0790326
Intrusion Detection and Prevention Systems

2023/2024 – Semester 2

Week 9

21st and 23rd April 2024

جامعة فيلادلفيا
Philadelphia University

Dr. Basil Elmasri
balmasri@philadelphia.edu.jo

External Material

- Rest of the slides for this week are based on (Stallings & Brown, 2024) book, chapter 8.
  - Footers, dates, and slides number have been added only to help students reading the material.
- Study and exams will be based on the book chapters, not the slides.

Intruder Behavior

- Target acquisition and information gathering
- Initial access
- Privilege escalation
- Information gathering or system exploit
- Maintaining access
- Covering tracks

Table 8.1 (1 of 4)

Examples of Intruder Behavior

(a) Target Acquisition and Information Gathering

- Explore corporate website for information on corporate structure, personnel, key systems, and details of specific Web server and OS used.
- Gather information on target network using DNS lookup tools such as dig, host, and others and query WHOIS database. (https://who.is/).
  - See https://www.shodan.io/ for IoT.
- Map network for accessible services using tools such as NMAP.
- Send query e-mail to customer service contact, review response for information on mail client, server, OS used, and details of person responding.
- Identify potentially vulnerable services, for example, vulnerable Web CMS.

Table 8.1 (2 of 4)

Examples of Intruder Behavior

(b) Initial Access

- Brute force (guess) a user's Web Content Management System (CMS) password.
- Exploit vulnerability in Web CMS plugin to gain system access.
- Send spear-phishing e-mail with link to Web browser exploit to key people.

(c) Privilege Escalation

- Scan system for applications with local exploit.
- Exploit any vulnerable application to gain elevated privileges.
- Install sniffers to capture administrator passwords.
- Use captured administrator password to access privileged information.

Table 8.1 (3 of 4)

Examples of Intruder Behavior

(d) Information Gathering or System Exploit

- Scan files for desired information.
- Transfer large numbers of documents to external repository.
- Use guessed or captured passwords to access other servers on network.

(e) Maintaining Access

- Install remote administration tool or rootkit with backdoor for later access.
- Use administrator password to access network later.
- Modify or disable anti-virus or IDS programs running on system.

Table 8.1 (4 of 4)

Examples of Intruder Behavior

(f) Covering Tracks

- Use rootkit to hide files installed on system.
- Edit logfiles to remove entries generated during the intrusion.

Key Element of Intrusion

- Use of guessed credentials to allow the attackers to move between systems
  - Attackers use a range of tools to access temporarily stored credentials that can be accessed using some previously compromised account
  - These are often not well protected

Recent Trends of Intrusion (1 of 3)

- Ransomware
  - Attackers target organizations with a broad network of users in a supply-chain attack
  - The 2021 attack on Colonial Pipeline in the U.S. caused serious fuel short-ages in parts of the country
  - The company paid the requested ransom of around $4.4 million to gain access to the recovery tool
  - Paying ransom means the attackers have succeeded, while not paying may result in the organization losing significant value

Recent Trends of Intrusion (2 of 3)

- Supply-chain attacks
  - Attacker targets an organization that provides key software or services to a large number of other customers and then targets those customers through the compromised software or services
  - In SolarWinds attack, the attackers first compromised the update mechanism in SolarWinds popular network monitoring product “Orion” to deliver a backdoor trojan to more than 18,000 customers
  - These attacks are hard to prevent and detect

Recent Trends of Intrusion (3 of 3)

- Business E-mail Compromise (BEC)
  - Cybercriminals compromise a business or personal e-mail account and impersonate a trusted supplier or business representative to scam victims
  - Can often evade security and technical controls
  - Often directed at smaller or medium size businesses with less sophisticated IT security systems

Definitions

- Security Intrusion:
  - Unauthorized act of bypassing the security mechanisms of a system
- Intrusion Detection:
  - A hardware or software function that gathers and analyzes information from various areas within a computer or a network to identify possible security intrusions

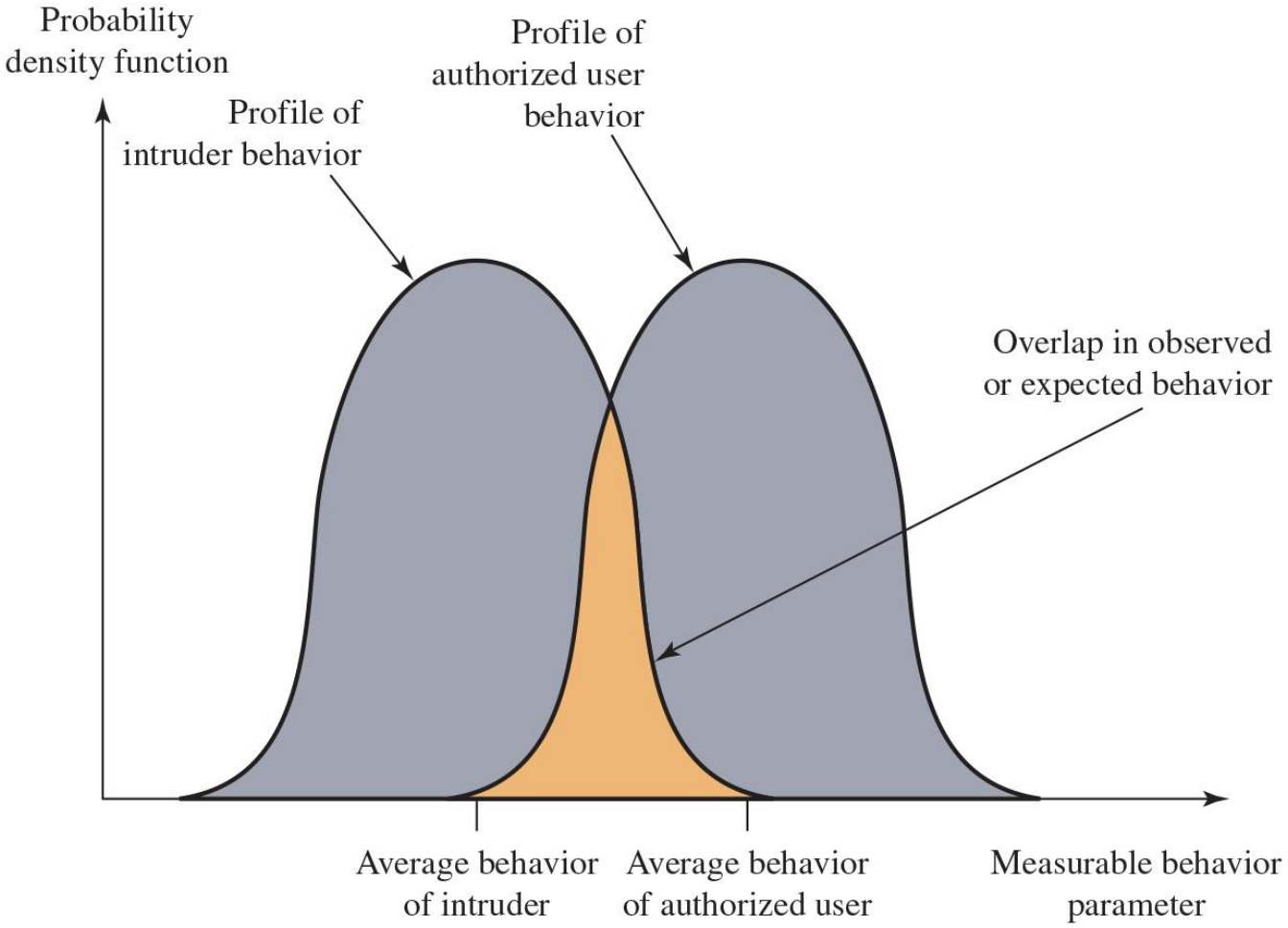
Intrusion Detection System (IDS)

- Host-based IDS (HIDS)
  - Monitors the characteristics of a single host for suspicious activity
- Network-based IDS (NIDS)
  - Monitors network traffic and analyzes network, transport, and application protocols to identify suspicious activity
- Distributed or hybrid IDS
  - Combines information from a number of sensors, often both host- and network-based, in a central analyzer that is able to better identify and respond to intrusion activity

- Comprises three logical components:
  - Sensors - collect data
  - Analyzers - determine if intrusion has occurred
  - User interface - view output or control system behavior

Figure 8.1

Profiles of Behavior of Intruders and Authorized Users



IDS Requirements

- Run continually
- Be fault tolerant
- Resist subversion
- Impose a minimal overhead on system
- Configured according to system security policies
- Adapt to changes in systems and users
- Scale to monitor large numbers of systems
- Provide graceful degradation of service
- Allow dynamic reconfiguration

Analysis Approaches

Anomaly detection

- Involves the collection of data relating to the behavior of legitimate users over a period of time
- Current observed behavior is analyzed to determine whether this behavior is that of a legitimate user or that of an intruder

Signature/heuristic detection

- Uses a set of known malicious data patterns or attack rules that are compared with current behavior
- Also known as misuse detection
- Can only identify known attacks for which it has patterns or rules

Anomaly Detection

- A variety of classification approaches are used:
  - Statistical
    - Analysis of the observed behavior using univariate, multivariate, or time-series models of observed metrics
  - Knowledge based
    - Approaches use an expert system that classifies observed behavior according to a set of rules that model legitimate behavior
  - Machine-learning
    - Approaches automatically determine a suitable classification model from the training data using data mining techniques

Machine-learning Approaches (I)

- Bayesian networks: Encode probabilistic relationships among observed metrics.
  - See Appendix I for more information.
    - Appendix I is NOT examinable.
- Markov models: Develop a model with sets of states, some possibly hidden, interconnected by transition probabilities.
- Neural networks: Simulate human brain operation with neurons and synapses between them to classify observed data.

Machine-learning Approaches (II)

- Fuzzy logic: Uses fuzzy set theory, in which reasoning is approximate and can accommodate uncertainty.
- Genetic algorithms: Uses techniques inspired by evolutionary biology, including inheritance, mutation, selection, and recombination, to develop classification rules.
- Clustering and outlier detection: Group the observed data into clusters based on some similarity or distance measure and then identify subsequent data either as belonging to a cluster or as outliers.

Signature or Heuristic Detection

- **Signature approaches**
  - Match a large collection of known patterns of malicious data against data stored on a system or in transit over a network
  - The signatures need to be large enough to minimize the false alarm rate while still detecting a sufficiently large fraction of malicious data
  - Widely used in anti-virus products, network traffic scanning proxies, and NIDS
- **Rule-based heuristic identification**
  - Involves the use of rules for identifying known penetrations or penetrations that would exploit known weaknesses
  - Rules that identify suspicious behavior can also be defined, even when the behavior is within the bounds of established patterns of usage
  - Typically rules used are specific
  - SNORT is an example of a rule-based NIDS

Host-Based Intrusion Detection (HIDS)

- Adds a specialized layer of security software to vulnerable or sensitive systems
- Can use either anomaly or signature and heuristic approaches
- Monitors activity to detect suspicious behavior
  - Primary purpose is to detect intrusions, log suspicious events, and send alerts
  - Can detect both external and internal intrusions

Data Sources and Sensors

- A fundamental component of intrusion detection is the sensor that collects data
- Common data sources include:
  - System call traces
  - Audit (log file) records
  - File integrity checksums
  - Registry access

References

Stallings, W., & Brown, L. (2024). Computer Security: Principles and Practice (5 ed.). Pearson. Retrieved from https://www.pearson.com/en-us/subject-catalog/p/computer-security-principles-and-practice/P200000010333/9780138091712