İTÜ

Computer Security

Intrusion Detection Systems

Dr. Şerif Bahtiyar
bahtiyars@itu.edu.tr

1

Before Starting

US bans sale of Huawei, ZTE tech amid security fears

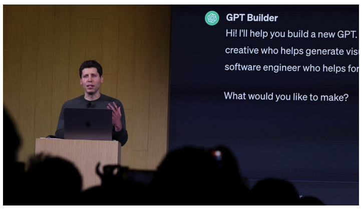
The US has banned the sale and import of new communications equipment from five Chinese companies, including Huawei and ZTE, amid concerns over national security.

https://www.bbc.com/news/world-us-canada-63764450

2

Before Starting

ChatGPT tool could be abused by scammers and hackers


GPT Builder
Hi! I'll help you build a new GPT.
creative who helps generate vis
software engineer who helps for
What would you like to make?

A ChatGPT feature allowing users to easily build their own artificial-intelligence assistants can be used to create tools for cyber-crime, a BBC News investigation has revealed.

https://www.bbc.com/news/technology-67614065

3

Outline

- Problems in Networks
- Intruders
- Intrusion Detection
- Intrusion Analysis
- Host-Based Intrusion Detection
- Network-Based Intrusion Detection
- Distributed Adaptive Intrusion Detection
- Honeypots

4

Problems in Networks

Some security problems in networks depend on hostile or unwanted trespass by user or software.

- User trespass**:** unauthorized logon, acquisition of privileges beyond those have been authorized
- Software trespass**:** virus, worm, Trojan….

5

Intruders

- Intruders are referred as hacker or cracker.
- Classes of intruders origin:
  - Masquerader: not authorized to use resources but penetrate access control to exploit a legitimate user’s account (outsider)
  - Misfeasor**:** A legitimate user who misuses his or her privileges (insider)
  - Clandestine user: A user who seizes supervisory control and uses this to evade auditing and access controls (outsider or insider)
- Intruder attacks range from benign to the serious.

6

Intruders

Classes of intruders by motivation:

- Cyber Criminals are either individuals or members of an organized crime group with a goal of financial reward.
- Activists are either individuals or members of a larger group of outsider attackers, who are motivated by social or political causes. (known as hacktivists)
- State sponsored organizations are groups of hackers sponsored by governments to conduct espionage or sabotage activities. (known as Advanced Persistent Threats, APTs)
- Others are hackers who have many classical hack motivations, such as hobby hackers.

7

Intruders

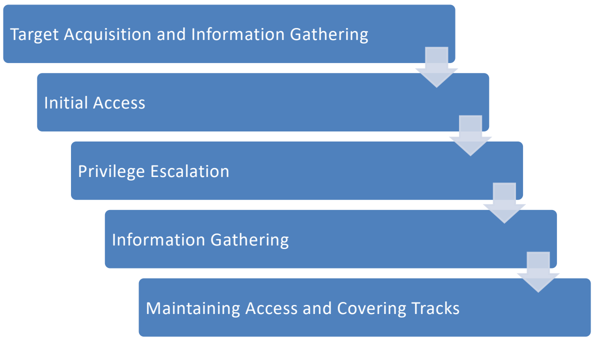
Classes of intruders by skill levels:

- Apprentice: Hackers with minimal technical skill who primarily use existing attack tools.
- Journeyman: Hackers with sufficient technical skills to modify and extend attack toolkits to use newly discovered vulnerabilities or to focus on different target groups.
- Master: Hackers with high-level technical skills capable of discovering brand new categories of vulnerabilities or writing new powerful attack toolkits.

8

Intruders

Intruder Behavior


Target Acquisition and Information Gathering

Initial Access

Privilege Escalation

Information Gathering

Maintaining Access and Covering Tracks

9

Intruders

Some examples of hacker behavior patterns

- Select target using IP lookup tools, NSLookup
- Map network for accessible services, NMAP
- Identify vulnerable services
- Guess passwords, pcAnywhere
- Install remote administration tools, DameWare

10

Intruders

Some intrusions

- Remote root compromise
- Web server defacement
- Password cracking or guessing
- Copying credit card numbers from a database
- Running a sniffer

11

Intruders

Hackers

- Those who hack into systems often motivated by thrill of access and status
  - Hacking community is a strong meritocracy
  - Status is determined by level of competence
- Benign intrudes consume resources and may decrease performance
- There is no way to know whether an intruder will be benign or malign
- IDS, IPS, and VPN are used to counter

12

Intruders

Criminals

- Organized group of hackers
- May be employed by a cooperation and government
- Common target is a credit card file at an e-commerce server
- The difference between traditional hacker and criminal hacker
  - Traditional hackers look for targets of opportunity
  - Criminal hackers have specific targets
- Once penetrated act quickly and get out
- IDS and IPS are less effective
- Sensitive data need strong protection

13

Intruders

Some criminal enterprise behavior

- Act quickly and precisely to make harder to detect
- Exploit perimeter via vulnerable ports
- Use Trojan horses to leave backdoors for reentry
- Use sniffer to capture passwords
- Make few or no mistake

14

Intruders

Insider Attacks

- Most difficult to detect and prevent
- Employees have access and knowledge
- May be motivated by revenge
  - When employment terminated
  - Taking customer data when move to competitor
- IDS and IPS may help but needs least privilege, monitor logs, strong authentication, after termination delete access,…

15

Intruders

Examples of insider behavior

- Create network accounts for themselves and friends
- Access accounts and applications they wouldn't normally use for their daily jobs.
- Conduct secret instant messaging chat
- Visit web sites that provide to dissatisfied employees
- Perform large downloads and copying
- Access the network during off hours

16

Intruders

Intrusion Techniques

- Objective is to gain access or increase privileges
- Initial attacks exploits vulnerabilities to execute code to get backdoor, such as buffer overflow
- Gain protected information such as passwords

17

Intrusion Detection

- Security Intrusion: A security event or a combination of multiple security events that constitutes a security incident in which an intruder gains, or attempts to gain, access to a system without having authorization to do so.
- Intrusion Detection: A security service that monitors and analyzes system events for the purpose of finding, and providing real-time or near real time warning of, attempts to access system resources in an unauthorized manner.

18

Intrusion Detection

IDS classification

- Host-based IDS: monitors single host characteristics and activities
- Network-based IDS: monitors network traffic and activity

IDS logical components

- Sensors: collect data (log files, network packets, system call traces,..)
- Analyzers: determine if an intrusion has occurred by receiving data from sensors.
- User interface: view output of system and control IDS

Intrusion Detection

IDS principles

- Detect quickly enough to identify intruder-> less damage
- Deterrent (caydırıcı) -> prevent intrusions
- Determine intrusion techniques -> strengthen intrusion prevention

Intrusion Detection

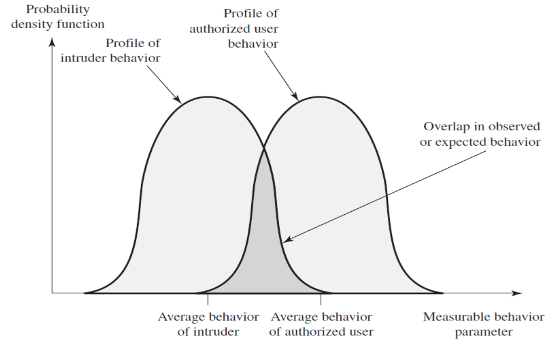


Figure 8.1 Profiles of Behavior of Intruders and Authorized Users

Intrusion Detection

Assumes intruder behavior differs from legitimate user

- Expect overlap
- Observe deviations from history
- Problems
  - False positives (authorized users identified as intruders)
  - False negatives (intruders not identified)

Intrusion Detection

IDS requirements

- Run continually
- Be fault tolerant
- Resist subversion
- Impose minimal overhead
- Configured according to security policy
- Adapt changes in system and users
- Monitor large number of hosts
- Graceful degradation of service (damaged components have less effects on IDS)
- Dynamic reconfiguration (no need restart)

Intrusion Analysis

Audit Records

- A fundamental tool for intrusion detection
- Variants
  - Native: provided by OS and collects information on user activity
    - Advantage: no additional software is needed
    - Disadvantage: may not contain the needed information
  - Detection-specific: IDS specific
    - Advantage: vendor independent and ported to a other systems
    - Disadvantage: extra overhead

Intrusion Analysis

Anomaly detection (statistically anomaly detection)

- Threshold detection
  - involves counting the number of occurrence of a specific event over an interval of time
  - crude and ineffective for sophisticated attacks
  - may be useful in conjunction with more sophisticated techniques.
- Profile based
  - Characterizes past behaviors of users or groups
  - Detect significant deviations
  - Uses analysis of audit records, such as gather metrics (counter and interval time), analyze (mean and standard deviation, markov process, time series)

Intrusion Analysis

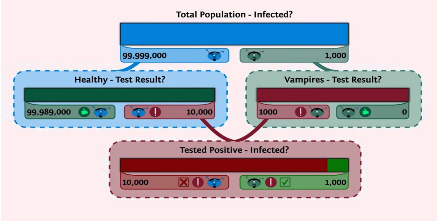
Signature Detection

- Detects intrusions by observing events and applying a set of rules
- Approaches
  - Rule-based anomaly detection
    - Historical records are analyzed to identify usage patterns and generate automatically rules
    - Does not require knowledge of security vulnerabilities (**statistically anomaly detection require!**)
  - Rule-based penetration identification
    - Use rules for identifying known penetrations and weaknesses
    - Often by analyzing attack script from Internet
    - Supplemented with rules from security experts

Intrusion Analysis

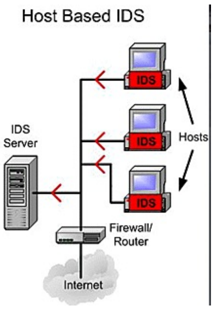
Base-rate fallacy

If the actual number of intrusions is low compared to the number of legitimate uses of a system, then the false alarm rate will be high unless the test is extremely discriminating.



Host-Based Intrusion Detection

- Host-based IDSs add a specialized layer of security software to monitor system activity to detect suspicious behavior.



- The primary benefit of host-based IDS is to detect both external and internal intrusions.

Host-Based Intrusion Detection

Host-Based IDS Approaches

- Anomaly detection: defines normal/expected behavior
  - Threshold detection
  - Profile based
  - Effective against masqueraders but not for misfeasors
- Signature detection: defines proper behavior
  - May be used against misfeasors

Host-Based Intrusion Detection

- Traditionally, host-based IDS focuses on single system stand-alone facilities -> needs to defend distributed collection of host in an organization.
- A more effective defense can be achieved by coordination and cooperation among IDSs across the network.
- Design issues of distributed host-based IDS
  - Different audit record formats
  - Collection point of network (confidentiality and integrity must be preserved)
  - Centralized versus decentralized architecture

Host-Based Intrusion Detection

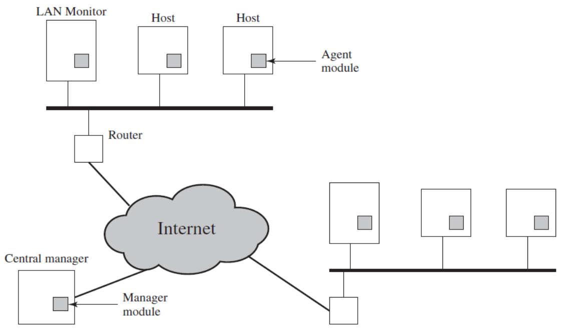


Figure 8.2 Architecture for Distributed Intrusion Detection

31

Host-Based Intrusion Detection

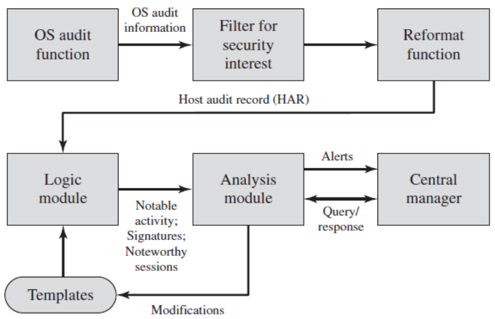


Figure 8.3 Agent Architecture

32

Network-Based Intrusion Detection

- A Network-Based IDS (NIDS)
  - monitors traffic at selected points on a network
  - examines the traffic packet by packet in real time or close to real time to detect intrusion patterns
  - examines network, transport, and application level protocol activity
- Host-Based IDS versus Network-Based IDS
  - NIDS examines packet traffic directed toward potentially vulnerable computer system on a network.
  - A host-based system examines user and software activity on a host.

33

Network-Based Intrusion Detection

- Comprises on a number of sensors
  - Inline sensor (possibly a part of a network device)
  - Passive sensor (monitors copy of traffic)
- Logging of alerts: When a sensor detects a potential violation, it sends an alert and logs information related to the event. -> NIDS analysis module uses this information.

34

Network-Based Intrusion Detection

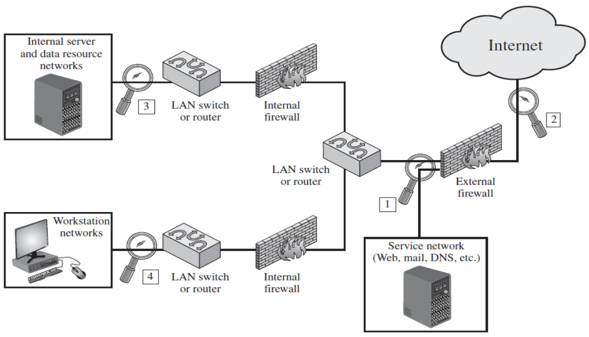


Figure 8.5 Example of NIDS Sensor Deployment

35

Network-Based Intrusion Detection

Intrusion Detection Techniques

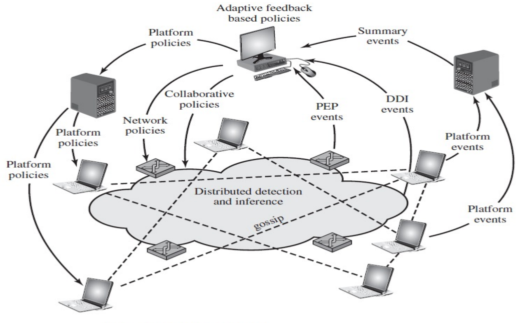
- Signature Detection
  - Application layer (DHCP, DNS, FTP,…)
  - Transport layer (TCP, UDP, ..)
  - Network layer (IP, ICMP,..)
  - Unexpected application services
  - Policy violations (inappropriate Web sites)
- Anomaly Detection
  - Denial-of-service (DoS) attacks
  - Scanning
  - Worms

36

Distributed Adaptive Intrusion Detection

- The concept of communicating IDSs has evolved to schemes that involve distributed systems that cooperate to identify intrusions and to adapt to changing attack profiles.
- In an adaptive cooperative system, a local node uses a peer-to-peer "gossip" protocol to inform other machines of its suspicion, in the form of probability that the network is under attack.

Distributed Adaptive Intrusion Detection



PEP = policy enforcement point
DDI = distributed detection and inference

Figure 8.6 **Overall Architecture of an Autonomic Enterprise Security System**

Honeypots

Honeypots are decoy systems that are designed to lure a potential attacker away from critical systems.

- Filled with fabricated information
- A legitimate user of the system wouldn't access.
- Instrumented with sensitive monitors and event loggers
- Information has no productive value

Honeypots

- If a honeypot initiates outbound communication, the system has probably been compromised.
- Honeypots are 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

Honeypots

Classification of Honeypots

- Low interaction honeypots
  - Consists of software package
  - Emulates particular IT services
  - Does not execute full version of services
- High interaction honeypots
  - Is a real system
  - Full OS, services and applications

Honeypots

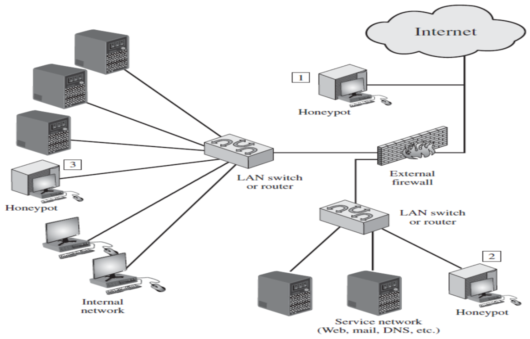
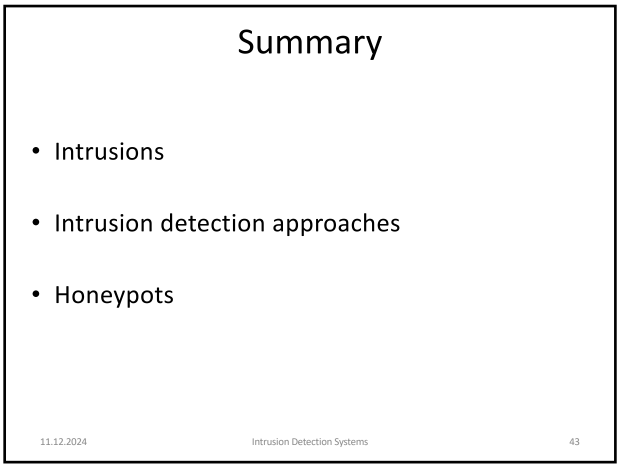


Figure 8.8 **Example of Honeypot Deployment**



Summary

- Intrusions
- Intrusion detection approaches
- Honeypots

43