



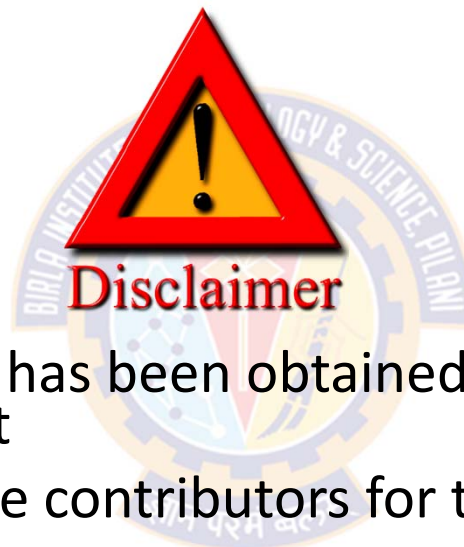
BITS Pilani
Pilani | Dubai | Goa | Hyderabad

Cyber Security

Strategic Defense Mechanisms and Defense-in-Depth (DiD)

Dr. Ramakrishna Dantu
Associate Professor, BITS Pilani

Disclaimer and Acknowledgement



- The content for these slides has been obtained from books and various other source on the Internet
- I here by acknowledge all the contributors for their material and inputs.
- I have provided source information wherever necessary
- I have added and modified the content to suit the requirements of the course

Strategic Defense Mechanisms



Agenda

- Strategic Defense Mechanisms and Defense-in-Depth (DiD):
 - Technical, Operational, Managerial and Physical Defenses
 - Defense-in-Depth Approach and Layered Security Model
 - Defense mechanisms like
 - Encipherment, digital signatures, access control, intrusion detection, authentication exchange, routing control,
 - Pervasive mechanisms like
 - Security audit trail, event detection, security recovery, trusted functionality, anti-malware solutions, VPNs.



Digital Signatures

Digital Signatures



Definition and Characteristics

- A digital signature is defined as
 - "The result of a cryptographic transformation of data that, when properly implemented, provides a mechanism for verifying *origin, authentication, data integrity, and signatory non-repudiation*"
 - --- NIST FIPS PUB 186-4 [Digital Signature Standard (DSS), July 2013]
- Digital signature
 - A digital signature is a data-dependent bit pattern
 - It is generated by an agent as a function of a file, message, or other form of data block
 - Another agent can access the data block and its associated signature and verify that
 - 1) the data block has been signed by the alleged signer, and
 - 2) the data block has not been altered since the signing
 - 3) the signer cannot repudiate the signature

Digital Signatures



Properties of Paper-Based Signatures

- Components and Characteristics of Signatures
 - A digital signature is a binary object associated with a file
 - To express the requirements for a digital signature, we need to understand the properties of human signatures
- Properties of Secure Paper-Based Signatures
 - Consider a situation of human need:
 - an order to transfer funds from one person to another
 - The properties of this transaction for a conventional paper check:
 - A check is a *tangible object* authorizing a financial transaction
 - The signature on the check *confirms authenticity* because (presumably) only the legitimate signer can produce that signature
 - In the case of an alleged forgery, a third party can be called in to *judge authenticity*
 - Once a check is cashed, it is canceled so that it *cannot be reused*
 - The paper check is *not alterable*. Or, any alteration can be easily detected

Digital Signatures



Scenario – Non-Repudiation, Authenticity, & Integrity

- Now, the requirements of such a situation, from the standpoint of both a bank and user
- Suppose Sheila sends her bank a message authorizing it to transfer \$100 to Robert
- Sheila's bank must be able to verify and prove that the message really came from Sheila if she should later disavow sending the message
 - This property is called **non-repudiation**
- The bank also wants to know that the message is entirely Sheila's, that it has not been altered along the way
- Sheila also wants to be certain that her bank cannot forge such messages
 - This property is called **authenticity**
- Both parties want to be sure that:
 - the message is **new**,
 - not a **reuse** of a previous message, and
 - that it has not been **altered** during transmission

Digital Signatures



Properties of Digital Signatures

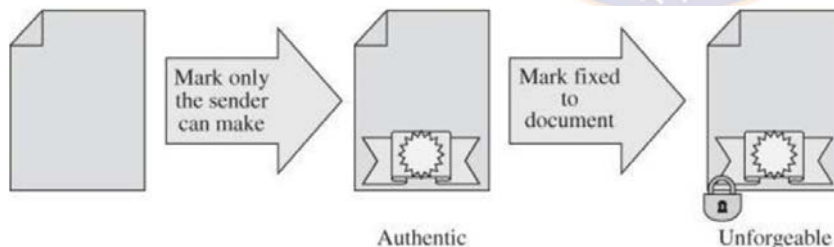
- A **digital signature** is a protocol that produces the same effect as a real signature:
 - It is a mark that only the sender can make and other people can easily recognize as belonging to the sender
- Just like a real signature, a digital signature confirms agreement to a message
- A digital signature must meet two primary conditions:
 - It must be **unforgeable**
 - If person S signs message M with signature $Sig(S,M)$, no one else can produce the pair $[M, Sig(S,M)]$
 - It must be **authentic**
 - If a person R receives the pair $[M, Sig(S,M)]$ purportedly from S , R can check that
 - the signature is really from S ,
 - only S could have created this signature, and
 - the signature is firmly attached to M

Digital Signatures



Properties of Digital Signatures

- Two more properties (also drawn from parallels with the paper-based environment) for digital signatures:
 - It is *not alterable*
 - After being transmitted, M cannot be changed by S , R , or an interceptor
 - It is *not reusable*
 - A previous message presented again will be instantly detected by R



- Two primary properties:
 - Signature must be authentic
 - Signature must be unforgeable

Digital Signatures

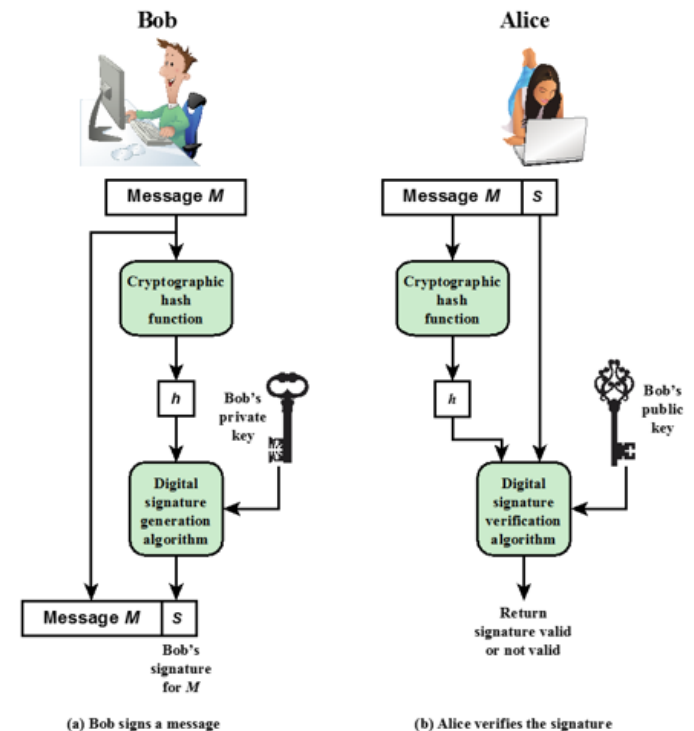
innovate

achieve

lead

Process of Digital Signature

- Suppose that Bob wants to send a message to Alice
- It is not important that the message be kept secret, but he wants Alice to be certain that the message is indeed from him
- For this purpose:
 - Bob uses a secure hash function, such as SHA-512, to generate a hash value for the message
 - Encrypts the hash code with his private key
 - Creates a **digital signature**
- Bob sends the message with the signature attached
- When Alice receives the message plus signature, she
 - 1) calculates a hash value for the message
 - 2) decrypts the signature using Bob's public key; and
 - 3) compares the calculated hash value to the decrypted hash value
- If the two hash values match, Alice is assured that the message must have been signed by Bob
- No one else has Bob's private key and therefore no one else could have created a ciphertext that could be decrypted with Bob's public key
- In addition, it is impossible to alter the message without access to Bob's private key
 - So, the message is authenticated both in terms of source and in terms of data integrity



Simplified Depiction of Essential Elements of Digital Signature Process

Digital Signatures



Maintaining Confidentiality Vs. Integrity

- The digital signature does not provide **confidentiality**
 - That is, the message being sent is safe from alteration but not safe from eavesdropping
- Thus, digital signatures provide **integrity**
- This is obvious in the case of a signature based on a portion of the message, because the rest of the message is transmitted *in the clear*
- Even in the case of complete encryption, there is no protection of confidentiality because any observer can decrypt the message by using the sender's public key



Intrusion Detection Systems

Intrusion Detection Systems



Introduction

- An intrusion occurs when an attacker attempts to gain entry into a company's network or information systems
- Perimeter controls, firewalls, and authentication and access controls block certain actions
 - Most of these controls are preventive:
 - They block known bad things from happening
- Although prevention is necessary, it is not always possible to prevent a security violation incident
- Detection during an incident is required when harm cannot be prevented in advance
- Intrusion detection system complement these preventive controls as the next line of defense

Intrusion Detection Systems



Some Terms

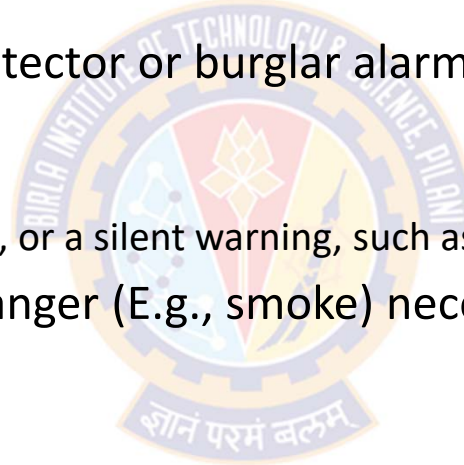
- **Intrusion *Detection*:**
 - Consists of procedures and systems that identify system intrusions
- **Intrusion *prevention*:**
 - Consists of activities that deter an intrusion. For example:
 - Writing and implementing good enterprise information security policy
 - Planning and executing effective information security programs
 - Installing and testing technology-based information security countermeasures, such as firewalls and intrusion detection and prevention systems
 - Conducting and measuring the effectiveness of employee training and awareness activities
- **Intrusion *reaction***
 - Encompasses the actions an organization takes when an intrusion is detected
 - These actions seek to limit the loss from an intrusion and return operations to a normal state as rapidly as possible
- **Intrusion *correction***
 - These activities complete the restoration of operations to a normal state
 - Seeks to identify the source and method of the intrusion to ensure that the same type of attack cannot occur again
 - Thus, reinitiating intrusion prevention

Intrusion Detection Systems



What is IDS?

- An intrusion detection system (IDS) is a device (or a computer) that monitors and identifies malicious or suspicious activity
- An IDS is a sensor (like a smoke detector or burglar alarm) in that it detects a violation and activates an alarm
- This alarm can be:
 - a sound, a light or other visual signal, or a silent warning, such as an e-mail message or pager alert
- As with some alarms, detecting danger (E.g., smoke) necessitates action:
 - Calling the fire department
 - Activating a sprinkler system
 - Sounding an evacuation alarm
 - Alerting the control team
- These actions depend on the advanced plans that have been made to handle the incident



Intrusion Detection Systems



What is IDS?

- IDSs allow system administrators to configure various alerts and the alarm levels associated with each type of alert
- For example:
 - IDS can be configured to notify them directly of trouble via e-mail or pagers
 - IDS can also be configured (like a burglar alarm) to notify an external security service of a "break-in."
- These IDS configurations to provide customized responses are quite complex
- Sometimes, IDS goes into protection mode to isolate a suspected intruder and constrain access
 - Such a system is called **Intrusion Protection System (IPS)**

Intrusion Detection Systems



Functions of an IDS

- An IDS receives raw input (data) from sensors
- It saves those inputs, analyzes them, and takes some controlling action
- IDSs perform a variety of functions:
 - Monitoring users and system activity
 - Auditing system configuration for vulnerabilities and misconfigurations
 - Correcting system configuration errors
 - Assessing the integrity of critical system and data files
 - Recognizing abnormal activity through statistical analysis
 - Managing audit trails and highlighting user violation of policy or normal activity
 - Installing and operating traps to record information about intruders
- No single IDS can perform all these functions

Intrusion Detection Systems



Intrusion Detection and Prevention System (IDPS)

- Sometimes, IDS incorporates intrusion prevention technology
- This technology can prevent an intrusion from successfully attacking the organization
 - This is done by means of an active response
- According to NIST SP 800-94, Rev. 1, the response techniques of IDPSs can be divided into the following groups:
 - Interdicting (prohibiting) the attack
 - Modifying configuration settings of other security controls
 - Changing an attack's components

Intrusion Detection Systems



Intrusion Detection and Prevention System (IDPS)

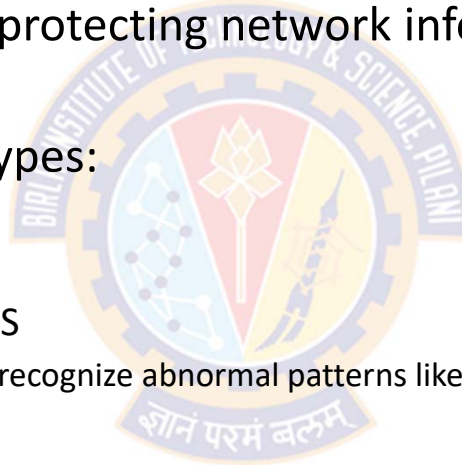
- Interdicting the attack
 - An IDPS is capable of forbidding the attack by itself, without human intervention. For example:
 - Terminating the user session or network connection over which the attack is being conducted
 - Blocking access to the target system (E.g., compromised user account, inbound IP address, or other attack characteristic) from the source of the attack
- Modifying configuration settings of other security controls
 - The IDPS can change the configuration of other security controls to disrupt an attack
 - For example, modifying a firewall's rule set or configuring another network device to shut down the communications channel to filter the offending packets
- Changing an attack's components
 - Some IDPSs are capable of changing an attack's components by replacing malicious content with benign (non-malicious) material or by quarantining a network packet's contents

Intrusion Detection Systems



Types of IDPSs

- IDPSs generally operate as network- or host-based systems
- A network-based IDPS focuses on protecting network information assets by examining network communications traffic
- Network-based IDPSs are of two types:
 - Wireless IDPS
 - Focuses on wireless networks
 - Network behavior analysis (NBA) IDPS
 - Examines traffic flow on a network to recognize abnormal patterns like DDoS, malware, and policy violations
- Host-based IDPS
 - Protects the server or host's information assets, by:
 - monitoring the files stored on the system and
 - sometimes by monitoring the actions of connected users

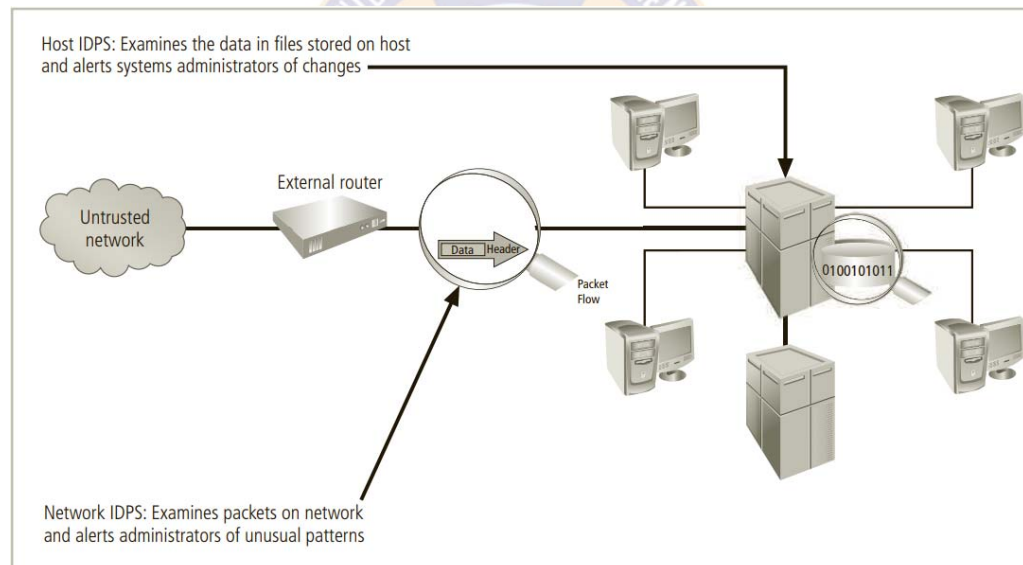


Intrusion Detection Systems



Types of IDPSs

- IDPS in the figure monitors both network connection activity and current information states on host servers



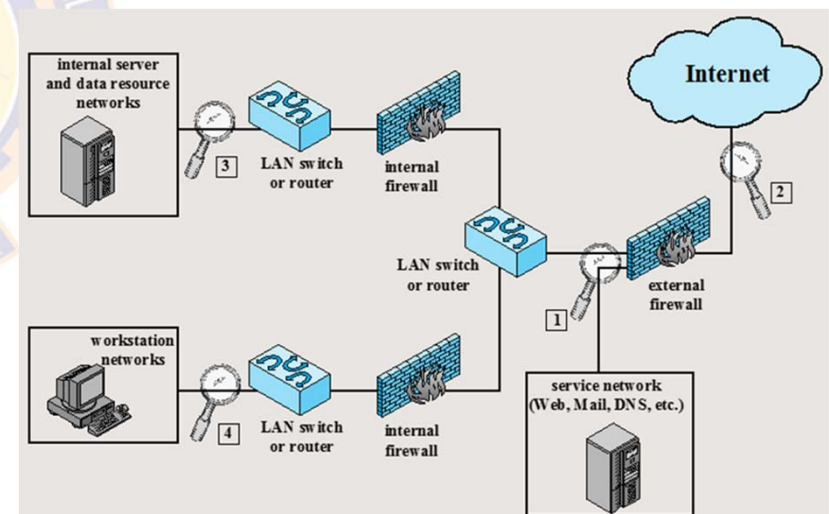
Intrusion detection and prevention systems

Intrusion Detection Systems



Network-Based IDPS (NIDPS)

- It includes:
 - Management software, referred to as a console, and
 - A number of specialized hardware and/or software components referred to as agents or sensors
- The agents
 - can be installed on other network segments and/or network technologies
 - remotely monitor network traffic at multiple locations for a potential intrusion and report back to the central NIDPS application



Intrusion Detection Systems



Functions of Network-Based IDPS (NIDPS)

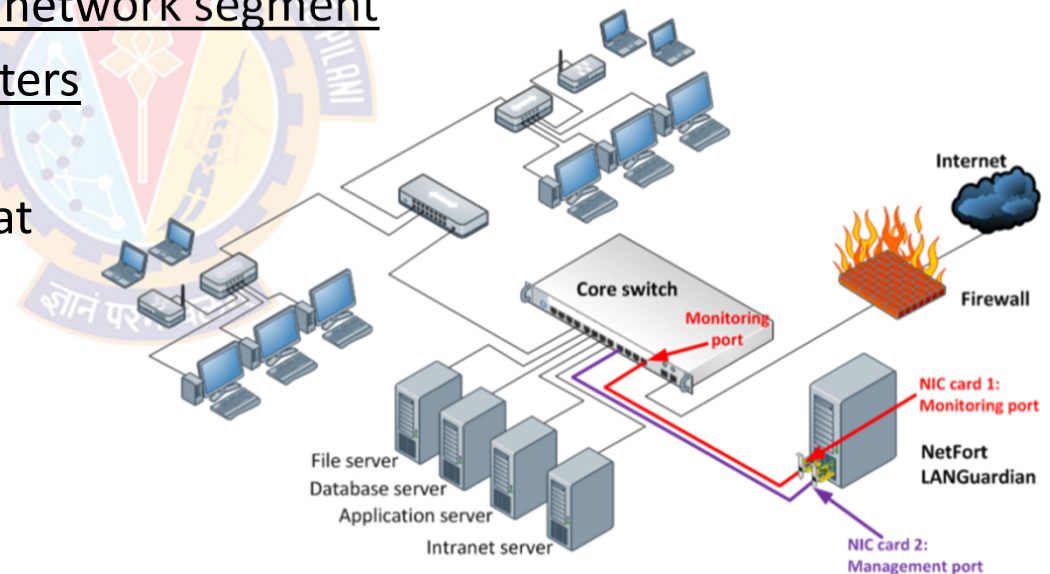
- DoS Attack
 - NIDPS looks for patterns in the incoming network traffic such as large collections of related items of a certain type
 - this could indicate that a DoS attack is under way
- Port scan
 - Examines the exchange of a series of related packets in a certain pattern
 - this could indicate that a port scan is in progress
- Notifying administrators
 - When the NIDPS identifies activity that it is programmed to recognize as an attack, it responds by sending notifications to administrators
- NIDPS can detect many more types of attacks than a host-based IDPS, but it requires a much more complex configuration and maintenance program

Intrusion Detection Systems



Network-Based IDPS (NIDPS)

- An NIDPS is/can be installed at a specific place in the network (E.g., inside an edge router or switch), where it is possible to monitor
 - traffic into and out of a particular network segment
 - a specific grouping of host computers on a specific network segment
 - all traffic between the systems that make up an entire network

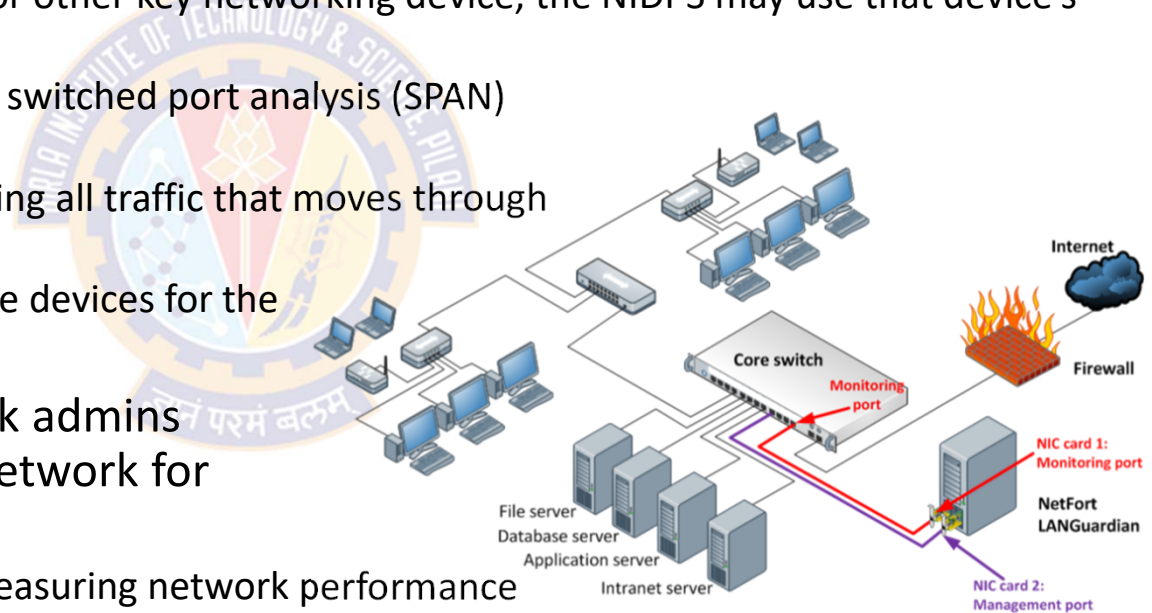


Intrusion Detection Systems



Network-Based IDPS (NIDPS)

- Using monitoring port
 - When placed next to a hub, switch, or other key networking device, the NIDPS may use that device's monitoring port
 - A monitoring port is also known as a switched port analysis (SPAN) port or mirror port
 - A monitoring port is capable of viewing all traffic that moves through the entire device
 - Monitoring ports are necessary in the devices for the functioning of an IDPS
- These connections enable network admins to collect traffic from across the network for analysis by the IDPS
 - for diagnosing network faults and measuring network performance



Intrusion Detection Systems



Network-Based IDPS (NIDPS) – Advantages & Disadvantages

- Advantages

- Good network design and placement of NIDPS devices can enable an organization to monitor a large network using only a few devices
- NIDPSs are usually passive devices and can be deployed into existing networks with little or no disruption to normal network operations
- NIDPSs are not usually susceptible to direct attack and may not be detectable by attackers

- Disadvantages

- Performance
 - An NIDPS can become overwhelmed by network volume and fail to recognize attacks it might otherwise have detected
 - Some IDPS vendors are accommodating the need for even faster network performance by improving the processing of detection algorithms in dedicated hardware circuits
 - Additional efforts to optimize rule set processing may also reduce the overall effectiveness of detecting attacks

Intrusion Detection Systems



Network-Based IDPS (NIDPS) – Advantages & Disadvantages

- Disadvantages

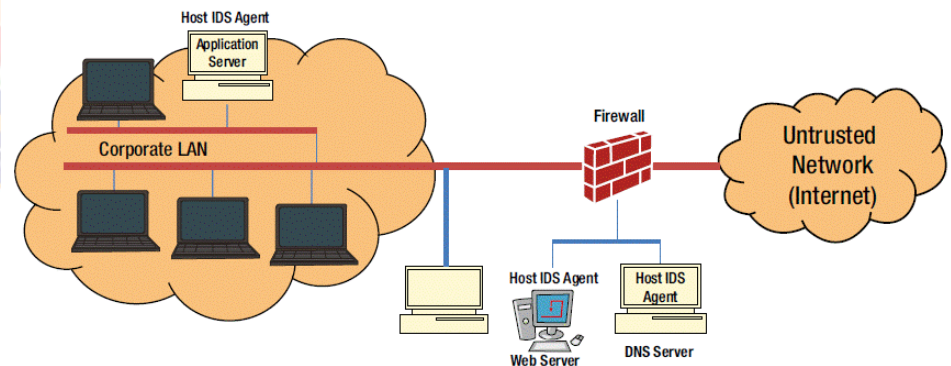
- NIDPSs require access to all traffic to be monitored
 - The broad use of switched Ethernet networks has replaced hubs
 - Because many switches have limited or no monitoring port capability, some networks are not capable of providing aggregate data for analysis by an NIDPS
 - Even when switches do provide monitoring ports, they may not be able to mirror all activity with a consistent and reliable time sequence.
- NIDPSs cannot analyze encrypted packets
 - This makes some network traffic invisible to the process
 - Increasing use of encryption hides the contents of some or all packets by some network services (such as SSL, SSH, and VPN)
 - This limits the effectiveness of NIDPSs
 - NIDPSs cannot reliably ascertain whether an attack was successful, which requires ongoing effort by the network administrator to evaluate logs of suspicious network activity

Intrusion Detection Systems



Host-Based IDPS (HIDPS)

- A host-based IDPS (HIDPS) or an HIDPS sensor resides on a particular computer or server, known as the host, and monitors activity only on that system
- They benchmark and monitor the status of key system files and detect when an intruder creates, modifies, or deletes monitored files
 - Thus, HIDPSs are also known as system integrity verifiers
- Unlike an NIDPS, an HIDPS can access encrypted data and use it to make decisions about potential or actual attacks
- Also, because the HIDPS works on only one computer system, all the traffic it examines traverses that system



Intrusion Detection Systems



Host-Based IDPS (HIDPS)

- HIDPSs work on the principle of configuration or change management
 - That is, they record the sizes, locations, and other attributes of system files
- HIDPS can monitor
 - stored configuration files like .ini, .cfg, .dat
 - system configuration databases, such as Windows registries
 - systems logs for predefined events
- The HIDPS examines these files and logs to determine
 - if an attack is under way or has occurred
 - whether the attack is succeeding or was successful

Intrusion Detection Systems



Host-Based IDPS (HIDPS)

- HIDPS triggers an alert when
 - file attributes change, new files are created, or existing files are deleted
- HIDPS maintains its own log file so that an audit trail is available even when hackers modify files on the target system to cover their tracks
- A properly configured HIDPS is very reliable
- HIDPS can produce a false positive alert when an authorized change occurs for a monitored file
- This action can be reviewed by an administrator, who may choose to disregard subsequent changes to the same set of files



Firewalls

Firewalls



Overview

- Firewalls are considered as first line defense for computer information systems
- The basic idea of firewalls is to protect the information system against outside and inside attacks
- Firewalls filter out suspicious incoming and outgoing packets
- Generally, most firewalls have two default policies
 - The first one is discard
 - That is, if an arriving packet does not match any rule in IPtable discard it
 - The second one is allow
 - That is, if an arriving packet dose not match any rule in IPtable allow it to pass
- Firewalls fall into several major categories of processing modes:
 - Packet-filtering firewalls
 - Application layer proxy firewalls
 - Media access control layer firewalls, and
 - Hybrids
- Hybrid firewalls use a combination of the other modes
 - In practice, most firewalls fall into this category because most implementations use multiple approaches.

Firewalls

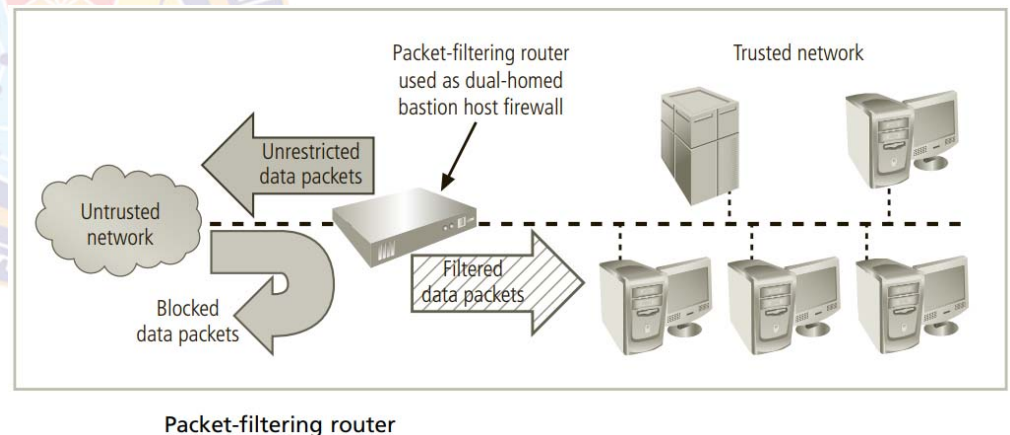
innovate

achieve

lead

Packet-Based Firewalls

- Packet-based firewall also called Packet filtering
- It works by inspecting or checking the IP field of each packet then it makes a decision whether to allow the packet to pass or deny it
- The decision is based on:
 - the IP address of the source,
 - the IP address of the destination,
 - the source port number,
 - whether it is TCP or UDP, and
 - the destination port
- This type of firewalls relies on IPTable

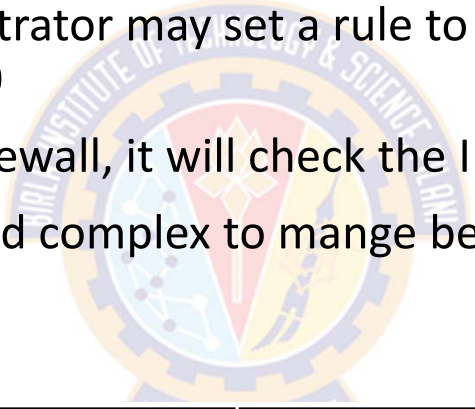


Firewalls



Packet-Based Firewalls

- IPtable is set of rules that have been set by network administrator
- For example, the network administrator may set a rule to deny any packet comes from 192.168.1.10 with port number 80
- When this packet arrives to the firewall, it will check the IPtable to take the decision
- Packet firewall is easy to install, and complex to mange because you need to set many rules



Source Address	Destination Address	Service (e.g., HTTP, SMTP, FTP)	Action (Allow or Deny)
172.16.x.x	10.10.x.x	Any	Deny
192.168.x.x	10.10.10.25	HTTP	Allow
192.168.0.1	10.10.10.10	FTP	Allow

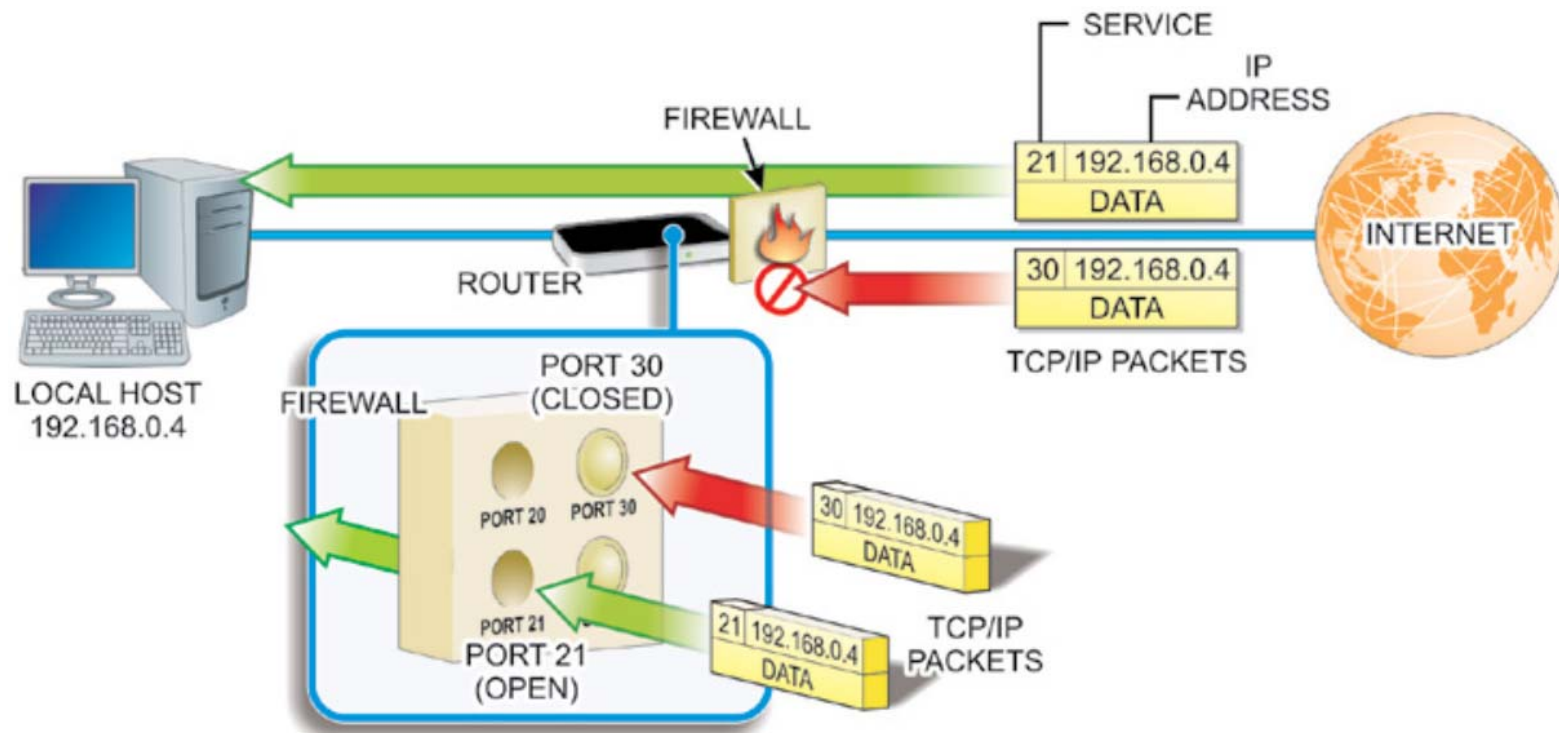
Firewalls

innovate

achieve

lead

Firewall Functionality



Firewalls



The application layer proxy firewall

- Also known as application firewall or proxy server (or reverse proxy)
- Is frequently installed on a dedicated computer separate from the filtering router
- It is commonly used in conjunction with a filtering router
- It can be configured to run special software that acts as a proxy for a service request
- For example, an organization that runs a Web server can avoid exposing it to direct user traffic by installing a proxy server configured with the registered domain's URL
- This proxy server receives requests for Web pages, accesses the Web server on behalf of the external client, and returns the requested pages to the users
- These servers can store the most recently accessed pages in their internal cache, and are thus also called cache servers

Firewalls



The application layer proxy firewall

- Advantages

- 1) the proxy server is placed in an unsecured area of the network or in the demilitarized zone (DMZ) so that it is exposed to the higher levels of risk from less trusted networks
 - rather than exposing the Web server to such risks
- 2) Additional filtering routers can be implemented behind the proxy server, limiting access to the more secure internal system and providing further protection

- Disadvantage

- Primary disadvantage of application layer proxy firewalls is that they are designed for one or a few specific protocols and cannot easily be reconfigured to protect against attacks on other protocols
- Because these firewalls work at the application layer by definition, they are typically restricted to a single application, such as FTP, Telnet, HTTP, SMTP, or SNMP
- The processing time and resources necessary to read each packet down to the application layer diminishes the ability of these firewalls to handle multiple types of applications

Firewalls



Media Access Control (MAC) Layer Firewall

- MAC layer firewalls make filtering decisions based on the host computer's media access control (MAC) or network interface card (NIC) address
- This firewall operates at the data link layer of the OSI model or the subnet layer of the TCP/IP model
- Thus, MAC layer firewalls link the addresses of specific host computers to Access Control List (ACL) entries
- ACL entries identify the specific types of packets that can be sent to each host, and block all other traffic

OSI (Open Source Interconnection) 7 Layer Model

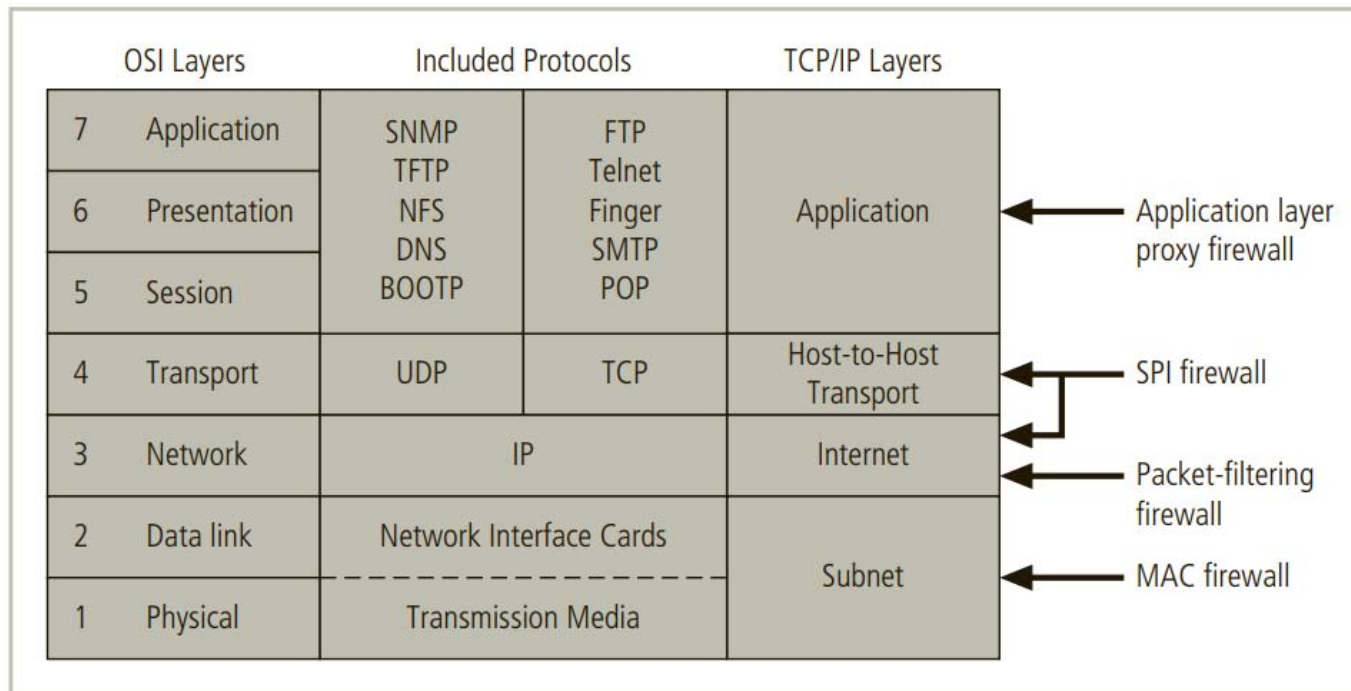
Layer	Application/Example	Central Device/Protocols	DOD4 Model
Application (7) Serves as the window for users and application processes to access the network services.	End User layer Program that opens what was sent or creates what is to be sent Resource sharing • Remote file access • Remote printer access • Directory services • Network management	User Applications SMTP	GATEWAY Process
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	Syntax layer encrypt & decrypt (if needed) Character code translation • Data conversion • Data compression • Data encryption • Character Set Translation	JPEG/ASCII EBDIC/TIFF/GIF PICT	
Session (5) Allows session establishment between processes running on different stations.	Synch & send to ports (logical ports) Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.	Logical Ports RPC/SQL/NFS NetBIOS names	
Transport (4) Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.	TCP Host to Host, Flow Control Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing	PACKET FILTERING TCP/SPX/UDP	Host to Host
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	Packets ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting		Internet
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	Frames ("envelopes", contains MAC address) [NIC card — Switch — NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control	Switch Bridge WAP PPP/SLIP	Can be used on all layers Network
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	Physical structure Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts	Hub Land Based Layers	

Source: Principles of Information Security by Whitman and Mattord

Firewalls



Firewalls



Stateful packet inspection (SPI or dynamic packet filtering) is a technology that monitors active connections and checks whether incoming data packets correspond to these connections. It then decides whether to grant or deny permission for them to pass the firewall.

Firewall types and protocol models



Thank You!