



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

ACCA5034

Data Security and Compliance

Week 8 : Intrusion Detection and Prevention Systems, and Other Security Tools

Trawsnewid Addysg; Trawsnewid Bywydau
Transforming Education; Transforming Lives



www.uwtsd.ac.uk

Learning Objective(s) and Key Concepts

Learning Objective(s)

- Identify and describe the categories and models of Intrusion Detection and Prevention Systems (IDPS).
- Describe the detection approaches used in modern IDPS.
- Define and explain honeypots, honeynets, and padded cell systems.
- List and define the major categories of scanning and analysis tools and their specific uses.

• Key Concepts

- IPS and IDS
- Honeypots, Honeynets and padded cell systems

Information Security Protection

- Managerial controls are as crucial as technical safeguards in protecting organisational assets.
- Policy-driven technical solutions are essential for effective security.
- Advanced technologies enhance information asset protection.

Intrusion Detection and Prevention Systems

- An intrusion occurs when an attacker attempts to gain entry into or disrupt the normal operations of an organisation's information systems.
- Intrusion prevention consists of activities that deter an intrusion.
- Intrusion detection consists of procedures and systems that identify system intrusions.
- Intrusion reaction encompasses actions an organisation undertakes when intrusion event is detected

Intrusion Detection and Prevention Systems

- Intrusion correction activities complete restoration of operations to a normal state and seek to identify source and method of intrusion.
- Intrusion detection systems detect a violation of its configuration and activate alarm.
- Many IDPSs enable administrators to configure systems to notify them directly of trouble via e-mail or pagers.
- Systems can also be configured to notify an external security service organisation of a “break-in”.

Intrusion Detection Systems

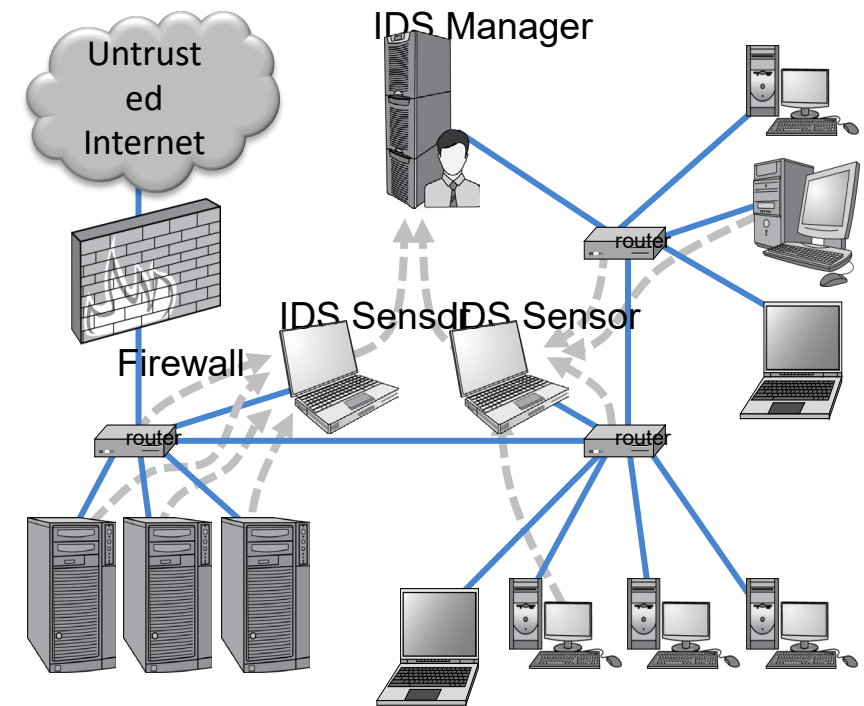
- **Intrusion**
 - Actions aimed at compromising the security of the target (confidentiality, integrity, availability of computing/networking resources)
- **Intrusion detection**
 - The identification through intrusion signatures and report of intrusion activities
- **Intrusion prevention**
 - The process of both detecting intrusion activities and managing automatic responsive actions throughout the network

Intrusion Detection Systems

- **Intrusion:** Unauthorised access or disruption of an organisation's systems.
- **Prevention:** Measures taken to deter intrusions.
- **Detection:** Systems and procedures identifying intrusions.
- **Reaction:** Actions taken in response to an intrusion.
- **Correction:** Restoring normal operations and identifying the attack source.
- **IDPS Alerts:** Detect violations, trigger alarms, and notify administrators or external security services.

IDS Components

- The **IDS manager** compiles data from the IDS sensors to determine if an intrusion has occurred.
- This determination is based on a set of **site policies**, which are rules and conditions that define probable intrusions.
- If an IDS manager detects an intrusion, then it sounds an **alarm**.



Intrusions

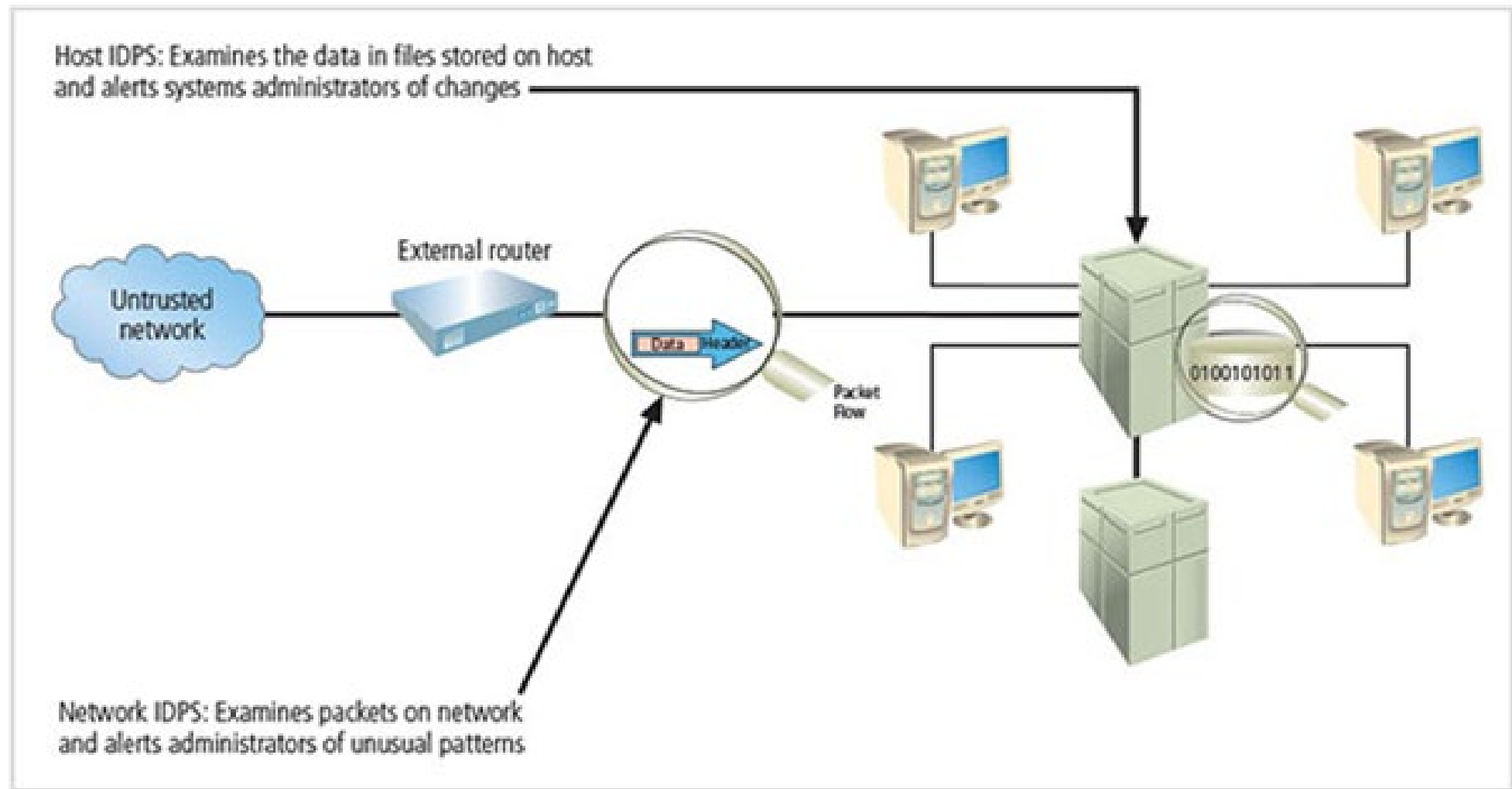
- An IDS is designed to detect a number of threats, including the following:
 - **Masquerader:** Unauthorised user posing as a legitimate one.
 - **Misfeisor:** Legitimate user exceeding authorised actions.
 - **Clandestine User:** Covers tracks by deleting logs.
- In addition, an IDS is designed to detect automated attacks and threats, including the following:
 - **Port Scans:** Identifies open TCP ports.
 - **Denial-of-Service (DoS):** Overwhelms a system to block legitimate access.
 - **Malware Attacks:** Includes Trojans, worms, and viruses.
 - **ARP Spoofing:** Redirects IP traffic within a network.
 - **DNS Cache Poisoning:** Alters DNS records to mislead users.

Why use an Intrusion Detection and Prevention system IDPS?

- While an IDS primary purpose to identify and report an intrusion, an IDS with a prevention mechanism can quickly contain an attack and prevent/mitigate the loss or damage.
 - An IPDS Detect and deal with preambles to attacks
 - Data collection allows the organisation to examine what happened after an intrusion and why.
 - Serves as a deterrent by increasing the fear of detection.
 - Can help management with quality assurance and continuous improvement

Types of IDPSs

- IDPSs operate as network-based or host-based systems.
- Network-based IDPS is focused on protecting network information assets.
 - Wireless IDPS focuses on wireless networks
 - Network behaviour analysis IDPS examines traffic flow on a network in an attempt to recognise abnormal patterns



© Cengage Learning 2015

Network-based IDPS (NIDPS)

- **Location:** Resides on a computer or appliance within a network segment, monitoring for attack indicators.
- **Packet Analysis:** Looks for attack patterns in network traffic.
- **Network Placement:** Installed to monitor traffic entering or exiting a specific network segment.
- **Attack Detection:** Compares activity against known attack signatures in the knowledge base.
- **TCP/IP Stack Implementation:**
 - Protocol Stack Verification: Detects invalid data packets.
 - Application Protocol Verification: Examines higher-level protocols for unexpected or improper packet behaviour.

Advantages of NIDPSs

- Good network design and placement of NIDPS can enable an organisation to monitor a large network with few devices
- NIDPSs are usually passive and can be deployed into existing networks with little disruption to normal network operations
- NIDPS are not usually susceptible to direct attack and may not be detectable by attackers

Disadvantages of NIDPSs

- Can become overwhelmed by network volume and fail to recognise attacks
- Require access to all traffic to be monitored
- Cannot analyse encrypted packets
- Cannot reliably ascertain if an attack was successful or not
- Some forms of attacks are not easily discerned by NIDPS's, specifically those involving fragmented packets

Wireless NIDPS

- Monitors and analyses wireless network traffic
- Issues associated with it include physical security, sensor range, wired network connections, cost, access point and wireless switch locations,

Network behaviour analysis systems

- Identify problems related to the flow of traffic
- Types of events commonly detected include denial-of-service (DoS) attacks, scanning, worms, unexpected application services, and policy violations
- Offer intrusion prevention capabilities that are passive, inline, and both passive and inline

Host-based IDPS (HIDPS)

- Resides on a particular computer or server (host) and monitors activity only on that system
- Benchmarks and monitors the status of key system files and detects when intruder creates, modifies, or deletes files
- Advantage over NIDPS: can access encrypted information traveling over network and make decisions about potential/actual attacks
- Most HIPDS's work on the principle of configuration and change management

Advantages of HIDPSs

- Can detect local events on host systems and detect attacks that may elude a network-based IDPS
- Functions on host system, where encrypted traffic will have been decrypted and is available for processing
- Not affected by use of switched network protocols
- Can detect inconsistencies in how applications and systems programs were used by examining records stored in audit logs

Disadvantages of HIDPSs

- Pose more management issues
- Vulnerable both to direct attacks and attacks against the host operating system
- Does not detect multihost scanning, nor scanning of non-host network devices
- Susceptible to some DoS attacks
- Can use large amounts of disk space
- Can inflict a performance overhead on its host systems

IDPS DETECTION METHODS

Signature-based detection

(or knowledge-based detection or misuse detection)

- Examines network traffic in search of patterns that match known signatures
- Widely used because many attacks have clear and distinct signatures
- Problem with this approach is that new attack patterns must continually be added to the IDPS's database of signatures
 - Slow methodical attack involving multiple events might escape detection

Anomaly-based detection (or behaviour-based detection)

- Anomaly-based detection collects statistical summaries by observing traffic known to be normal
- When measured activity is outside the baseline parameters or clipping level, IDPS sends an alert to the administrator
- IDPS can detect new types of attacks
 - Requires much more overhead and processing capacity than signature-based detection

SPA protocol analysis

- Compares normal protocol profiles with observed traffic.
- **Detection:** Uses session data to identify multi-session attacks (deep packet inspection).
- **Drawbacks**
 - High analytical complexity and processing overhead.
 - May miss intrusions unless protocols violate basic behaviour.
 - Can interfere with normal protocol operations.

Log file monitors

- Similar to NIDPS, reviews log files from servers, network devices, and other IDPSs for attack patterns and signatures.
- **Advantage**
 - Easier to identify attack patterns by analysing the entire network and its systems as a whole.
- **Disadvantage**
 - Requires significant resources for collecting, moving, storing, and analysing large volumes of log data.

IDS Data

- An Intrusion detection should record for each event the following:
 - **Subject:** Initiator of an action on a target.
 - **Object:** Targeted resource (e.g., file, command, device, network protocol).
 - **Action:** Operation performed by the subject on the object.
 - **Exception-Condition:** Errors or exceptions raised by the action.
 - **Resource Usage:** System resources consumed during the action.
 - **Time-Stamp:** Unique identifier marking when the action was initiated.

Deployment and Implementation of an IDPS

- An IDPS can be implemented via one of three basic control strategies:
 - Centralised: All IDPS control functions are implemented and managed in a central location.
 - Fully distributed: All control functions are applied at the physical location of each IDPS component.
 - Partially distributed: Combines the two; while individual agents can still analyse and respond to local threats, they report to a hierarchical central facility to enable organisation to detect widespread attacks.

STRENGTHS AND LIMITATIONS OF AN IDPS

Functions IDPSs Perform Well

- Monitoring and analysing system events and user behaviour.
- Testing and baselining system security states, tracking changes.
- Recognising known attack patterns and deviations from normal activity.
- Managing OS audit logs and alerting staff on attack detection.
- Measuring enforcement of security policies and providing default policy information.
- Enabling non-security experts to monitor security effectively.

Functions IDPSs Cannot Perform

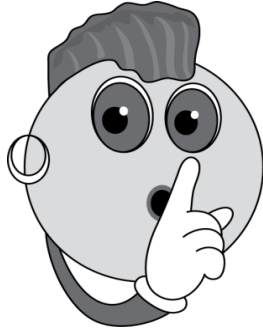
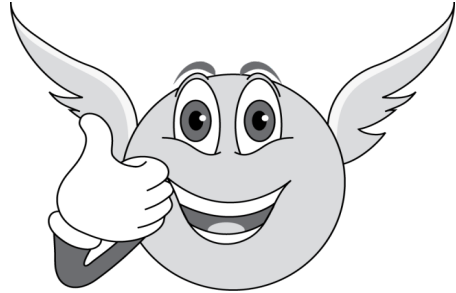
- Compensating for weak or missing security mechanisms.
- Instantaneous detection, reporting, and response during heavy network loads.
- Detecting new or variant attacks.
- Effectively responding to attacks from sophisticated attackers.
- Automatically investigating attacks without human intervention.
- Resisting attacks aimed at circumventing the system.
- Compensating for issues with data fidelity or dealing with switched networks.

IDPS Response Behaviour

- IDPS responses vary based on configuration and function, with many available options.
- An **Active Response** involves collecting more data, modifying the network, and taking action against the intrusion.
- A **Passive Response** includes triggering alarms/notifications and collecting data via SNMP traps.
- Many IDPSs have **addition features**:
 - Generate routine **reports** and detailed **documentation**.
 - Or have the **Failsafe Features**, designed to prevent the IDPS from being bypassed

Possible Alarm Outcomes

- Alarms can be sounded (positive) or not (negative)

	Intrusion Attack	No Intrusion Attack
Alarm Sounded	 NYPD 03539480 True Positive	 NYPD 03539480 False Positive
No Alarm Sounded	 False Negative	 True Negative

The Base-Rate Fallacy

- It is difficult to create an intrusion detection system with the desirable properties of having both a high true-positive rate and a low false-negative rate.
- If the number of actual intrusions is relatively small compared to the amount of data being analysed, then the effectiveness of an intrusion detection system can be reduced.
- In particular, the effectiveness of some IDSs can be misinterpreted due to a statistical error known as the **base-rate fallacy**.
- This type of error occurs when the probability of some conditional event is assessed without considering the “base rate” of that event.

Base-Rate Fallacy Example

- Suppose an IDS is 99% accurate, having a 1% chance of false positives or false negatives. Suppose further...
- An intrusion detection system generates 1,000,100 log entries.
- Only 100 of the 1,000,100 entries correspond to actual malicious events.
- Because of the success rate of the IDS, of the 100 malicious events, 99 will be detected as malicious, which means we have **1 false negative**.
- Nevertheless, of the 1,000,000 benign events, 10,000 will be mistakenly identified as malicious. That is, we have **10,000 false positives!**
- Thus, there will be 10,099 alarms sounded, 10,000 of which are false alarms. That is, roughly 99% of our alarms are false alarms.

HONEYPOTS, HONEYNETS, AND PADDED CELL SYSTEMS

Honeypots and Honeynets

- Honeypots: Decoy systems designed to divert attackers from critical systems and gather information about their activities.
- Honeynets: A network segment with multiple interconnected honeypots.
- Honeypots are designed to:
 - Divert attackers from accessing important systems.
 - Collect data on the attacker's actions.
 - Encourage attackers to remain on the system long enough for administrators to document and potentially respond.

Padded cell system

- Padded cell system: protected honeypot that cannot be easily compromised
- In addition to attracting attackers with tempting data, a padded cell operates in tandem with a traditional IDPS
- When the IDPS detects the attackers, padded cell system seamlessly transfers them to a special simulated environment where they can cause no harm—hence the name padded cell

References

- Slides are devised from the recommended books:
 - Whitman & Mattord, Principles of Information Security, 6th Edition
 - Chapter 9: Intrusion Detection and Prevention Systems and Other Security Tools
- Some of the slides are devised from my own notes



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Any Questions?

Trawsnewid Addysg; Trawsnewid Bywydau
Transforming Education; Transforming Lives



www.uwtsd.ac.uk