Intruders & Intrusion Detection

Module VI

Intruders

Intro

Two most publicized threats to security

1. Intruder
2. Viruses

We will be focussing on Intruders - Also known as Hacker or Cracker

Classes of intruders

1. **Masquerader**
2. **Misfeasor**
3. **Clandestine user**

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
- Likely to be an 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
- Generally is an 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 an outsider or an insider

Attack Levels

- Benign

  People who simply wish to explore internets and see what is out there

- Serious

  Attempting to read privileged data, perform unauthorized modifications to data, or disrupt the system

Hacker Levels

- The high level

  Sophisticated users with a thorough knowledge of the technology

- The low level

  Used the supplied cracking programs with little understanding of how they worked

Intrusion Techniques

The Password file protection

- One-way function

  When the user presents a password, the system transforms that password and compares it with the stored value.

- Access control

  Access to the password file is limited to one or a very few accounts

Techniques for learning passwords

1. Try default passwords used with standard accounts that are shipped with the system. Many administrators do not bother to change these defaults.
2. Exhaustively try all short passwords (those of one to three characters).
3. 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.

Techniques for learning passwords

4. Collect information about users, such as their full names, the names of their spouse and children, pictures in their office, and books in their office that are related to hobbies.
5. Try users' phone numbers, Social Security numbers, and room numbers.
6. Try all legitimate license plate numbers for this state.
7. Use a Trojan horse to bypass restrictions on access.
8. Tap the line between a remote user and the host system.

Techniques for learning passwords

4. **Collect information about users, such as their full names, the names of their spouse and children, pictures in their office, and books in their office that are related to hobbies.**
5. **Try users′ phone numbers, Social Security numbers, and room numbers.**
6. **Try all legitimate license plate numbers for this state.**
7. **Use a Trojan horse to bypass restrictions on access.**
8. **Tap the line between a remote user and the host system.**

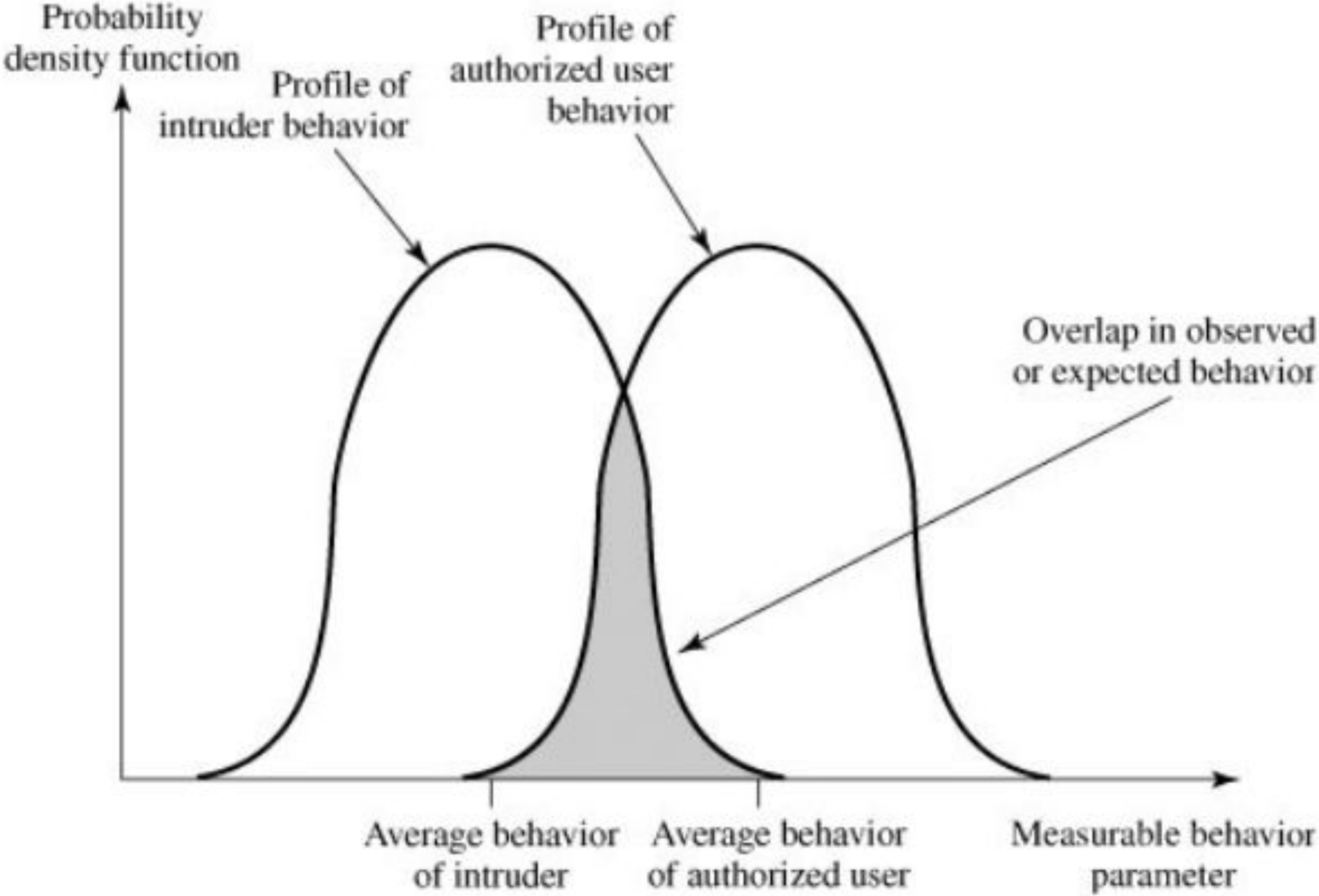
Intrusion Detection

Prevention not really better than cure.

The best prevention system will be broken. So most efforts go into detecting intrusion at the earliest

Why Intrusion Detection?

- If an intrusion is detected quickly enough, the intruder can be identified and ejected from the system before any damage is done or any data are compromised.
- Can serve as a deterrent, so acting to prevent intrusions.
- enables the collection of information about intrusion techniques that can be used to strengthen the intrusion prevention facility.


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

From the Figure

- **Find where masquerader , Legitimate user , misfeasor and clandestine user would be?**

Audit Records

- Some record of ongoing activity by users must be maintained as input to an intrusion detection system.
- Basically, two plans are used:
  - Native audit records
  - Detection-specific audit records

Audit Records - Native audit records

- Virtually all multiuser operating systems include accounting software that collects information on user activity
- Advantage: No additional collection software is needed
- Disadvantage : Native audit records may not contain the needed information or may not contain it in a convenient form.

Audit Records - Detection-specific audit records

- A collection facility can be implemented that generates audit records containing only that information required by the intrusion detection system
- Advantage : It could be made vendor independent and ported to a variety of systems
- Disadvantage : The extra overhead involved in having, in effect, two accounting packages running on a machine.

Detection-specific audit records Fields

1. **Subject:**

- **Initiators of actions.**
- **Typically a terminal user but might also be a process acting on behalf of users or groups of users.**
- **All activity arises through commands issued by subjects.**
- **Subjects may be grouped into different access classes, and these classes may overlap.**

Detection-specific audit records Fields

2. Action

- Operation performed by the subject on or with an object; for example, login, read,perform I/O, execute.

Detection-specific audit records Fields

3 . Object

- Receptors of actions. EG: files, programs, messages, records, terminals,printers, and user- or program-created structures.
- When a subject is the recipient of an action,such as electronic mail, then that subject is considered an object.
- Objects may be grouped by type.
- Object granularity may vary by object type and by environment.

Detection-specific audit records Fields

4 . Exception-Condition

- Denotes which, if any, exception condition is raised on return.

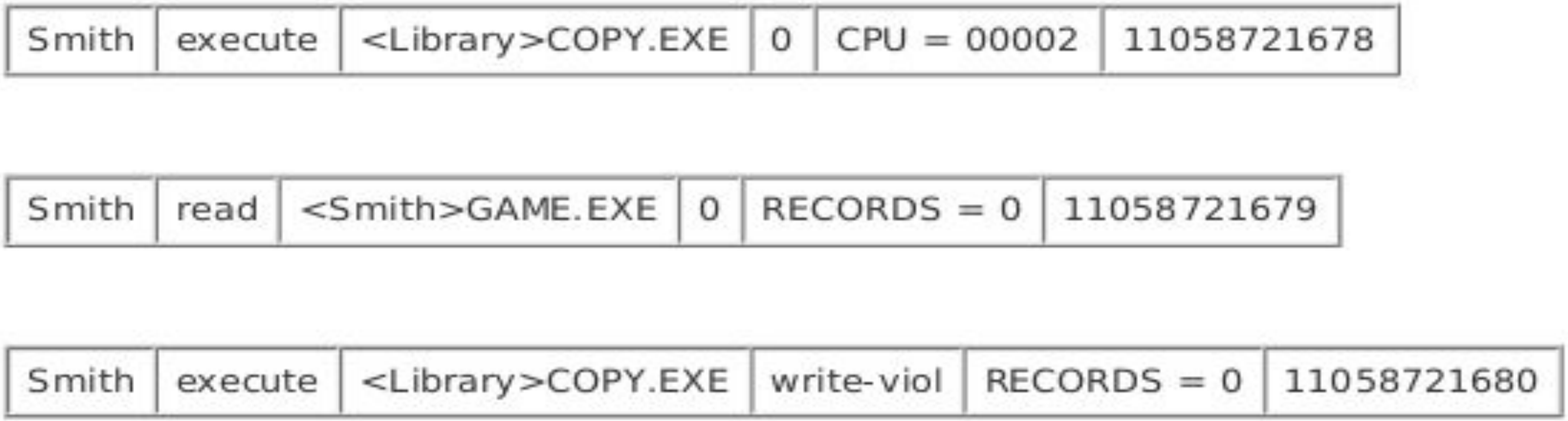
5 . Resource-Usage

- A list of quantitative elements in which each element gives the amount used of some resource

6 . Time-Stamp

- Unique time-and-date stamp identifying when the action took place.

Decomposition of user operation into elementary actions



Smith	execute	<Library>COPY.EXE	0	CPU = 00002	11058721678

Smith	read	<Smith>GAME.EXE	0	RECORDS = 0	11058721679

Smith	execute	<Library>COPY.EXE	write-viol	RECORDS = 0	11058721680

A copy action on file game.exe

Decomposition of user operation into elementary actions

Advantages

1. Enables an audit of all behavior affecting an object. Thus, the system can detect attempted subversions of access controls and successful subversions
2. Single-object, single-action audit records simplify the model and the implementation.
3. Easy to obtain information by a straightforward mapping from existing native audit records to the detection-specific audit records.

Approaches to intrusion detection

1. Statistical anomaly detection
   1. Threshold detection
   2. Profile based
2. Rule-based detection
   1. Anomaly detection
   2. Penetration identification

Statistical anomaly detection

Threshold detection & Profile based

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 to observed behavior to determine with a high level of confidence whether that behavior is not legitimate user behavior.

Statistical Anomaly Detection - Threshold detection

- This approach involves defining thresholds, independent of user, for the frequency of occurrence of various events.
- Involves counting the number of occurrences of a specific event type over an interval of time. If the count surpasses what is considered a reasonable number that one might expect to occur, then intrusion is assumed.

Statistical Anomaly Detection - Threshold detection

- Because of the variability across users, such thresholds are likely to generate either a lot of false positives or a lot of false negatives.
- Simple threshold detectors may be useful in conjunction with more sophisticated techniques

Statistical Anomaly Detection - Profile based

- A profile of the activity of each user is developed and used to detect changes in the behavior of individual accounts.
- A profile may consist of a set of parameters, so that deviation on just a single parameter may not be sufficient in itself to signal an alert.

Statistical Anomaly Detection - Profile based

- Foundation of this approach is an analysis of audit records
- An analysis of audit records over a period of time can be used to determine the activity profile of the average user. Thus, the audit records serve to define typical behavior.
- Second, current audit records are the input used to detect intrusion. That is, the intrusion detection model analyzes incoming audit records to determine deviation from average behavior.

Profile based - Examples of metrics

- Counter: A count of certain event types is kept over a particular period of time.
- Gauge: Used to measure the current value of some entity.
- Interval timer: The length of time between two related events.
- Resource utilization: Quantity of resources consumed during a specified period.

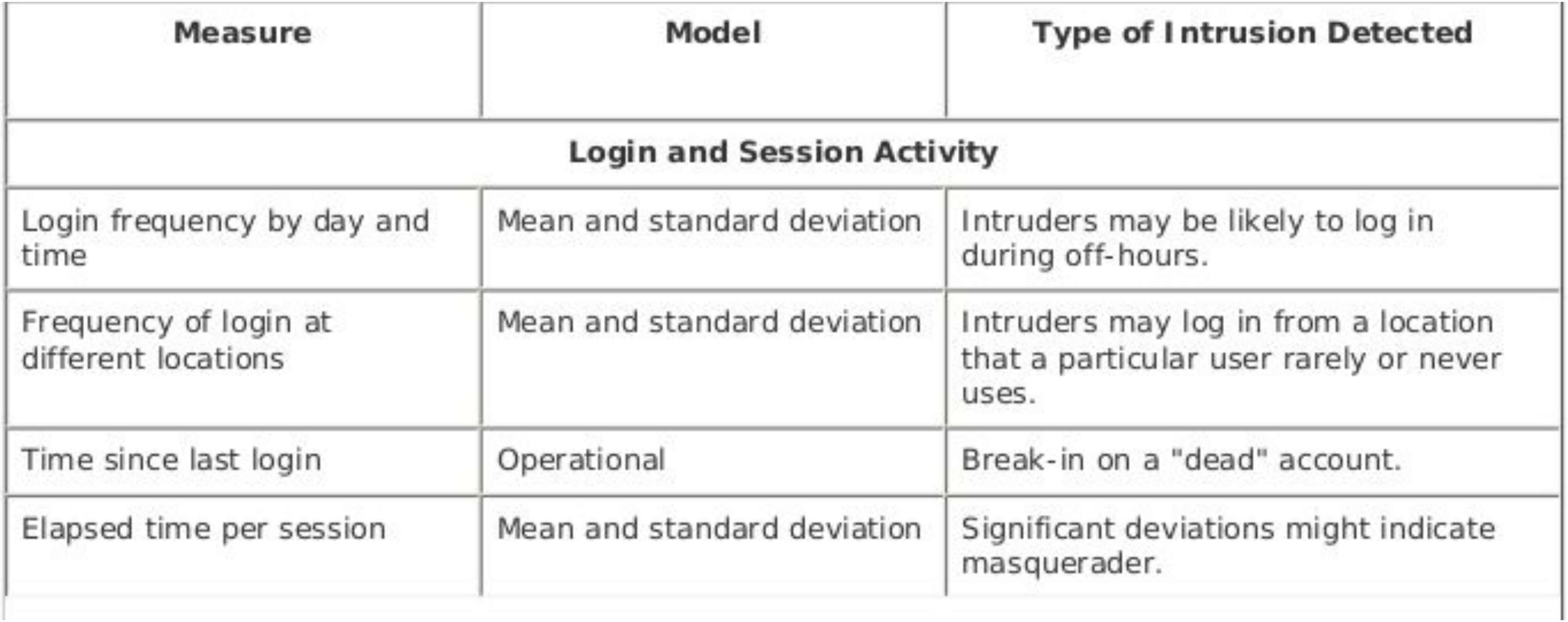
Profile based - Examples of metrics

- **Counter: A count of certain event types is kept over a particular period of time.**
- **Gauge: Used to measure the current value of some entity.**
- **Interval timer: The length of time between two related events.**
- **Resource utilization: Quantity of resources consumed during a specified period.**

Profile based - Examples of Model

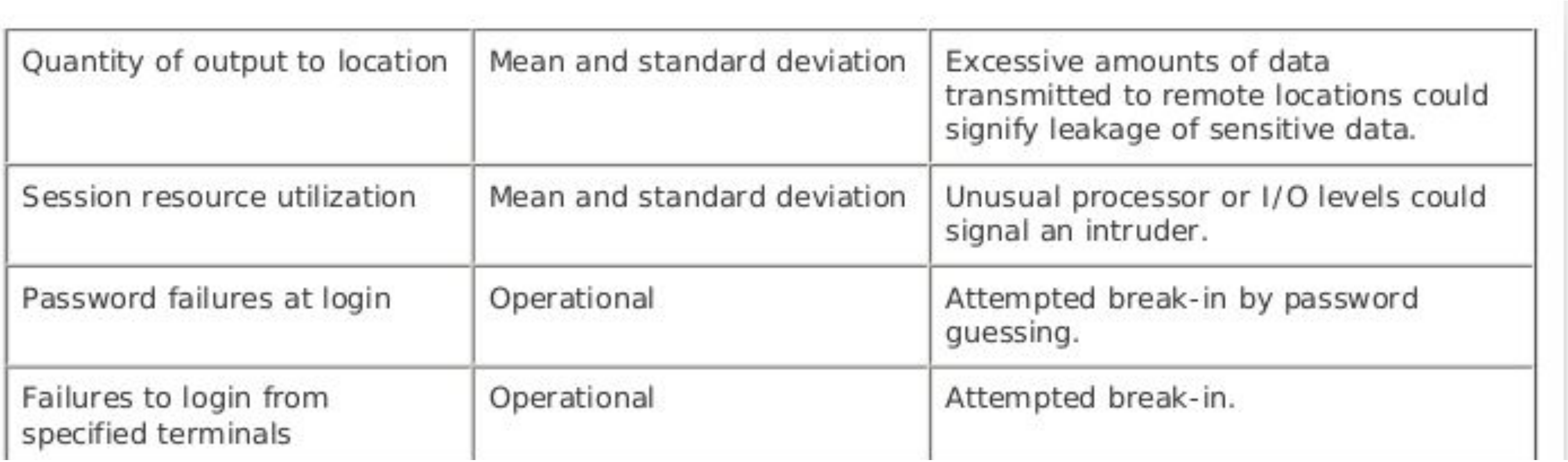
- **A multivariate model : Based on correlations between two or more variables.**
- **A Markov process model : Used to establish transition probabilities among various states.**
- **A time series model : Focuses on time intervals, looking for sequences of events that happen too rapidly or too slowly.**
- **Operational model is based on a judgment of what is considered abnormal, rather than an automated analysis of past audit records.**

Statistical Anomaly Detection - Profile based



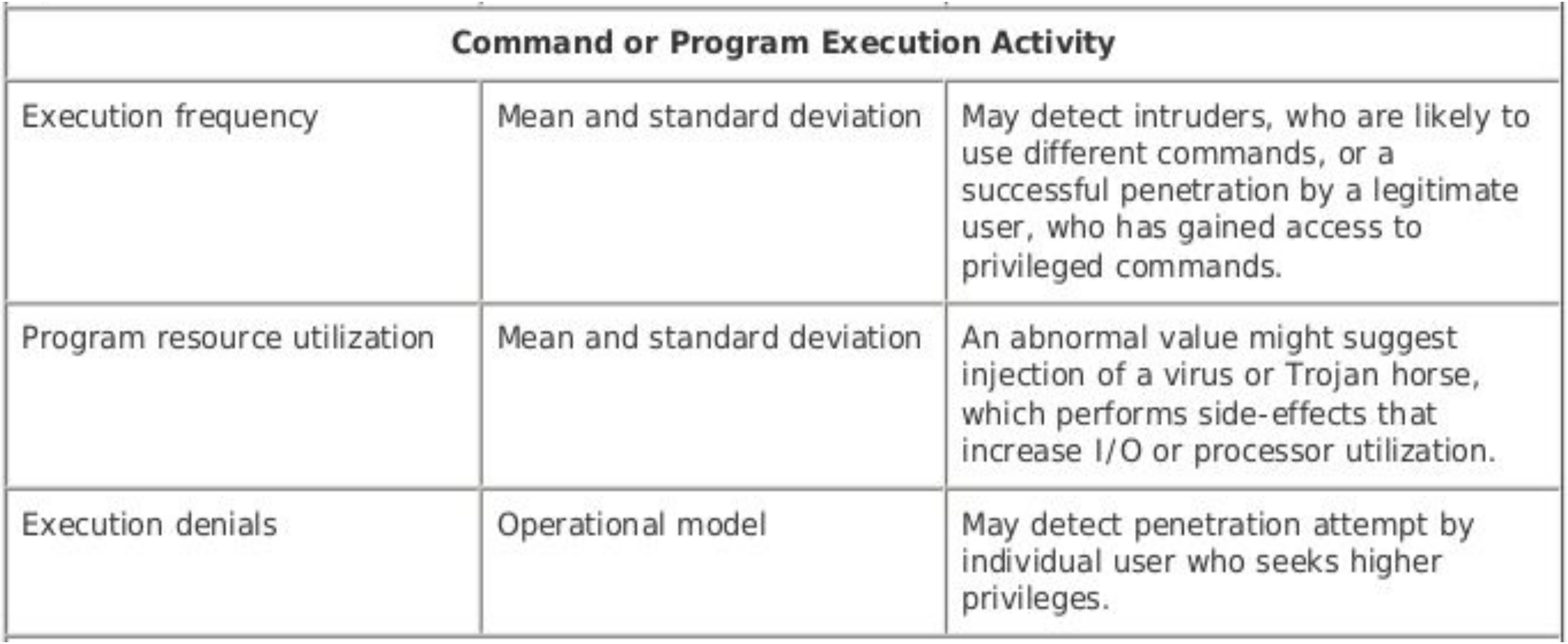
Measure	Model	Type of Intrusion Detected
Login and Session Activity		
Login frequency by day and time	Mean and standard deviation	Intruders may be likely to log in during off-hours.
Frequency of login at different locations	Mean and standard deviation	Intruders may log in from a location that a particular user rarely or never uses.
Time since last login	Operational	Break-in on a "dead" account.
Elapsed time per session	Mean and standard deviation	Significant deviations might indicate masquerader.

Statistical Anomaly Detection - Profile based



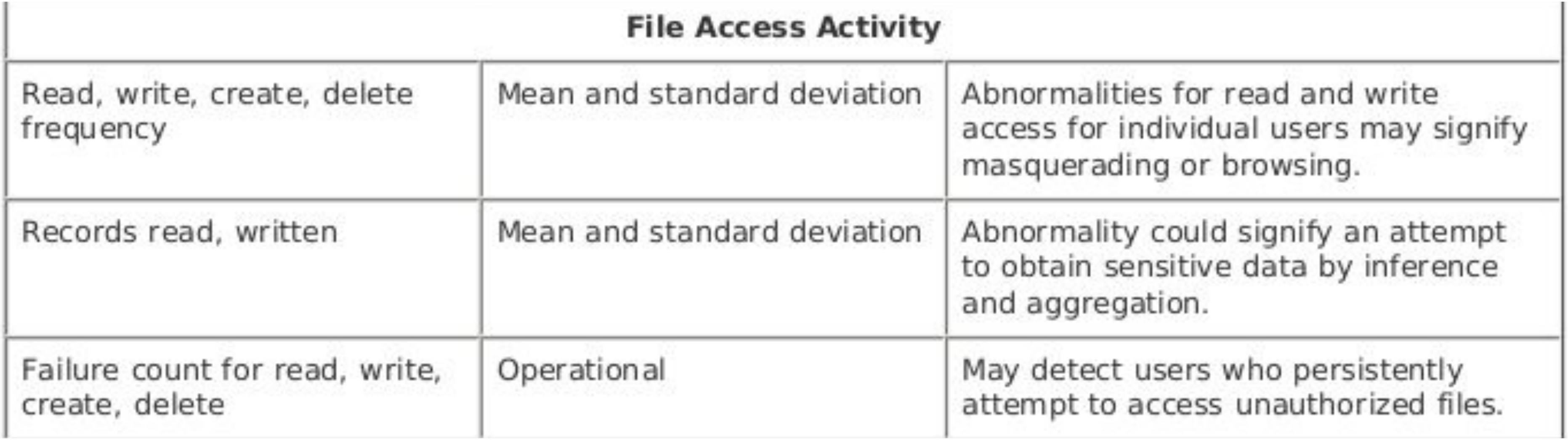
Quantity of output to location	Mean and standard deviation	Excessive amounts of data transmitted to remote locations could signify leakage of sensitive data.
Session resource utilization	Mean and standard deviation	Unusual processor or I/O levels could signal an intruder.
Password failures at login	Operational	Attempted break-in by password guessing.
Failures to login from specified terminals	Operational	Attempted break-in.

Statistical Anomaly Detection - Profile based



Command or Program Execution Activity		
Execution frequency	Mean and standard deviation	May detect intruders, who are likely to use different commands, or a successful penetration by a legitimate user, who has gained access to privileged commands.
Program resource utilization	Mean and standard deviation	An abnormal value might suggest injection of a virus or Trojan horse, which performs side-effects that increase I/O or processor utilization.
Execution denials	Operational model	May detect penetration attempt by individual user who seeks higher privileges.

Statistical Anomaly Detection - Profile based



File Access Activity		
Read, write, create, delete frequency	Mean and standard deviation	Abnormalities for read and write access for individual users may signify masquerading or browsing.
Records read, written	Mean and standard deviation	Abnormality could signify an attempt to obtain sensitive data by inference and aggregation.
Failure count for read, write, create, delete	Operational	May detect users who persistently attempt to access unauthorized files.

Rule-Based Intrusion Detection

Threshold detection & Profile based

Rule-Based Intrusion 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.

- Anomaly detection
- Penetration identification

Rule-Based Intrusion Detection - Anomaly detection

- Rules are developed to detect deviation from previous usage patterns.
- Current behavior is observed, and each transaction is matched against the set of rules to determine if it conforms to any historically observed pattern of behavior.
- A rather large database of rules will be needed. For example, a scheme described in [VACC89] contains anywhere from 10^4 to 10^6 rules.

Rule-Based Intrusion Detection - Penetration identification

- An expert system approach that searches for suspicious behavior.
- Key feature of such systems is the use of rules for identifying known penetrations or penetrations that would exploit known weaknesses.
- Rules used in these systems are specific to the machine and operating system.

Penetration identification - Example Heuristics

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.**

The Base-Rate Fallacy

- To be of practical use, an intrusion detection system should detect a substantial percentage of intrusions while keeping the false alarm rate at an acceptable level.
- If only a modest percentage of actualintrusions are detected, the system provides a false sense of security.
- On the other hand, if the system frequently triggers an alert when there is no intrusion (a false alarm), then either system managers will begin to ignore the alarms, or much time will be wasted analyzing the false alarms.

Distributed Intrusion Detection

- **A more effective defense can be achieved by coordination and cooperation among intrusion detection systems across the network.**

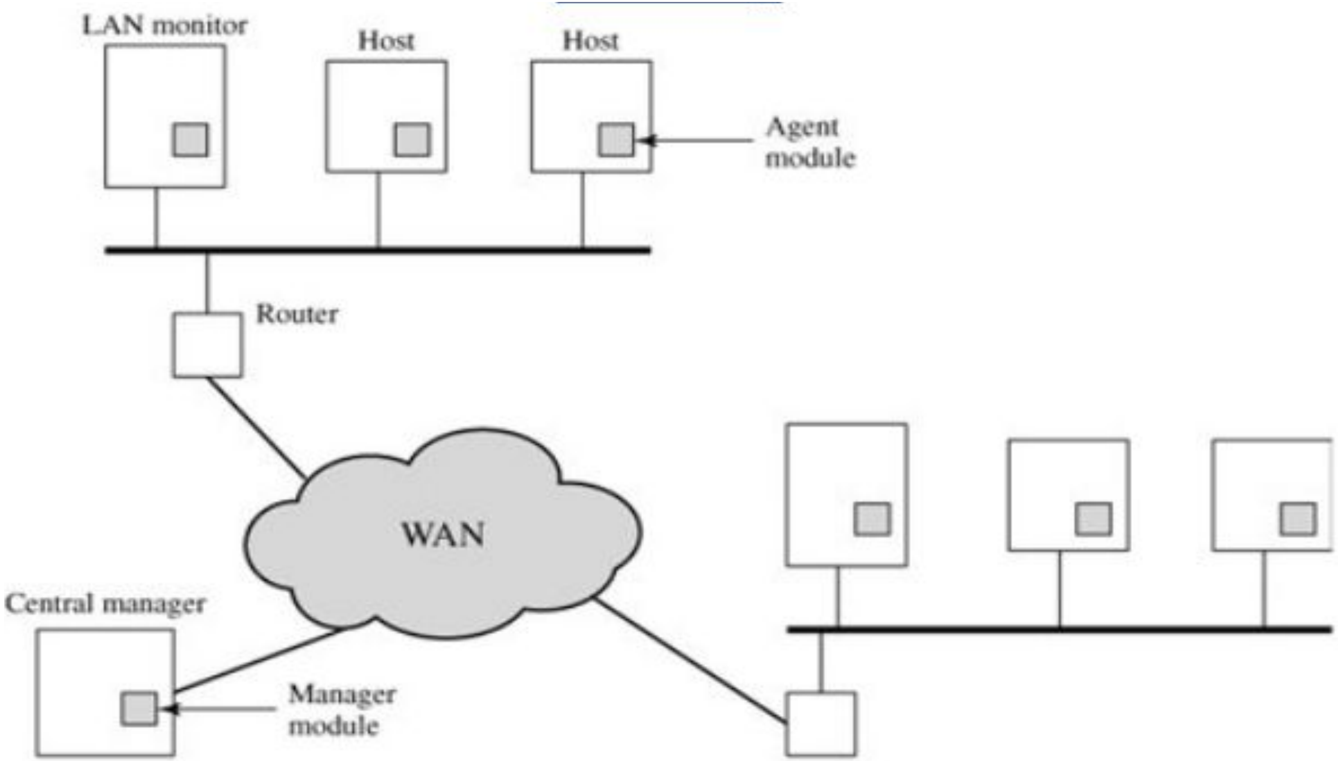
Distributed Intrusion Detection - Challenges

- Different audit record formats.
- One or more nodes in the network will serve as collection and analysis points for the data from the systems on the network. Thus, either raw audit data or summary data must be transmitted across the network.
- Either a centralized or decentralized architecture can be used.

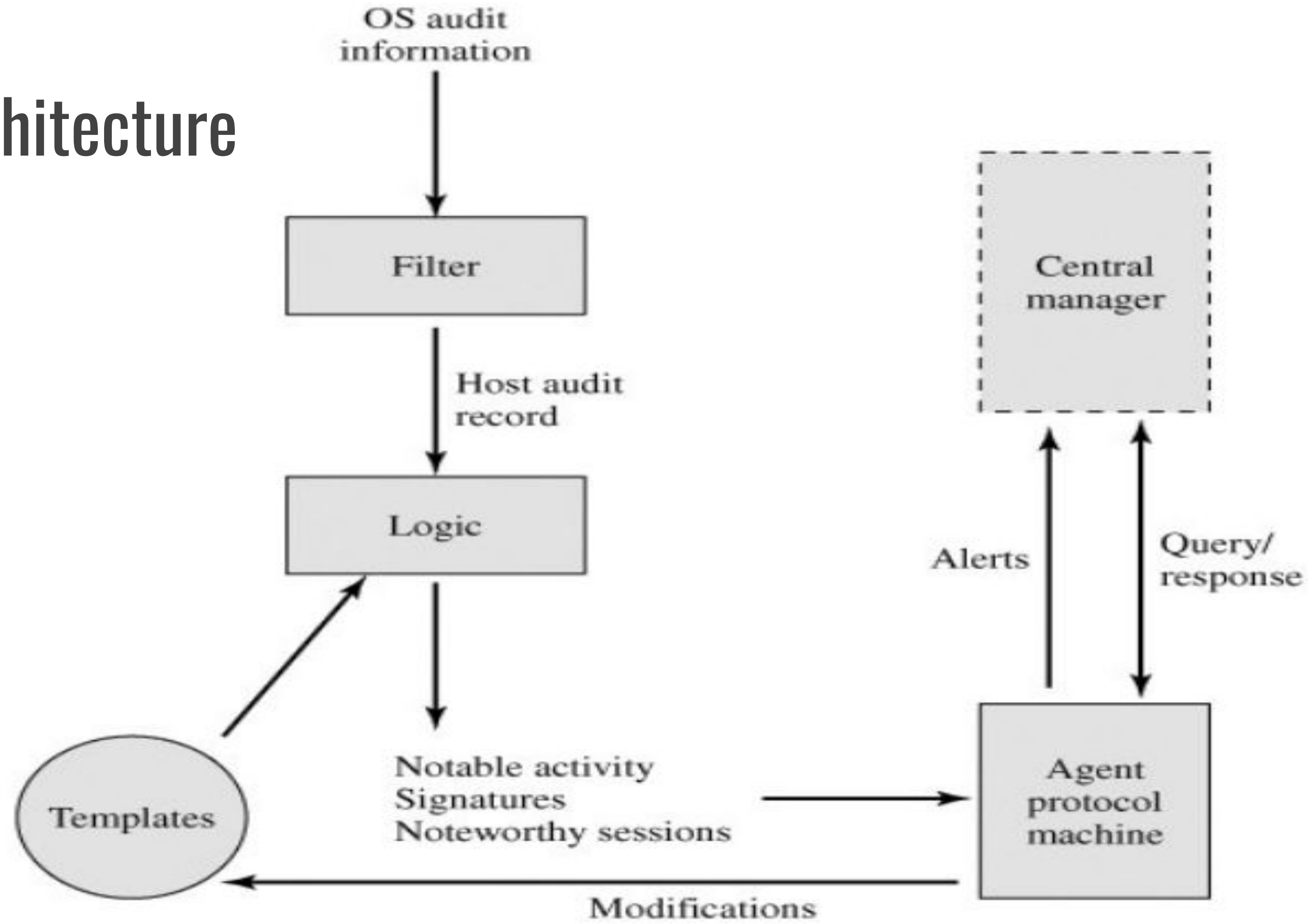
Distributed Intrusion Detection - Main Components

- **Host agent module:**
  - An audit collection module operating as a background process on a monitored system. Its purpose is to collect data on security-related events on the host and transmit these to the central manager.
- **LAN monitor agent module**
  - Operates in the same fashion as a host agent module except that it analyzes LAN traffic and reports the results to the central manager.
- **Central manager module:**
  - Receives reports from LAN monitor and host agents and processes and correlates these reports to detect intrusion.

Distributed Intrusion Detection



Agent Architecture



Honeypots

- Decoy systems that are designed to lure a potential attacker away from critical systems.
- Designed to divert an attacker from accessing critical systems collect information about the attacker's activity encourage the attacker to stay on the system long enough for administrators to respond.
- Filled with fabricated information designed to appear valuable but that a legitimate user of the system wouldn't access.

Intrusion Detection Exchange Format - must include

1. A requirements document
   - Describes the high-level functional requirements for communication between intrusion detection systems
   - Requirements for communication between intrusion detection systems and with management systems, including the rationale for those requirements.
   - Scenarios will be used to illustrate the requirements.

Intrusion Detection Exchange Format - must include

2. **A common intrusion language specification, which describes data formats that satisfy the requirements.**
3. **A framework document, which identifies existing protocols best used for communication between intrusion detection systems, and describes how the devised data formats relate to them.**

Textbook

Cryptography and Network Security Principles and Practices, Fourth Edition

By William Stallings

“Thank you”