

Protection and Security

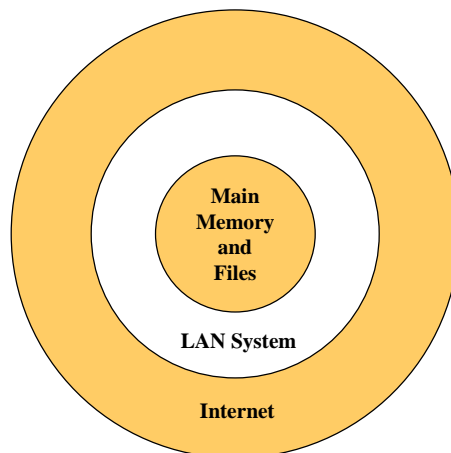


CS 502
Spring 99
WPI MetroWest/Southboro Campus

Three Circles of Computer Security



- Inner Circle – Memory, CPU, and File protection.
- Middle Circle – Security Perimeter. Authentication and authorization.
- Outer Circle – The network; interaction with the computer from the outside.



Protection and Security Outline



- Protection
 - Goals of Protection
 - Domain of Protection
 - Access Matrix
 - Implementation of Access Matrix
 - Revocation of Access Rights
 - Capability-Based Systems
 - Language-Based Protection
- Security
 - The Security Problem
 - Authentication
 - Program Threats
 - System Threats
 - Threat Monitoring
 - Encryption

3/26/99

2

Protection Goals



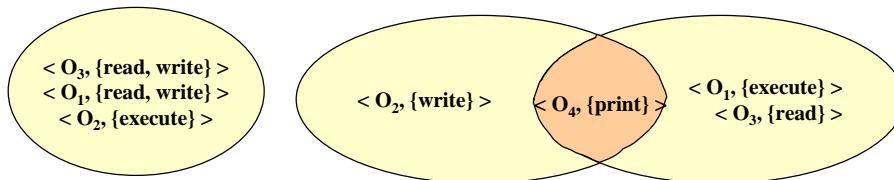
- Operating system consists of a collection of objects, hardware or software.
- Each object has a unique name and can be accessed through a well-defined set of operations.
- Protection problem – ensure that each object is accessed correctly and only by those processes that are allowed to do so.

3/26/99

3

Domain Structure

- Access-right = $\langle \text{object-name, rights-set} \rangle$
Rights-set is a subset of all valid operations that can be performed on the object.
- Domain = set of access-rights



3/26/99

4

Domain Implementation

- System consists of 2 domains:
 - User
 - Supervisor
- UNIX
 - Domain = user-id
 - Domain switch accomplished via file system.
 - Each file has associated with it a domain bit (setuid bit).
 - When file is executed and setuid = on, then user-id is set to owner of the file being executed. When execution completes user-id is reset.

3/26/99

5

Protection of Memory

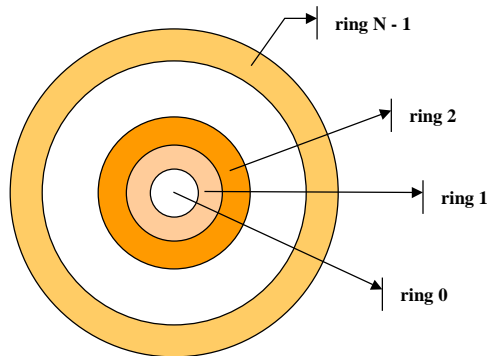
- Security
- Ensure correct function of various processes that are active

3/26/99

6

Multics Rings

- Let D_i and D_j be any two domain rings.
- If $j < i \Rightarrow D_i \subseteq D_j$.



3/26/99

7

Access Matrix

- Rows – domains
- Columns – domains + objects
- Each entry – Access rights; Operator names

Domain	Object			
	F ₁	F ₂	F ₃	Printer
D ₁	Read		Read	
D ₂				Print
D ₃		Read	Execute	
D ₄	Read Write		Read Write	

3/26/99

8


Use of Access Matrix

- If a process in Domain D_i tries to do “op” on object O_j , then “op” must be in the access matrix.
- Can be expanded to dynamic protection.
 - Operations to add, delete access rights.
 - Special access rights:
 - owner of O_i
 - copy op from O_i to O_j
 - control – D_i can modify D_j ’s access rights
 - transfer – switch from domain D_i to D_j

3/26/99

9

Domain Switching




Domain	F ₁	F ₂	F ₃	Printer	D ₁	D ₂	D ₃	D ₄
D ₁	Read		Read			Switch		
D ₂				Print			Switch	Switch
D ₃		Read	Execute					
D ₄	Read Write		Read Write		Switch			

3/26/99

10

Use of Access Matrix (Cont.)

- 
- Access matrix design separates mechanism from policy.
 - Mechanism
 - Operating system provides Access-matrix + rules.
 - It ensures that the matrix is only manipulated by authorized agents and that rules are strictly enforced.
 - Policy
 - User dictates policy.
 - Who can access what object and in what mode.

3/26/99

11

Implementation of Access Matrix

- Each column = Access-control list for one object
Defines who can perform what operation.
 - Domain 1 = Read,Write
 - Domain 2 = Read
 - Domain 3 = Read
 - ...
- Each Row = Capability List (like a key)
For each domain, what operations allowed on what objects.
 - Object 1 – Read
 - Object 4 – Read,Write,Execute
 - Object 5 – Read,Write,Delete,Copy

3/26/99

12

Revocation of Access Rights

- Access List – Delete access rights from access list.
 - Simple
 - Immediate
- Capability List – Scheme required to locate capability in the system before capability can be revoked.
 - Reacquisition
 - Back-pointers
 - Indirection
 - Keys

3/26/99

13

Capability-Based Systems



- Hydra
 - Fixed set of access rights known to and interpreted by the system.
 - Interpretation of user-defined rights performed solely by user's program; system provides access protection for the use of these rights.
- Cambridge CAP System
 - *Data capability* – provides standard read, write, execute of individual storage segments associated with object.
 - *Software capability* – interpretation left to the subsystem, through its protected procedures.

3/26/99

14

Language-Based Protection



- Specification of protection in a programming language allows the high-level description of policies for the allocation and use of resources.
- Language implementation can provide software for protection enforcement when automatic hardware-supported checking is unavailable.
- Interpret protection specifications to generate calls on whatever protection system is provided by the hardware and the operating system.

3/26/99

15

The Security Problem

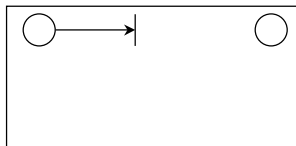
- Security must consider external environment of the system, and protect it from:
 - unauthorized access.
 - malicious modification or destruction.
 - accidental introduction of inconsistency.
- Easier to protect against accidental than malicious misuse.

3/26/99

16

Types of Threats

- **Interruption**
 - an asset of the system is destroyed or becomes unavailable or unusable
 - destruction of hardware
 - cutting of a communication line
 - disabling the file management system



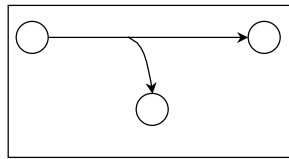
3/26/99

17

Types of Threats

- **Interception**

- an unauthorized party gains access to an asset
- wiretapping to capture data in a network
- illicit copying of files or programs



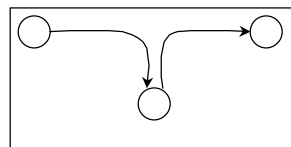
3/26/99

18

Types of Threats

- **Modification**

- an unauthorized party not only gains access but tampers with an asset
- changing values in a data file
- altering a program so that it performs differently
- modifying the content of messages being transmitted in a network

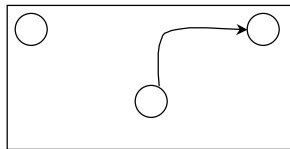


3/26/99

19

Types of Threats

- Fabrication
 - an unauthorized party inserts counterfeit objects into the system
 - insertion of spurious messages in a network
 - addition of records to a file



3/26/99

20

Computer System Assets

- Hardware
 - threats include accidental and deliberate damage
- Software
 - threats include deletion, alteration, damage
 - backups of the most recent versions can maintain high availability

3/26/99

21

Computer System Assets



- Data
 - involves files
 - threats include unauthorized reading of data
 - statistical analysis can lead to determination of individual information which threatens privacy

3/26/99

22

Computer System Assets



- Communication Lines and Networks
 - threats include eavesdropping and monitoring
 - a telephone conversation, an electronic mail message, and a transferred file are subject to these threats
 - encryption masks the contents of what is transferred so even if obtained by someone, they would be unable to extract information

3/26/99

23

Computer System Assets

- **Communication Lines and Networks**
 - masquerade takes place when one entity pretends to be a different entity
 - message stream modification means that some portion of a legitimate message is altered, delayed, or reordered
 - denial of service prevents or inhibits the normal use or management of communications facilities
 - disable network or overload it with messages

3/26/99

24

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.
 - Log all invalid access attempts.

3/26/99

25

Techniques for Learning Passwords

- Try default password used with standard accounts shipped with computer
- Exhaustively try all short passwords
- Try words in dictionary or a list of likely passwords
- Collect information about users and use these items as passwords

3/26/99

26

Techniques for Learning Passwords

- Try user's phone numbers, social security numbers, and room numbers
- Try license plate numbers
- Use a Trojan horse to bypass restrictions on access
- Tap the line between a remote user and the host system

3/26/99

27

ID Provides Security

- Determines whether the user is authorized to gain access to a system
- Determines the privileges accorded to the user
 - guest or anonymous accounts have more limited privileges than others
- ID is used for discretionary access control
 - a user may grant permission to files to others by ID

3/26/99

28

Password Selection Strategies

- Computer generated passwords
 - users have difficulty remembering them
 - need to write it down
 - have history of poor acceptance
- Eliminate guessable passwords while allowing the user to select a password that is memorable

3/26/99

29

Password Selection Strategies



- Reactive password checking strategy
 - system periodically runs its own password cracker to find guessable passwords
 - system cancels passwords that are guessed and notifies user
 - consumes resources to do this
 - hacker can use this on their own machine with a copy of the password file

3/26/99

30

Password Selection Strategies

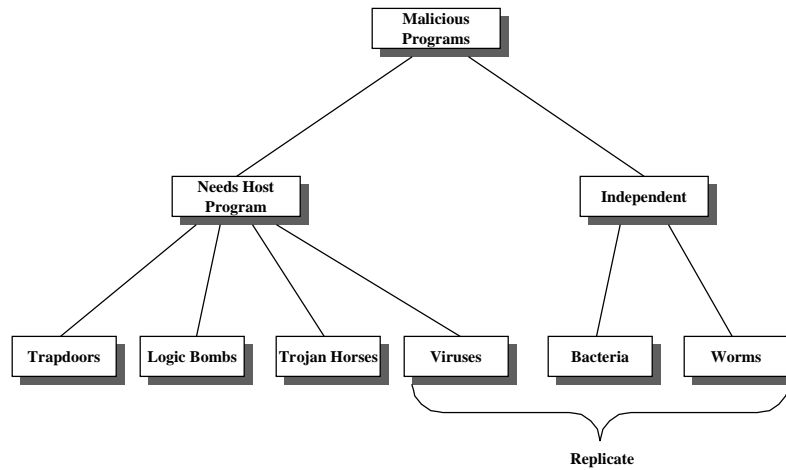


- Proactive password checker
 - the system checks at the time of selection if the password is allowable
 - with guidance from the system users can select memorable passwords that are difficult to guess

3/26/99

31

Taxonomy of Malicious Programs



3/26/99

32

Program Threats

- Trojan Horse
 - Code segment that misuses its environment.
 - Exploits mechanisms for allowing programs written by users to be executed by other users.
- Trap Door
 - Specific user identifier or password that circumvents normal security procedures.
 - Could be included in a compiler.

3/26/99

33

System Threats

- Worms – use spawn mechanism; standalone program.
- Internet worm
 - 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.
 - Mainly effect microcomputer systems.
 - Downloading viral programs from public bulletin boards or exchanging floppy disks containing an infection.
 - *Safe computing.*

3/26/99

34

Threat Monitoring and Detection

- Assume the behavior of the intruder differs from the legitimate user
- Statistical anomaly detection
 - collect data related to the behavior of legitimate users over a period of time
 - statistical tests are used to determine if the behavior is not legitimate behavior
 - attempt to define normal, or expected behavior
- Rule-based detection
 - rules are developed to detect deviation form previous usage pattern
 - expert system searches for suspicious behavior
 - attempt to define proper behavior

3/26/99

35

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.

3/26/99

36

Threat Monitoring (Cont.)



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

3/26/99

37

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.
- *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.

3/26/99

38

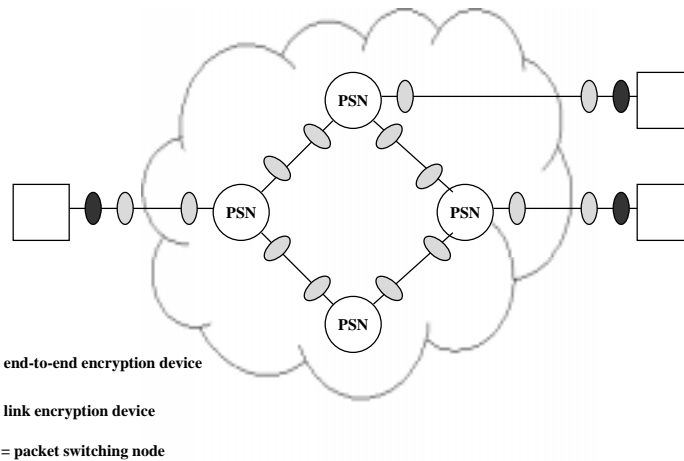
Encryption (Cont.)

- 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.

3/26/99

39

Encryption Across a Packet-Switching Network



3/26/99

40

Key Distribution

- Deliver a key to two parties that wish to exchange data
 - no else is allowed to see the key
- Key could be selected by A and physically delivered to B
- A third party could physically deliver the keys
- Encrypt a new key from the old key and transmit the new key
- A third party could deliver a key on encrypted links

3/26/99

41

Keys

- Session key
 - all user data are encrypted with a one-time session key
- Permanent key
 - used between two entities for the purpose of distributing session keys

3/26/99

42

Windows NT Security

- Access Control Scheme
 - name/password
 - access token associated with each process object indicating privileges associated with a user
 - security descriptor
 - access control list
 - used to compare with access control list for object

3/26/99

43

Access Token



Security ID (SID)
Group SIDs
Privileges
Default Owner
Default ACL

3/26/99

44

Security Descriptor

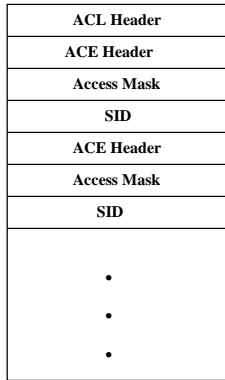


Flags
Owner
System Access Control List (SACL)
Discretionary Access Control List (DACL)

3/26/99

45

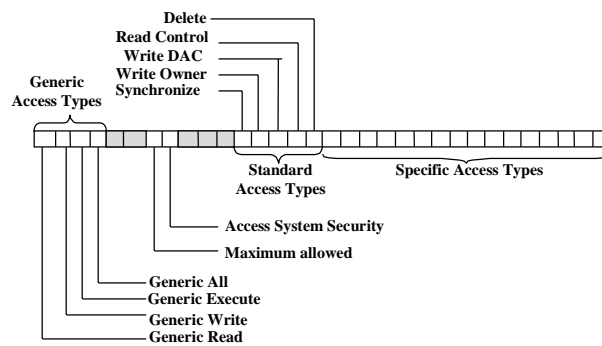
Access Control List



3/26/99

46

Access Mask



3/26/99

47

History

- Memory Protection Hardware (1960)
- File Access Controls
 - CTSS, CMAS 1962
- One-way functions to protect passwords (1967)
- Multics Security Kernel (1968)
- ARPANET (1969–1989); Internet (1977+)
- Unix–Unix System Mail (UUCP); mail trap doors (1975)
- Public key cryptography (1976)
- Vulnerability Study of Passwords
 - Morris and Thompson 1978
- RSA public-key cryptosystem (1978)

3/26/99

48

History (Cont.)

- Electronic cash (Chaum 1978)
- Domain Naming System of the Internet (1983)
- Computer Viruses “Formal Problem” (Cohen 1984)
- Novel Password Schemes (1985)
 - Callback
 - Challenge-response
 - One-time password
- Distributed Authentication (Kerberos 1988)
- Internet Worm (1988)
- PEM (1989); PGM (1989)
 - Privacy Enhanced Electronic Mail

3/26/99

49

History (Cont.)

- Wily hacker attack (Stoll 1988)
- Network sniffing; Packet Spoofing; firewalls; (1993)
- Java Security Problems (1996+)