Chapter Two

Overview of Commercial Issues
Basic of Cryptography

Cryptography

- Cryptography is the science of using mathematics to encrypt and decrypt data.
- While cryptography is the science of securing data, cryptanalysis is the science of analysing and breaking secure communication.
- Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern finding, patience, determination, and luck. Cryptanalysts are also called attackers.

Cryptography (Encryption Techniques)

- **Cryptography:** Schemes for encryption and decryption.
- **Encryption:** The process by which plaintext is converted into cipher-text.
- **Decryption:** Recovering plaintext from the cipher-text.
- **Secret key:** Used to set some or all of the various parameters used by the encryption algorithm.
- **Cryptanalysis:** The study of "breaking the code".
- **Cryptology:** Cryptography and cryptanalysis together constitute the area of cryptology.

Cryptography has five ingredients

- Plaintext
- Encryption algorithm
- Secret Key
- Cipher text
- Decryption algorithm

.

What is Web Security?

The web poses some additional security troubles because:

- so very many different computers are involved in any networked environment.
- the fundamental protocols of the Internet were not designed with security in mind.

Layers Involved in Web Security

- Many "layers" must work in concert to produce a functioning web-based system. Each layer has its own security vulnerabilities, and its own procedures and techniques for coping with these vulnerabilities.

.

Continued...

a. Hardware

- Physical access to computer hardware gives even a slightly-skilled person total control of that hardware. Without physical security to protect hardware (i.e. doors that lock) nothing else about a computer system can be called secure.

b. Operating System

- As the software charged with controlling access to the hardware, the file system, and the network, weaknesses in an operating system are the most valued amongst crackers.
- Most OS authentication is handled through user names and passwords. Biometric (e.g. voice, face, retina, iris, fingerprint) and physical token-based (swipe cards, pin-generating cards)

Continued...

c. Service

- For our purposes, a "service" is any class of software that typically runs unattended on a server-style computer and performs some task in response to a network-originated request. Web servers (e.g. Apache, IIS, including server-side scripting platforms), FTP servers, email servers (e.g. Sendmail, Qmail, Exim), Telnet and SSH servers, file and print servers (e.g. SMB/Samba), database servers (e.g. Oracle, SQL Server, MySQL, DB/2, PostgreSQL) and so on are all example of these services.

Continued...

d. Data

- As an organization's most valuable IT asset, the nonchalant treatment and security of data is often surprising.
- What is not surprising is that crackers know this and most of their efforts are ultimately focused on displaying, corrupting, or stealing an organization's data.

Continued...

e. Application

- The main vulnerability of web applications is Cross-Site Scripting (XSS).
- Cross-Site Scripting (a.k.a. XSS, script embedding, or script injection) is more an attack on the users of a web application, than on the web system itself.

Continued...

f. Network Protocol

- It is at the network protocol layer that most of the web system security is addressed by product marketing departments. While important, as we've seen this is only one piece of a very large pie.
- The primary technology that protects the web application protocol in question, HTTP, is the Secure Sockets Layer (SSL), now renamed Transport Layer Security (TLS).
- TLS provides both authentication and encryption services to communicating computers using digital certificates issued by Certificate Authorities (CAs) also known as Trust Authorities.

Continued...

g. Browser

- Unfortunately, given the design of the HTTP protocol (even when secured through SSL/TLS), there is very little that can be done to protect the web system at the browser layer. Hence, web applications may never trust any data originating from a client browser.
- TLS-based client digital certificates can be used to more positively identify clients to servers, but they are as yet rarely used, partially because of expense, but also because they are difficult to move from one client computer to another, thereby diminishing one of the benefits of web systems: client location transparency.

Public-Key Infrastructure (PKI)

- A public key infrastructure (PKI) is a set of rules, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption.
- The purpose of a PKI is to facilitate the secure electronic transfer of information for a range of network activities such as e-commerce, internet banking and confidential email

Continued...

A PKI consists of:

- **A certificate authority (CA)**: that stores, issues and signs the digital certificates
- **A registration authority**: which verifies the identity of entities requesting their digital certificates to be stored at the CA
- **A central directory**: a secure location in which to store and index keys
- **A certificate management system**: managing things like the access to stored certificates or the delivery of the certificates to be issued.
- **A certificate policy**: stating the PKI's requirements concerning its procedures. Its purpose is to allow outsiders to analyze the PKI's trustworthiness

Overview of Intrusion Detection Systems

- Intrusion Detection System (IDS) is designed to monitor an entire network activity, traffic and identify network and system attack with only a few devices.
- Intrusion Detection System (IDS) is the combination of hardware and software that monitors a network or system.
- Intrusion Detection System (IDS) is used for detecting any malicious activity.

Continued...

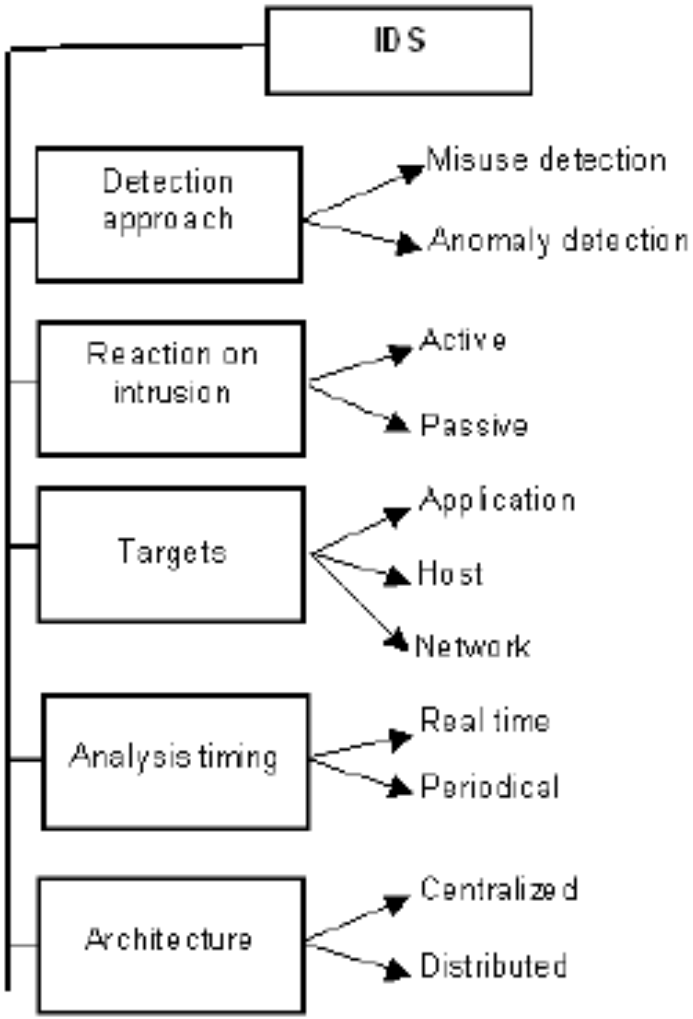
What are intrusions?

- Any set of actions that threatens the integrity, availability, or confidentiality of a network resource.
- *EXP:Denial of service (DOS):* Attempts to starve a host of resources needed to function correctly.

What is intrusion detection?

- Intrusion detection is the process of monitoring the events occurring in a computer system or network and analysing them for signs of *intrusions*.
- Intrusions are caused by attackers accessing the systems from the Internet, authorized users of the systems who attempt to gain additional privileges for which they are not authorized, and authorized users who misuse the privileges given them.
- Intrusion Detection Systems (IDSs) are software or hardware products that automate this monitoring and analysis process.

IDS Toxonomy



Continued...

- A *distributed intrusion detection system* is one where data is collected and analyzed in multiple host, as opposed to a *centralized intrusion detection system*. Both distributed and centralized intrusion detection systems may **use host- or network-based** data collection methods, or most likely a combination of the two.
- **--**IDS can react to intrusion in two ways:
- ***Active*** - takes some action as a reaction to intrusion (such shutting down services, connection, logging user…)
- ***Passive*** - generates alarms or notification.
- --Audit information analysis can be done generally in two modes.
- Intrusion detection process can run continuously, also called in *real-time*. The term "real-time" indicates not more than a fact that IDS reacts to an intrusion "quick enough".
- Intrusion detection process also can be run *periodically*.

IDS Analysis

- There are two primary approaches to analysing events to detect attacks:
- ***1. misuse detection***
- ***2. anomaly detection.***
- Misuse detection, in which the analysis targets something known to be "bad", is the technique used by most commercial systems.
- Anomaly detection, in which the analysis looks for abnormal patterns of activity, has been, and continues to be, the subject of a great deal of research. Anomaly detection is used in limited form by a number of IDSs.

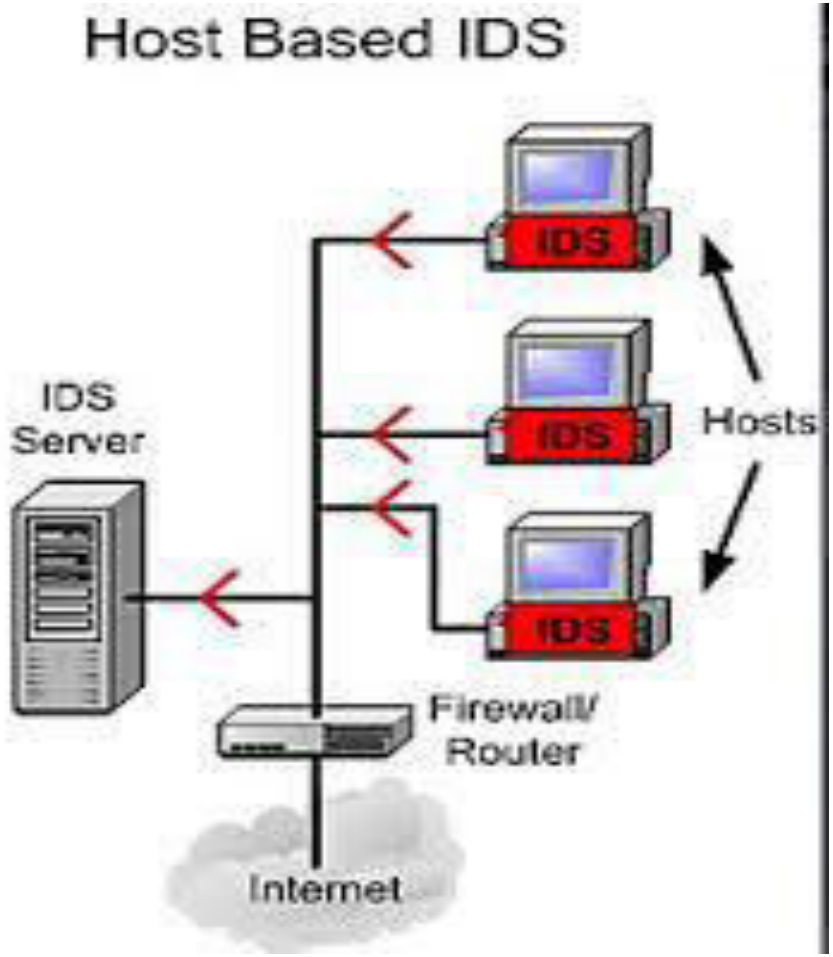
Five Major Types of Intrusion Detection System (IDS)

- 1. Host Based IDS
- 2. Network Based IDS
- 3. Stack Based IDS
- 4. Signature Based IDS
- 5. Anomaly Based IDS

1. **Host Based**

- **IDS Host Intrusion Detection Systems** (HIDS) are installed on the individual devices in the network.
- HIDS analyses the incoming and outgoing packets from a particular device.
- HIDS is better than Network IDS as a comparison to detecting malicious activities for a particular device.

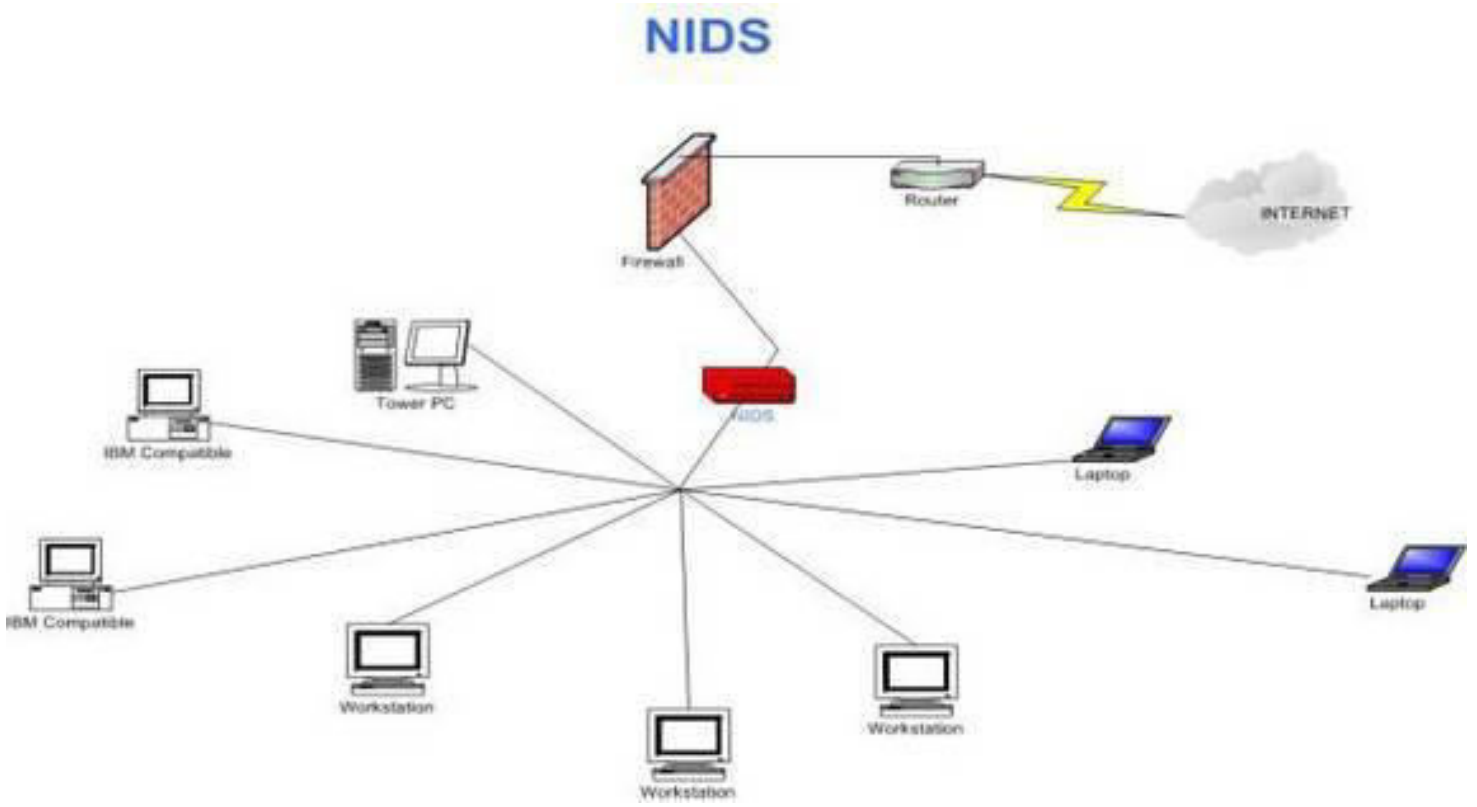
Continued…


Host Based IDS
IDS
IDS
IDS
Hosts
IDS
Server
Firewall/
Router
Internet

2. Network Based IDS

- Network Intrusion Detection Systems (NIDS) are monitoring traffic at strategic points on the network.
- IDS uses as a dedicated platform for use to analyze all the passing network traffic.
- NIDS work with the network and analyses the ethernet packet to be decide to apply rules.

Continued...


NIDS
Firewall
Router
INTERNET
Tower PC
IBM Compatible
NIDS
Laptop
IBM Compatible
Laptop
Workstation
Workstation
Workstation

Continued...

3. **Stack Based IDS:**

- Stack IDS is a technology, which are integrated with the **TCP/IP stack**.
- Stack Intrusion Detection System allows the IDS to be watching the packets, than IDS pull the packet from the stack before the Operating system

4. Signature Based IDS:

- IDS Signature detection work well with the threats that are already determined or known. It implicates searching a series of bytes or sequence that are termed to be malicious.
- One of the most profitable point is that IDS Signatures are easy to apply and develop once you will figure out the sort of network behaviour to be find out

5. Anomaly Based IDS

- Anomaly detection technique is a centralized process that works on the concept of a **baseline for network behaviour.**
- This baseline is a description of accepted network behaviour, which is learned or specified by the network administrators, or both.
- It's like a guard dog personally interviewing everyone at the gate before they are let down the drive.

Intrusion Prevention System and types of Network Threats

What is an Intrusion Prevention System (IPS)?

- An Intrusion Prevention System is a network device/software that goes deeper than a firewall to identify and block network threats by assessing each packet based on the network protocols in the application layer, the context of the communication and tracking of each session.
- Intrusion prevention systems are network security devices that monitor network and/or system activities for malicious activity (intrusion)

Con---

Main functions of Intrusion Prevention System (IPS) are,

- – Identify intrusion
- – Log information about intrusion
- – Attempt to block/stop intrusion and
- – Report intrusion
- - Intrusion Detection System (IDS) only detect intrusions.

What are the ways in which Intrusion Prevention Systems work?

- **1. Signature based threat detection:** Intrusion detection/prevention systems contain a large repository of signatures that help identify attacks by matching attempts to known vulnerability patterns.
- **2. Anomaly threat detection:** Anomaly detection techniques protect against first strike or unknown threats. This is done by comparing the network traffic to a baseline to identify abnormal and potentially harmful behaviour.
- **3. Passive Network Monitoring:** IPS can also be set to passively monitor network traffic at certain points and identify abnormal behaviour/ deviation of certain security threshold parameters and report the same by generating reports/alerts (like email alerts) about the device communications to the security administrator.

Difference between Firewall and Intrusion Detection System

- A firewall is a hardware and/or software which functions in a networked environment to block unauthorized access while permitting authorized communications.
- Firewall is a device and/or a software that stands between a local network and the Internet, and filters traffic that might be harmful.
- An Intrusion Detection System (IDS) is a software or hardware device installed on the network (NIDS) or host (HIDS) to detect and report intrusion attempts to the network.

Thank You!