This Week's News

- Platform for lab 4
- Lab 3 back tomorrow
- Exam
  17 June, 9:30 am
- Workload survey

System Security

Comp 305 Lecture 11

Some Definitions

- Security
  - Protection against external events
- Reliability
  - Ability to handle internal errors
- Availability
  - Measure of how often a system is available

Security Threats

Asset	*Availability*	*Secrecy*	*Integrity*
Hardware	Equipment is stolen or disabled, denying service		
Software	Programs are deleted, denying access	An unauthorised copy of software is made	A working program is modified, either to fail or to do some unintended task
Data	Files are deleted, denying access	An unauthorised read of data is performed; an analysis of statistical data reveals underlying information	Existing files are modified or new files are fabricated
Communication Lines	Messages are destroyed or deleted; communication lines or networks are rendered unavailable	Messages are read; the traffic pattern of messages is observed	Messages are modified, delayed, reordered, or duplicated; false messages are fabricated

Security Issues

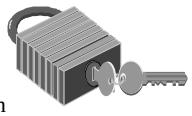
- Policy v Mechanism
  - Who, from Where, When and to What
- Physical Security
- Operational Security
- System Security

System Security

- Authentication
- Access Control
- Information Flow Control
- Data Transmission Security

Authentication

- Problems with passwords
  - They are private
  - They get written down
  - Short ones are easily broken
  - Easy to remember means easy to guess
  - Stored in the machine



Trapdoor Encryption

- Store only encrypted password:

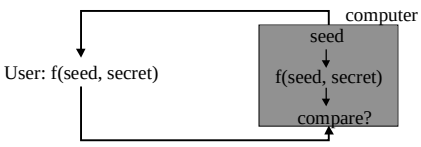
f(P) = DES(*const*, password.*salt*)

Translation Table Sizes

Password length	*26 lowercase letters*	*36 lowercase letters and digits*	*62 alphanumeric characters*	*95 printable characters*
1	1	1.4	2.4	3.7
2	26	50	148	347
3	676	1.8k	9.2k	33k
4	17.6k	64.6k	568k	3.1M
5	0.5M	2.33M	35.2M	289M
6	11.9M	83.7M	2.18(	28.3(

Algorithmic Passwords

- Challenge - Response
- One-time passwords
- Shared secret



The Login Process

- Always read both username and password
- Always encrypt password
- Slow down the process
- Disable after 3 failures

Access Matrix Model

- Domain:
  - User, site, program, time of day

	Objects			
	file A	file B	device-12	process X
domain 1	e	e		
domain 2	re	e		stop
domain 3	rwed	re		

Example Problem

- Information in **F** is to be available to any user through program **P** at company site **S** during normal hours **T**.
- Information in **F** is to be available to any boss, **B**, at site **S**, through program **P** at any time of day.
- Information in **F** is updated by a program **Q** which runs continually during normal hours.
- Maintenance of **F** is done by the sys admin, **A**, and must be done at site **S**.

Example Access Matrix

	F	*P*	*Q*	*D*$_5$
D$_1$ (A,*,S,*)				
D$_2$ (*,*,S,T)		exec		switch
D$_3$ (B,*,S,*)				
D$_4$ (*,Q,*,T)				
D$_5$ (*,P,S,*)	read	exec		

Information in **F** is to be available to any user through program **P** at company site **S** during normal hours **T**.

Example Access Matrix

	F	*P*	*Q*	*D*$_5$
D$_1$ (A,*,S,*)				
D$_2$ (*,*,S,T)		exec		switch
D$_3$ (B,*,S,*)		exec		switch
D$_4$ (*,Q,*,T)				
D$_5$ (*,P,S,*)	read	exec		

Information in **F** is to be available to any boss, **B**, at site **S**, through program **P** at any time of day.

Example Access Matrix

	F	*P*	*Q*	*D*$_5$
D$_1$ (A,*,S,*)				
D$_2$ (*,*,S,T)		exec		switch
D$_3$ (B,*,S,*)		exec		switch
D$_4$ (*,Q,*,T)	write		exec	
D$_5$ (*,P,S,*)	read	exec		

Information in **F** is updated by a program **Q** which runs continually during normal hours.

Example Access Matrix

	F	*P*	*Q*	*D*$_5$
D$_1$ (A,*,S,*)	all			
D$_2$ (*,*,S,T)		exec		switch
D$_3$ (B,*,S,*)		exec		switch
D$_4$ (*,Q,*,T)	write		exec	
D$_5$ (*,P,S,*)	read	exec		

Maintenance of **F** is done by the sys admin, **A**, and must be done at site **S**.

Implementations

- Access List

  File A:

domain – 1	e
domain – 2	re
domain – 3	rwed

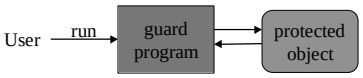
- Capability

  Domain - 2:

file A	file B	process X
re	e	stop

Dynamic Protection Structures

	Objects				
	file A	file B	process X	domain 1	domain 2
domain 1		e			switch
domain 2	r	e	stop		
domain 3	r*w	re			
domain 4	owner	e		switch	



Protection in Primary Memory