Stockholm University

Intrusion Detection

Network Security (NETSEC)

Yuhong Li

Outline

- Intruder and intrusion detection
- Intrusion detection approaches
    - Audit records
    - Statistical anomaly detection
    - Rule-based intrusion detection
    - Distributed intrusion detection
- Honeypots
- Summary

Intruders

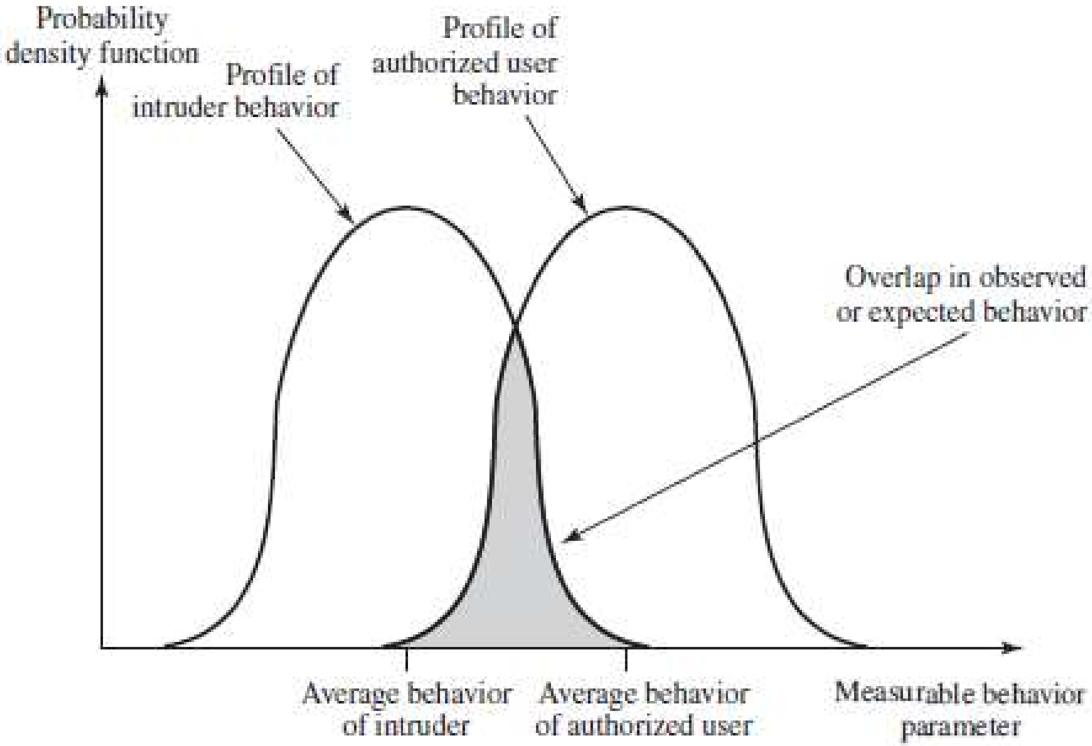
- Hackers
  - Criminals (organized crime)
  - Insiders
  - Corporate competitors

- Objective of intruders: gain access to a system or increase the range of privileges accessible on a system
  - Allow a user to execute code that opens a back door into the system
  - Attempts to acquire information that should have been protected.

Intrusion Detection

- Intrusion prevention: inevitably, the best intrusion prevention system will fail
- Detection: based on the assumption that the behavior of the intruder differs from that of a legitimate user in ways that can be quantified
- Considerations:
  - 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
  - An effective intrusion detection system can serve as a deterrent, so acting to 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

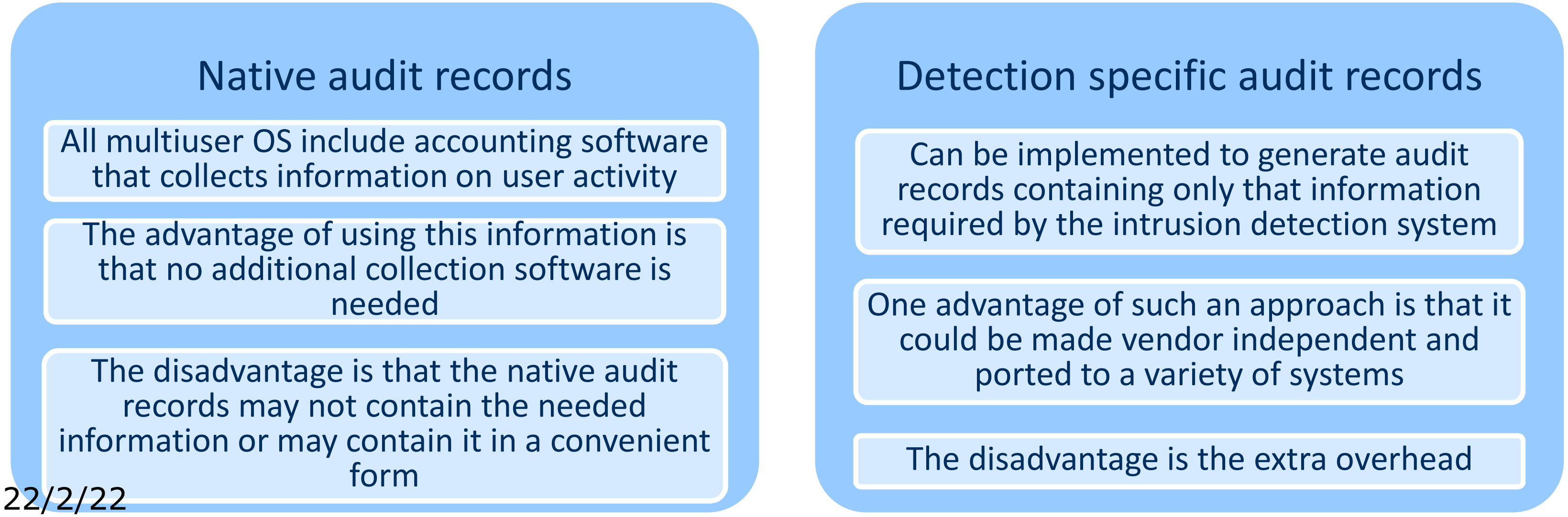

Probability density function
Profile of intruder behavior
Profile of authorized user behavior
Overlap in observed or expected behavior
Average behavior of intruder
Average behavior of authorized user
Measurable behavior parameter

Approaches of Intrusion 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 to observed behavior
  - Threshold detection vs. profile based detection
- Rule-based detection
  - Involves an attempt to define a set of rules or attack patterns that can be used to decide that a given behavior is that of an intruder
  - Anomaly detection vs. penetration identification

Audit Records

- Fundamental tool for intrusion detection
- Some records of ongoing activity by users must be maintained as input to an intrusion detection system. Two plans are used:



Native audit records

All multiuser OS include accounting software that collects information on user activity

The advantage of using this information is that no additional collection software is needed

The disadvantage is that the native audit records may not contain the needed information or may contain it in a convenient form

Detection specific audit records

Can be implemented to generate audit records containing only that information required by the intrusion detection system

One advantage of such an approach is that it could be made vendor independent and ported to a variety of systems

The disadvantage is the extra overhead

Statistical Anomaly Detection

- Threshold detection
  - involves defining thresholds, independent of user, for the frequency of occurrence of various events
  - Ineffective detector. Both the threshold and the time interval must be determined.
  - May generate many “false positives” and “false negatives”
- Profile-based
  - Focuses on characterizing the past behavior of individual users or related groups of users and then detecting significant deviations
  - A profile may consist of a set of parameters, deviation on just a single, parameter may not be sufficient in itself to signal an alert
  - Audit records serve to define typical behavior
- Advantages: learning the behaviors, no prior knowledge of security flaws is required.

Rule-based Anomaly Detection

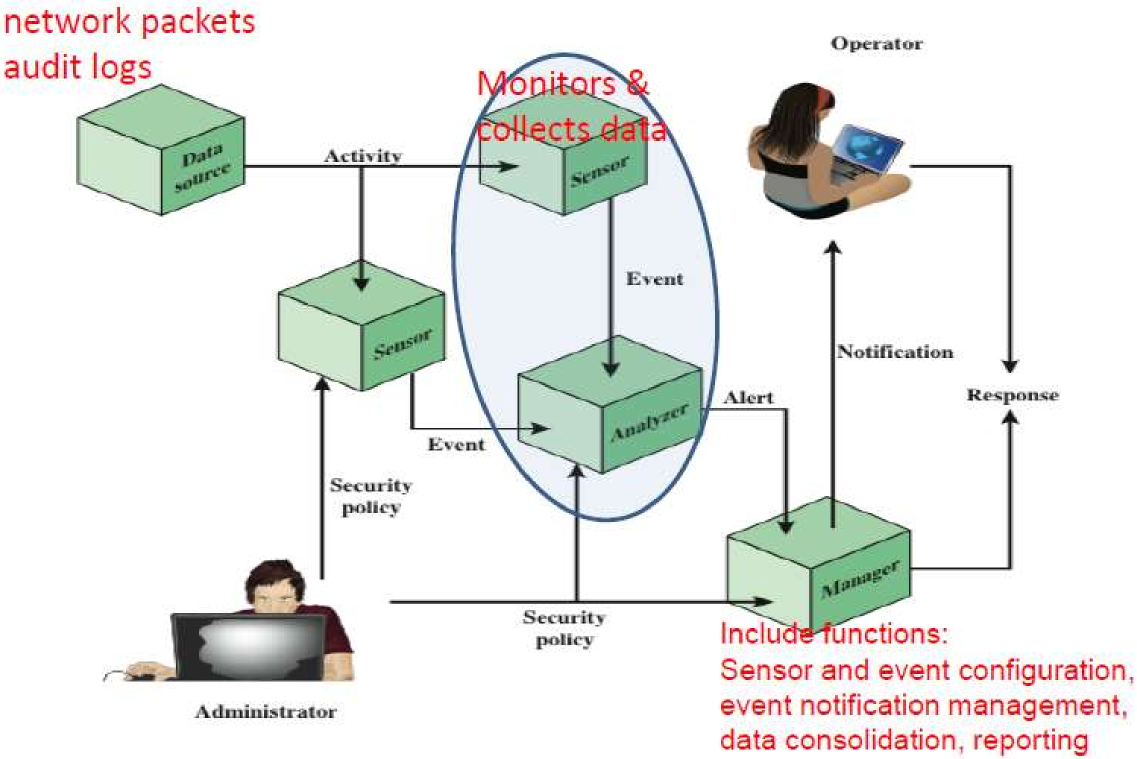
- Detects intrusion by observing events in the system
- Applying a set of rules that lead to a decision regarding whether a given pattern of activity is or is not suspicious
- Detection is similar to statistical anomaly detection (in terms of its approach and strengths)
  - Historical audit records are analyzed to identify usage patterns and to automatically generate rules that describe those patterns
  - Current behavior is then observed, and each transaction is matched against the set of rules to determine if it conforms to any historically observed pattern of behavior
  - In order for this approach to be effective, a rather large database of rules will be needed

Rule-based Penetration Identification

- Rule-based penetration identification
  - Use rules for identifying known penetrations or penetrations that would exploit known weaknesses
- The best approach to develop such rules is to
  - Analyze attack tools and scripts collected on the Internet
  - Interview knowledgeable security personnel
- Audit records are examined as they generated, and matched against the rule base
  - If match is found then user’s suspicion rating is increased.
  - If enough rules matched->rating pass threshold->report anomaly

Elements of IDS

- Information collecting
- Information analyzing
- Alert/event notification, response



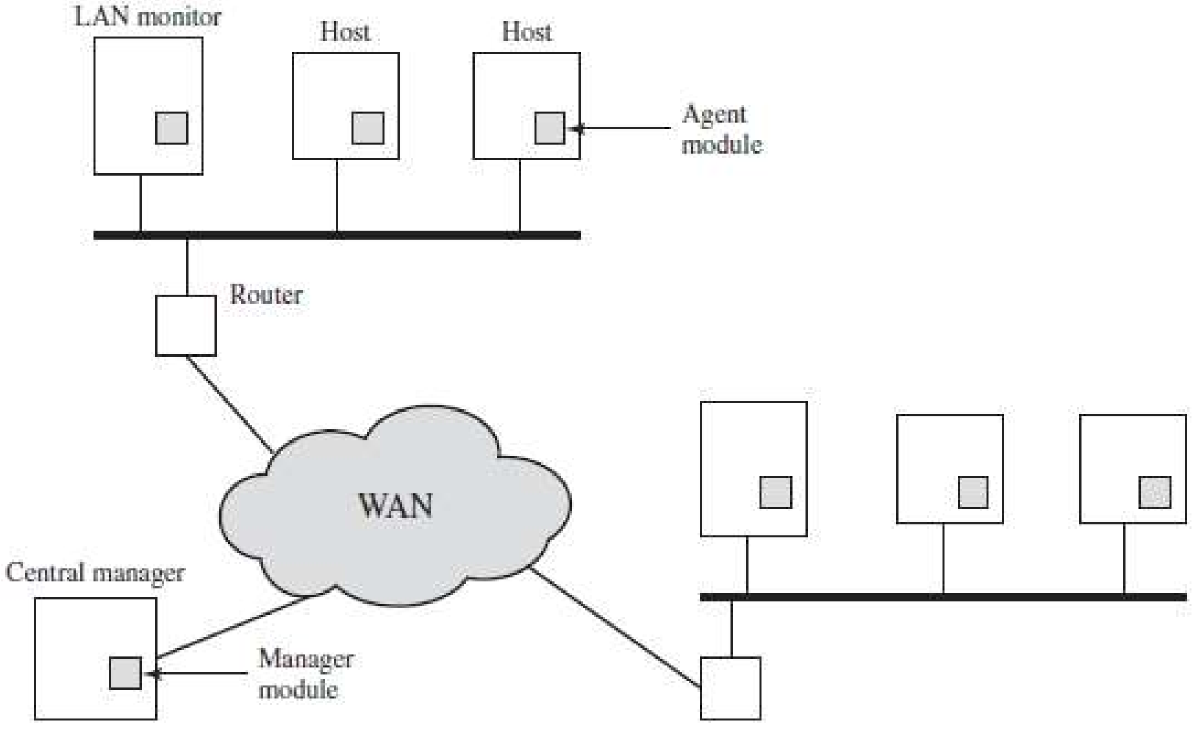
Include functions:
Sensor and event configuration, event notification management, data consolidation, reporting

2022/2/22

Distributed Intrusion Detection

- Traditional systems focused on single-system stand-alone facilities
- The typical organization needs to defend a distributed collection of hosts supported by a LAN or internetwork
- A more effective defense can be achieved by coordination and cooperation among intrusion detection systems across the network
- Major design issues:
  - A distributed intrusion detection system may need to deal with 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. Raw audit data or summary data must be transmitted across the network ➡ integrity and confidentiality is required!
  - Either a centralized or decentralized architecture can be used

Architecture for Distributed Intrusion Detection – an Example



2022/2/22

Honeypots

- Fake systems that are designed to fool a potential attacker away from critical systems
- Has no production value
  - These systems are filled with fabricated information designed to appear valuable but that a legitimate user of the system wouldn’t access
  - Any attempt to communicate with the system is most likely a probe, scan, or attack
- Designed to:
  - Distract/draw away 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

Strength and Limitations

- Improve with the increase of the knowing models/problems (knowledge base)

- Attackers: trying to avoid IDS. ->IDS must be very well done, otherwise, useless.
- Sensitivity: difficult to measure and adjust

Summary

- Intrusion detection can detect unusual patterns of activity or patterns of activity that are known to correlate with intrusions
- IDS is used to provide early warning of an intrusion so that defensive action can be taken to prevent or minimize damage.

Expected Learning Outcomes

- Understand and explain the principles of intrusion detection
- Understand and explain the principles of different intrusion detection methods
- Describe the functions of IDS and the functions of each element constructing the IDS and distributed IDS
- Design a basic IDS according to certain requirements

Thank you!

References

1. Chapter 11 W. Stallings
2. Firewalls and Internet Security. 2ndEd., W.R.Cheswick, S.M. Bellovin, A.D. Rubin