Network Security

Asim Rasheed

Where we are …

- Introduction to network security
- Vulnerabilities in IP
- I. CRYPTOGRAPHY
  - Symmetric Encryption and Message Confidentiality
  - Public-Key Cryptography and Message Authentication
- II. NETWORK SECURITY APPLICATIONS
  - Authentication Applications (Kerberos, X.509)
  - Electronic Mail Security (PGP, S/MIME)
  - IP Security (IPSec, AH, ESP, IKE)
  - Web Security (SSL, TLS, SET)
- III. SYSTEM SECURITY
  - Intruders and intrusion detection
  - Malicious Software (viruses)
  - Firewalls and trusted systems

Intruders

Intruders

- Significant security problem for networked systems is hostile or unwanted access
- Cyber attacks still on rise
- Threat of cyber-terrorism, more coordinated
- Even sensitive installations not well secured, regular break-ins
- Can happen either through a network or locally
- Varying levels of competence for intruders

Classes of Intruders

- Masquerader:
  - An individual who is not authorized to use the computer and penetrates a system’s access control to exploit a legitimate user’s account
  - Likely to be an outsider
- Misfeasor:
  - A legitimate user who accesses data, programs, resources for which he is not authorized
  - Misuses his privileges
  - Generally an insider

Classes of Intruders….

- Clandestine user:
  - An individual who seizes supervisory control of system and uses his control to evade auditing and access control or to suppress audit collection
  - Either an insider or outsider

Intruders

- Intruders attack range from benign to the serious
  - Benign intruders:
    - users who simply wish to explore internets and see what is out there
    - Tolerable, but they consume resources and effect performance of legitimate users
    - May use compromised system to launch other attacks
  - Serious intruders:
    - Individuals who are attempting to read privileged data or disrupt the system
- Clearly a growing publicized problem

Intrusion

- Definition :
  - An intrusion is an action or set of actions aimed at compromising the confidentiality, integrity or availability of a service or system
- Principal defense categories:
  - Prevention
  - Detection
  - Response

Intrusion Techniques

- Aim to increase privileges on system
- Basic attack methodology
  - Target acquisition and information gathering
  - Initial access
  - Privilege escalation
  - Covering tracks
- Key goal often is to acquire passwords
- So then exercise access rights of owner

Intrusion Techniques

- System maintains a file that associates a password with each user
- Two ways to protect this file
    - One way encryption
    - Access control
- If these counter measures are in place then some effort is needed to learn passwords
- Different password guessing techniques have been observed

Password Guessing

- One of the most common attacks
- Attacker knows a login (from email/web page etc)
- Then attempts to guess password for it
  - Try default passwords shipped with systems
  - Try all short passwords
  - Then try by searching system's online dictionaries of common words
  - Intelligent searches try passwords associated with the user (variations on names, birthday, phone, common words/interests)

Password Guessing …

- Check by login attempt or against stolen password file
- Success depends on password chosen by user
- Surveys show many users choose passwords poorly

Password Capture

- Another attack involves password capture
  - Watching over shoulder as password is entered
  - Using a Trojan horse program
  - Monitoring an insecure network login (e.g., telnet, FTP, web, email)
  - Extracting recorded info after successful login (web history/cache, last number dialed, etc.)
- Users need to be educated to use suitable precautions/countermeasures

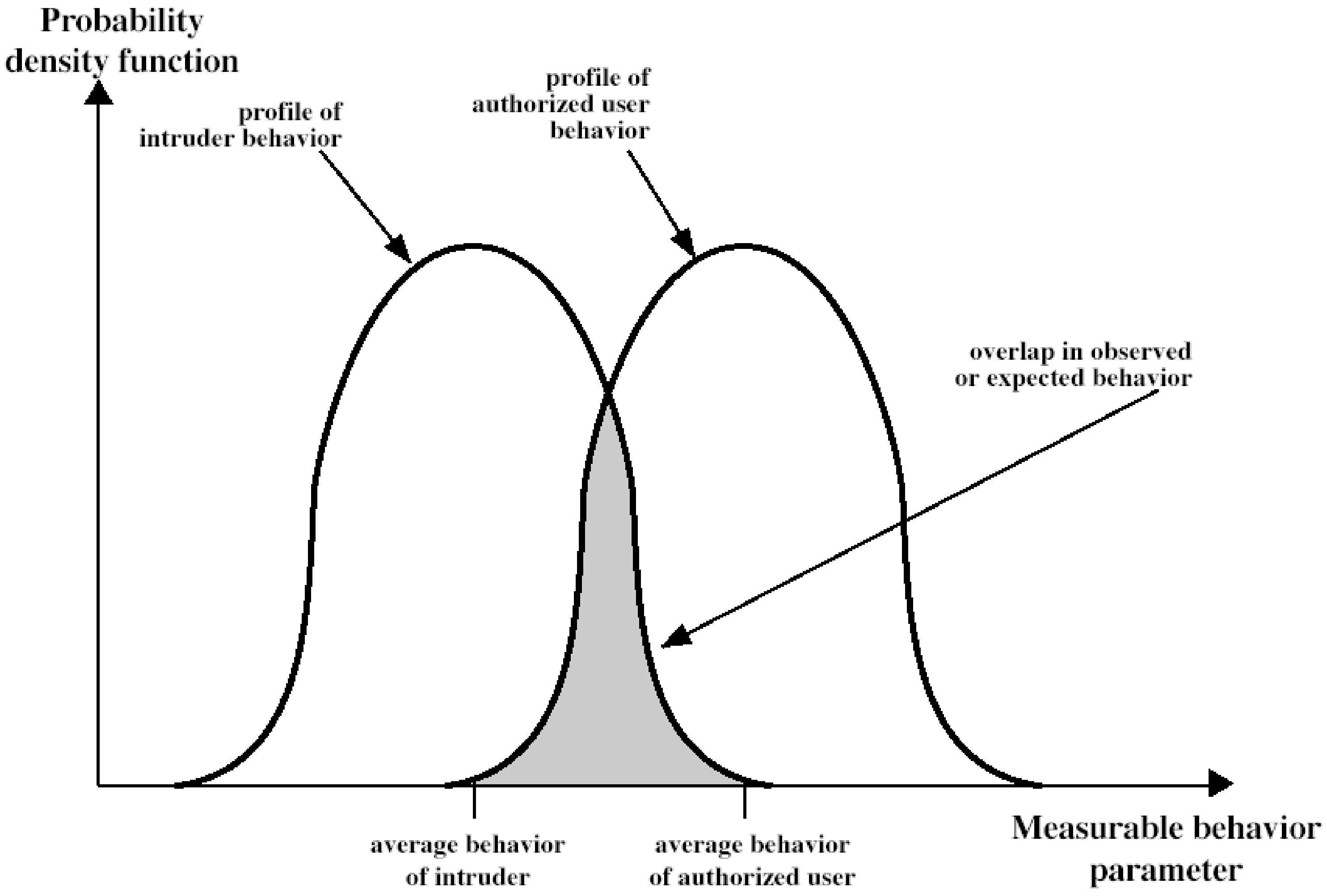
Why is prevention not sufficient?

- Because it is too expensive to prevent all potential attack techniques
- Because legitimate users get annoyed by too many preventive measures and may even start to circumvent them (introducing new vulnerabilities)
- Because preventive measures may fail:
  - Incomplete or erroneous specification / implementation / configuration
  - Inadequate deployment by users (just think of passwords…)

Intrusion Detection

- Inevitably the best intrusion prevention will have security failures
- Need also to detect intrusions so that:
  - If intrusion is detected quickly, can be blocked
  - Act as deterrent
  - Collect info to improve security
- Assumption: Intruder will behave differently from a legitimate user
  - But will have imperfect distinction between the two

Behavior of Intruders & Authorized Users


Probability density function
profile of intruder behavior
profile of authorized user behavior
overlap in observed or expected behavior
average behavior of intruder
average behavior of authorized user
Measurable behavior parameter

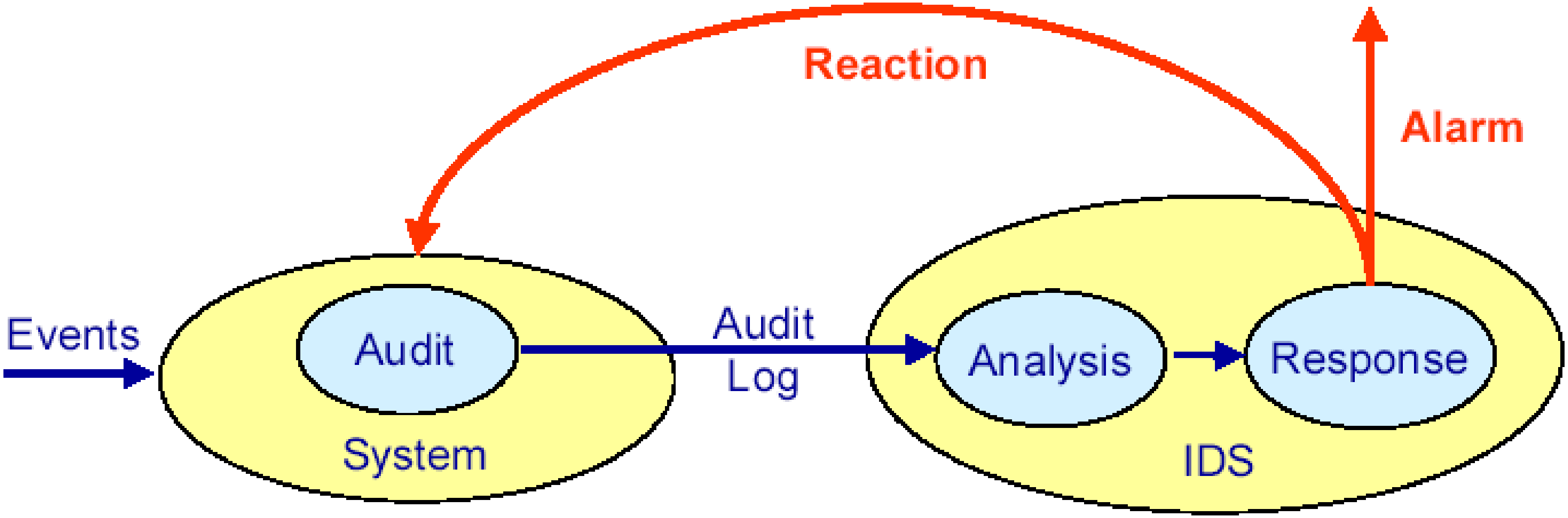
Intrusion Detection Systems

- Overall goal:
  - Supervision of computer systems and communication infrastructures in order to detect intrusions and misuse
- What can be attained with intrusion detection?
  - Detection of attacks and attackers
  - Detection of system misuse (includes misuse by legitimate users)
  - Damage limitation (if response mechanisms exist)
  - Gain of experience in order to improve preventive measures
  - Deterrence of potential attackers

Classification of IDS

- Host-based: Analysis of system events
- Network-based: Analysis of exchanged information (IP packets)
- Hybrid: Combined analysis of system events and network traffic

Schematic Overview of IDS



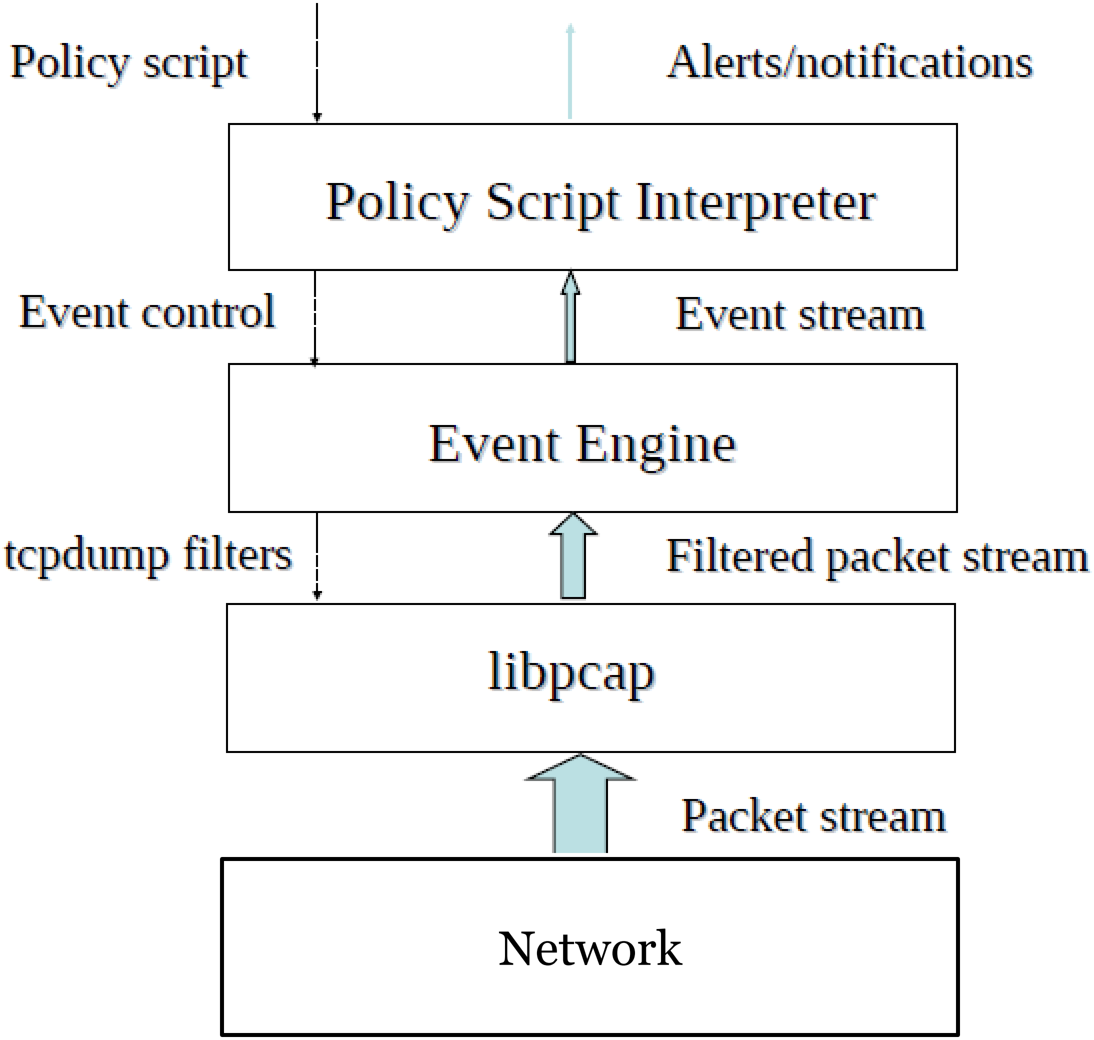
Host-Based IDS

- Using OS auditing mechanisms
  - e.g., BSM on Solaris: logs all direct or indirect events generated by a user
  - *strace for system calls made by a program*
- Monitoring user activities
  - e.g., Analyze shell commands
- Monitoring executions of system programs
  - e.g., Analyze system calls made by *sendmail*

Network IDS

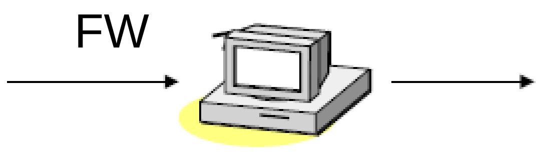
- Deploying sensors at strategic locations
  - E.G., Packet sniffing via *tcpdump at routers*
- Inspecting network traffic
  - Watch for violations of protocols and unusual connection patterns
- Monitoring user activities
  - Look into the data portions of the packets for malicious command sequences
- May be easily defeated by encryption
  - Data portions and some header information can be encrypted

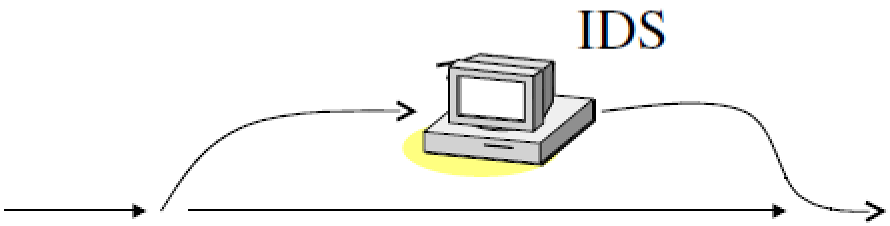
Architecture of Network IDS



Firewall Versus Network IDS

- Firewall
  - Active filtering
  - Fail-close
- Network IDS
  - Passive monitoring
  - Fail-open





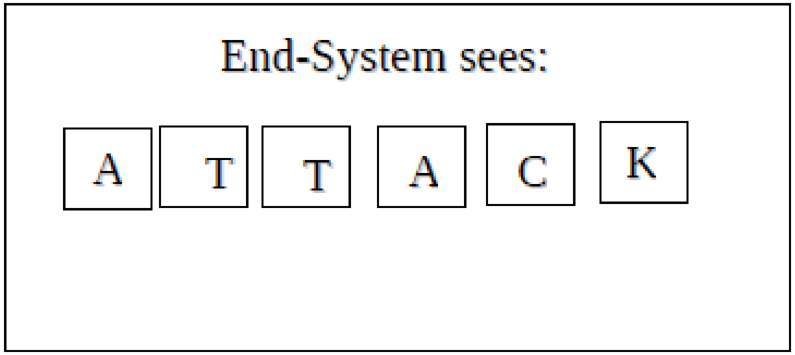
Requirements of Network IDS

- High-speed, large volume monitoring
  - No packet filter drops
- Real-time notification
- Mechanism separate from policy
- Extensible
- Broad detection coverage
- Economy in resource usage
- Resilience to stress
- Resilience to attacks upon the IDS itself!

Eluding Network IDS

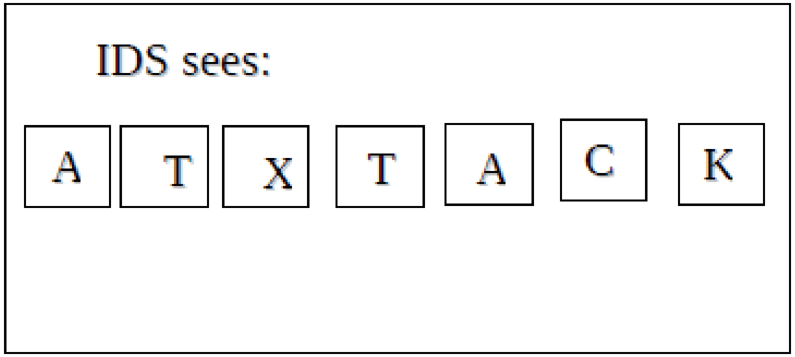
- What the IDS sees may not be what the end system gets.
  - Insertion and evasion attacks.
- IDS needs to perform full reassembly of packets.
  - But there are still ambiguities in protocols and operating systems:
    - E.G. TTL, fragments.
    - Need to “normalize” the packets

Insertion Attack



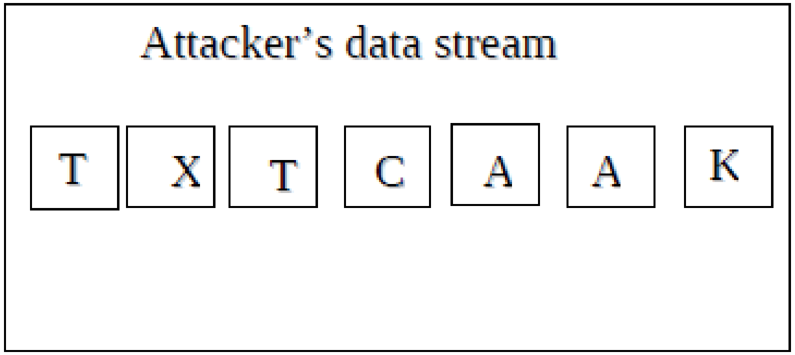
End-System sees:

A T T A C K



IDS sees:

A T X T A C K

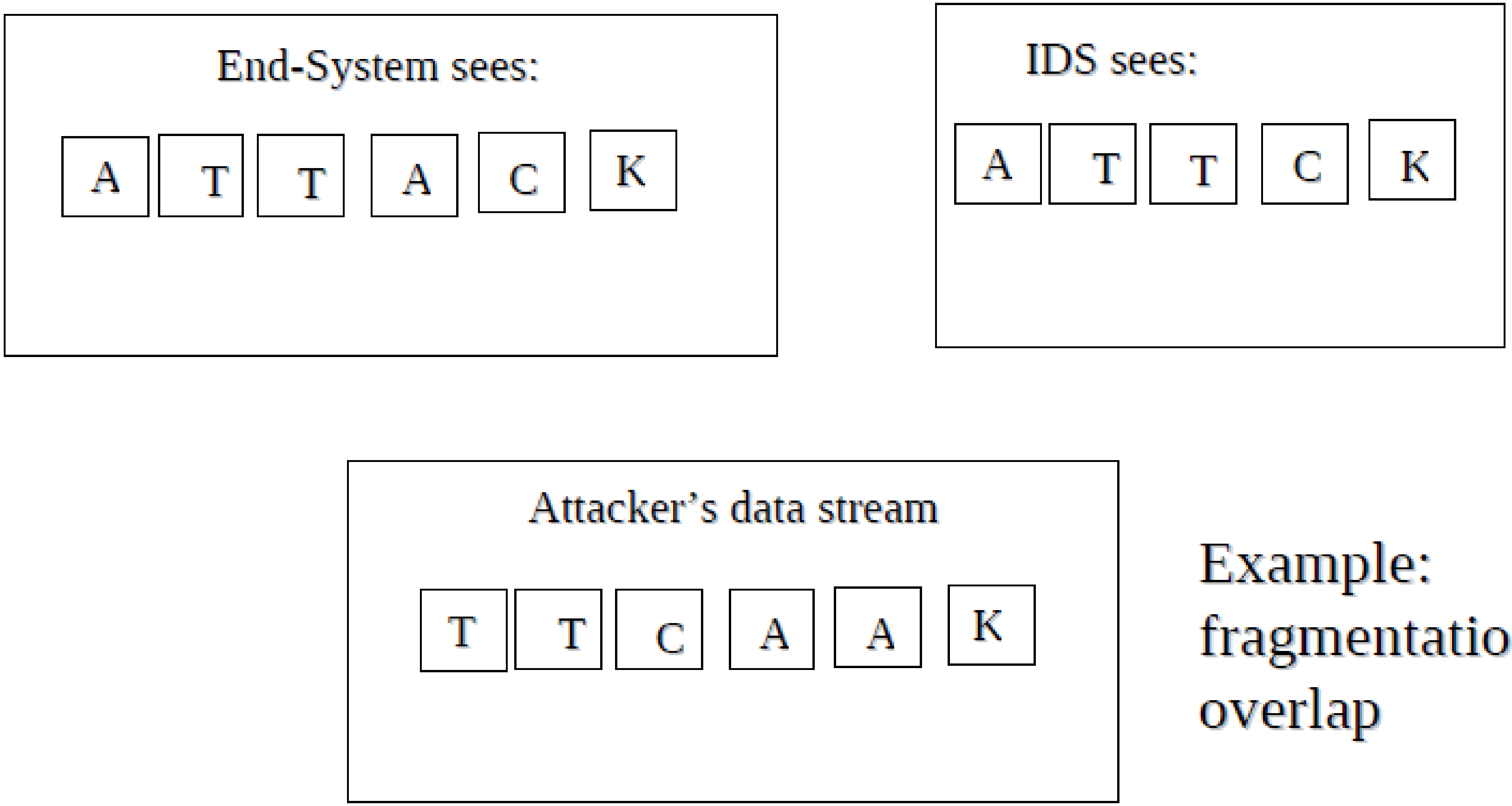


Attacker's data stream

T X T C A A K

Examples: bad checksum, TTL.

Evasion Attack



End-System sees:

A T T A C K

IDS sees:

A T T C K

Attacker's data stream

T T C A A K

Example: fragmentation overlap

Approaches to Intrusion Detection

- Statistical Anomaly Detection: Involves collection of data relating to the behavior of legitimate user over a period.
    - Threshold
    - Profile based
- Rule-based detection: Involves an attempt to define a set of rules that can be used to detect an intruder
    - Anomaly
    - Penetration identification

Audit Records

- Fundamental tool for intrusion detection
- Native audit records
  - ▫ Part of all common multi-user O/S
  - ▫ Already present for use
  - ▫ May not have info wanted in desired form
- Detection-specific audit records
  - ▫ Created specifically to collect wanted info
  - ▫ At cost of additional overhead on system

Audit Record Fields

- Each audit records contains following fields
  - Subject:
    - A terminal user but can also be a process acting on behalf of users
  - Action:
    - Operation performed by the subject on or within an object e.g., login, read, execute, etc.
  - Object:
    - Receptors of action e.g., files, programs, messages, etc.

Audit Record Fields…

- Exception-condition:
  - Denotes which exception condition is raised on return
- Resource-usage:
  - List of quantitative elements in which each element gives the amount used of some resources
- Time-stamp:
  - Identifying when the action took place

Statistical Anomaly Detection

- Threshold detection
  - Count occurrences of specific event over time
  - If exceed reasonable value assume intrusion
  - Alone is a crude & ineffective detector
- Profile based
  - Characterize past behavior of users
  - Detect significant deviations from this
  - Profile usually multi-parameter

Audit Record Analysis

- Foundation of statistical approaches
- Analyze records to get metrics over time
  - Counter, gauge, interval timer, resource use
- Use various tests on these to determine if current behavior is acceptable
  - Mean & standard deviation, multivariate, markov process, time series, operational
- Key advantage is no prior knowledge used

Rule-Based Intrusion Detection

- Observe events on system & apply rules to decide if activity is suspicious or not
- Rule-based anomaly detection
    - Analyze historical audit records to identify usage patterns & auto-generate rules for them
    - Then observe current behavior & match against rules to see if conforms
    - Like statistical anomaly detection does not require prior knowledge of security flaws

Rule-Based Intrusion Detection

- Rule-based penetration identification
  - Uses expert systems technology
  - With rules identifying known penetration, weakness patterns, or suspicious behavior
  - Rules usually machine & O/S specific
  - Rules are generated by experts who interview & codify knowledge of security administrators
  - Quality depends on how well this is done
  - Compare audit records or states against rules

Examples of Heuristics Used for Rules

- Users should not read files in other user's personal directories
- Users must not write other user's files
- Users who log on in after hours often access the same files they used earlier
- Users do not generally open disk devices directly but rely on higher level operating system utilities
- Users should not be logged in more than once to the same system
- Users do not make copies of system programs

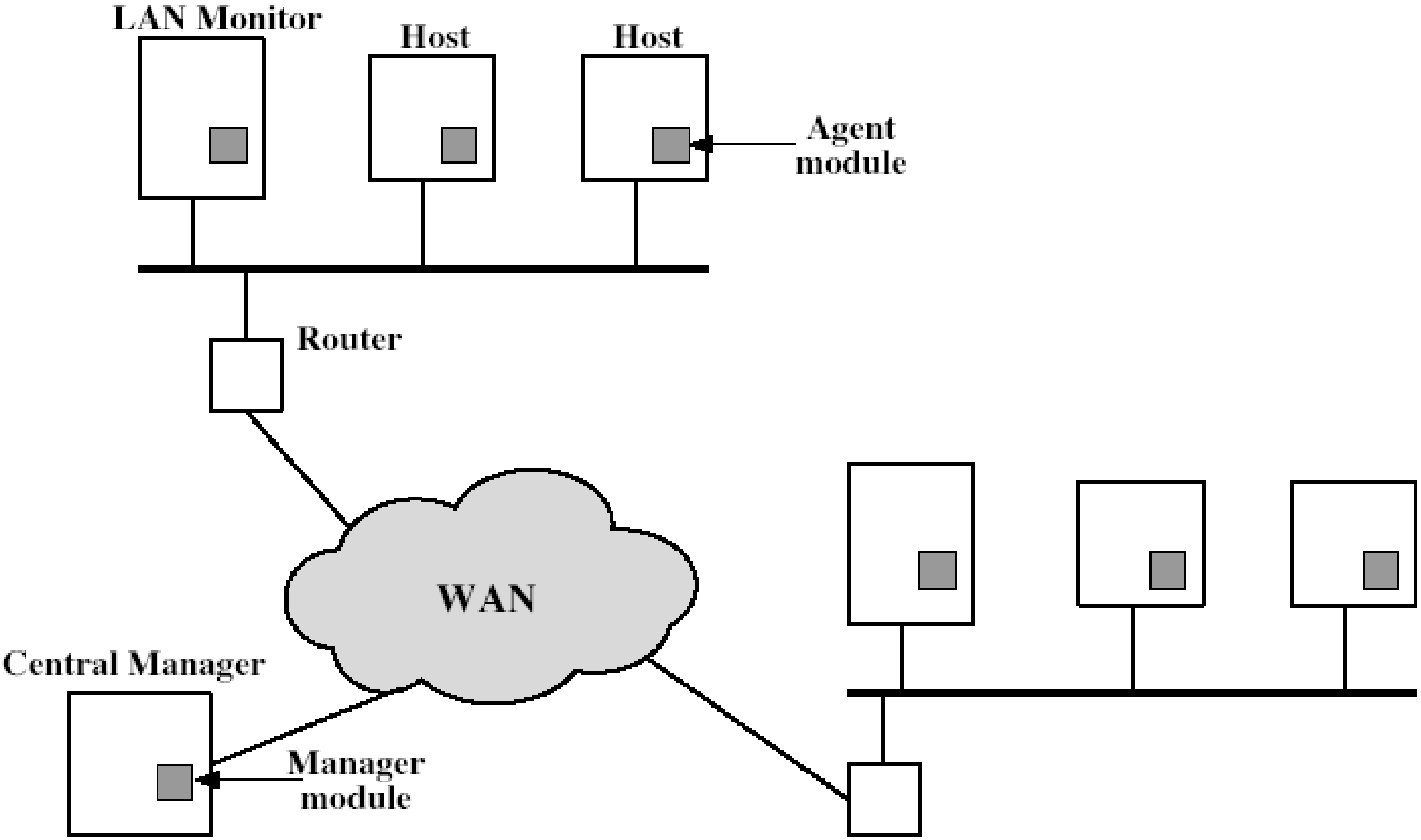
Base-Rate Fallacy

- Practically an intrusion detection system, needs to detect a substantial percentage of intrusions with few false alarms
  - ▫ If too few intrusions detected -> false security
  - ▫ If too many false alarms -> ignore / waste time
- This is very hard to do
- Existing systems seem not to have a good record

Distributed Intrusion Detection

- Traditional focus is on single systems
- But typically have networked systems
- More effective defense has these working together to detect intrusions
- Issues
  - Dealing with varying audit record formats
  - Integrity & confidentiality of networked data
  - Centralized or decentralized architecture

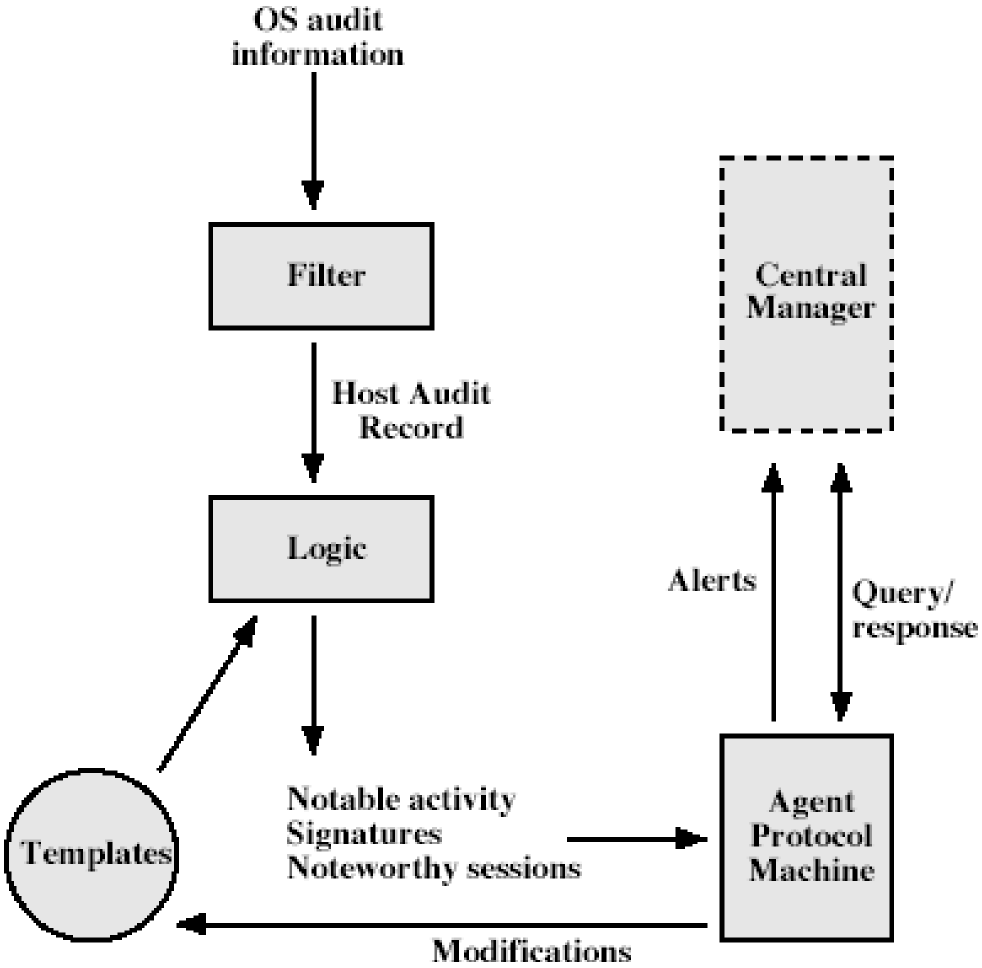
Distributed Intrusion Detection - Architecture



Distributed Intrusion Detection

- Host Agent Module:
  - An audit collection module operating as a background process on a monitored system
  - Collects events and transmits to the central manager
- LAN Monitor Agent Module:
  - Operates in the same fashion as hot agent module except that it analyzes LAN traffic
- Central Manager Module:
  - Receives reports from LAN monitor and host agents processes and correlates these reports to detect intrusion

Distributed Intrusion Detection – Agent Implementation



Honeypots

- Decoy systems deigned to lure attackers:
  - Away from accessing critical systems
  - To collect information of their activities
  - To encourage attacker to stay on system so administrator can respond
- Are filled with fabricated information
- Instrumented to collect detailed information on attackers activities
- May be single or multiple networked systems

Intrusion Detection Exchange Format

- The goal of IETF Intrusion Detection Working Group is to come up with a standard
- Outputs of this working group so far include:
    - A requirements document, which describes the high level functional requirements for communication between IDSs
    - A common intrusion language specification
    - A framework document, which identifies existing protocols best used for communication between IDSs.

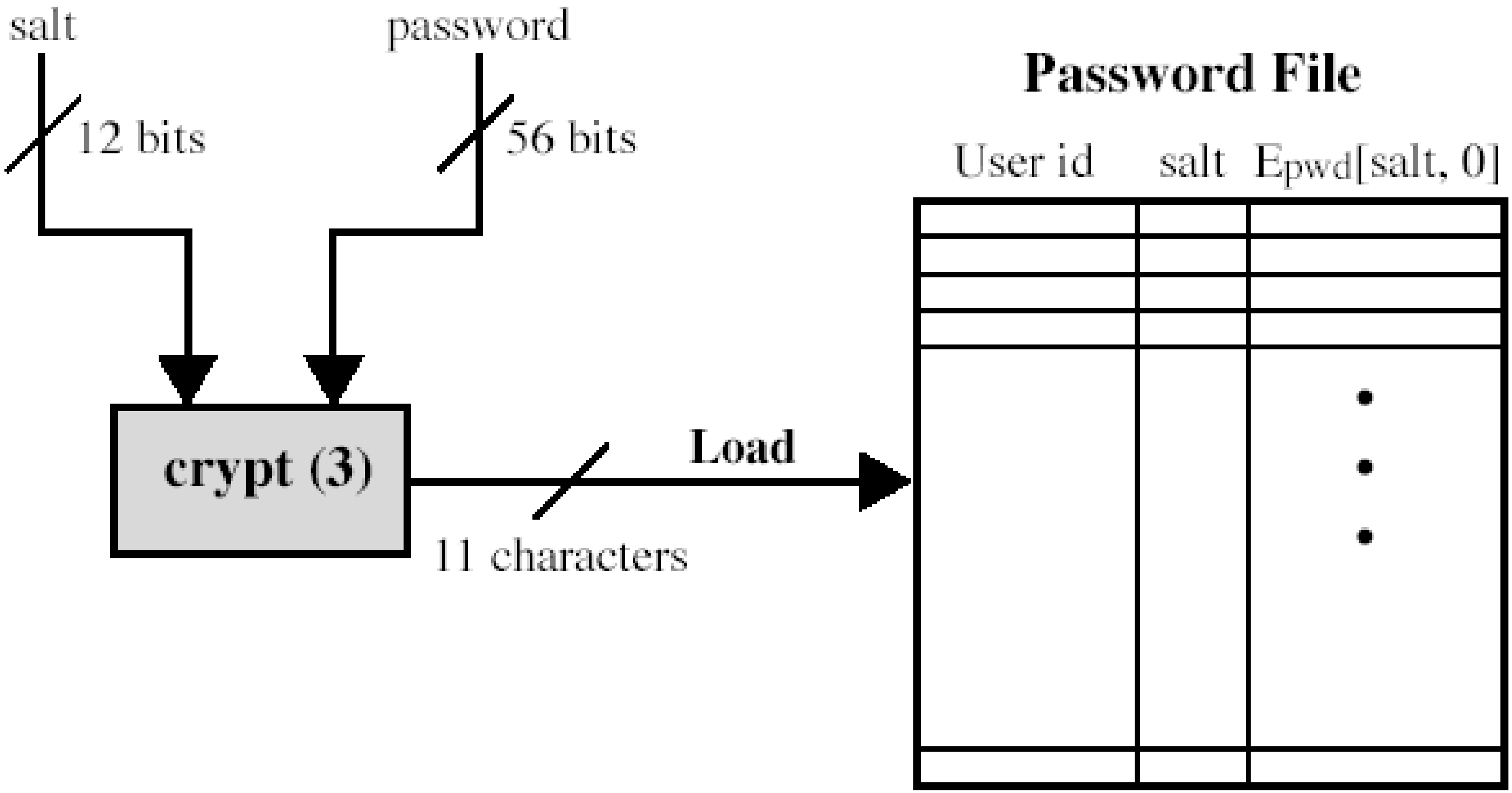
Password Management

- Front-line of defense against intruders
- Users supply both:
  - Login – determines privileges of that user
  - Password – to identify them
- Passwords are often stored encrypted
  - Unix uses multiple DES (variant with salt)
  - More recent systems use crypto hash function

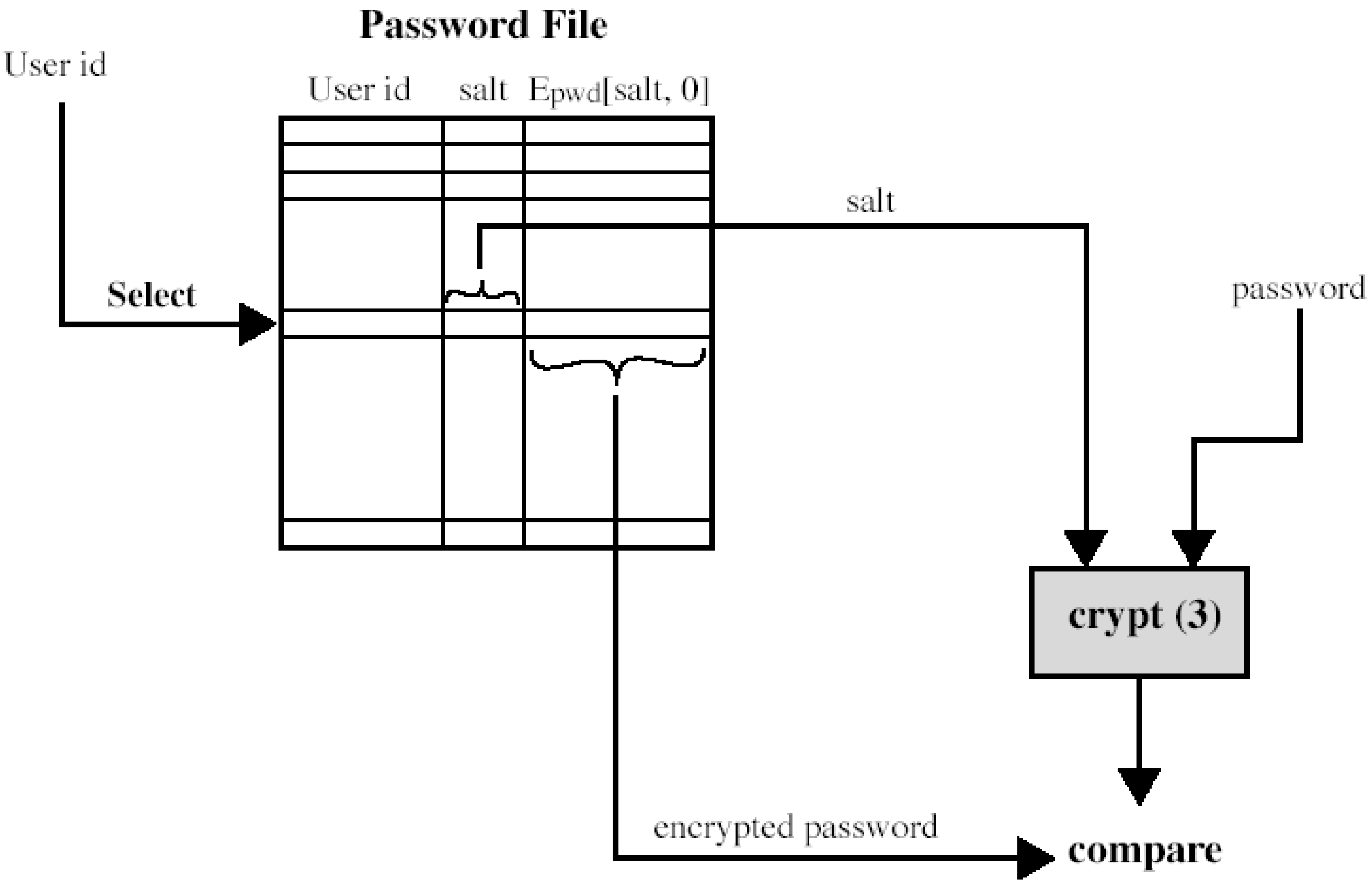
UNIX Password Scheme

- Each user selects a password of up to 8 characters
- This is converted into a 56 it value
  - This serves as input key to encryption scheme based on DES
- DES algorithm is modified using a 12 bit salt value
  - Value is related to time at which the password is assigned
- Output from crypt(3) is of 11 character sequence
- Password is stored in then stored, together with a plaintext copy of the salt, in the password file for corresponding user ID

Loading a New Password



Verifying a Password



Advantages of Salt

- Prevents duplicate passwords from being visible
- If two users choose the same password, the time will be different
- It increases the length of the password
- Prevents the use of hardware implementation of DES

Managing Passwords

- Need policies and good user education
- Ensure every account has a default password
- Ensure users change the default passwords to something they can remember
- Protect password file from general access
- Set technical policies to enforce good passwords
    - Minimum length (>6)
    - Require a mix of upper & lower case letters, numbers, punctuation
    - Block known dictionary words

Managing Passwords

- May reactively run password guessing tools
  - Note that good dictionaries exist for almost any language/interest group
- May enforce periodic changing of passwords
- Have system monitor failed login attempts, & lockout account if see too many in a short period
- Do need to educate users and get support
- Balance requirements with user acceptance
- Be aware of social engineering attacks

Password Selection

- Many users choose password either too short or too easy to guess
- Devices can assign users password and makes cracking impossible
  - ▫ But impossible for most users to remember passwords

Password Selection

- Goal: To eliminate guessable passwords
- Basic techniques
  - User education
  - Computer-generated passwords
  - Reactive password checking
  - Proactive password checking

User Education

- Users be told the importance of using hard-to-guess passwords
- Provide guidelines for selecting passwords
- Unlikely to succeed in large user population
  - Many users may ignore the guidelines

Computer Generated Passwords

- Passwords are quite random in nature
- Users may not be able to remember them
  - Even if it is pronounceable
- Scheme has history of poor acceptance

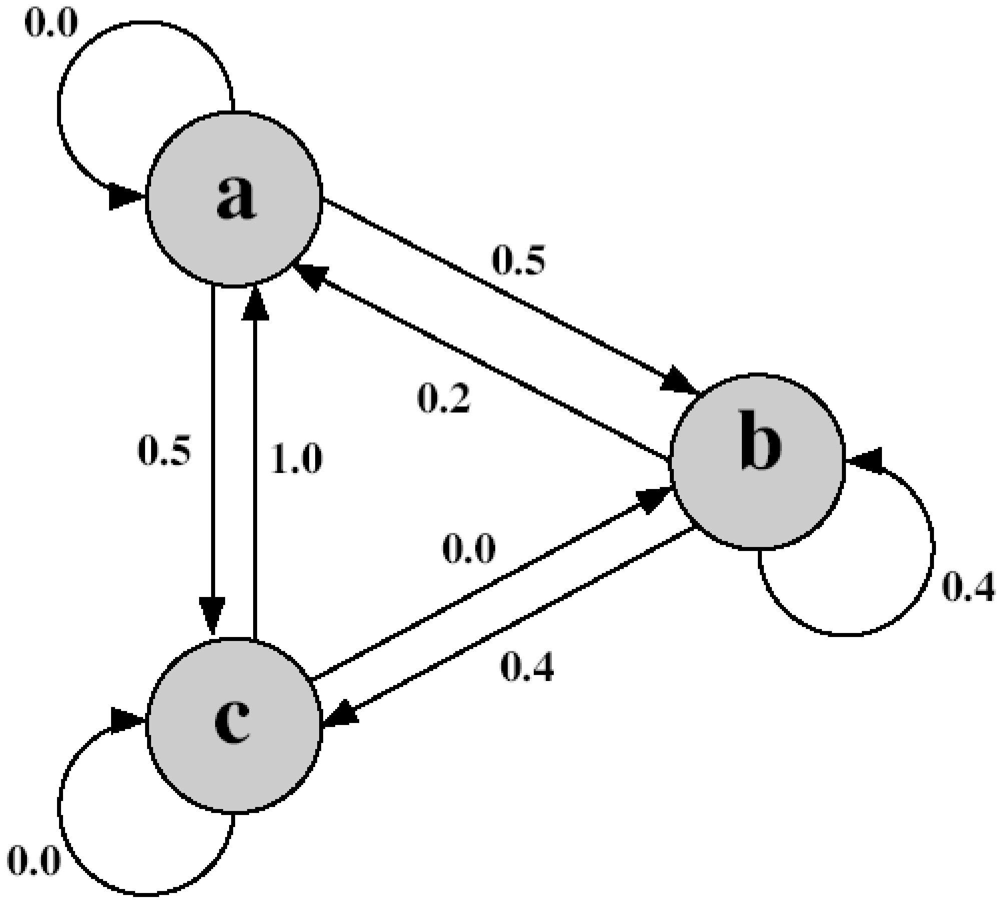
Reactive Password Checking

- System periodically checks for guessable passwords
- Cancels the guessed passwords and notifies the user
  - Number of drawbacks
- Most importantly resource intensive

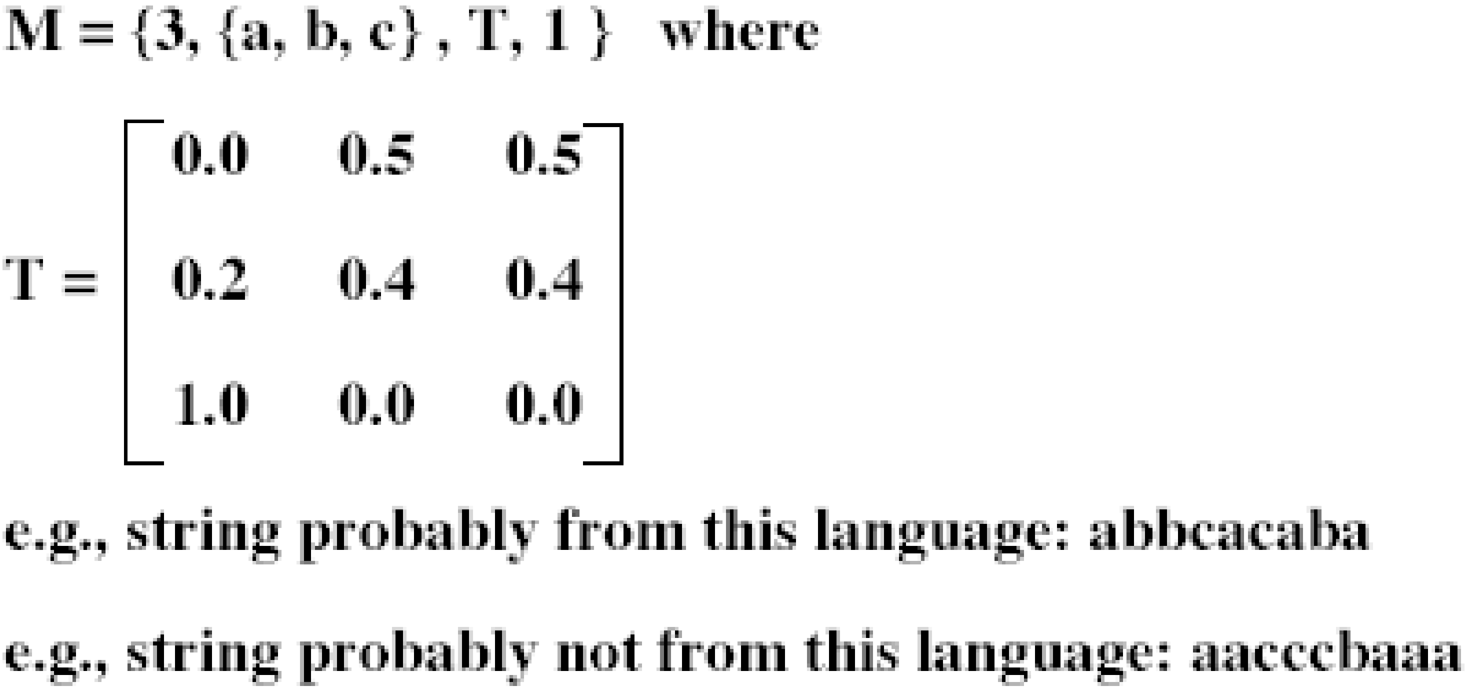
Proactive Password Checking

- Most promising approach to improving password security
- Allow users to select own password
- But have system verify it is acceptable
  - Simple rule enforcement
  - Compare against dictionary of bad passwords
  - Use algorithms (markov model or bloom filter) to detect poor choices

Markov Model



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

Markov Model

- Markov Model is quadruple [m, A, T, k]
  - m is the number of states in the model
  - A is state space
  - T is matrix if transition probabilities
  - k is order of the model

Any question ?