Information Security
CS3002
(Sections BDS-7A/B)
Lecture 25

Instructor: Dr. Syed Mohammad Irteza

Assistant Professor, Department of Computer Science

18 November, 2024

Previous Lecture

- IPsec
  - Maps to some parts of Chapter 22 in Computer Security: Principles and Practices (William Stallings)

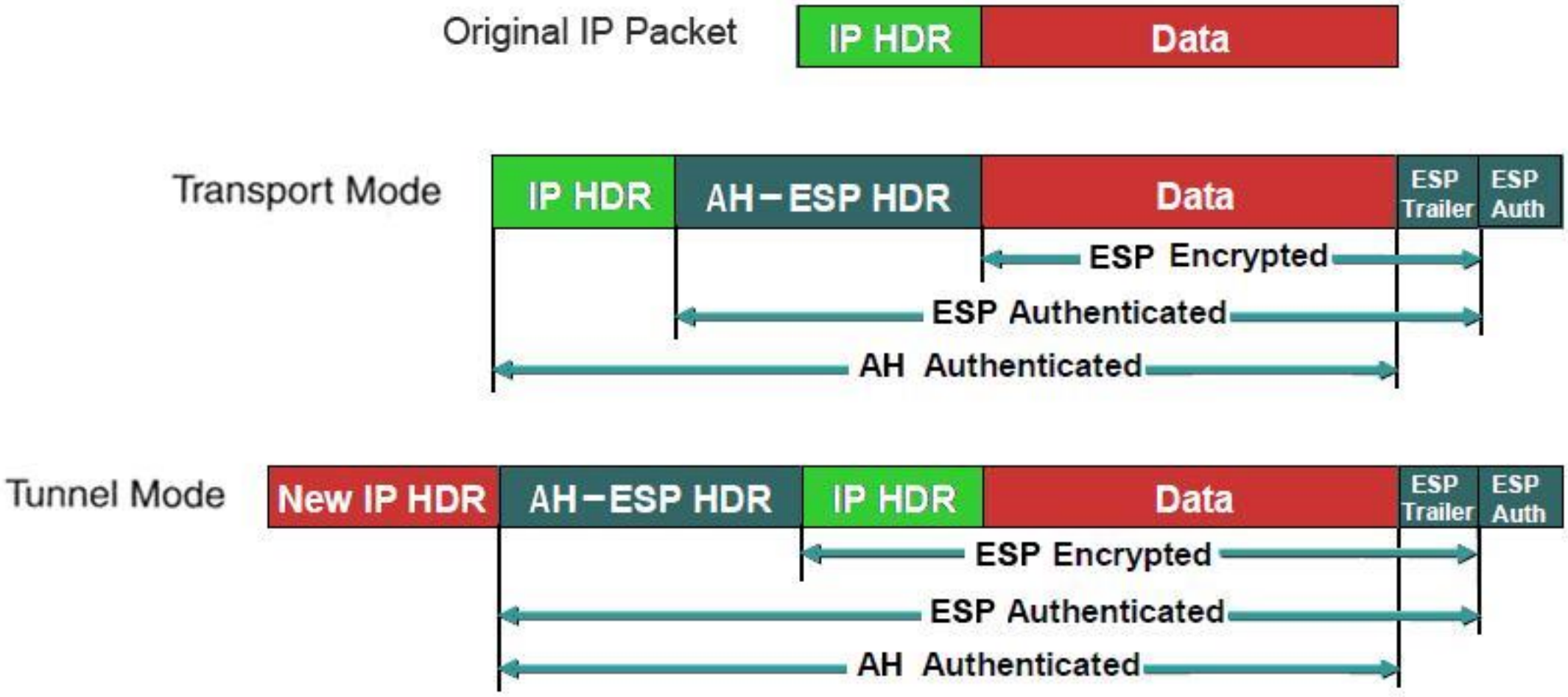
22.5 IPv4 AND IPv6 SECURITY

Before Final Exam

Remaining Lectures (Content)

- ***Network Security (2 lectures left, including this lecture)***
- Theoretical Models of Access Control (1 lecture)
- Cybercrime Laws and Ethics (1 lecture)
- Project Presentations (2 lectures at least)

IPSec: AH & ESP packet format



Network Security – III

Intrusion Detection Systems (IDSs)

- Components of IDS
- Classification of IDS
  - Anomaly
  - Signature
  - Hybrid
- Types
  - Host-based
  - Network based

Intrusion – Definition

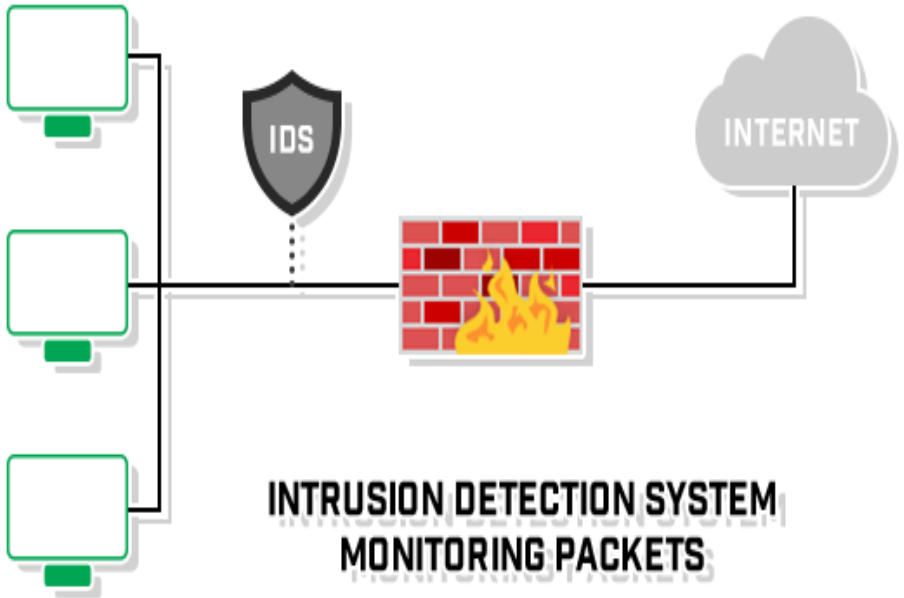
- Attempt to *break into or misuse* a system
- Intruders may be from *outside the network* or *legitimate users* of the network
- Three classes of intruders:
  - ***Masquerader***: an individual who is not authorized to use the computer and who penetrates a system's access controls to exploit a legitimate user's account.
    - Usually from outside
  - ***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 them.
    - Usually from inside
  - ***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.
    - Can be either from inside or outside

Types of Attacks using Intrusion

- Performing a remote root compromise of an e-mail server
  - How is root level compromise different to an account level compromise?
- Defacing a *web server*
- Guessing and *cracking passwords*
- Copying a *database containing credit card numbers*
- *Viewing sensitive data* (i.e., payroll records & media without authorizations)
- Running a *packet sniffer* on a workstation to capture *usernames and passwords*
- Using an *unattended, logged-in workstation* without permission

Intrusion Detection System (IDS)

- 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.
- Intrusion Detection Systems look for *attack signatures* (patterns that usually indicate malicious or suspicious intent)



Components of an IDS

An IDS comprises of three logical components:

- ***Sensors***: sensors are responsible for *collecting data* (i.e. network packets, log files, and system call traces)
- ***Analyzers***: analyzers receive inputs from one or more sensors or from other analyzers. The analyzer is *responsible for determining if an intrusion* has occurred.
- ***User Interface***: it enables a user to *view output from the system* or control behavior of the system. (i.e. UI may associate to a manager, director, or console component)

1. eject intruder quickly
2. serve as deterrent,prevent intrusion
3. collect info about intrusion techniques for strengthening and prevention in future.

Basic Principles of IDSs

- If an intruder is detected quickly enough, the intruder *can be identified and ejected* from the system before any damage.
  - Even if the detection is not that quick, the sooner the intrusion is detected, the *less the amount of damage and more quickly the recovery can be achieved*.
- An effective IDS can *serve as a deterrent*, thus acting to prevent intrusion.
- Intrusion detection enables the *collection of information about intrusion techniques* that can be used to strengthen intrusion prevention measures.

Classifying Intrusion Detection Systems

- Anomaly Based Detection
- Signature Based Detection (or Misuse Detection)
- Hybrid Detection
  - Specification Based Detection

Anomaly Based Detection

- It involves a collection of information about *legitimate user behavior over a period of time*. Then, statistical tests are applied to observe them.
- Anything *distinct from the usual behavior is assumed to be an intrusion* activity.
  - For example, flooding a host with lots of packet.
- The primary strength is its ability to *recognize novel attacks*.
- Such IDS *generate many false alarms* and hence compromise the effectiveness of the IDS.

Signature Based Detection

- Involves an attempts to *define a set of rules or attack patterns* that can be used to decide that a given behavior is that of an intruder.
- The question of *what information is relevant* to an IDS depends upon what it is trying to detect.
  - For example, DNS, FTP etc.
- Most signature analysis systems are based on *simple pattern matching algorithms*
  - For example, the IDS simply looks for a *substring within a stream of data* carried by network packets.
  - When it finds this *substring* (for example, the ``phf'' in ``GET /cgi-bin/phf?''), it identifies those network packets as *vehicles of an attack*.

rule based anomaly detection-> historical audits based
statsical anomoly detection - > no prior knowledge

signature based - > observe events and apply rules like pattern matchining keywords

Signature Based Detection

Signature techniques detect intrusion by observing events on a system & *apply rules to decide if activity is suspicious or not*.

Rule-based anomaly detection:

- *Analyze historical audit records* to identify usage patterns & *auto-generate rules* for them
- Then *observe current behavior* & match against rules to see if conforms
- Like statistical anomaly detection, *does not require prior knowledge* of security flaws
- It requires to have a *large database of rules to be effective*.

Specification Based Intrusion Detection

manually implemented rules and policies

- The *desirable behavior of a system* is described through its *functionalities* and through the *security policy*. Any sequence of operations executed *outside of the system's specifications* is considered to be a security violation
- Use of *manually specified program behavioral specifications* is the basis to detect attacks
- It has been proposed as a *promising alternative* that combine the strengths of *misuse detection (accurate detection of known attacks)* and *anomaly detection (ability to detect novel attacks)*
- The development of the specifications is an expensive and tedious process and *specifications are often very difficult to evaluate and verify*.

Effectiveness of an IDS

- Practically, an intrusion detection system needs to detect a *substantial percentage of intrusions* while keeping the *false alarms rate at acceptable level*.
  - If *too few intrusions detected* -> false security
  - If *too many false alarms* -> ignore/waste time while analyzing the false alarm

- Achieving this fate is very hard to achieve
- Existing systems seem to not have a good record

Types of IDS

Intrusion Detection Systems (IDSs) can be classified into:

- ***Host-based IDS***:
  - Monitors the characteristics of *a single host* and the events occurring within that host for suspicious activity.
- ***Network-based IDS***:
  - Monitors network traffic for *particular network segments or devices* and analyzes network, transport, and application protocols to identify suspicious activity.

Host/Applications Based IDS

- The host *operating system* or *the application logs* in the audit information.
- This audit information includes events like the use of *identification and authentication mechanisms* (logins, etc.) , *file opens* and *program executions*, *admin activities*, etc.
- This audit is then analyzed to detect *trails of intrusion*.

Drawbacks of the Host Based IDS

- The kind of information needed to be logged in is a *matter of experience*.
- Unselective logging of messages *may greatly increase the audit and analysis* burdens.
- Selective logging runs the risk that *attack manifestations could be missed*.

Strengths of the Host Based IDS

- Attack verification
- System specific activity
- Encrypted and switch environments
- Monitoring key components
- Near Real-Time detection and response
- No additional hardware

CPU usage

Network based IDS

Filter is applied on routers and network

- A network-based IDS *monitors traffic at selected points on a network* or interconnected set of networks.
- It examines the traffic *packet by packet in real time or close to real time* in order to detect intrusion patterns.
- A *filter* is usually applied to determine which traffic will be discarded or passed on to an attack recognition module. This helps to filter out *known non-malicious traffic*.

Strengths of Network based IDS

- Cost of ownership reduced
- Packet analysis
- Evidence removal (*harder for the attacker*)
- Real time detection and response
- Malicious intent detection
- Complement and verification
- Operating system independence

Honeypots

- Decoy systems that are designed to *lure a potential attacker away from critical systems*
- An asset that *solely exists to be attacked*
- It could be an *individual item*, a *system or entire network*
- It could be a *real system or emulated*.

Purpose

- *Divert an attacker* from accessing critical systems
- *Collect information* about the attacker's activity
- Good at *detecting new or unknown threats*
- Engage the attacker to *stay on the system long enough* for administration to respond

Deception Technology

- Honeypots are limited in scope
  - it uses *static decoys* due to which adversary *starts to understand the decoys*
  - *requires expensive resources* to implement and maintain

Deception technology is a *proactive cyber defense system* through the use of decoys to *lure, detect and defend*, without the issues of scalability, skilled and available resources.

- Uses *automated dynamic traps generated by AI*
- Immediate alerts with *minimum false positive rates*
- Deploy *traps according to the behavioral patterns* of the hacker
- Provide *detailed reports* for post cyber defense investigation

Deception Technology

- Decoy Files
  - Used as a "*marker*"
  - In case of an *access, read, copy, or deletion*, it serves as an alert to monitors
  - It could be anything: *file, database, picture, email, account, etc.*
  - Normally used to *deliver bogus information to attackers*
- Honeynet
  - Collection of *two or more* honeypots/decoy devices
  - Could be at the *same location* or *distributed*
  - Managed by the same entity

Interaction Level

The capability to mimic a real asset or object

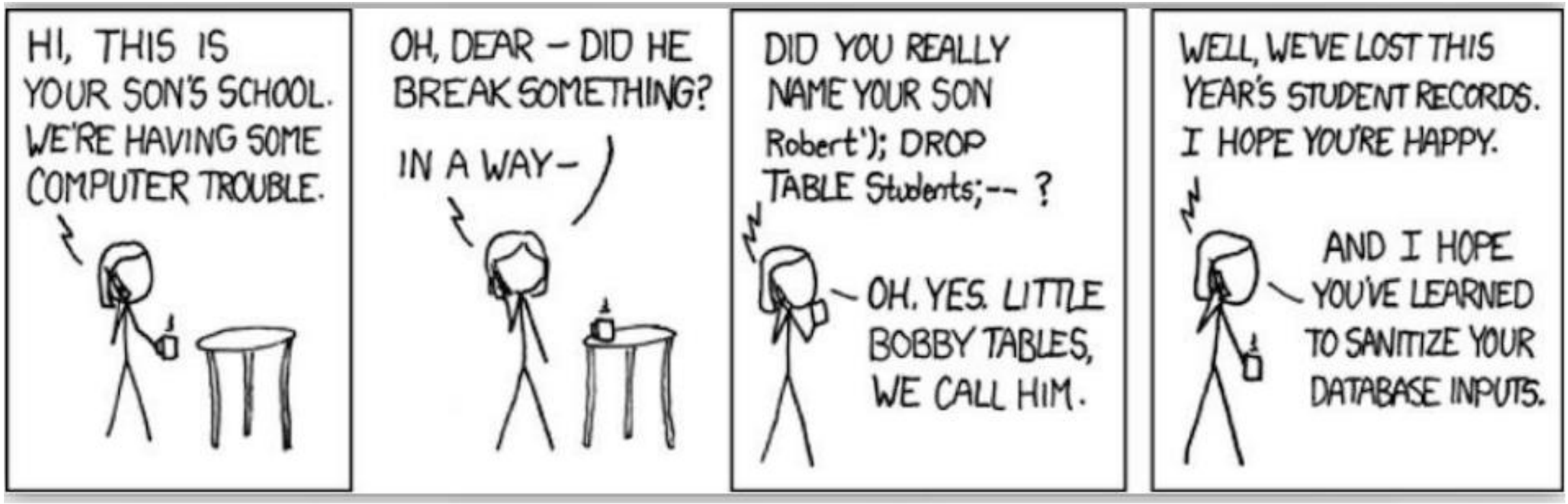
- ***High*** – more realistic, that mimics real, legitimate computer or device with applications, activity, and changing content
  - Needed for more hacker interaction, intent, etc.
  - More involved setup and maintenance
- ***Low*** – does very little to mimic real, legitimate device
  - Usually just TCP/IP port advertising or basic logon prompts
  - For early warning honeypots • Quicker setup, less ongoing maintenance, less risk
- If you can actually logon to a decoy, then you're at least at ***Medium*** interaction

Comparing IDS with IPS (source)

	Intrusion Prevention System	IDS Deployment
Placement in Network Infrastructure	Part of the direct line of communication (inline)	Outside direct line of communication (out-of-band)
System Type	Active (monitor & automatically defend) and/or passive	Passive (monitor & notify)
Detection Mechanisms	1. Statistical anomaly-based detection 2. Signature detection: - Exploit-facing signatures - Vulnerability-facing signatures	1. Signature detection: - Exploit-facing signatures

Exploit facing sign = identify unique exploits based on their unique paterns
Vulnerablilty facing sign = parameter used to identify type of vulnerability triggered in system OR automate vulnerability analysis process also increase risk of FP(false positives).

Some Humor (source)



Appendix

- Honeypot - Interaction Levels (Deception Technology)

GOOD LINK : https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips

Acknowledgments

- Dr. Haroon Mahmood and other FAST-NU instructors