

System Security

The Joy of Tech by Nitroze & Snaggy

© 2000: Geek Culture™
joyoftech.com

COMP 6370 – Lecture 4 – System Security

The Security Environment

Threats

Goal	Threat
Data confidentiality	Exposure of data
Data integrity	Tampering with data
System availability	Denial of service

Security goals and threats

COMP 6370 – Lecture 4 – System Security

Intruders

Common Categories

1. Casual prying by nontechnical users
2. Snooping by insiders
3. Determined attempt to make money
4. Commercial or military espionage

Example: (be careful with this site!!!!)

<http://tools.rosinstrument.com>

COMP 6370 – Lecture 4 – System Security

Accidental Data Loss

Common Causes

1. Acts of God
 - fires, floods, wars
2. Hardware or software errors
 - CPU malfunction, bad disk, program bugs
3. Human errors
 - data entry, wrong tape mounted

COMP 6370 – Lecture 4 – System Security

Security Design Principles (Gollmann)

1. In a given application, should the protection mechanisms focus on data, operations or users?
2. In which layer of the computer system should a security mechanism be placed?
3. Do you prefer simplicity – and higher assurance – to a feature rich security environment?
4. Should the tasks of defining and enforcing security be given to a central entity or should they be left to individual components in a system?
5. How can you prevent an attacker from getting access to a layer below the protection mechanism?

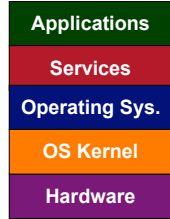
COMP 6370 – Lecture 4 – System Security

Should the protection mechanisms focus on data, operations or users?

COMP 6370 – Lecture 4 – System Security

Which layer should a security mechanism be placed?

- Users run application programs
- Application programs use services such as a DBMS or an ORB
- Applications and services run on top of an OS
- The OS has a kernel that handles every access to the hardware
- The hardware physically stores and manipulates the data in the system



Layers of an IT System



COMP 6370 – Lecture 4 – System Security



Simplicity – and higher assurance – or a feature rich security environment?

- A simple generic mechanism will badly match specific protection requirements, but to choose the right options in a feature-rich security environment users have to be security experts.
- Security-unaware users are definitely in a no-win situation.
- According to Gollmann – fundamental dilemma of computer security.



Human Oriented

Specific
Complex
Focus on users

Generic
Simple
Focus on data



Machine Oriented

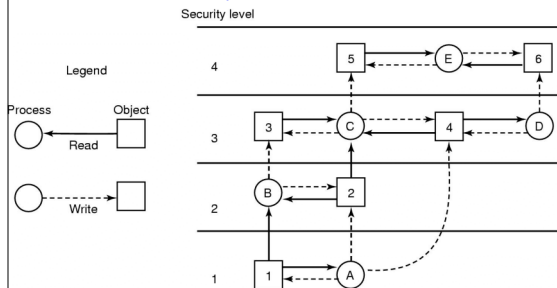


COMP 6370 – Lecture 4 – System Security



Centralized vs Decentralized Security

- Example: Bell-LaPadula model
 - Processes can write up and read down



COMP 6370 – Lecture 4 – System Security



Preventing an attacker from accessing a layer below the protection mechanism

- Every protection mechanism defines a security perimeter (boundary)
- An attacker with access to the layer “below” is in a position to subvert protection mechanisms further up.
- Examples
 - Recovery tools
 - UNIX devices
 - poor access definitions
 - Object reuse (memory release)
 - context switch/stale memory
 - Backup
 - Core Dumps



COMP 6370 – Lecture 4 – System Security



User Authentication

Basic Principles. Authentication must identify:

1. Something the user knows
2. Something the user has
3. Something the user is

This is done before user can use the system



COMP 6370 – Lecture 4 – System Security



Authentication Using Passwords

LOGIN: ken
PASSWORD: FooBar
SUCCESSFUL LOGIN

(a)

LOGIN: carol
INVALID LOGIN NAME
LOGIN:

(b)

LOGIN: carol
PASSWORD: Idunno
INVALID LOGIN
LOGIN:

(c)

- (a) A successful login
(b) Login rejected after name entered
(c) Login rejected after name and password typed



COMP 6370 – Lecture 4 – System Security



Authentication Using Passwords

```
LBL> telnet elxsi
ELXSI AT LBL
LOGIN: root
PASSWORD: root
INCORRECT PASSWORD, TRY AGAIN
LOGIN: guest
PASSWORD: guest
INCORRECT PASSWORD, TRY AGAIN
LOGIN: uuucp
PASSWORD: uuucp
WELCOME TO THE ELXSI COMPUTER AT LBL
```

- How a cracker broke into LBL
 - a U.S. Dept. of Energy research lab



COMP 6370 – Lecture 4 – System Security



13

Authentication Using Passwords

Bobbie, 4238, e(Dog4238)
Tony, 2918, e(6%%TaeFF2918)
Laura, 6902, e(Shakespeare6902)
Mark, 1694, e(XaB@Bwcz1694)
Deborah, 1092, e(LordByron,1092)

Salt Password

The use of salt to defeat precomputation of encrypted passwords



COMP 6370 – Lecture 4 – System Security



14

Passwords

- Length
 - case
 - digit/special character
 - no nouns/words
- One-time passwords
- Challenge-Response



COMP 6370 – Lecture 4 – System Security



15

Password Length – How Much is Enough? guess rate, password lifetime, and password space

- L = maximum lifetime that a password can be used to log into the system.
- P = probability that a password can be guessed within its lifetime, assuming continuous guesses for this period.
- R = number of guesses per unit of time that it is possible to make.
- S = password space, i.e., the total number of unique passwords that the password generation algorithm can generate.
- Considering only the cases where S is greater than L x R and therefore P is less than 1, the relationship between these parameters is expressed by the equation: $P = (L \times R) / S$



COMP 6370 – Lecture 4 – System Security



16

State of the Art – Circa 1985

Maximum Lifetime (months)	26 Character Alphabet	36 Character alpha-numeric Alphabet
6	9	8
12	9	8



COMP 6370 – Lecture 4 – System Security



17

Password Guidance – The Green Book

- DOD Password Management Guideline, 12 Apr 85
- Password Vulnerabilities
 1. a password must be initially assigned to a user when enrolled on the ADP system;
 2. a user's password must be changed periodically;
 3. the ADP system must maintain a "password database";
 4. users must remember their passwords; and
 5. users must enter their passwords into the ADP system at authentication time.
- Green Book Guidelines
 - Users should be able to change their own passwords.
 - Passwords should be machine-generated rather than user-created.
 - Certain audit reports (e.g., date and time of last login) should be provided by the system directly to the user.



COMP 6370 – Lecture 4 – System Security



18

Protecting Passwords – Green Book

- Use of Access Control Mechanisms
- Use of Encryption
- Transmission
- Login Attempt Rate
- Audit Trails
- Real-time Notification to System Personnel
 - Recommended 5 or more unsuccessful attempts
- Notification to the User
 - Upon successful login, the user should be notified of:
 - The date and time of user's last login;
 - The location of the user (as can best be determined) at login; and
 - Each unsuccessful login attempt to this user ID since the last successful login.



COMP 6370 – Lecture 4 – System Security



19

Intrusion Techniques (passwords)

- Techniques for guessing passwords:
 - Try default passwords.
 - Try all short words, 1 to 3 characters long.
 - Try all the words in an electronic dictionary(60,000).
 - Collect information about the user's hobbies, family names, birthday, etc.
 - Try user's phone number, social security number, street address, etc.
 - Try all license plate numbers (MUP103).
 - Use a Trojan horse
 - Tap the line between a remote user and the host system.

Prevention: Enforce good password selection (lJ4Gf4Se%l#) – Stallings' recommendation!

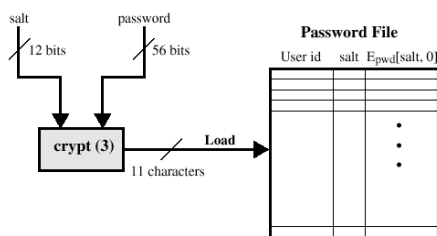


COMP 6370 – Lecture 4 – System Security



20

UNIX Password Scheme



Loading a new password

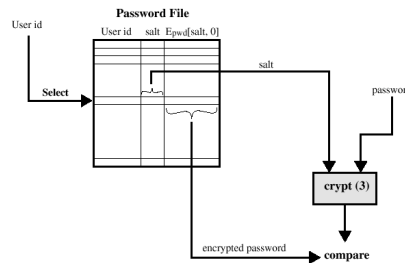


COMP 6370 – Lecture 4 – System Security



21

UNIX Password Scheme



Verifying a password file



COMP 6370 – Lecture 4 – System Security



22

Storing UNIX Passwords

- UNIX passwords were kept in in a publicly readable file, etc/passwords.
- Now they are kept in a “shadow” directory and only visible by “root.”
- The salt serves three purposes:
 - Prevents duplicate passwords.
 - Effectively increases the length of the password.
 - Prevents the use of hardware implementations of DES
 - Salt is an n-bit random number



COMP 6370 – Lecture 4 – System Security



23

Password Selecting Strategies

- User education
- Computer-generated passwords
- Reactive password checking
- Proactive password checking




COMP 6370 – Lecture 4 – System Security





24

Passwords in Obscure OSs

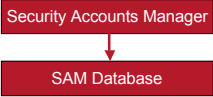


(c) Fidgen 2001


COMP 6370 – Lecture 4 – System Security


Windows 2000 Passwords

- **LM**
 - an encrypted, fixed, hex no.
- **NT Password Hash**
 - 3 rounds of MD4 hashing algorithm





Security Accounts Manager
↓
SAM Database

User Mode Security Subsystem

Kernel Mode Security Ref. Monitor



1. Checks user and program permissions before allowing access to objects
2. Defines how audit settings translate into the actual capture of events by the Event Log

1. 2 password entries for each account.
2. Format:
ID:LM representation :NT Hash


COMP 6370 – Lecture 4 – System Security


LM (LanManager) Password Representation


1. Adjust password length to 14 characters by either truncation or padding.
2. Divide string into 2 parts, add one bit of parity to each part.
 - Parity required for using DES
 - Each part used as a key for DES encryption of a hexadecimal number
 - Splitting the string into two parts allows an attacker to attack each half independently
- **LM representation is neither a hash nor an encrypted password, it is an encrypted, fixed hex number in which the password is used as the key.**


COMP 6370 – Lecture 4 – System Security


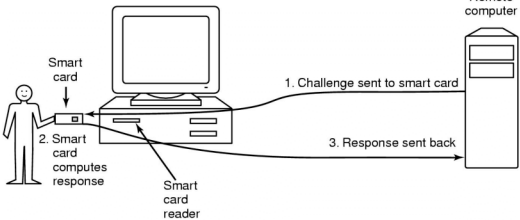
NT Password Representation

1. Adjust password length to 14 characters
2. Use MD-4 hashing algorithm three times to produce a hash of the password.



- NT Password is not salted
- NT password cracking programs only need to access a dictionary.


COMP 6370 – Lecture 4 – System Security

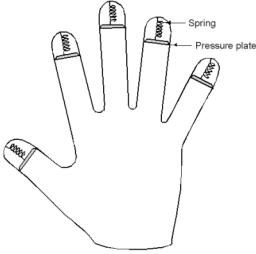

Authentication Using a Physical Object





- **Magnetic cards**
 - magnetic stripe cards
 - chip cards: stored value cards, smart cards


COMP 6370 – Lecture 4 – System Security


Authentication Using Biometrics



A device for measuring finger length.


COMP 6370 – Lecture 4 – System Security


Countermeasures

- Limiting times when someone can log in
- Automatic callback at number prespecified
 - taps
- Limited number of login tries
- A database of all logins
- Simple login name/password as a trap
 - security personnel notified when attacker bites

