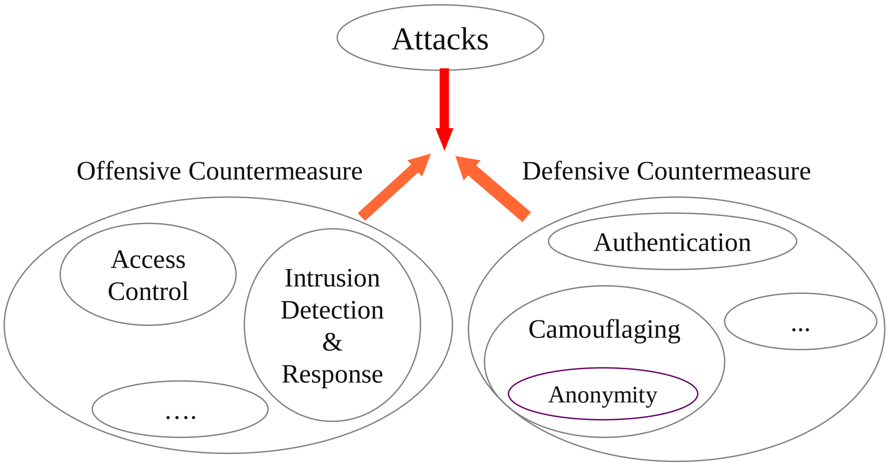
15

What Is Information Technology Security?



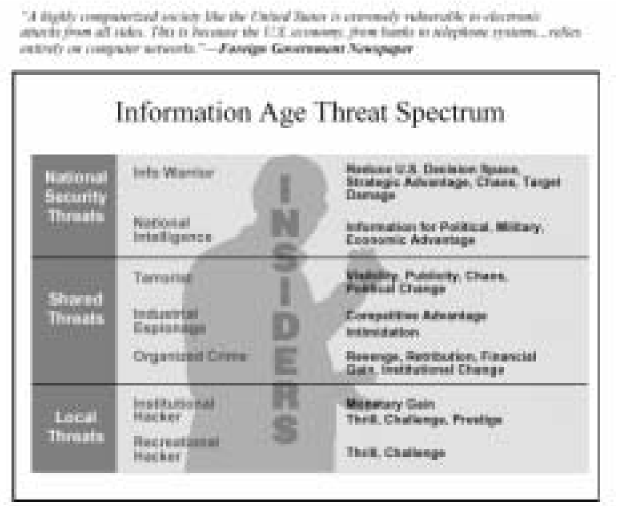
16

Security Countermeasures



Camouflage: To hide the existence of the protected object.

Information Age Threat Spectrum



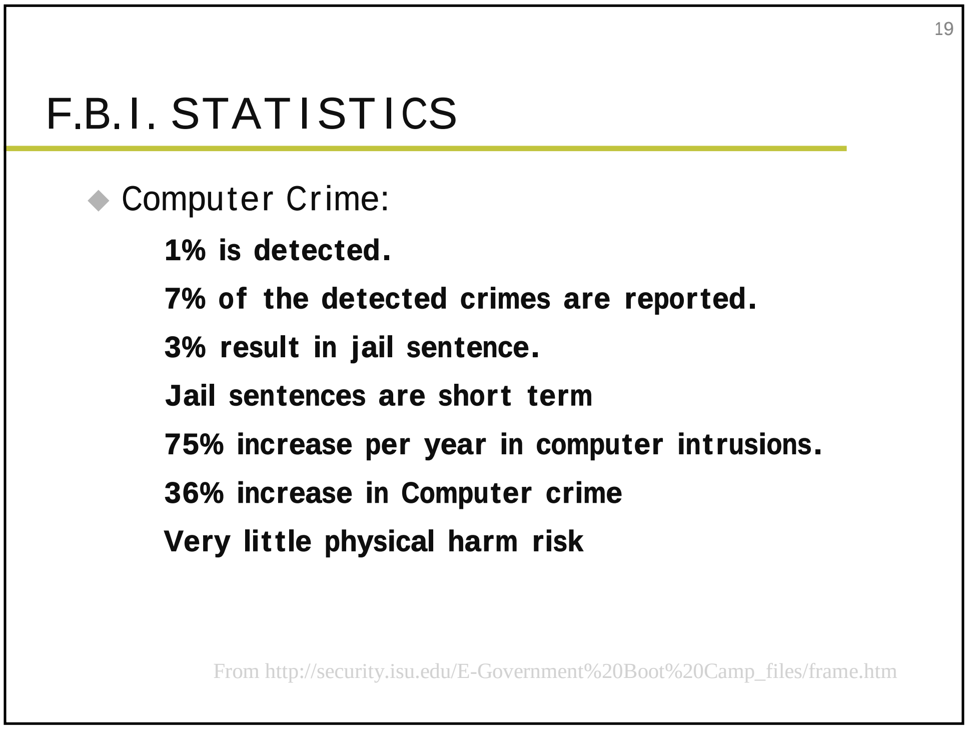
"A highly computerized society like the United States is extremely vulnerable to electronic attacks from all sides. This is because the U.S. economy, from banks to telephone systems...relies entirely on computer networks."—***Foreign Government Newspaper***

Information Age Threat Spectrum

National Security Threats	Info Warrior	Reduce U.S. Decision Space, Strategic Advantage, Chaos, Target Damage
	National Intelligence	Information for Political, Military, Economic Advantage
Shared Threats	Terrorist	Visibility, Publicity, Chaos, Political Change
	Industrial Espionage	Competitive Advantage Intimidation
	Organized Crime	Revenge, Retribution, Financial Gain, Institutional Change
Local Threats	Institutional Hacker	Monetary Gain Thrill, Challenge, Prestige
	Recreational Hacker	Thrill, Challenge

The Question Are:

- What is Information Technology Security?
- Why should you care?
- Who is responsible?
- How do you get there?



F.B.I. STATISTICS

- Computer Crime:

  1% is detected.

  7% of the detected crimes are reported.

  3% result in jail sentence.

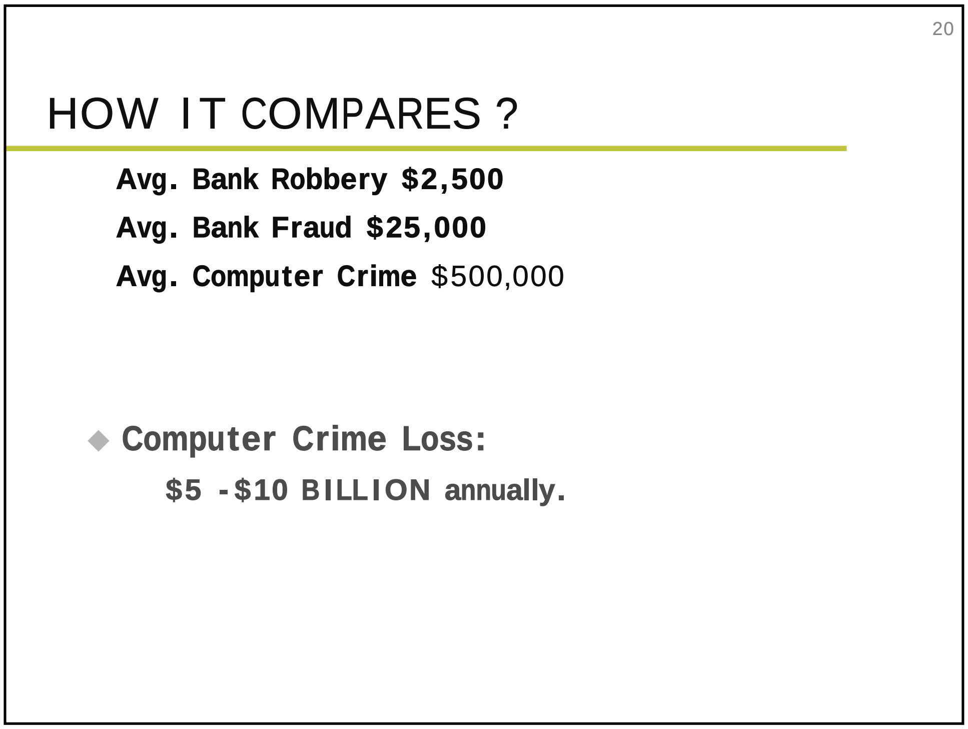
  Jail sentences are short term

  75% increase per year in computer intrusions.

  36% increase in Computer crime

  Very little physical harm risk

From http://security.isu.edu/E-Government%20Boot%20Camp_files/frame.htm



HOW IT COMPARES ?

Avg. Bank Robbery $2,500

Avg. Bank Fraud $25,000

Avg. Computer Crime $500,000

- **Computer Crime Loss:**

  $5 -$10 BILLION annually.

THREATS TO COMPUTER SYSTEMS

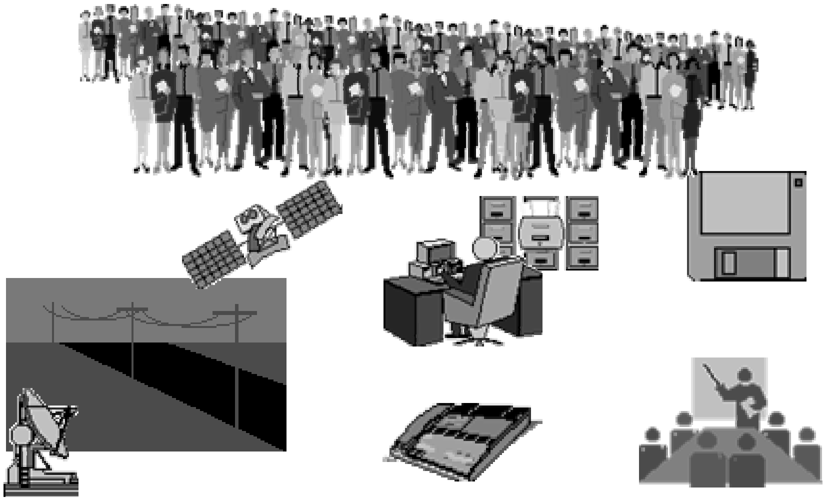
- Threats By People
  - **Unintentional Employee Action 50-60%**
  - **Intentional Employee Action 15-20%**
  - **Outside Actions 1- 3%**
- Physical & Environmental Threats
  - **Fire Damage 10-15%**
  - **Water Damage 1-5%**
  - **Natural Disaster 1%**

The Question Are:

- What is Information Technology Security?
- Why should you care?
- Who is responsible?
- How do you get there?

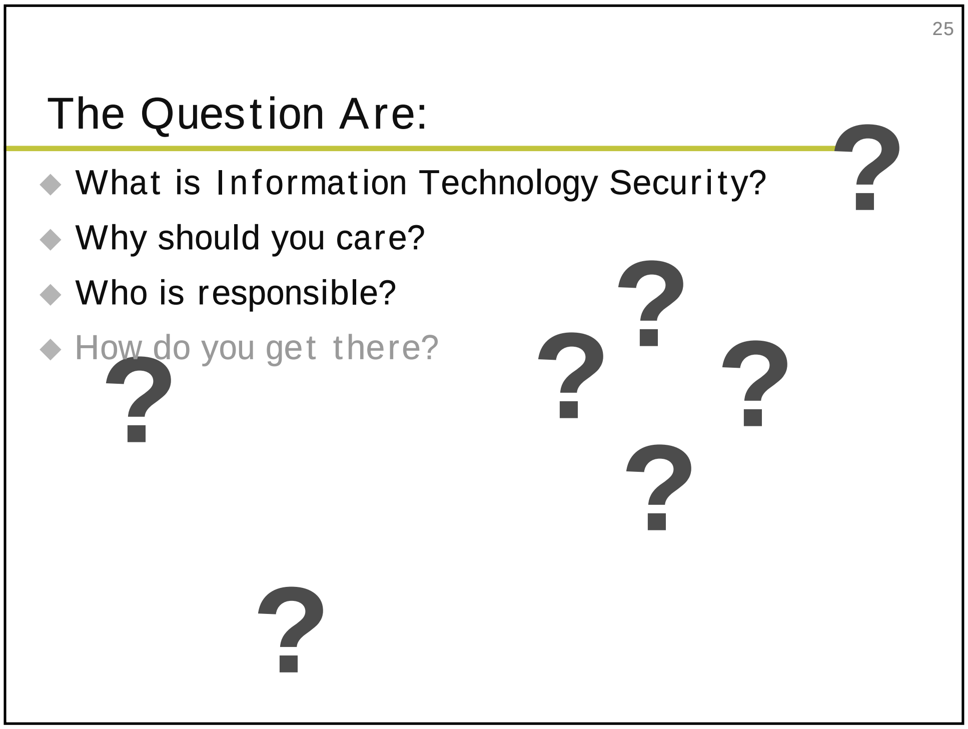
Information Technology Security Is Everyone's Responsibility

23



24

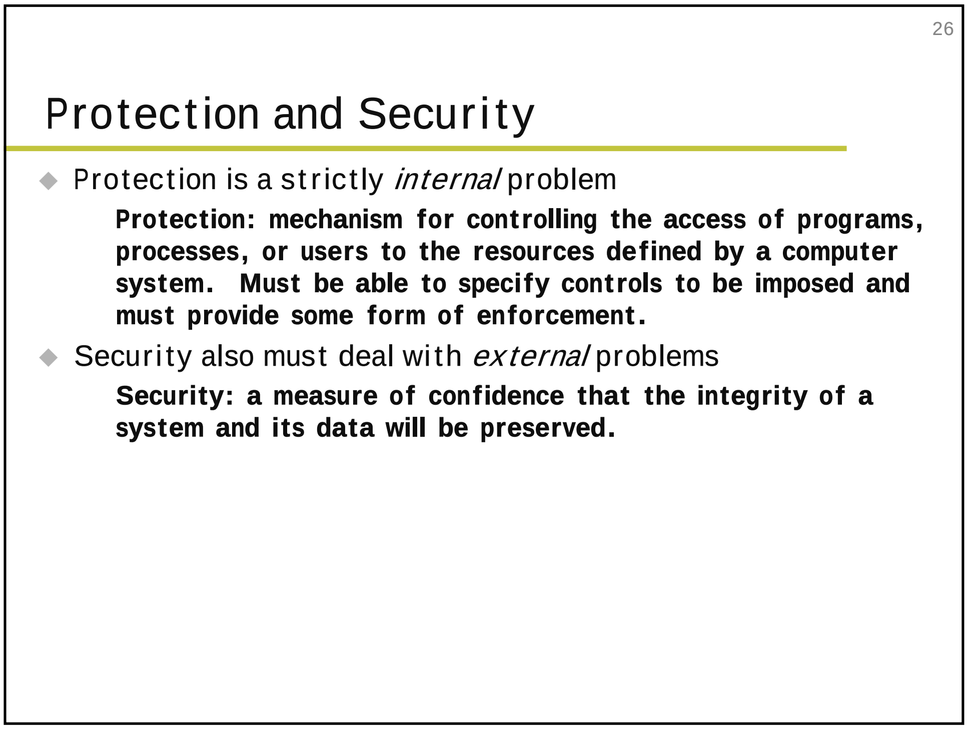
YOUR ROLE?



25

The Question Are:

- What is Information Technology Security?
- Why should you care?
- Who is responsible?
- How do you get there?



26

Protection and Security

- Protection is a strictly *internal* problem

  Protection: mechanism for controlling the access of programs, processes, or users to the resources defined by a computer system. Must be able to specify controls to be imposed and must provide some form of enforcement.

- Security also must deal with *external* problems

  Security: a measure of confidence that the integrity of a system and its data will be preserved.

Security

- Security must consider external environment of the system, and protect it from:
  - **unauthorized access.**
  - **malicious modification or destruction.**
  - **accidental introduction of inconsistency.**
- Easier to protect against accidental than malicious misuse.

Security

- Security measures must be taken at two levels
  - **Physical: site (or sites) containing the computer systems must be physically secured against intruders**
  - **Human: Users must be screened carefully to reduce the chance of a user authorizing access for an intruder**

29

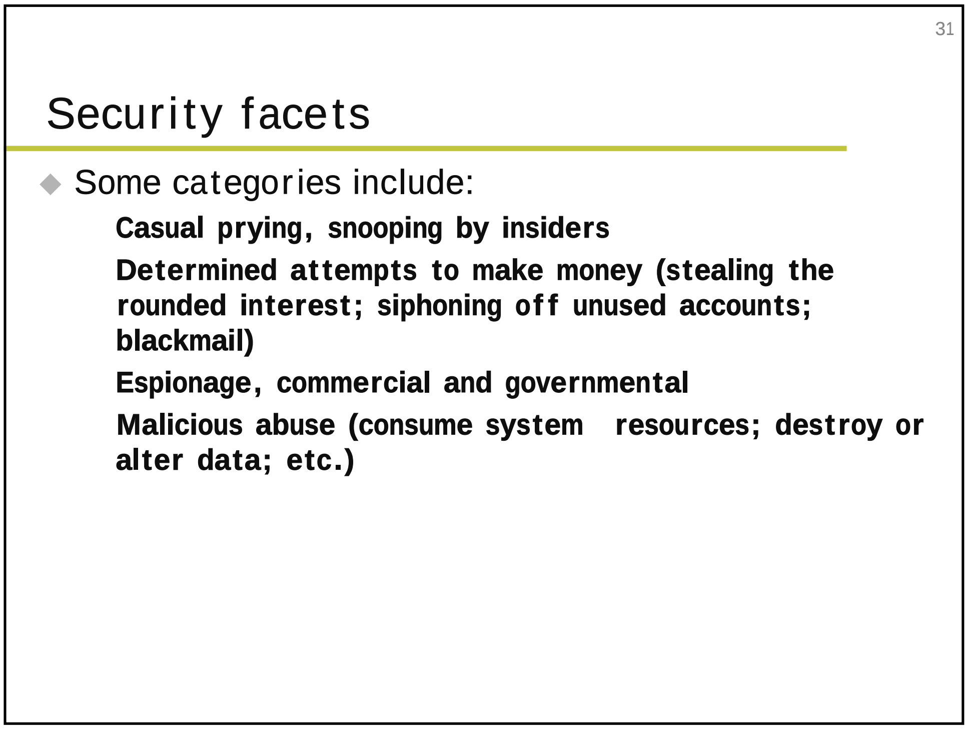
Physical security

- Some things to consider:
  - **securing computer sites**
  - **securing communication links**
    - **listening to network traffic (net snoopers)**
    - **protecting microwave links**
  - **electromagnetic radiation from computer sites**

30

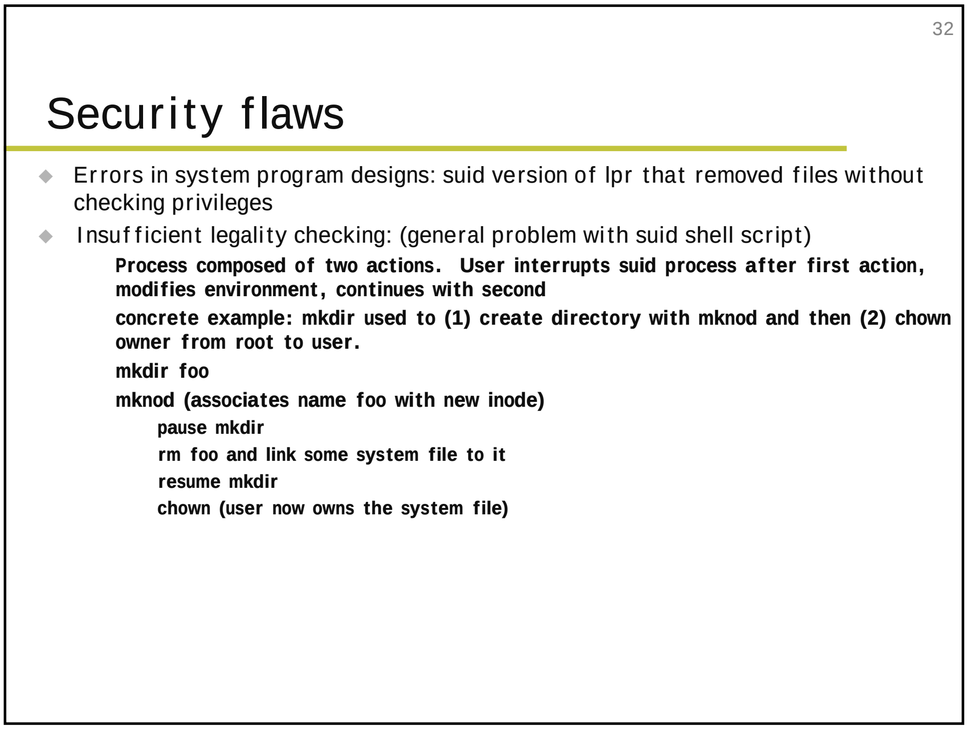
Security facets

- Security facets: major ones are data loss and intruders
  - **Data loss (relatively manageable by backups)**
  - **Acts of God (fire, floods, earthquakes, wars, etc.)**
  - **Hardware or software errors: Unreadable disks and tapes, program bugs, etc.**
  - **Human errors: Incorrect data entry, wrong tape or disk mounted, etc.**
  - **Intruders: passive (just looking around) and active (modifying data)**



Security facets

- Some categories include:
  - Casual prying, snooping by insiders
  - Determined attempts to make money (stealing the rounded interest; siphoning off unused accounts; blackmail)
  - Espionage, commercial and governmental
  - Malicious abuse (consume system resources; destroy or alter data; etc.)



Security flaws

- Errors in system program designs: suid version of lpr that removed files without checking privileges
- Insufficient legality checking: (general problem with suid shell script)
  - Process composed of two actions. User interrupts suid process after first action, modifies environment, continues with second
  - concrete example: mkdir used to (1) create directory with mknod and then (2) chown owner from root to user.
  - mkdir foo
  - mknod (associates name foo with new inode)
    - pause mkdir
    - rm foo and link some system file to it
    - resume mkdir
    - chown (user now owns the system file)

Penetration and Countermeasure

Access sensitive information	Encryption
Features not used	Implement protection
Implied Sharing	Capabilities
Parameters	Check user supplied
Line disconnect	Hang up
Carelessness	Employee Training
Passwords	Proper Management
Repetition	Hang up & Notify
Leakage	Shielding, Encryption
Waste	Destroy

Building Bolcks for Generic Security Services

- Authentication
- Access Control
- Confidentiality
- Integrity and non-repudiation

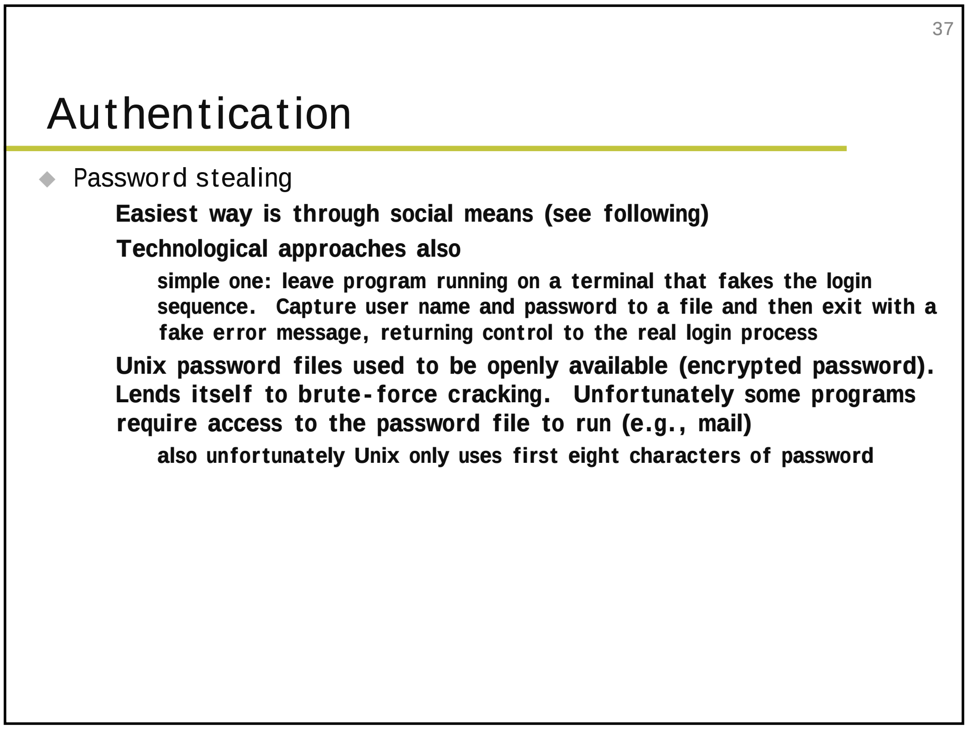
35

Authentication

36

Authentication

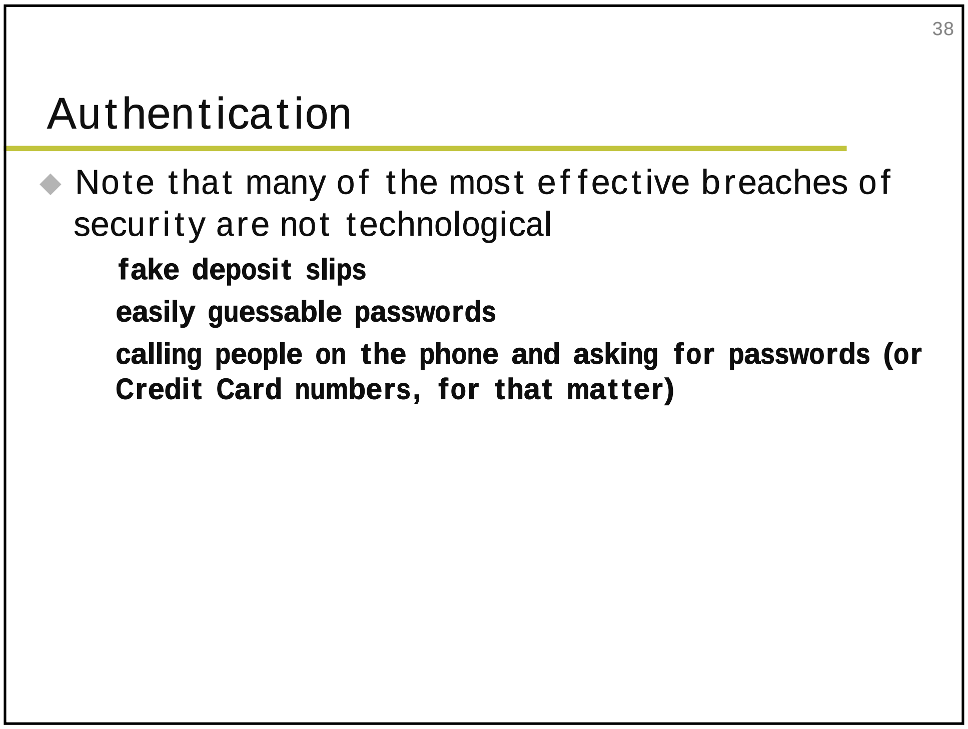
- User identity most often established through passwords,can be considered a special case of either keys or capabilities.
- Passwords must be kept secret.
  - **Frequent change of passwords.**
  - **Use of “non-guessable” passwords (user-chosen passwords are often easy to guess)**
  - **Log all invalid access attempts.**



37

Authentication

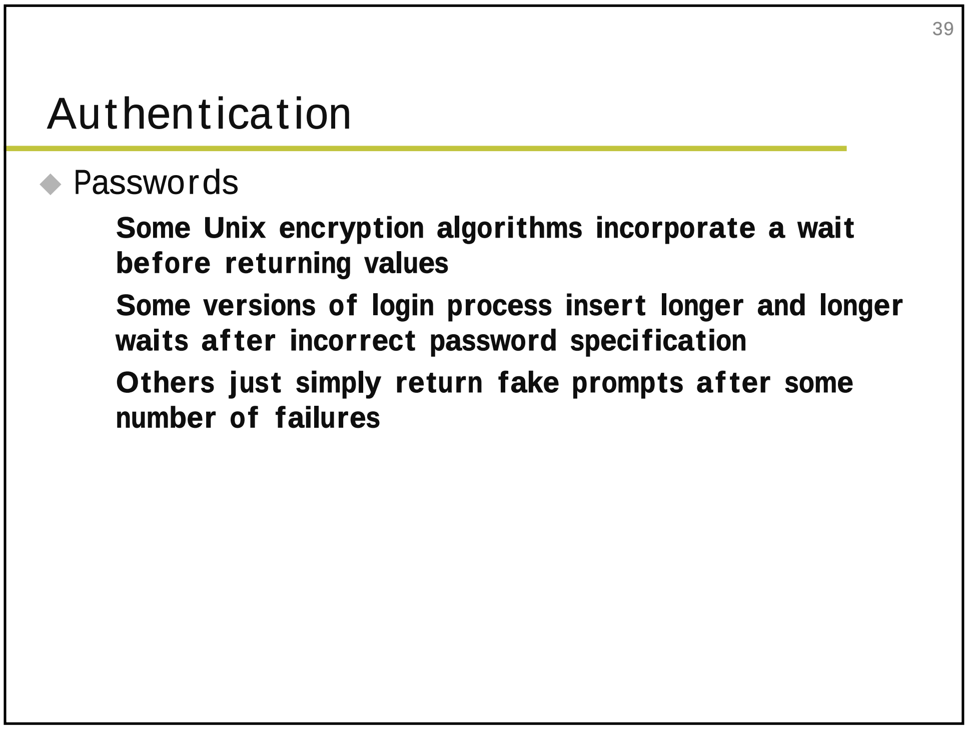
- Password stealing
  - Easiest way is through social means (see following)
  - Technological approaches also
    - simple one: leave program running on a terminal that fakes the login sequence. Capture user name and password to a file and then exit with a fake error message, returning control to the real login process
  - Unix password files used to be openly available (encrypted password). Lends itself to brute-force cracking. Unfortunately some programs require access to the password file to run (e.g., mail)
    - also unfortunately Unix only uses first eight characters of password



38

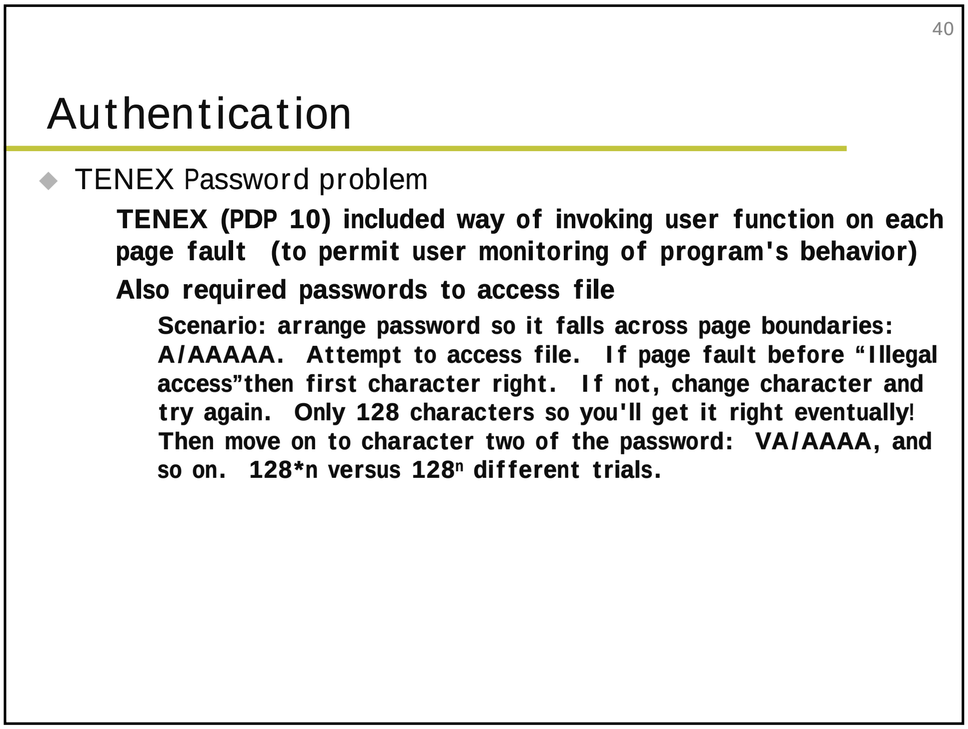
Authentication

- Note that many of the most effective breaches of security are not technological
  - fake deposit slips
  - easily guessable passwords
  - calling people on the phone and asking for passwords (or Credit Card numbers, for that matter)



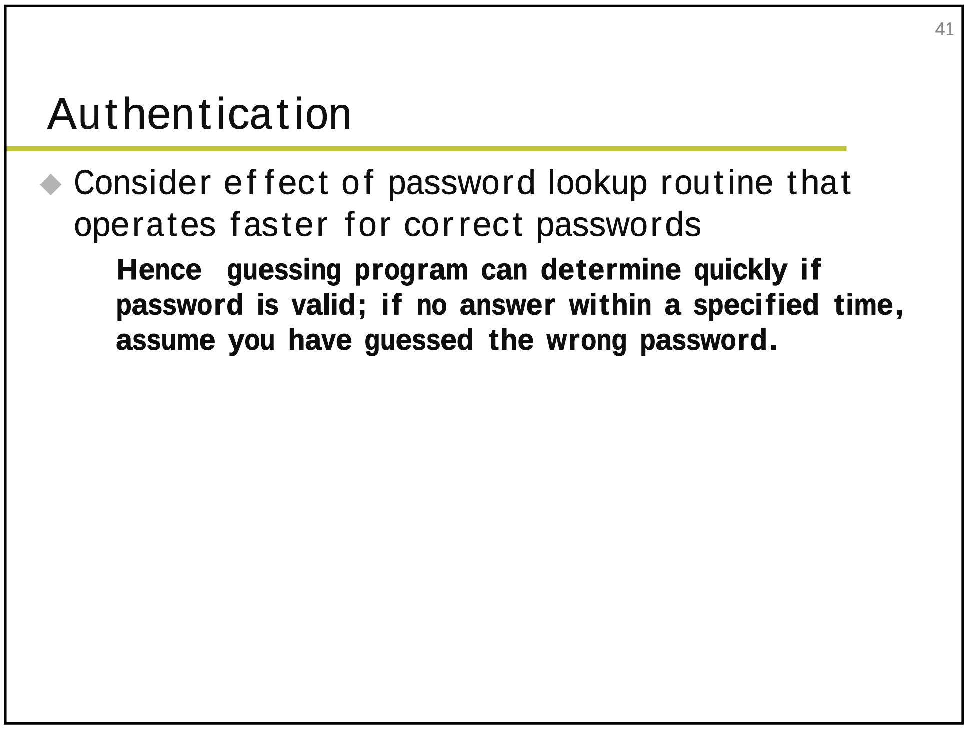
Authentication

- Passwords
  - Some Unix encryption algorithms incorporate a wait before returning values
  - Some versions of login process insert longer and longer waits after incorrect password specification
  - Others just simply return fake prompts after some number of failures



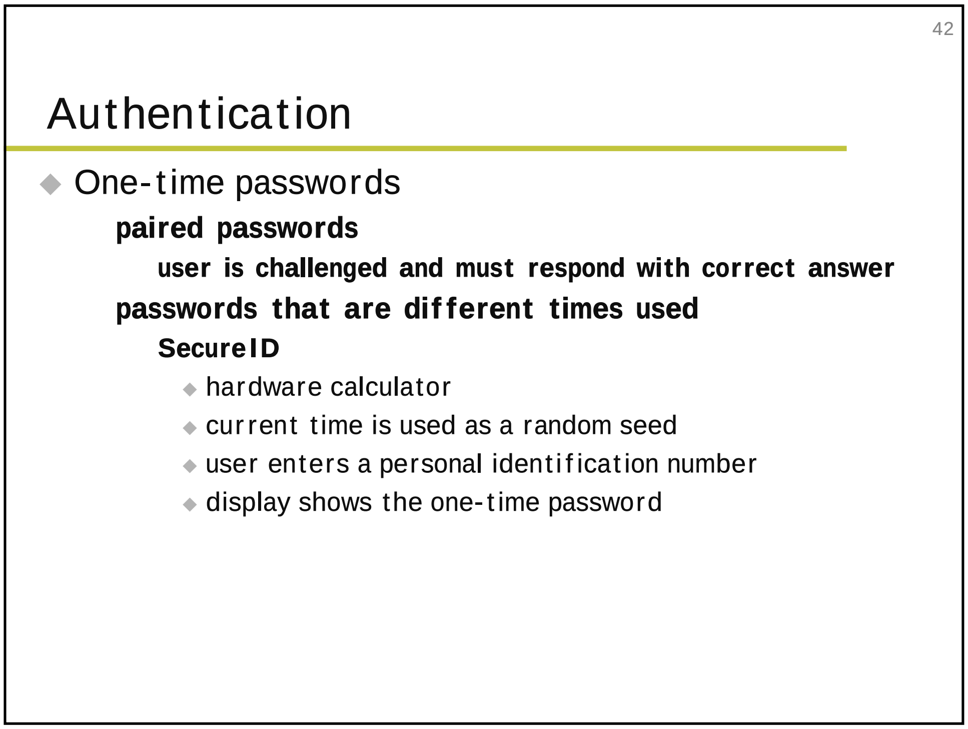
Authentication

- TENEX Password problem
  - TENEX (PDP 10) included way of invoking user function on each page fault (to permit user monitoring of program's behavior)
  - Also required passwords to access file
    - Scenario: arrange password so it falls across page boundaries: A/AAAAA. Attempt to access file. If page fault before "Illegal access"then first character right. If not, change character and try again. Only 128 characters so you'll get it right eventually! Then move on to character two of the password: VA/AAAA, and so on. 128*n versus 128^n different trials.



Authentication

- Consider effect of password lookup routine that operates faster for correct passwords
  - **Hence guessing program can determine quickly if password is valid; if no answer within a specified time, assume you have guessed the wrong password.**



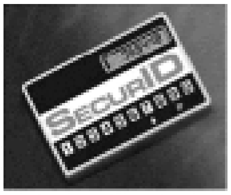
Authentication

- One-time passwords
  - **paired passwords**
    - **user is challenged and must respond with correct answer**
  - **passwords that are different times used**
    - **SecureID**
      - hardware calculator
      - current time is used as a random seed
      - user enters a personal identification number
      - display shows the one-time password

Passwords

- The Use of Passwords Should Follow These Guidelines
- No repeat guesses
- Log unsuccessful attempts
- Review log
- Never write down sensitive combinations
- Hard to guess passwords
- Change frequently
- Easy to recall, hard to guess
- Don't disclose

SecureID



← DISPLAY SCREEN in upper right hand corner

← numeric KEYPAD below the word SECURID

← P key (protect/clear key) below the number 9

← ♦ key (enter key) below the number 7

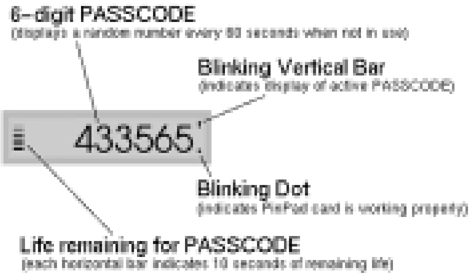
(NOT SHOWN: serial number of card on reverse)

SecurID® PinPad™ card²

45

SecureID

The DISPLAY SCREEN includes the four elements:



6-digit PASSCODE
(displays a random number every 60 seconds when not in use)

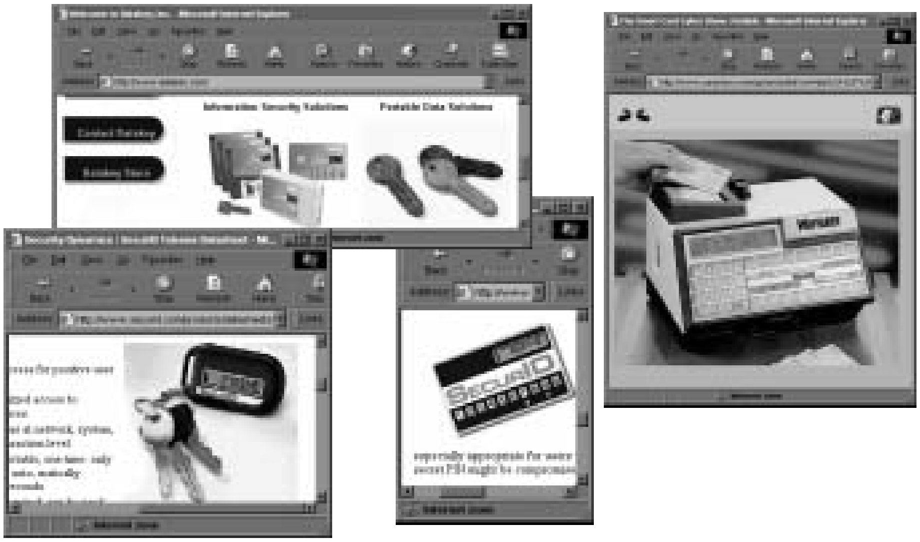
Blinking Vertical Bar
(indicates display of active PASSCODE)

Blinking Dot
(indicates PinPad card is working properly)

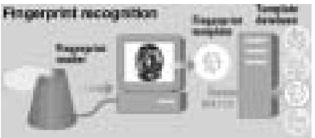
Life remaining for PASSCODE
(each horizontal bar indicates 10 seconds of remaining life)

46

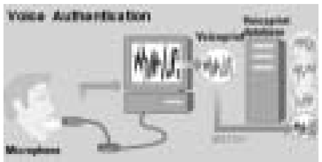
Passwords Plus



Biometrics Solutions



Face Recognition
Face pattern
Face pattern database
Camera



- Face recognition
- Fingerprints
- Voice recognition
- Retinal scans

Pictures from PC magazine

Access Control

Program threats

- Trojan horse
  - Code segment that misuses its environment.
  - Exploits mechanisms for allowing programs written by users to be executed by other users.
  - example already given in fake login process
  - another example--unexpected effects of including “.” early on a Unix path
    - Why . is no longer first on many people's path (e.g., executable file named "ls" in /tmp). If behaves as real ls (but not showing itself) many people will never notice!

Program threats

- Trap doors left by some previously trusted person
  - Doomsday machine scenarios of “trash the system if I am not in the payroll file”
  - Insert special code in system programs that give special privileges to specific users or on specific password
  - But this is easy to detect---how about putting code in the compiler to generate such instructions for any program compiled with the compiler?
    - People rarely compare object to source!
    - Still possible to detect if someone else starts maintaining compiler. But what if we are bootstrapping and the code is in an early version of the compiler but then taken out? Object code retains the functions but source doesn't show them anymore!

51

System threats

- Worms – use spawn mechanism; standalone program.
  - **Internet worm (more later)**
    - **Exploited UNIX networking features (remote access) and bugs in finger and sendmail programs.**
    - **Grappling hook program uploaded main worm program.**
  - **Viruses: fragment of code embedded in a legitimate program; spread into other programs.**

52

Internet worm
(November, 1988)

- Caused by Robert Tappan Morris, Jr.
  - **(His father) Sr. is NSA expert, previously at Bellcore**
- Consisted of a bootstrap and the worm proper
- Bootstrap, 99 lines of C named l1.c, tried to install itself and if successful acquired worm from the machine it came from and started it
- Worm tried to hide its existence, checked to see if it was already running on the machine and in 6/7 cases terminated if so. If not terminated, it tried to (1) break user passwords and (2) spread to other machines

Internet worm

- Primary effect of worm was to occupy most of machines' cycles (1/7 not enough to keep it from taking over). This is main reason why it was noticed.
- Spreading to other machines

  (1) use broken passwords to get to other machines user has accounts on

  (2) attempt to find "trusted hosts" and rsh to them

Internet worm

- Spreading to other machines (continued)

  (3) exploit bug in finger program

  finger / fingerd relationship

  fingerd failed to check for buffer size

  finger a specially crafted 536-byte long string

  on fingerd side, this overflows allocated buffer, overwriting parts of data stack (e.g., return vector)

  fingerd thus caused to returns control to this corrupted area code here attempts to create a shell (execute /bin/sh). If successful then successful penetration of system

Internet worm

- Spreading to other machines (continued)
  - **(4) exploit system administration sloppiness**
    - **sendmail has a "debug" option that is supposed to be disabled if not disabled permits execution of commands**
    - **worm checked to see if destination hosts had debug disabled and took advantage if not**

Threat monitoring

- Two line of defense
  - **Principles of Perimeter Defense: watch your boundaries: firewall and VPN**
  - **Intruder Detection: watch out for intruders**
    - Second line of defense**. Even the best intrusion detection system can fail. Many intruders are insiders.**
    - Ejection**. Catch intruders before they can do much damage.**
    - Deterrent**. Intruders may stay out if they think they'll be caught.**
    - Educational**. Learn how intruders do what they do and use this to improve both prevention and detection techniques.**

57

Threat monitoring

- Check for suspicious patterns of activity – i.e., several incorrect password attempts may signal password guessing.
- Audit log – records the time, user, and type of all accesses to an object; useful for recovery from a violation and developing better security measures.
- Scan the system periodically for security holes; done when the computer is relatively unused.

58

Threat monitoring

- Check for:

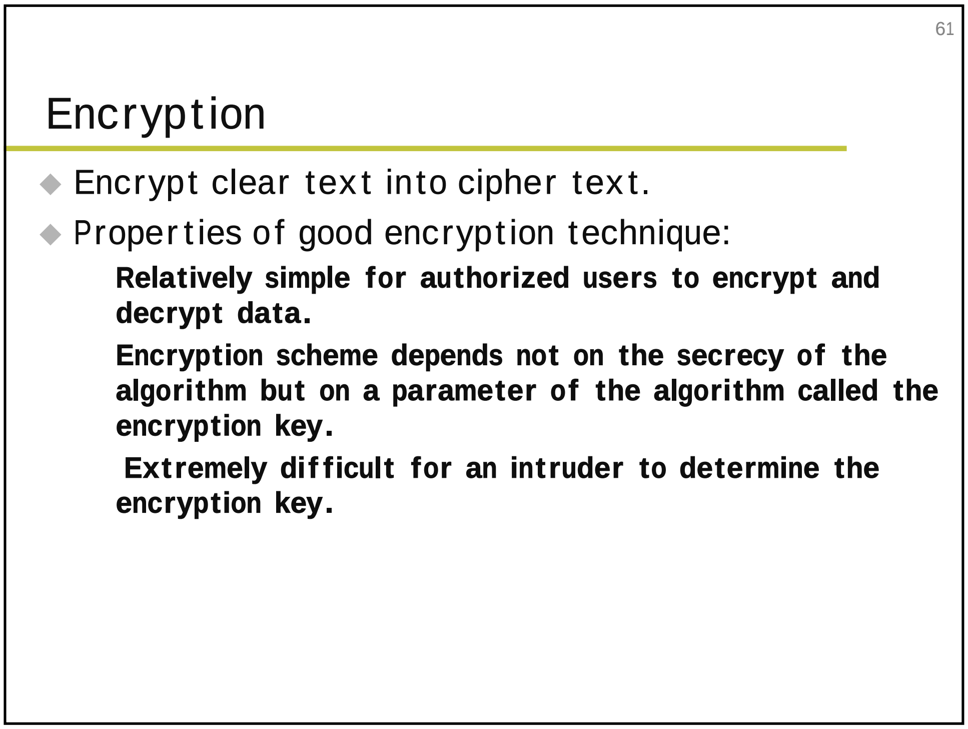
  Short or easy-to-guess passwords
  Unauthorized set-uid programs
  Unauthorized programs in system directories
  Unexpected long-running processes
  Improper directory protections
  Improper protections on system data files
  Dangerous entries in the program search path (Trojan horse)
  Changes to system programs; monitor checksum values

Threat monitoring

- Firewall: separates trusted and untrusted systems

  limits network access between two security domains

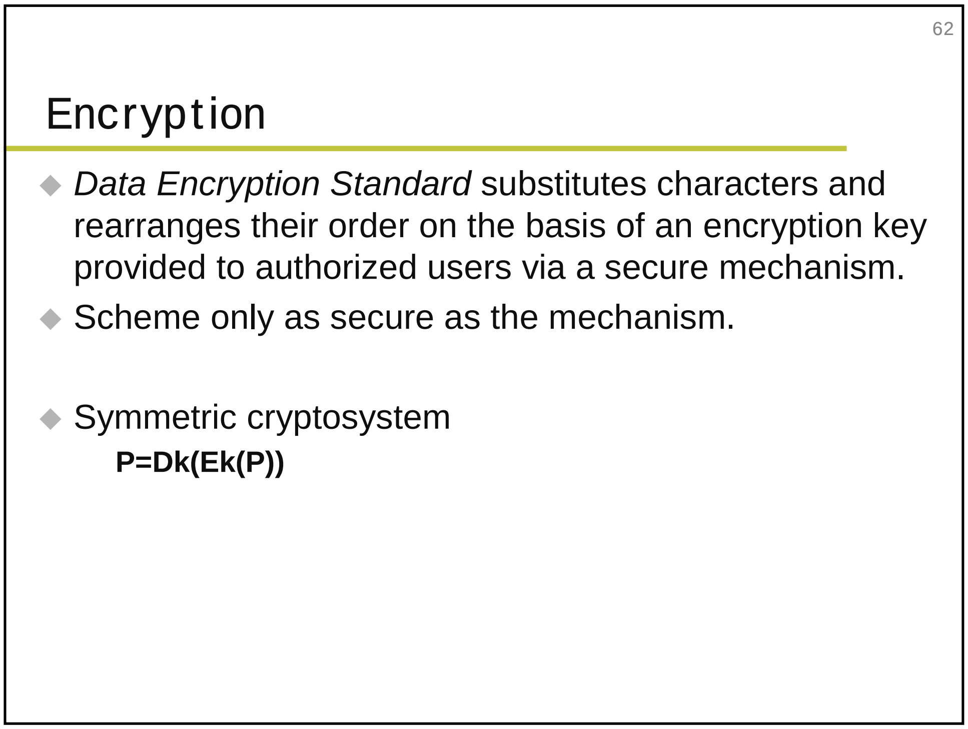
Confidentiality, Integrity, and non-repudiation



61

Encryption

- Encrypt clear text into cipher text.
- Properties of good encryption technique:
  - **Relatively simple for authorized users to encrypt and decrypt data.**
  - **Encryption scheme depends not on the secrecy of the algorithm but on a parameter of the algorithm called the encryption key.**
  - **Extremely difficult for an intruder to determine the encryption key.**



62

Encryption

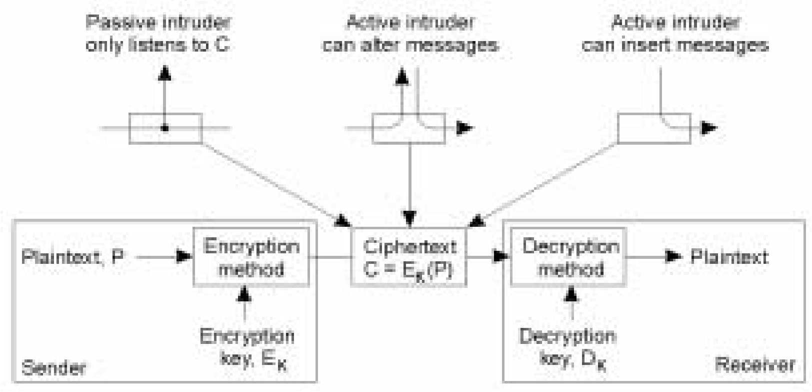
- *Data Encryption Standard* substitutes characters and rearranges their order on the basis of an encryption key provided to authorized users via a secure mechanism.
- Scheme only as secure as the mechanism.
- Symmetric cryptosystem
  - **P=Dk(Ek(P))**

Encryption

- Public-key encryption based on each user having two keys:
  - **public key – published key used to encrypt data.**
  - **private key – key known only to individual user used to decrypt data.**
- Must be an encryption scheme that can be made public without making it easy to figure out the decryption scheme.
  - **Efficient algorithm for testing whether or not a number is prime.**
  - **No efficient algorithm is known for finding the prime factors of a number.**
- Asymmetric Cryptosystem

$P=D_{Kd}(E_{Ke}(P))$

Encryption



Intruders and eavesdroppers in communication.

Hash Function

- h=H(m)

  m: arbitrary length input

  h: fixed length output

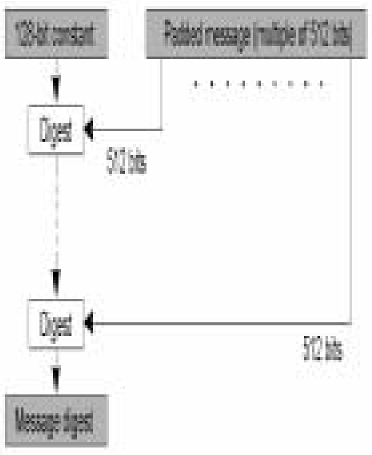
- **One-way function**: It is computationally infeasible to find the input m corresponds to a known output h.

  It is easy to compute h from m.

- **Weak collision resistance**: it is computationally infeasible to find another m’, where H(m)=H(m’), given that m and h are known.
- **Strong collision resistance**: Given H, it is computationally infeasible to find another m’, where H(m)=H(m’).

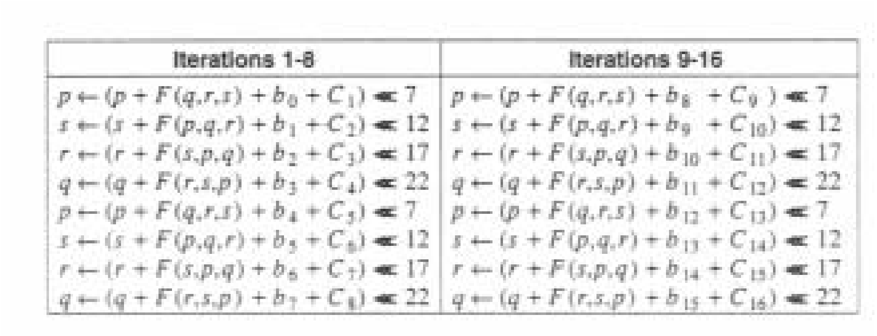
MD5

- A hash function for computing a 128bit fixed length message digest from an arbitrary length binary input string



The structure of MD5

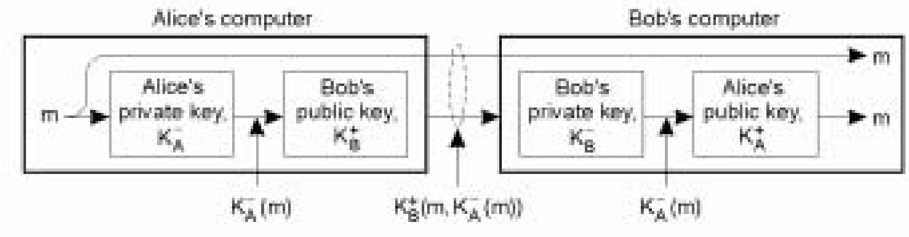
MD5



Iterations 1-8	Iterations 9-16
$p \leftarrow (p + F(q,r,s) + b_0 + C_1) \lll 7$	$p \leftarrow (p + F(q,r,s) + b_8 + C_9) \lll 7$
$s \leftarrow (s + F(p,q,r) + b_1 + C_2) \lll 12$	$s \leftarrow (s + F(p,q,r) + b_9 + C_{10}) \lll 12$
$r \leftarrow (r + F(s,p,q) + b_2 + C_3) \lll 17$	$r \leftarrow (r + F(s,p,q) + b_{10} + C_{11}) \lll 17$
$q \leftarrow (q + F(r,s,p) + b_3 + C_4) \lll 22$	$q \leftarrow (q + F(r,s,p) + b_{11} + C_{12}) \lll 22$
$p \leftarrow (p + F(q,r,s) + b_4 + C_5) \lll 7$	$p \leftarrow (p + F(q,r,s) + b_{12} + C_{13}) \lll 7$
$s \leftarrow (s + F(p,q,r) + b_5 + C_6) \lll 12$	$s \leftarrow (s + F(p,q,r) + b_{13} + C_{14}) \lll 12$
$r \leftarrow (r + F(s,p,q) + b_6 + C_7) \lll 17$	$r \leftarrow (r + F(s,p,q) + b_{14} + C_{15}) \lll 17$
$q \leftarrow (q + F(r,s,p) + b_7 + C_8) \lll 22$	$q \leftarrow (q + F(r,s,p) + b_{15} + C_{16}) \lll 22$

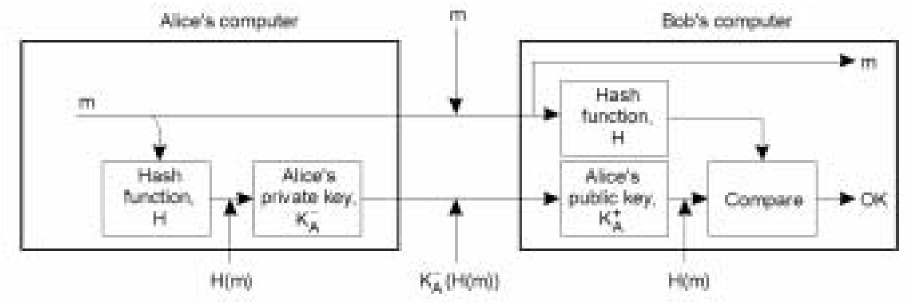
The 16 iterations during the first round in a phase in MD5.

Digital Signatures

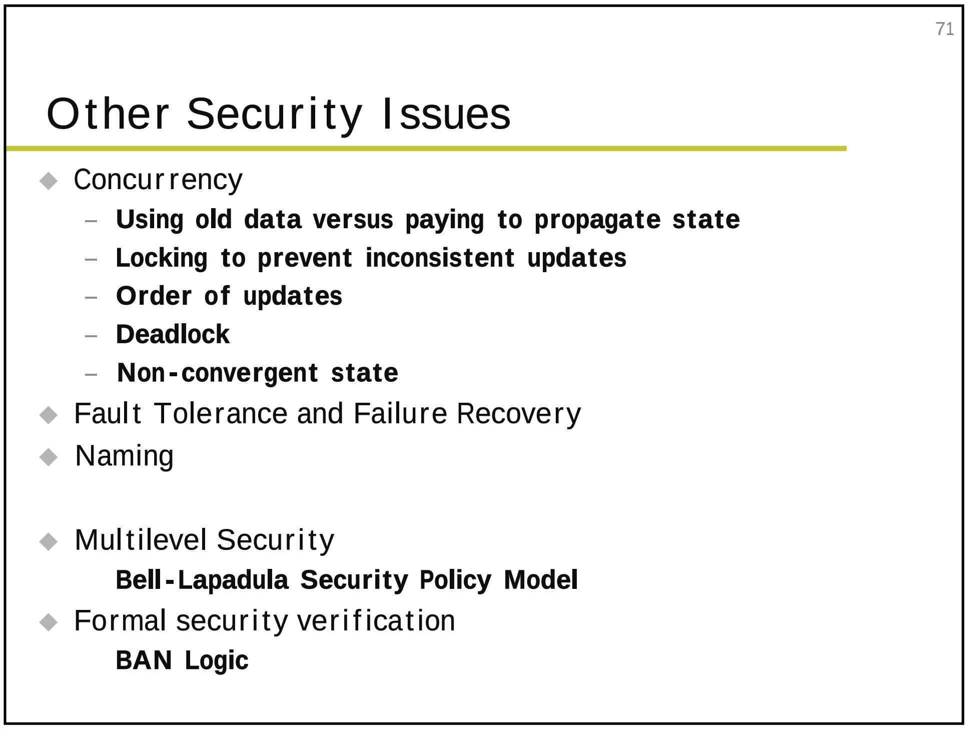

Alice's computer
Bob's computer
m
Alice's private key, K_A^-
Bob's public key, K_B^+
Bob's private key, K_B^-
Alice's public key, K_A^+
m
m
$K_A^-(m)$
$K_B^+(m, K_A^-(m))$
$K_A^-(m)$

- Digital signing a message using public-key cryptography.

Digital Signatures



Digitally signing a message using a message digest.



Other Security Issues

- Concurrency
  - **Using old data versus paying to propagate state**
  - **Locking to prevent inconsistent updates**
  - **Order of updates**
  - **Deadlock**
  - **Non-convergent state**
- Fault Tolerance and Failure Recovery
- Naming

- Multilevel Security

  Bell-Lapadula Security Policy Model
- Formal security verification

  BAN Logic