Chapter 9

Intruders

Outline

- Intruders
  - Intrusion Techniques
  - Password Protection
  - Password Selection Strategies
  - Intrusion Detection
    - Statistical detection
    - Rule-Based detection
- Summary

Intruders

- Three classes of intruders (hackers or crackers):
  - Masquerader: no account but to have an account
  - Misfeasor: try to access unauthorized resources (a legitimate user)
  - Clandestine user: take a root account or control without any evidence.

Intrusion Techniques

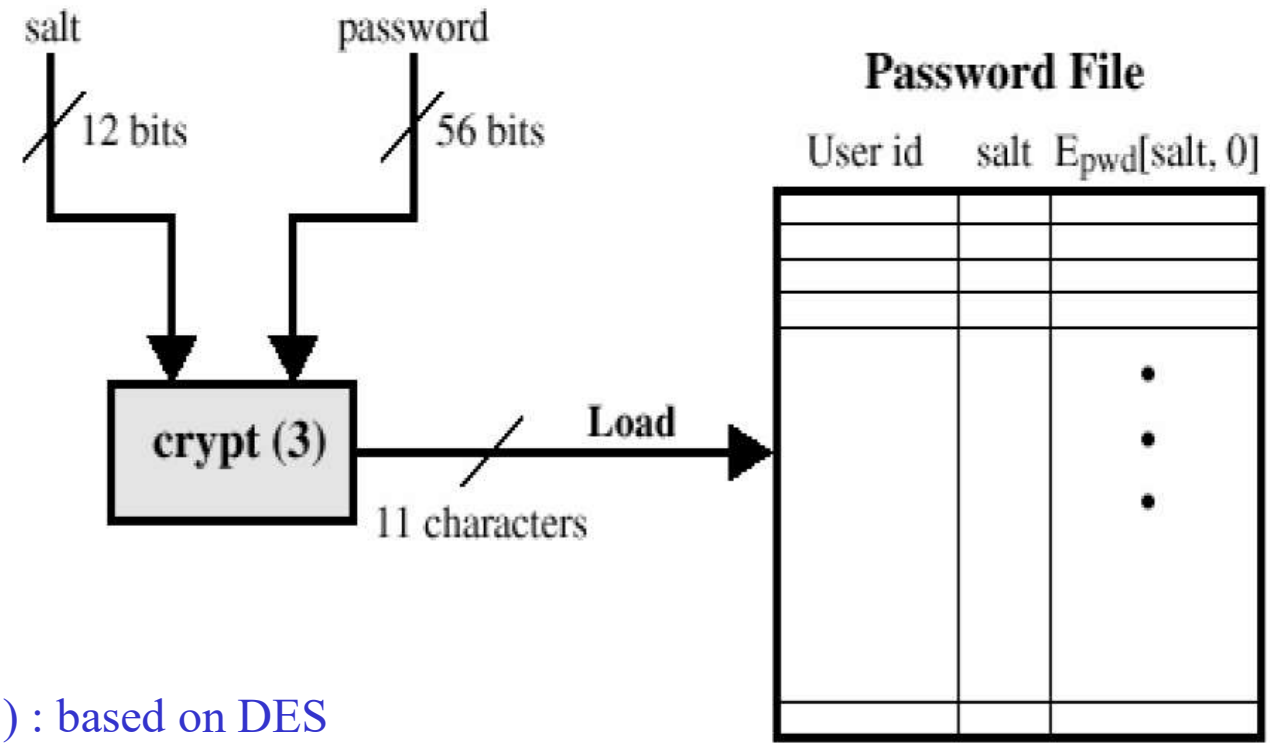
- System maintains a file that associates a password with each authorized user.
- Password file can be protected with:
  - One-way encryption: performing one-way transformation (not reversable)
  - Access Control : limitation to password file

Intrusion Techniques

- 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.
  - Use a Trojan horse
  - Tap the line between a remote user and the host system.

Prevention: Enforce good password selection (Ij4Gf4Se%f#)

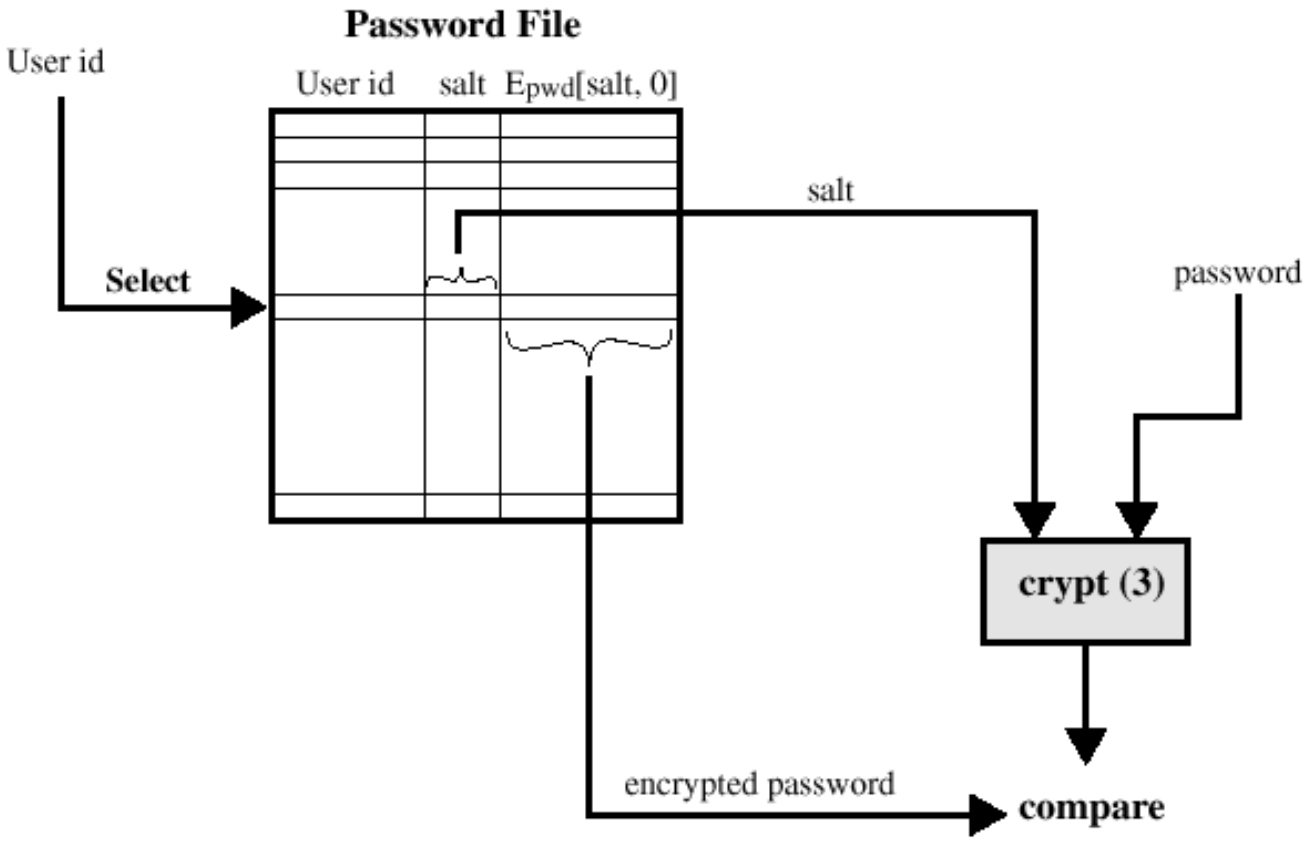
UNIX Password Scheme I



crypt(3) : based on DES

Loading a new password

UNIX Password Scheme II



Verifying a password file

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”.

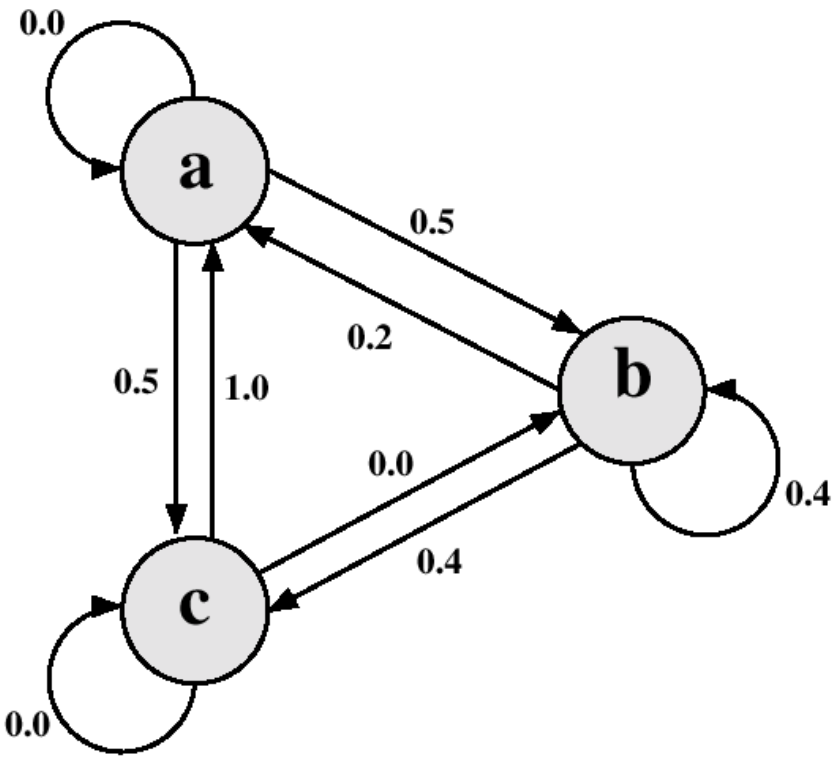
"Salt"

- Salt is a "value" related with the time pw assigned
- The salt serves three purposes:
  - Prevents duplicate passwords.
  - Effectively increases the length of the password.
  - Prevents the use of hardware implementations of DES

Password Selecting Strategies

- User education
- Computer-generated passwords;
- Reactive password checking: cracker estimates and notify to change
- Proactive password checking: user selection but system test if allowable

Markov Model



M = {3, {a, b, c} , T, 1 } where

$$T = \begin{bmatrix} 0.0 & 0.5 & 0.5 \\ 0.2 & 0.4 & 0.4 \\ 1.0 & 0.0 & 0.0 \end{bmatrix}$$

e.g., string probably from this language: abbcacaba

e.g., string probably not from this language: aacccbaaa

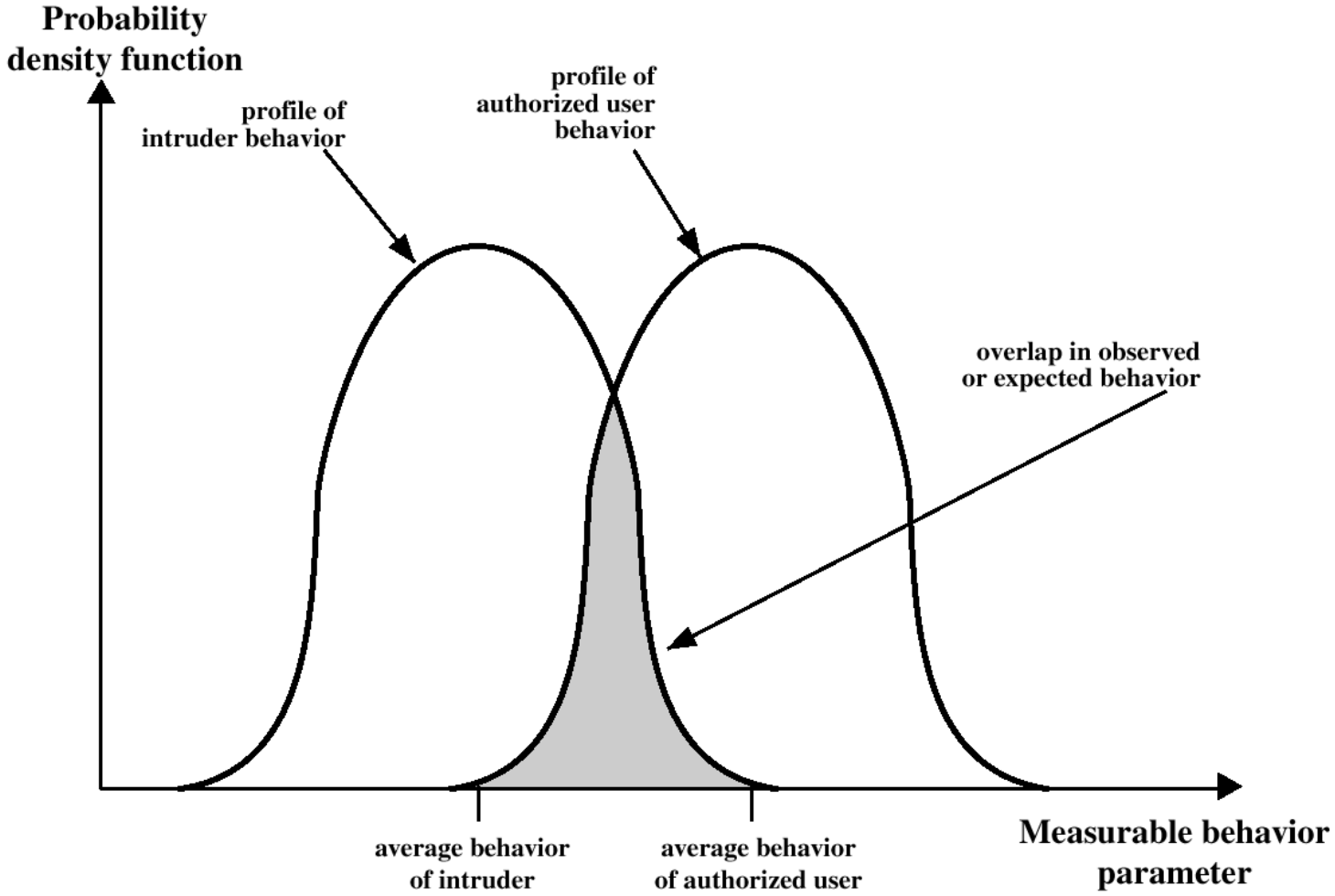
The Stages of a Network Intrusion

1. Scan the network to:
   - locate which IP addresses are in use,
   - what operating system is in use,
   - what TCP or UDP ports are “open” (being listened to by Servers).
2. Run “Exploit” scripts against open ports
3. Get access to Shell program which is “suid” (has “root” privileges).
4. Download from Hacker Web site special versions of systems files that will let Cracker have free access in the future without his cpu time or disk storage space being noticed by auditing programs.
5. Use IRC (Internet Relay Chat) to invite friends to the feast.

Intusion Detection

- The intruder can be identified and ejected from the system.
- An effective intrusion detection can prevent intrusions.
- Intrusion detection enables the collection of information about intrusion techniques that can be used to strengthen the intrusion prevention facility.

Profiles of Behavior of Intruders and Authorized Users(1)



Profiles of Behavior of Intruders and Authorized Users (2)

- False Positive : authorized users identified as intruders
- False Negative : intruders not identified as intruders

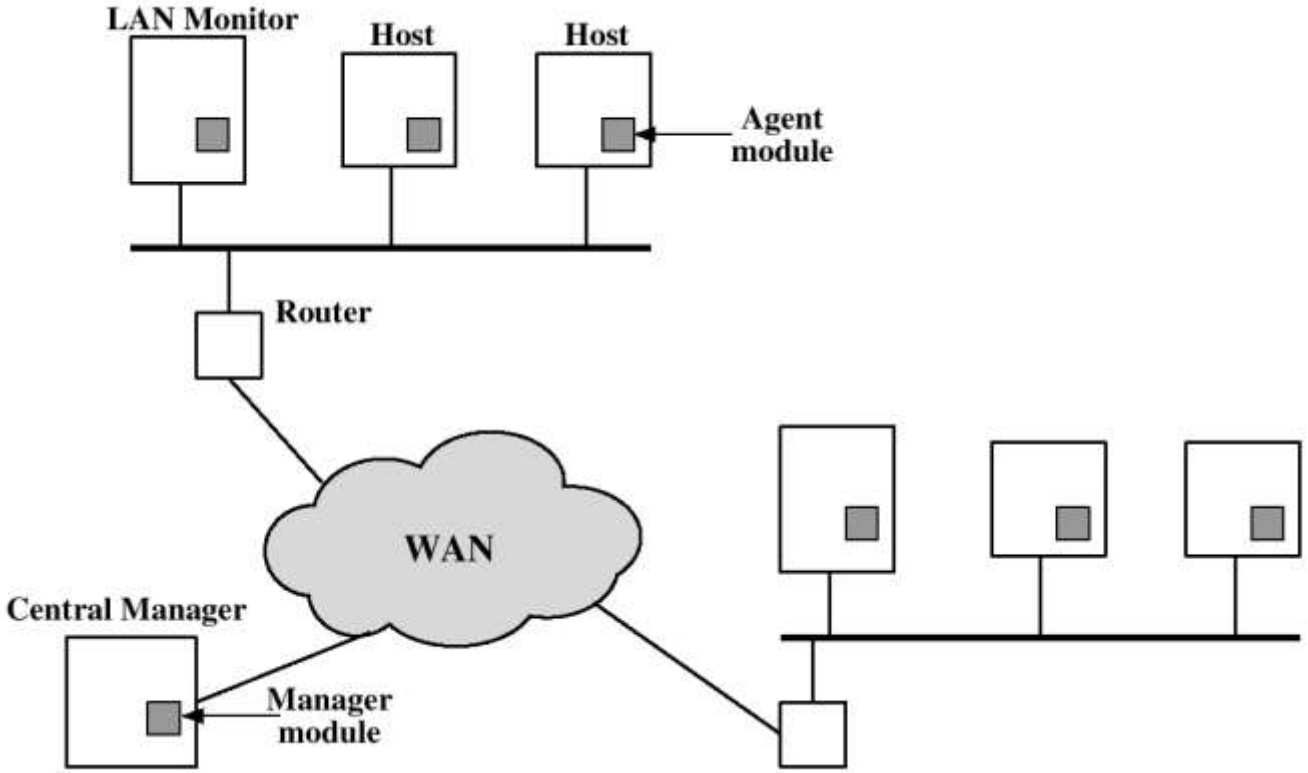
Intrusion Detection

- Statistical anomaly detection
  - Threshold detection: # of events
  - Profile based: keep user's activity
    - Counter
    - Gauge
    - Interval timer
    - Resource utilization
  - Detection: Mean/STD, TIME series, Markov process
- Rule based detection
  - Anomaly detection: different from previous pattern
  - Penetration identidication: expert system detecting abnormal use

Measures used for Intrusion Detection

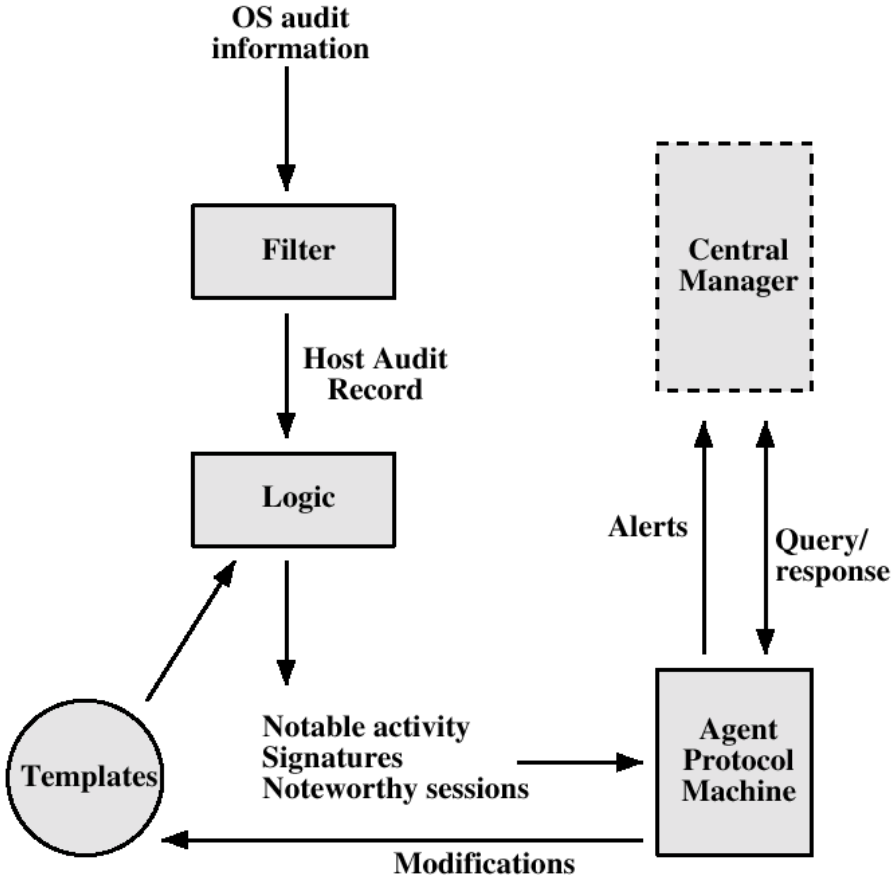
- Login frequency by day and time.
- Frequency of login at different locations.
- Time since last login.
- Password failures at login.
- Execution frequency.
- Execution denials.
- Read, write, create, delete frequency.
- Failure count for read, write, create and delete.

Distributed Intrusion Detection



Developed at University of California at Davis

Distributed Intrusion Detection



Agent Architecture

Honeypots

- Decoy system (유인 시스템)
  - Divert an attacker from accessing critical systems
  - Collect information about the attacker's activity
  - Make the attacker stay on the system

Summary

- Unauthorized intrusion into a computer system or network is one of the most serious threat to computer security
- IDSs have been developed to provide early warning of an intrusion
- Intrusion detection involves detecting unusual pattern of activity
- One important element of intrusion is password management