Intruders and Intrusion Detection

Intruders

- Significant issue for networked systems is hostile or unwanted access by users or software
  - user trespass
    - unauthorized logon, privilege abuse
  - software trespass
    - virus, worm, or trojan horse
- Either via network or local
- can identify 3 classes of intruders:
  - **Masquerader-**An individual who is not authorized to use the computer (outsider)
  - **Misfeasor-** A legitimate user who accesses unauthorized data, programs, or resources (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 (either)

Intruders

- Intruder attacks range from the benign (simply exploring net to see what is there); to the serious (who attempt to read privileged data, perform unauthorized modifications, or disrupt system)
- clearly a growing publicized problem
  - from "Wily Hacker" in 1986/87
  - to clearly escalating CERT stats
- Problem at Bell Labs
  - Copy pwd file
  - RPC
  - Connect to nonexistent machines

Intruders

- may seem benign, but still cost resources, slow performance
- may use compromised system to launch other attacks
- Two levels of hackers
  - Sophisticated users
  - Foot soldiers
- awareness of intruders has led to the development of CERTs
- Collect info about system vulnerabilities and disseminate to system managers
- Intruders modify login software

Intrusion Techniques

- aim to gain access and/or increase privileges on a system
- basic attack methodology
  - target acquisition and information gathering
  - initial access
  - privilege escalation
  - covering tracks
- key goal often is to acquire passwords
- then exercise access rights of owner
- Pwd files can be protected by
  - One-way encryption
  - Access control

Password Guessing

- one of the most common attacks
- attacker knows a login (from email/web page etc)
- then attempts to guess password for it
  - defaults, short passwords, common word searches
  - user info (variations on names, birthday, phone, common words/interests, room number, licence plate no)
  - exhaustively searching all possible passwords
  - Trojan horse
- check by login 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
- Counter measures – prevention and detection

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

Intrusion Detection

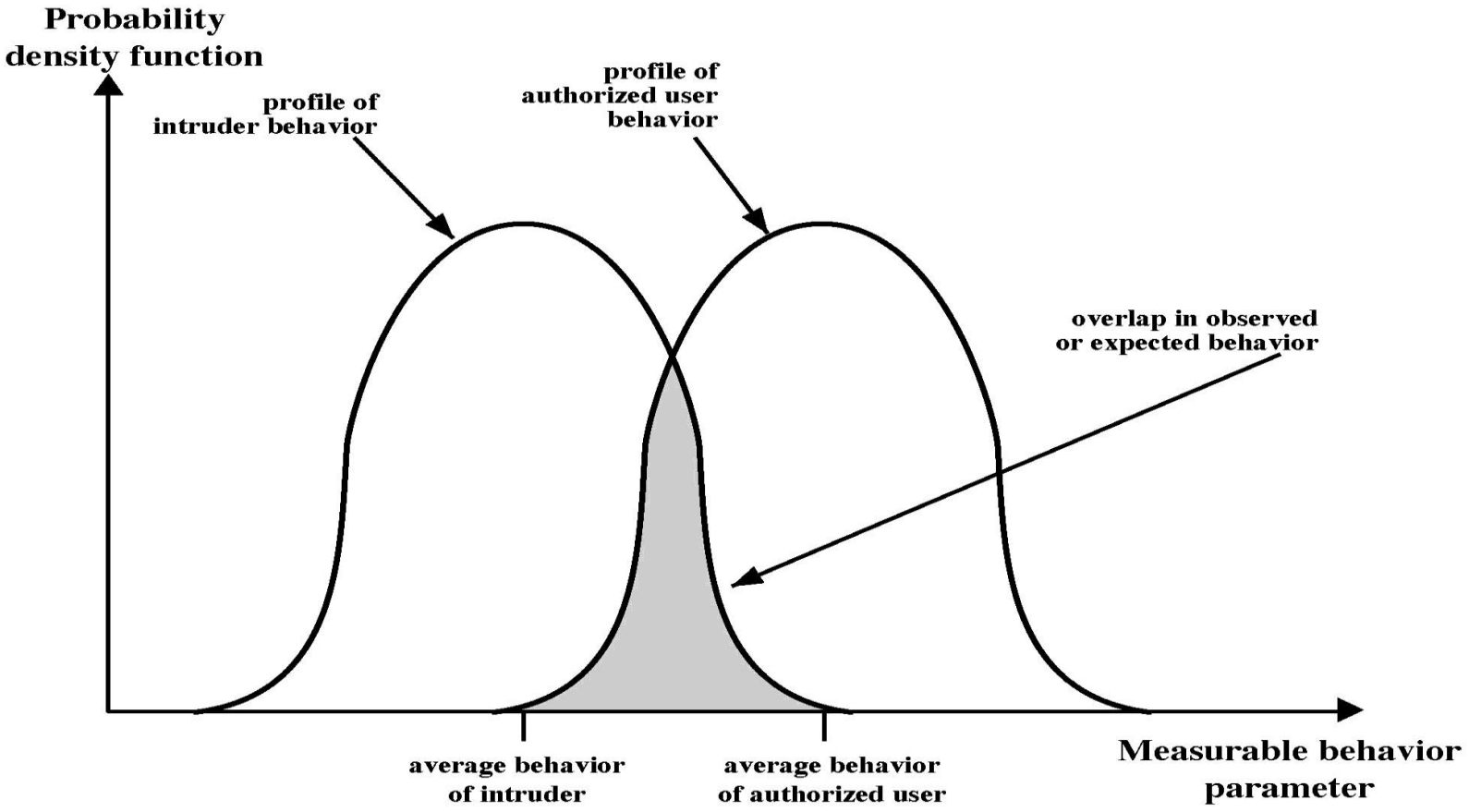


Figure 18.1 Profiles of Behavior of Intruders and Authorized Users

Approaches to Intrusion Detection

- Masquerader Vs legitimate user – Easy
- Misfeasor – difficult
- Clandstine user – beyond the scope of automated techniques
- **statistical anomaly detection**
- **rule-based detection**

Statistical Anomaly Detection

1. Statistical anomaly detection: collect data relating to the behavior of legitimate users, then use statistical tests to determine with a high level of confidence whether new behavior is legitimate user behavior or not.

a. Threshold detection: define thresholds, independent of user, for the frequency of occurrence of events.

b. Profile based: develop profile of activity of each user and use to detect changes in the behavior

- Define normal or expected behavior
- Effective against Masqueraders

Rule-based Detection

2. Rule-based detection: attempt to define a set of rules used to decide if given behavior is an intruder

   a. Anomaly detection: rules detect deviation from previous usage patterns

   b. Penetration identification: expert system approach that searches for suspicious behavior

- Attempt to define proper behavior
- Effective for misfeasors

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
  - advantage is it can be vendor independent and portable, disadvantage is extra overhead involved

Sample Audit Record

- Subject : Initiators of action
- Action : Operation performed by the subject
- Object : Receptors of action
- Exception – condition
- Resource – usage : quantitative elements
- Time –stamp: 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 – Non negative integer that may be incremented
  - Gauge- incremented or decremented
  - interval timer – length of time between two related events
  - resource use – quantity of resources consumed during a specified period
- use various tests on these to determine if current behavio is acceptable
  - mean & standard deviation, multivariate, markov process time series, operational

Audit Record Analysis

- mean & standard deviation of a parameter over some historical period
- Multivariate – Based on correlations between two variables
- markov process – Used to establish transition probabilities among various states
- time series – looking for sequences of events that happen too rapidly or too slowly
- Operational – judgment of what is considered abnormal

- key advantage is no prior knowledge of security flaws is not required. Thus it should be readily portable among a variety of systems

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
  - Based on past behaviour and assume that future will be like the past

Rule-Based Intrusion Detection

- rule-based penetration identification
  - uses expert systems technology
  - with rules identifying known penetration, weakness patterns, or suspicious behavior
  - compare audit records or states against rules
  - 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

Rule-Based Intrusion Detection

1. Users should not read files in other users' personal directories.

2. Users must not write other users' files.

3. Users who log in after hours often access the same files they used earlier.

4. Users do not generally open disk devices directly but rely on higher-level operating system utilities.

5. Users should not be logged in more than once to the same system.

6. Users do not make copies of system programs

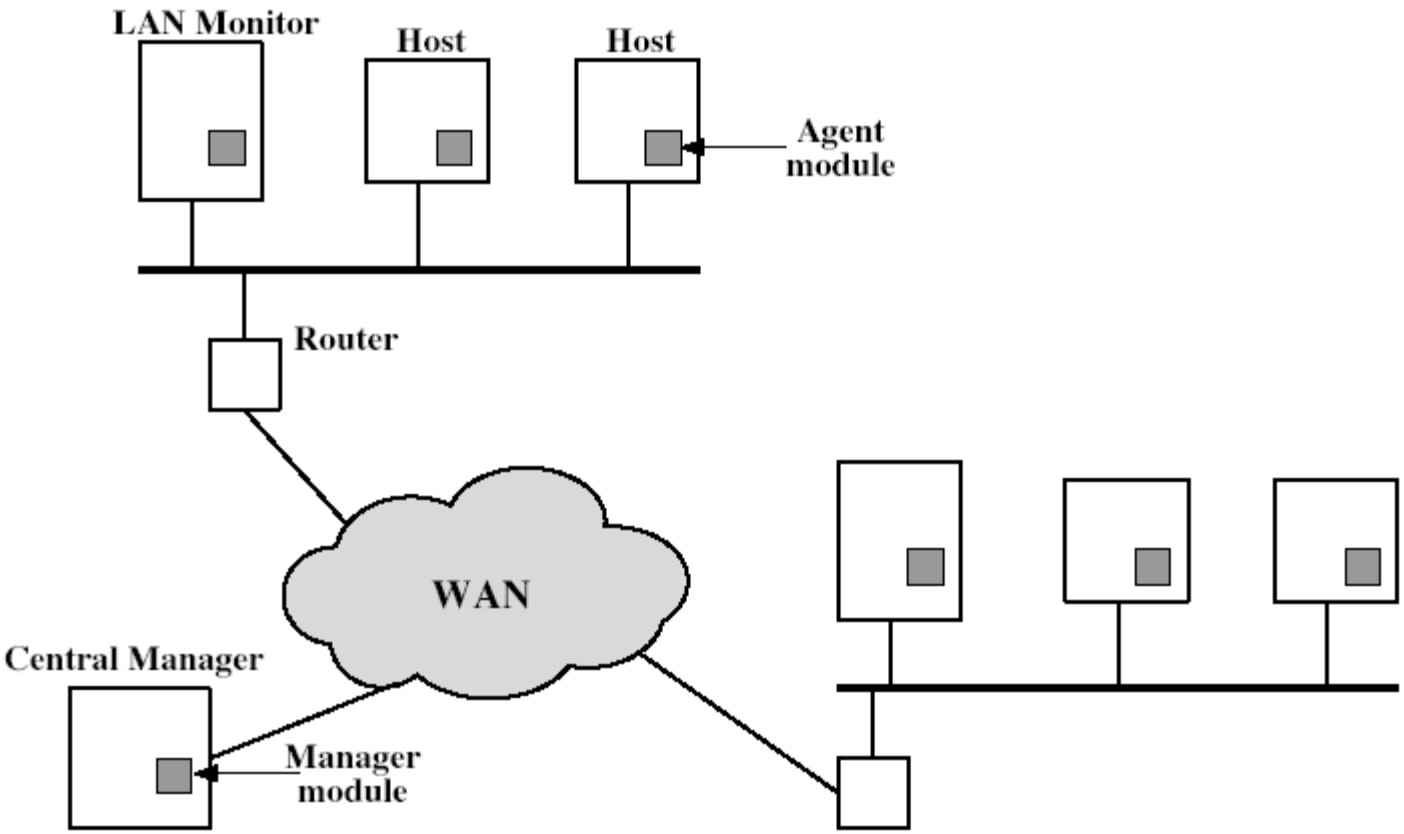
Base-Rate Fallacy

- 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

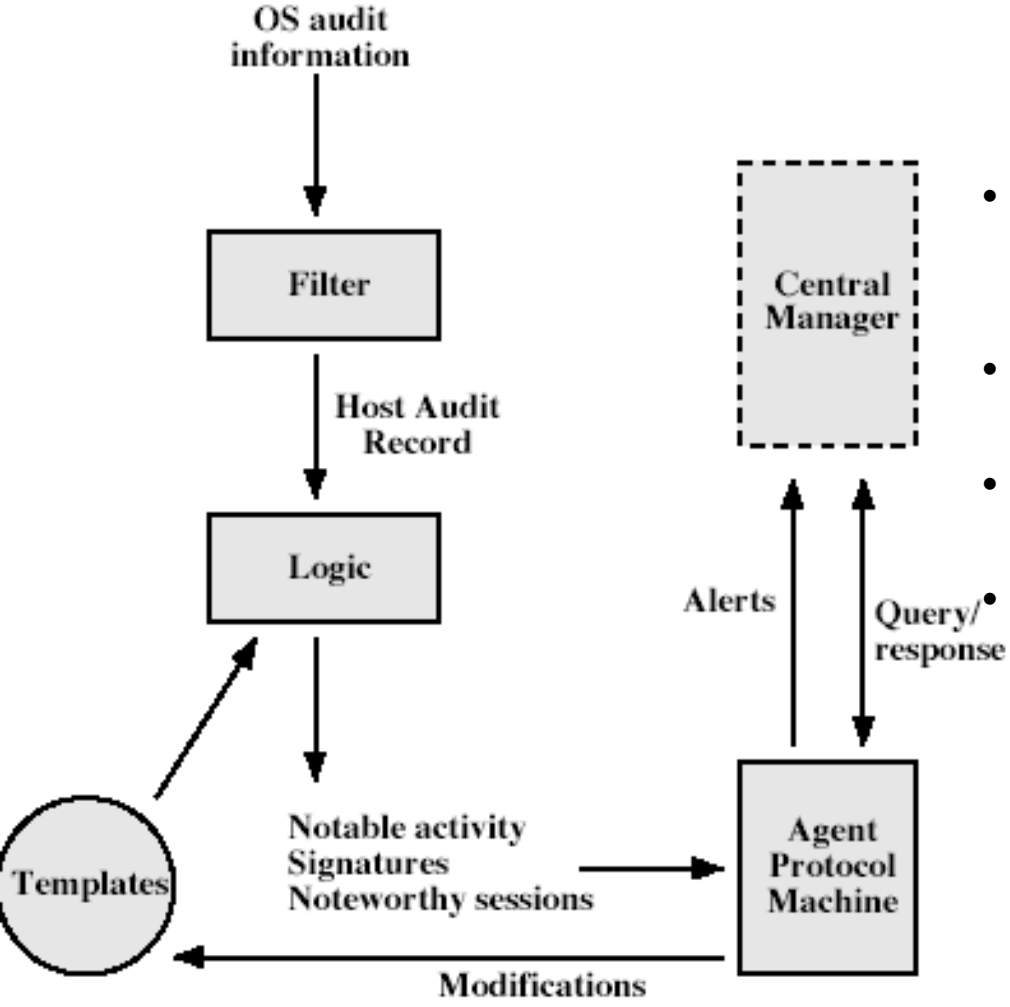


Distributed Intrusion Detection - Architecture

The components are:

- Host agent module: audit collection module operating as a background process on a monitored system
- LAN monitor agent module: like a host agent module except it analyzes LAN traffic
- Central manager module: Receives reports from LAN monitor and host agents and processes and correlates these reports to detect intrusion

Distributed Intrusion Detection – Agent Implementation



- agent captures each native O/S audit record, & applies a filter that retains only records of security interest
- reformatted into a standardized format (HAR).
- template-driven logic module analyzes the records for suspicious activity
- When suspicious activity is detected, an alert is sent to the central manager

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 with sensitive monitors and even loggers that detect these accesses and to collect detailed information on attackers activities
- Have seen evolution from single host honeypot to honeynets of multiple dispersed system
- single or multiple networked systems

Intrusion Detection Exchange Format

- standards are needed to support interoperability
- IETF Intrusion Detection WG standards
- define data formats and exchange procedures for sharing information of interest
- The outputs of this working group include the following
  - A requirements document
  - A common intrusion language specification
  - A framework document

Summary

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