Course: Information Security Management in e-Governance

Day 2

Session 1: Securing your network (WAN and LAN)
Agenda

➢ Introduction to Data Networks, LAN and WAN
➢ Introduction to infrastructure elements of LAN and WAN
➢ Introduction to Data Center and IT infrastructure elements in a Data Center
➢ Security challenges and risks surrounding LAN and WAN environments
➢ Security challenges and risks surrounding IT Infrastructure in Data Center environments
➢ Information security measures and solutions for securing LAN, WAN and Data Center
Basic Terminology

Network

- A network is a group of computers/IT components connected together in such a way as to facilitate:
  
  • Data/voice/video Communication among people within and across building, locations, cities and countries
  
  • Sharing of data/files/documents within office, across offices (in the same city or across the cities)
  
  • Accessing the software applications and databases for performing business functions
How are Computers Connected on a Network?

IP (Internet Protocol): unique address that devices use in order to identify and communicate with each other on a computer network using the IP standard.
Some Network Terminologies

**LAN (Local Area Network)**
- A group of computers and associated devices that share a common communications line and typically share resources within a small geographic area (for example, within an office building)
- Used for connecting IT infrastructure (computers, printers, servers, scanners etc) existing in a particular office or building or a campus to facilitate sharing of information among the users

**WAN - (Wide Area Network)**
- Connecting systems or networks (LANs) spread across multiple locations/geographies/cities/countries
- Relies on a shared or a common communication backbone
- Used for connecting the IT infrastructure/LANs across multiple locations to facilitate sharing of information among users spread across different locations
LAN and WAN

Office 1 in Delhi

Office 2 in Mumbai

Leased Line

LAN

WAN

Switch

Serve

ROUTE

ROUTE

WA
Network Architectures

What is internet

A computer network consisting of a worldwide network of computer networks that use the TCP/IP network protocols to facilitate data transmission and exchange.

Internet is a public network for facilitating communication among the group of networks connected to the public network

What is Intranet

An intranet is a private computer network that uses Internet Protocol technologies to securely share any part of an organization's information or operational systems within that organization across multiple locations/geographies.
Importance of Security

• The Internet has undoubtedly become the largest public data network, enabling and facilitating both personal and business communications worldwide.

• The volume of traffic moving over the Internet, as well as corporate networks, is expanding exponentially every day.

• While the Internet has transformed and greatly improved the way we do business, this vast network and its associated technologies have opened the door to an increasing number of security threats from which corporations must protect themselves.

• An attack may directly cause several hours of downtime for employees, and networks must be taken down in order for damage to be repaired or data to be restored.

• Clearly, loss of precious time and data can greatly impact employee efficiency and morale !!!
Threats to Data

• A single hacker working from a basic computer can generate damage to a large number of computer networks that wreaks havoc around the world.

• Perhaps even more worrisome is the fact that the threats can come from people we know.

• In fact, most network security experts claim that the majority of network attacks are initiated by employees who work inside the corporations where breaches have occurred.

• Employees, through mischief, malice, or mistake, often manage to damage their own companies’ networks and destroy data.

• Remote employees and partners pose the same threats as internal employees, as well as the risk of security breaches if their remote networking assets are not properly secured and monitored.
Who are the enemies?

Hackers

- This generic term applies to computer enthusiasts who take pleasure in gaining access to other people’s computers or networks.

- Many hackers are content with simply breaking in and leaving their “footprints,” which are joke applications or messages on computer desktops.

- Other hackers, often referred to as “crackers,” are more malicious, crashing entire computer systems, stealing or damaging confidential data, defacing Web pages, and ultimately disrupting business.

- Some amateur hackers merely locate hacking tools online and deploy them without much understanding of how they work or their effects.
Who are the enemies?

Unaware Staff

• As employees focus on their specific job duties, they often overlook standard network security rules

• They might choose passwords that are very simple to remember so that they can log on to their networks easily

• Such passwords might be easy to guess or crack by hackers using simple common sense or a widely available password cracking software utility

• Employees can unconsciously cause other security breaches including the accidental contraction and spreading of computer viruses

• One of the most common ways to pick up a virus is from a floppy disk or by downloading files from the Internet. Employees who transport data via floppy disks can unwittingly infect their corporate networks with viruses they picked up from computers in copy centers or libraries

• They might not even know if viruses are resident on their PCs. Corporations also face the risk of infection when employees download files, such as PowerPoint presentations, from the Internet
Who are the enemies?

Disgruntled Staff

- Far more unsettling than the prospect of employee error causing harm to a network is the potential for an angry or vengeful staff member to inflict damage.
- Angry employees, often those who have been reprimanded, fired, or laid off, might vindictively infect their corporate networks with viruses or intentionally delete crucial files.
- This group is especially dangerous because it is usually far more aware of the network, the value of the information within it, where high-priority information is located, and the safeguards protecting it.
Causes of Intrusion

Intruders are always discovering new vulnerabilities (informally called "holes") to exploit in computer software.

• Users fail to obtain and install the latest patches/updates, or correctly configure the software to operate more securely.
• Most of the incidents could have been prevented if system administrators and users kept their computers up-to-date with patches and security fixes.
• Some default settings that allow other users to access your computer unless you change the settings to be more secure
What can these enemies do to Organizations

- Unauthorized Intrusions
- Denial of Service (DoS) Attacks
- Viruses, Worms, Trojan Horses (Backdoors)
- Vandals
- Data Interception
- Website Defacements
- Internal Attacks
- Non-compliance
Approach for securing IT Infrastructure
Eight Security Dimensions Address the Breadth of Network Vulnerabilities

- **Access Control**
  - Limit & control access to network elements, services & applications
  - Examples: password, ACL, firewall

- **Authentication**
  - Provide Proof of Identity
  - Examples: shared secret, PKI, digital signature, digital certificate

- **Non-repudiation**
  - Prevent ability to deny that an activity on the network occurred
  - Examples: system logs, digital signatures

- **Data Confidentiality**
  - Ensure confidentiality of data
  - Example: encryption

- **Communication Security**
  - Ensure information only flows from source to destination
  - Examples: VPN, MPLS, L2TP

- **Data Integrity**
  - Ensure data is received as sent or retrieved as stored
  - Examples: MD5, digital signature, anti-virus software

- **Availability**
  - Ensure network elements, services and application available to legitimate users
  - Examples: IDS/IPS, network redundancy, BC/DR

- **Privacy**
  - Ensure identification and network use is kept private
  - Examples: NAT, encryption

---

*Eight Security Dimensions applied to each Security Perspective (layer and plane)*
Defense-in-Depth

- Perimeter Defense
  - Perimeter Defences: Packet Filtering, Stateful Inspection of Packets, Intrusion Detection
  - Network Defences: VLAN Access Control Lists, Internal Firewall, Auditing, Intrusion Detection
  - Host Defences: Server Hardening, Host Intrusion Detection, IPSec Filtering, Auditing
  - Application Defences: AV, Content Scanning, Layer 7 (URL) Switching Source, Secure Web and Mail Servers
  - Data and Resources: Databases, Network Services and Applications, File Shares

- Network Defense
- Host Defense
- Application Defense
- Data & Resources

Assume Prior Layers Fail
We will discuss the following network security components

- Firewalls
- Intrusion Detection System
- Intrusion Prevention Systems
- Quarantine
- Routers
- AAA server
- Antivirus Gateway
- Virtual Private Networks
- Network Monitoring Tools
Firewalls

• A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both.

• Frequently used to prevent unauthorized internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

• A firewall is considered a first line of defense in protecting private information. For greater security, data can be encrypted.
Control Capabilities of Firewalls
Firewall rule sets

• A static rule-set is an unchanging statement to be applied to packet header, such as blocking all incoming traffic with certain source addresses.
• A dynamic rule set often is the result of coordinating a firewall and an IDS.

For example, an IDS that alerts on malicious activity may send a message to the firewall to block the incoming IP address.

The firewall, after ensuring the IP is not on a “white-list”, creates a rule to block the IP. After a specified period of time the rule expires and traffic is once again allowed from that IP.
Packet Filter Firewalls

• Packet filter firewalls evaluate the headers of each incoming and outgoing packet to ensure it has a valid internal address, originates from a permitted external address, connects to an authorized protocol or service, and contains valid basic header instructions.
• If the packet does not match the pre-defined policy for allowed traffic, then the firewall drops the packet.

Stateful Inspection Firewalls

• Stateful inspection firewalls are packet filters that monitor the state of the TCP connection. Each TCP session starts with an initial “handshake” communicated through TCP flags in the header information.
• When a connection is established the firewall adds the connection information to a table.
• The firewall can then compare future packets to the connection or state table. This essentially verifies that inbound traffic is in response to requests initiated from inside the firewall
Proxy Server Firewalls

- Proxy servers act as an intermediary between internal and external IP addresses and block direct access to the internal network.

- Essentially, they rewrite packet headers to substitute the IP of the proxy server for the IP of the internal machine and forward packets to and from the internal and external machines. Due to that limited capability, proxy servers are commonly employed behind other firewall devices.

- Proxy servers provide another layer of access control by segregating the flow of Internet traffic to support additional authentication and logging capability, as well as content filtering.

- They may implement anti-virus and anti-spam filtering, disallow connections to potentially malicious servers, and disallow the downloading of files in accordance with the institution’s security policy.
Application-Level Firewalls

- Application-level firewalls perform application-level screening, typically including the filtering capabilities of packet filter firewalls with additional validation of the packet content based on the application.

- Application-level firewalls capture and compare packets to state information in the connection tables. Unlike a packet filter firewall, an application level firewall continues to examine each packet after the initial connection is established for specific application or services such as telnet, FTP, HTTP, SMTP, etc.

- The application-level firewall can provide additional screening of the packet payload for commands, protocols, packet length, authorization, content, or invalid headers.

- Application level firewalls provide the strongest level of security, but are slower and require greater expertise to administer properly.
Firewall Services and Configuration

Firewalls may provide some additional services:

Network address translation (NAT)
- NAT readdresses outbound packets to mask the internal IP addresses of the network.
- Untrusted networks see a different host IP address from the actual internal address. NAT allows an institution to hide the topology and address schemes of its trusted network from untrusted networks.

Dynamic host configuration protocol (DHCP)
- DHCP assigns IP addresses to machines that will be subject to the security controls of the firewall.
Firewall Services and Configuration cont’d

Virtual Private Network (VPN) gateways

- A VPN gateway provides an encrypted tunnel between a remote external gateway and the internal network.
- Placing VPN capability on the firewall and the remote gateway protects information from disclosure between the gateways but not from the gateway to the terminating machines.
- Placement on the firewall, however, allows the firewall to inspect the traffic and perform access control, logging, and malicious code scanning.
Firewall Policy

- A firewall policy states management’s expectations for how the firewall should function and is a component of the overall security policy.

- It should establish rules for traffic coming into and going out of the security domain and how the firewall will be managed and updated.

- Therefore, it is a type of security policy for the firewall and forms the basis for the firewall rules.

- The firewall selection and the firewall policy should stem from the ongoing security risk assessment process.

- Accordingly, management needs to update the firewall policy as the institution's security needs and the risks change.
Firewall Policy - Contd

At a minimum, the policy should address

- Firewall topology and architecture,
- Type of firewall(s) being utilized,
- Physical placement of the firewall components,
- Monitoring firewall traffic,
- Permissible traffic,
- Firewall updating,
- Coordination with security monitoring and intrusion response mechanisms,
- Responsibility for monitoring and enforcing the firewall policy,
- Protocols and applications permitted,
- Regular auditing of a firewall’s configuration and testing of the firewall’s effectiveness, and
- Contingency planning.
Intrusion Detection System

**IDS** system analyzes and identifies attempts to hack or break into a computer system.

- Identifies attacks through various methods including
  - anomaly detection
  - signature matching

- Types
  - Host IDS
  - Network IDS

**IPS**

- Inline device
- Single box approach
- False Positive
Types of IDS

**Application IDS**
- Watch application logs
- Watch user actions
- Stop attacks targeted against an application
- Advantages
  - Encrypted data can be read
- Problems
  - Positioned too high in the attack chain (the attacks reach the application)

**Host IDS**
- Watch kernel operations
- Watch network interface
- Stop illegal system operations
- Drop attack packets at network driver
- Advantages
  - Encrypted data can be read
  - Each host contributes to the detection process
- Problems
  - Positioned too high in the attack chain (the attacks reach the network driver)

**Network IDS**
- Watch network traffic
- Watch active services and servers
- Report and possibly stop network level attacks
- Advantages
  - Attacks can be stopped early enough (before they reach the hosts or applications)
  - Attack information from different subnets can be correlated
- Problems
  - Encrypted data cannot be read
  - Annoyances to normal traffic if for some reason normal traffic is dropped
Positioning of IDS / IPS
Network Intrusion Prevention Systems

Network Intrusion Prevention Systems (NIPS) are an access control mechanism that allow or disallow access based on an analysis of packet headers and packet payloads.

An **Intrusion Prevention System** is a network security device that monitors network and/or system activities for malicious or unwanted behavior and can react, in real time, to block or prevent those activities.

They are similar to firewalls because they are located in the communications line, compare activity to preconfigured or preprogrammed decisions of what packets to pass or drop, and respond with pre-configured actions.
Network Intrusion Prevention Systems (contd)

The IPS units generally detect security events in a manner similar to IDS units and are subject to the same limitations.

After detection, however, the IPS unit may take actions beyond simple alerting to potential malicious activity and logging of packets.

For example, the IPS unit may block traffic flows from the offending host. The ability to sever communications can be useful when the activity can clearly be identified as malicious.

When the activity cannot be clearly identified, for example where a false positive may exist, IDS-like alerting commonly is preferable to blocking.
IPS basics

• **Intrusion detection**: It is the process of monitoring the events occurring in a computer systems or network and analyzing them for signs of possible intrusions (incident)

• **Intrusion detection systems**: It is a software that automates the intrusion detection process. The primary responsibility of an IDS is to detect unwanted and malicious activities

• **Intrusion prevention systems**: It is a software that has all the capabilities of an intrusion detection system and can also attempt to stop possible incidents
Intrusion Detection - Definition

Intrusion detection is a technique of detecting unauthorized access to a computer system or a computer network.

An intrusion into a system is an attempt by an outsider to the system to illegally gain access to the system. Intrusion prevention, on the other hand, is the art of preventing an unauthorized access of a system’s resources.

The two processes are related in a sense that while intrusion detection passively detects system intrusions, intrusion prevention actively filters network traffic to prevent intrusion attempts.
What can an IPS do?

IPS can detect and block:

- OS, Web and database attacks
- Spyware / Malware
- Instant Messenger
- Peer to Peer (P2P)
- Worm propagation
- Critical outbound data loss (data leakage)
Functions of IDS

The functions of Intrusion detection includes:

• Monitoring and analyzing both user and system activities
• Analyzing system configurations and vulnerabilities
• Assessing system and file integrity
• Ability to recognize patterns typical of attacks
• Analysis of abnormal activity patterns
• Tracking user policy violations.
IDS Working Procedures

Types of IDS
- Host Based IDS
- Network Based IDS
- Hybrid Intrusion Detection
- Network-Node Intrusion Detection (NNID)
Host-based Intrusion Detection Systems

- Host-based Intrusion Detection Systems are designed to monitor, detect, and respond to user and system activities and attacks on a given host.
- Host Intrusion can be used to fight out internal threats because of its ability to monitor and respond to specific user actions and file accesses on the host.

Host based IDS are equipped with tools which will:
- Audit policy management and centralization
- Supply data forensics
- Statistical analysis and evidentiary support
- Provide some measure of access control in certain instances
HIDS Advantages

Some of the HIDS advantages are

- **Host Level protection**: They are better than NIDS at monitoring and keeping track of local system events. Because Host-based only protects a single system, switches, VPN, and routers do not affect their functionality.

- **Encrypted Attacks**: They aren’t typically hindered by encrypted attacks. Host-based IDS can read transmitted packets before they are encrypted and received packets after they are decrypted.

- **Integrity Breaches**: They can help to detect software integrity breaches, such as Trojan horse software, file modifications, and so on.

Periodically analyze logs, perform file system integrity check
Network IDS

Network intrusion detection deals with data packets flowing through the wire between the hosts.

Also referred to as “packet-sniffers,” NID devices intercept packets traveling along various communication mediums and protocols, usually TCP/IP

Network Based IDS Advantages-
- Increase overall security
- Protect multiple systems
- Allow monitoring traffic inside your firewall
- Alert you to incoming attacks
- Detect slow attacks
- Delayed analysis
- Take corrective action
Hybrid Intrusion Detection

- A Hybrid IDS is a combination of host-based IDS and network IDS technologies. Hybrid intrusion detection provides attack recognition on the network packets flowing to and from a single and is host system-based.
- Hybrid IDS offer management and alert notification from both network and host based intrusion detection devices.
- A Hybrid IDS offers the best of HIDS and NIDS technologies providing attack recognition on the network packets flowing to and from single hosts.
Network-node Intrusion Detection

- Network-node captures the packet-intercepting technology of the wire and puts it on the hosts.

- With NNID, the *packet-sniffer* is positioned in such a way that it captures packets after the destination host.

**Advantages of NNIDS**

- The advantage to NNID is its ability to defend specific hosts against packet-based attacks in these complex environments where conventional NID is ineffective.

- Since the NNIDS system is not expected to examine individual packet on the wire it is relatively much faster and also less resource intensive. Thus it can be installed on existing servers without imposing too much burden.

- NNID is suitable for heavy traffic networks, switched network environments, or VPN implementations with encrypted traffic on the wire.
Quarantine

- Quarantining a device protects the network from potentially malicious code or actions.
- Typically, a device connecting to a security domain is queried for conformance to the domain’s security policy.
- If the device does not conform, it is placed in a restricted part of the network until it does conform.
- For example, if the patch level is not current, the device is not allowed into the security domain until the appropriate patches are downloaded and installed.
Routers

In larger, more complex networks, data must be directed specifically to the intended destination. **Routers** direct network data messages, or packets, based on internal addresses and tables of routes, or known destinations that serve certain addresses. Directing data between portions of a network is the primary purpose of a router.
Controlling access to a router by administrators is an important issue. There are two types of access: Local and Remote.

- Local access usually involves a direct connection to a console port on the router with a dumb terminal or a laptop computer.
- Remote access typically involves allowing Telnet or SNMP connections to the router from some computer on the same subnet or a different subnet.
  - It is recommended only allow local access because during remote access all telnet passwords or SNMP community strings are sent in clear to the router.
  - If an attacker can collect network traffic during remote access then he can capture passwords or community strings.
Router - Secure Remote Management Access

If the router that needs to be managed is remote from the actual administrator; often it is only accessible over public networks.

To secure the management traffic between client/administrator and target network device, encrypting protocols are required.

- SSH is the de-facto standard for all remote command line configurations and file transfers.
- For Web-based management, using Secure Socket Layer (SSL) or Transport Layer Security (TLS) secures HTTP traffic.
- SNMP is used to discover, monitor and configure networking devices. The secure implementation of SNMP version 3 is essential to ensure confidential and authenticated communications.
Router- Secure Remote Management Access

If the router that needs to be managed is remote from the actual administrator; often it is only accessible over public networks.

To secure the management traffic between client/administrator and target network device, encrypting protocols are required.

- The best way to control the identity of the administrator and the privileges allocated to that individual is to authenticate an administrator prior to granting access.
- This can be done through Authentication, Authorization and Accounting (AAA) servers, such as Remote Authentication Dial-in User Service (RADIUS), Terminal Access Controller Access Control System (TACACS) or Lightweight Directory Access Protocol (LDAP) directory servers.
- AAA servers can also be supplemented by strong authentication techniques.
AAA Components

AAA server
- Authenticates users accessing a device or network
- Authorizes user to perform specific activities
- Performs accounting of device or user activities

Network Access Server (NAS) or Access Device
- A router, switch, or other network device that can perform AAA functions on users or devices connecting to it

RADIUS or TACACS+
- Protocols that can be used by an access device to communicate with the AAA server
Note: AAA server may communicate with a Windows domain controller or a Unix server that has the user password database.
How the AAA server works

1. User name/password entered on client device
2. Protocol
   - VPN: L2TP/IPSec
   - LAN: 802.1x
   - Web: HTTPS
   ...Etc.
3. Web Server, VPN Gateway, Firewall, WLAN Acess Point, Unix (login/SSH,...) etc
4. Protocol
   - RADIUS
5. AAA Server
   - Authenticates password
   - Tracks and logs user session
Virtual Private Networks
Traditional Connectivity

[From Gartner Consulting]
What is VPN?

- Virtual Private Network is a type of private network that uses public telecommunication, such as the Internet, instead of leased lines to communicate.

- Became popular as more employees worked in remote locations.
Private Networks vs. Virtual Private Networks

- Employees can access the network (Intranet) from remote locations.
- Secured networks.
- The Internet is used as the backbone for VPNs
- Saves cost tremendously from reduction of equipment and maintenance costs.
- Scalability
Remote Access Virtual Private Network

(From Gartner Consulting)
Brief Overview of How VPN Works

- Two connections – one is made to the Internet and the second is made to the VPN.
- Datagrams – contains data, destination and source information.
- Firewalls – VPNs allow authorized users to pass through the firewalls.
- Protocols – protocols create the VPN tunnels.
Four Critical Functions

• Authentication – validates that the data was sent from the sender.
• Access control – limiting unauthorized users from accessing the network.
• Confidentiality – preventing the data to be read or copied as the data is being transported.
• Data Integrity – ensuring that the data has not been altered
Encryption

- Encryption -- is a method of “scrambling” data before transmitting it onto the Internet.
- Public Key Encryption Technique
- Digital signature – for authentication
Tunneling

A virtual point-to-point connection made through a public network. It transports encapsulated datagrams.

Two types of end points:
- Remote Access
- Site-to-Site
Virtual Private Networks (VPN)
Basic Architecture
Antivirus Gateway

- The most common transmission routes for viruses and worms are through email and Web traffic.
- In addition, the growing volume of unsolicited email (spam) and inappropriate Web surfing poses risks to corporate security, liability, and employee productivity.
- Effective security at every network tier—especially virus protection at the Internet gateway—is essential in today’s Internet-enabled network environments.
- Gateway Solution provides multi-layered protection against viruses, spam, and unwanted email and Web content at the Internet gateway.
Managing Enterprise Network Security
What are Network Monitoring Tools?

- Allows the administrator to know the health status of the network.
- It provides information about collected data and the analysis of such raw data with a view to using scarce or limited resources effectively.
- Uses network probe. Probes let you isolate traffic problems and congestions slowing your network to a crawl.
- Network Monitoring tools can apply various security policies at the click of a mouse to all the network devices available in the network.
Network Management: Why is it needed

- Lowers costs by eliminating the need for many administrators at multiple locations performing the same function
- Makes network administration and monitoring easier and more convenient
- Coherent presentation of data
Network Management: Why is it needed cont’d

• Performance Management – how smoothly is the network running

• Fault Management - reactive and proactive network fault management (deals with problems and emergencies in the network)

• Configuration Management – keeping track of device settings and how they function

• Accounting Management - cost management and charge back assessment

• Security Management - SNMP (Version 1 and 2) doesn’t provide much here
What can we use the tools for?

- Identifying unofficial services or servers
- Monitoring usage and traffic statistics
- Troubleshooting your network
- Investigating a security incident
- Keeping logs of users activities for accountability
- Application of organization wide security policies to the network devices
Who? What? Where? How? When?.. Some question you need to know

Who is accessing your network?
- students, academics, staff, visitors or others

What are they accessing your network for?
- academic study, social use, business use, illegal use

Where are they accessing your network from?
- internal, external

How are they accessing your network?
- remote user, local Ethernet, WAN, dial-up, Wi-Fi, VPN

When did they access your network?
- today, yesterday, last week, last month...
Active vs. Passive

- Active – relies upon data gathered from probe packets injected into the network.

- Passive – relies upon data gathered from active network traffic.
Thank you