Cryptography and Network Security

Intruder Detection

Intruders

- significant issue for networked systems is hostile or unwanted access
- either via network or local
- can identify classes of intruders:
  - masquerader
  - misfeasor
  - clandestine user
- varying levels of competence

- **Masquerader: An individual who is not authorized to use the computer and who penetrates a** system’s access controls to exploit a legitimate user’s account.
- Normally Outsider

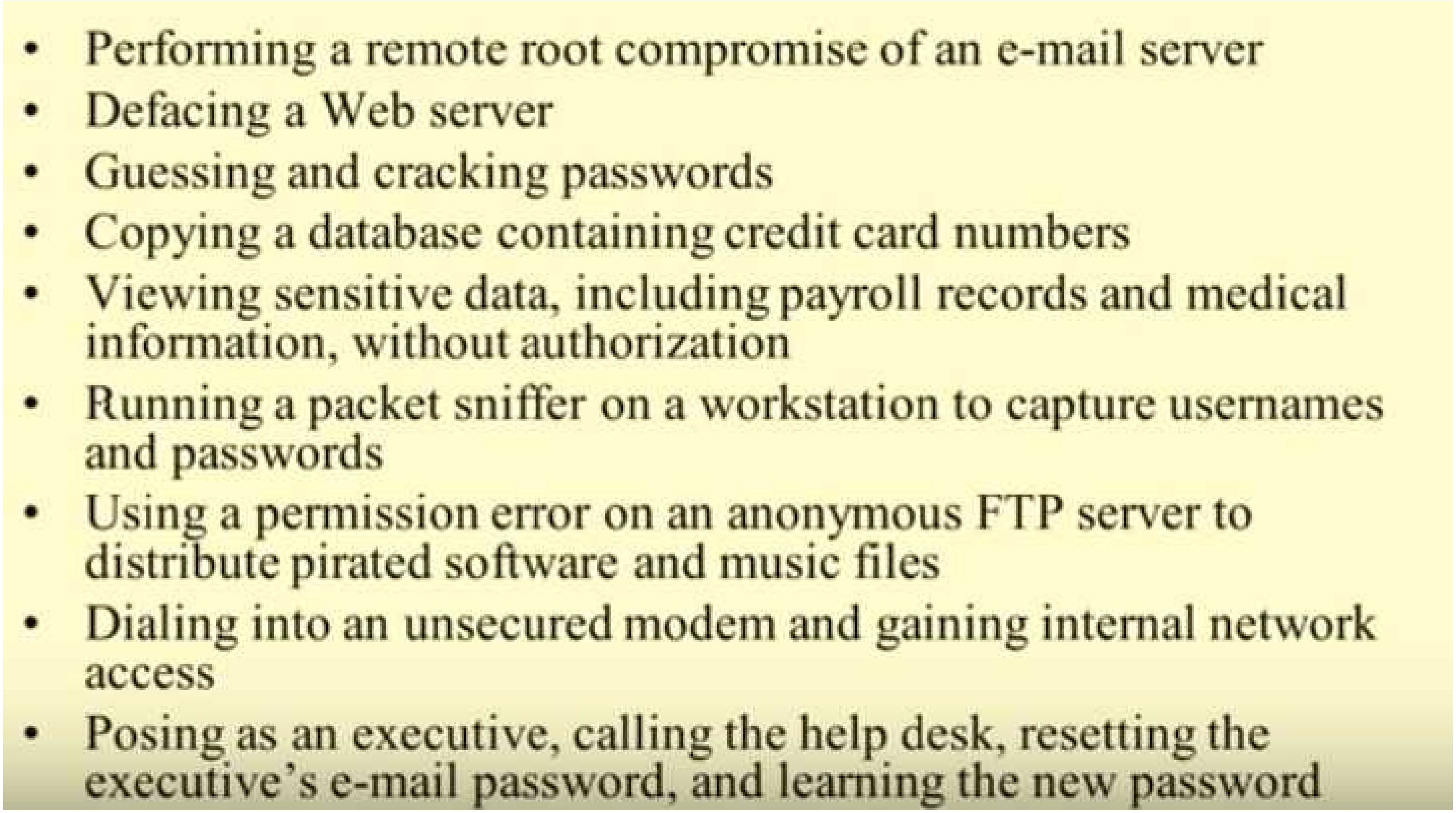
- **Misfeasor: A legitimate user who accesses data, programs, or resources for which such access** is not authorized, or who is authorized for such access but misuses his or her privileges.
- Insider

- **Clandestine user: An individual who seizes supervisory control of the system and uses this** control to evade auditing and access controls or to suppress audit collection.
- Outsider / Insider

Intruders

- clearly a growing publicized problem
  - from “Wily Hacker” in 1986/87
  - to clearly escalating CERT stats
- may seem benign, but still cost resources
- may use compromised system to launch other attacks

Examples of Intrusion



- Performing a remote root compromise of an e-mail server
- Defacing a Web server
- Guessing and cracking passwords
- Copying a database containing credit card numbers
- Viewing sensitive data, including payroll records and medical information, without authorization
- Running a packet sniffer on a workstation to capture usernames and passwords
- Using a permission error on an anonymous FTP server to distribute pirated software and music files
- Dialing into an unsecured modem and gaining internal network access
- Posing as an executive, calling the help desk, resetting the executive's e-mail password, and learning the new password

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

Password Guessing

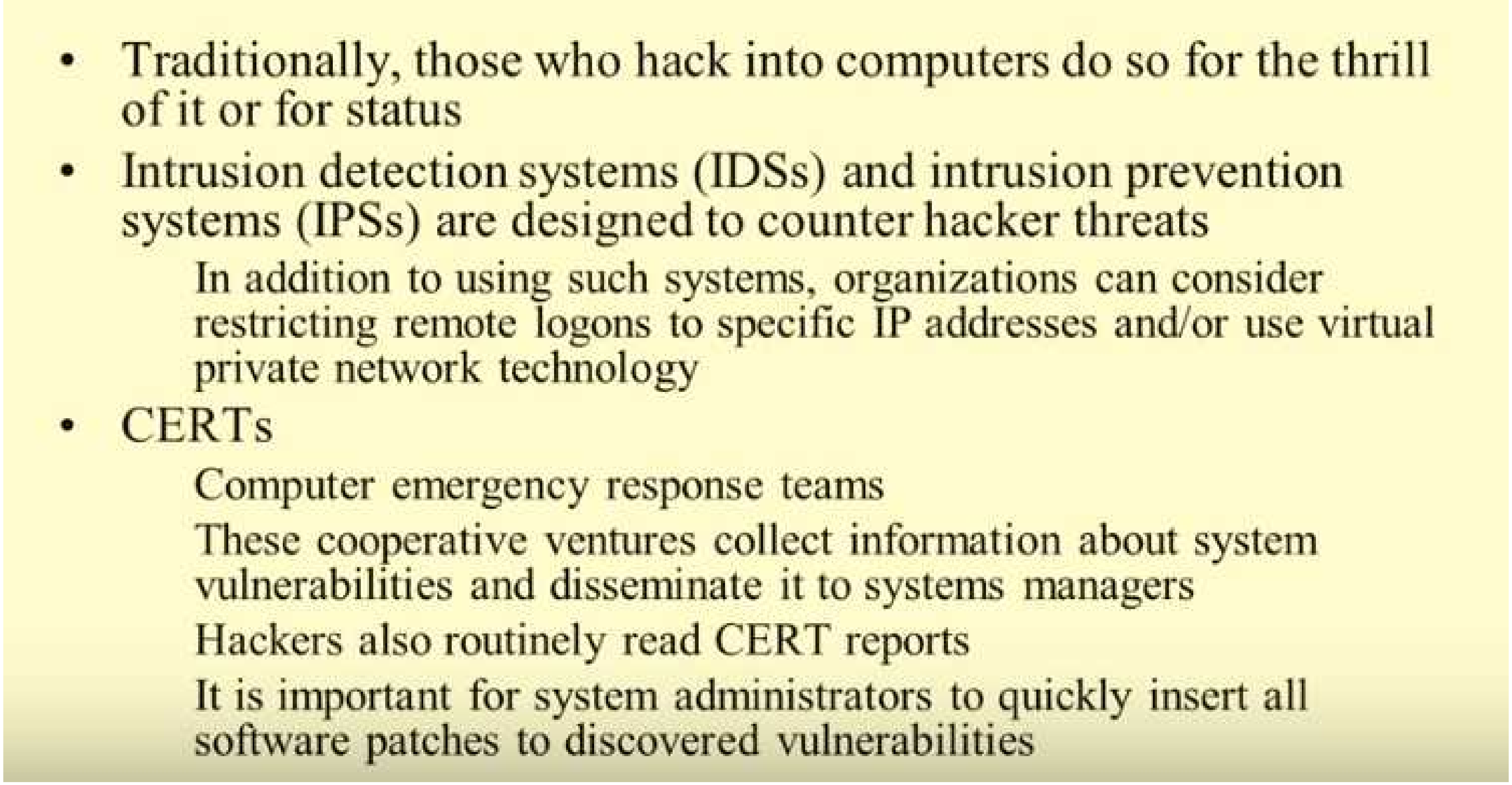
- one of the most common attacks
- attacker knows a login (from email/web page etc)
- then attempts to guess password for it
  - try default passwords shipped with systems
  - try all short passwords
  - then try by searching dictionaries of common words
  - intelligent searches try passwords associated with the user (variations on names, birthday, phone, common words/interests)
  - before exhaustively searching all possible passwords
- check by login attempt or against stolen password file
- success depends on password chosen by user
- surveys show many users choose poorly

Password Capture

- another attack involves **password capture**
  - watching over shoulder as password is entered
  - using a trojan horse program to collect
  - monitoring an insecure network login (eg. telnet, FTP, web, email)
  - extracting recorded info after successful login (web history/cache, last number dialed etc)
- using valid login/password can impersonate user
- users need to be educated to use suitable precautions/countermeasures

Intrusion Detection

- inevitably will have security failures
- so need also to detect intrusions so can
  - block if detected quickly
  - act as deterrent
  - collect info to improve security
- assume intruder will behave differently to a legitimate user
  - but will have imperfect distinction between



- Traditionally, those who hack into computers do so for the thrill of it or for status
- Intrusion detection systems (IDSs) and intrusion prevention systems (IPSs) are designed to counter hacker threats

    In addition to using such systems, organizations can consider restricting remote logons to specific IP addresses and/or use virtual private network technology

- CERTs

    Computer emergency response teams

    These cooperative ventures collect information about system vulnerabilities and disseminate it to systems managers

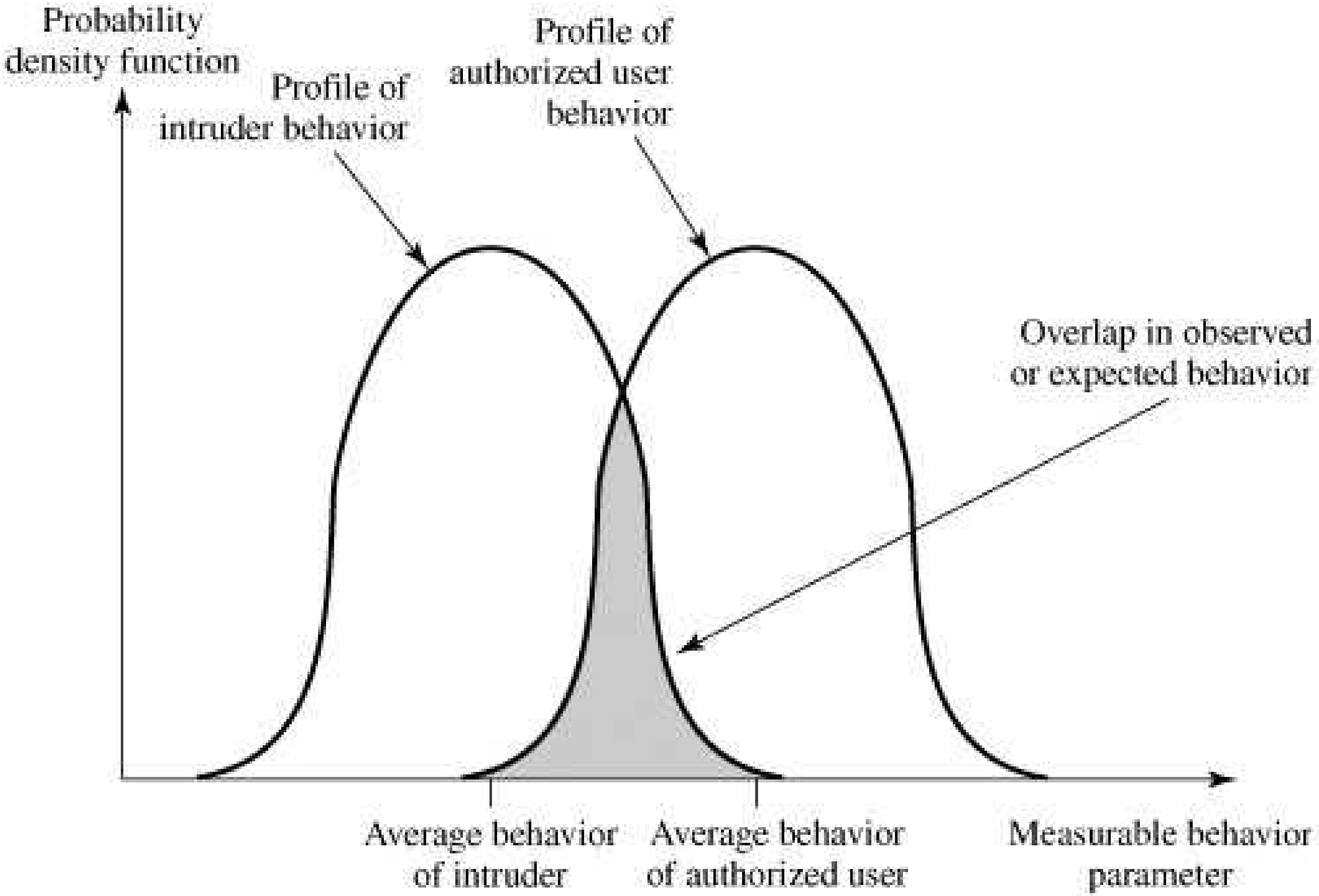
    Hackers also routinely read CERT reports

    It is important for system administrators to quickly insert all software patches to discovered vulnerabilities

- One-way function: The system stores only the value of a function based on the user’s password. When the user presents a password, the system transforms that password and compares it with the stored value.
- Access Control:

- Try default passwords used with standard accounts that are shipped with the system. Many administrators do not bother to change these defaults.
- Exhaustively try all short passwords (those of one to three characters).
- Try words in the system’s online dictionary or a list of likely passwords. Examples of the latter are readily available on hacker bulletin boards.

- two principal countermeasures: detection and prevention.
- Detection is concerned with learning of an attack, either before or after its success.
- Prevention is a challenging security goal and an uphill battle at all times.


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

- the typical behavior of an intruder differs from the typical behavior of an authorized user, there is an overlap in these behaviors. Thus, a loose interpretation of intruder behavior, which will catch more intruders, will also lead to a number of "false positives," or authorized users identified as intruders.

Approaches to Intrusion Detection

- statistical anomaly detection
  - threshold
  - profile based
- rule-based detection
  - anomaly
  - penetration identification

Statistical anomaly detection

- **Statistical anomaly detection: Involves the collection of data relating to the behavior of** legitimate users over a period of time. Then statistical tests are applied.
- statistical approaches attempt to define normal, or expected, behavior, whereas
- rulebased approaches attempt to define proper behavior

Types

- Threshold detection: This approach involves defining thresholds, independent of user, for the frequency of occurrence of various events.
- Profile based: A profile of the activity of each user is developed and used to detect changes in the behavior of individual accounts.

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

Rule based Detection

- **Rule-based detection: Involves an attempt to define a set of rules that can be used to decide** that a given behavior is that of an intruder.

Types

- Anomaly detection: Rules are developed to detect deviation from previous usage patterns.
- Penetration identification: An expert system approach that searches for suspicious behavior.

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 admins
  - quality depends on how well this is done
  - compare audit records or states against rules

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 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

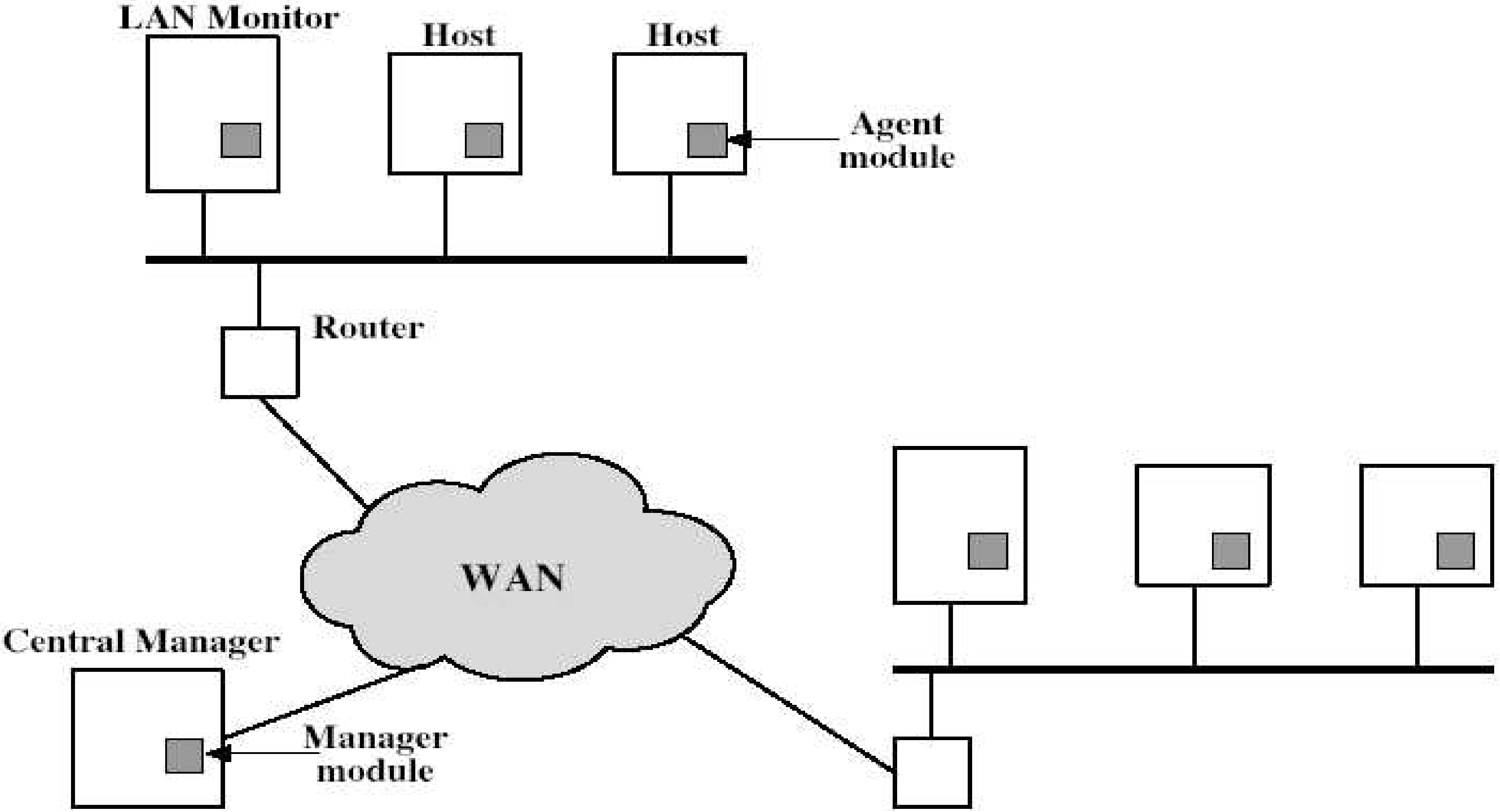
Base-Rate Fallacy

- 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

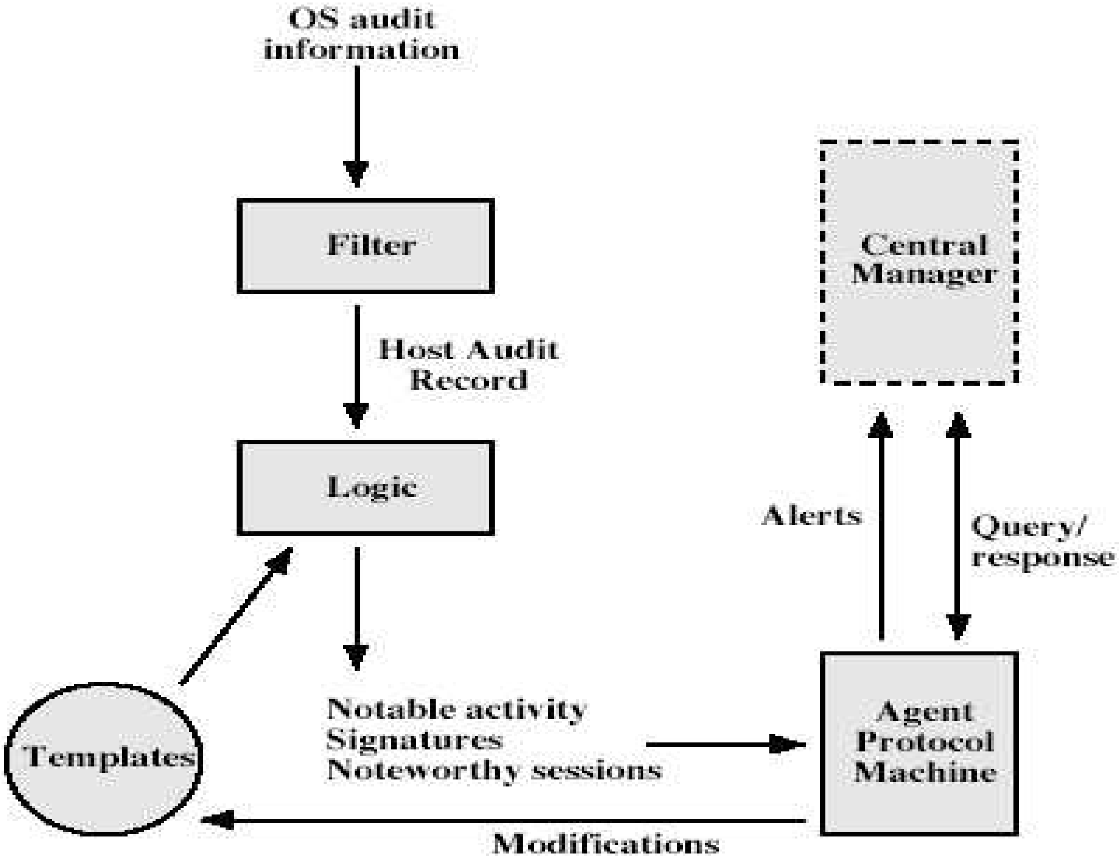
Distributed Intrusion Detection

- 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 – Agent Implementation



Honeypots

- decoy systems 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

Password Management

- front-line defense against intruders
- users supply both:
  - login – determines privileges of that user
  - password – to identify them
- passwords often stored encrypted
  - Unix uses multiple DES (variant with salt)
  - more recent systems use crypto hash function

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 know 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

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 (see previous slide)
  - compare against dictionary of bad passwords
  - use algorithmic (markov model or bloom filter) to detect poor choices

Summary

- have considered:
  - problem of intrusion
  - intrusion detection (statistical & rule-based)
  - password management