IA 221: Network Security

Lecture 1: Introduction to Network Security

What is Network Security?

- Network security deals with provisions and policies adopted to prevent and monitor unauthorized access, misuse, modification, or denial of the computer network and network-accessible resources.
- Reasons for Network Security
  - Network security breaches can disrupt e-commerce, cause the loss of business data, threaten people’s privacy, and compromise the integrity of information.

Security Objectives

- **Confidentiality**: prevent/detect/deter improper **disclosure** of information
- **Integrity**: prevent/detect/deter improper modification of information
- **Availability**: prevent/detect/deter improper **denial of access** to services

Military Example

- **Confidentiality**: target coordinates of a missile should not be improperly disclosed
- **Integrity**: target coordinates of missile should be correct
- **Availability**: missile should fire when proper command is issued

Commercial Example

- **Confidentiality**: patient’s medical information should not be improperly disclosed
- **Integrity**: patient’s medical information should be correct
- **Availability**: patient’s medical information can be accessed when needed for treatment

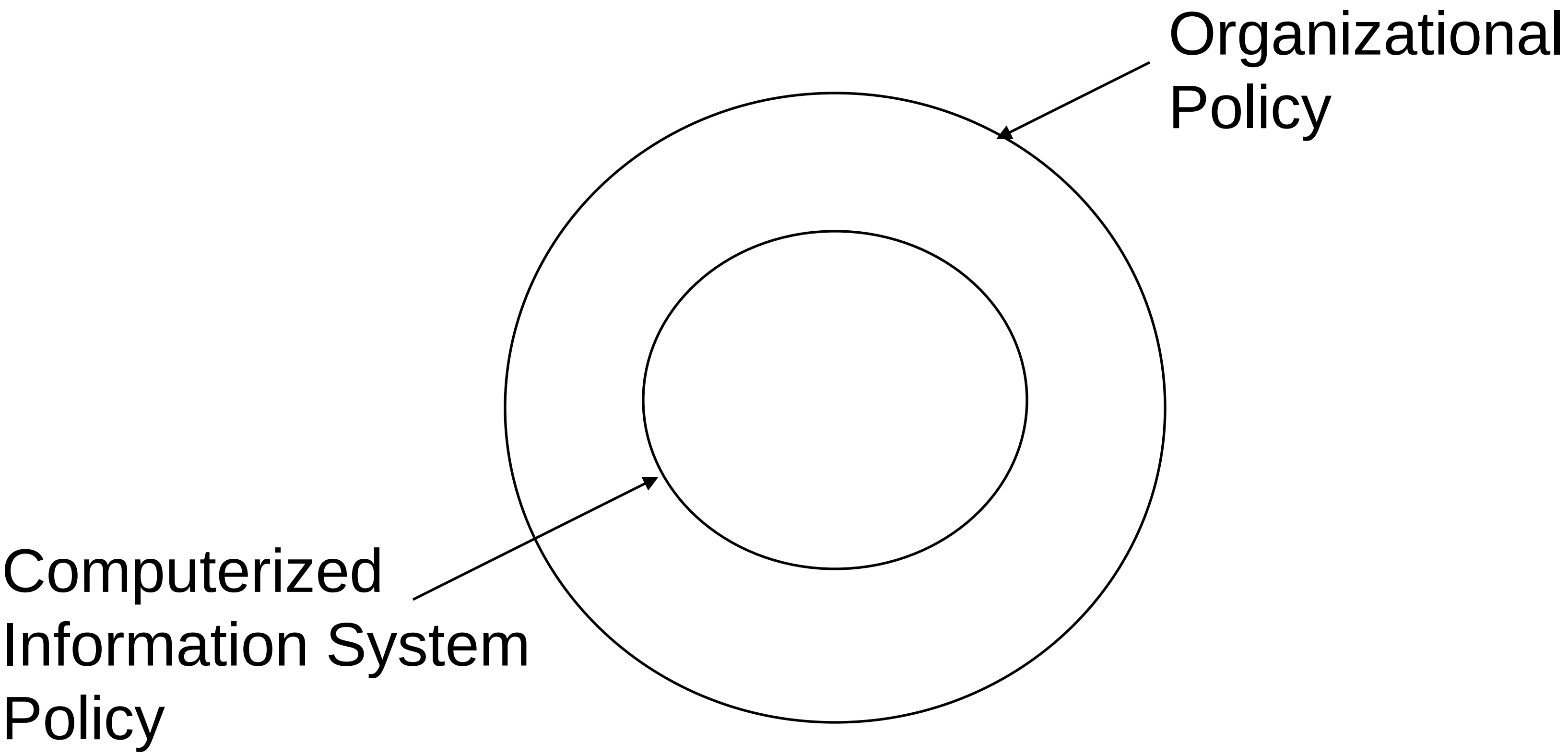
Fourth Objective

- Securing **computing resources**: prevent/detect/deter improper **use** of computing resources
    - Hardware
    - Software
    - Data
    - Network

Achieving Security

- Policy
  - What to protect?
- Mechanism
  - How to protect?
- Assurance
  - How good is the protection?

Security Policy



Organizational Policy

Computerized Information System Policy

Security Mechanism

- Prevention
- Detection
- Tolerance/Recovery

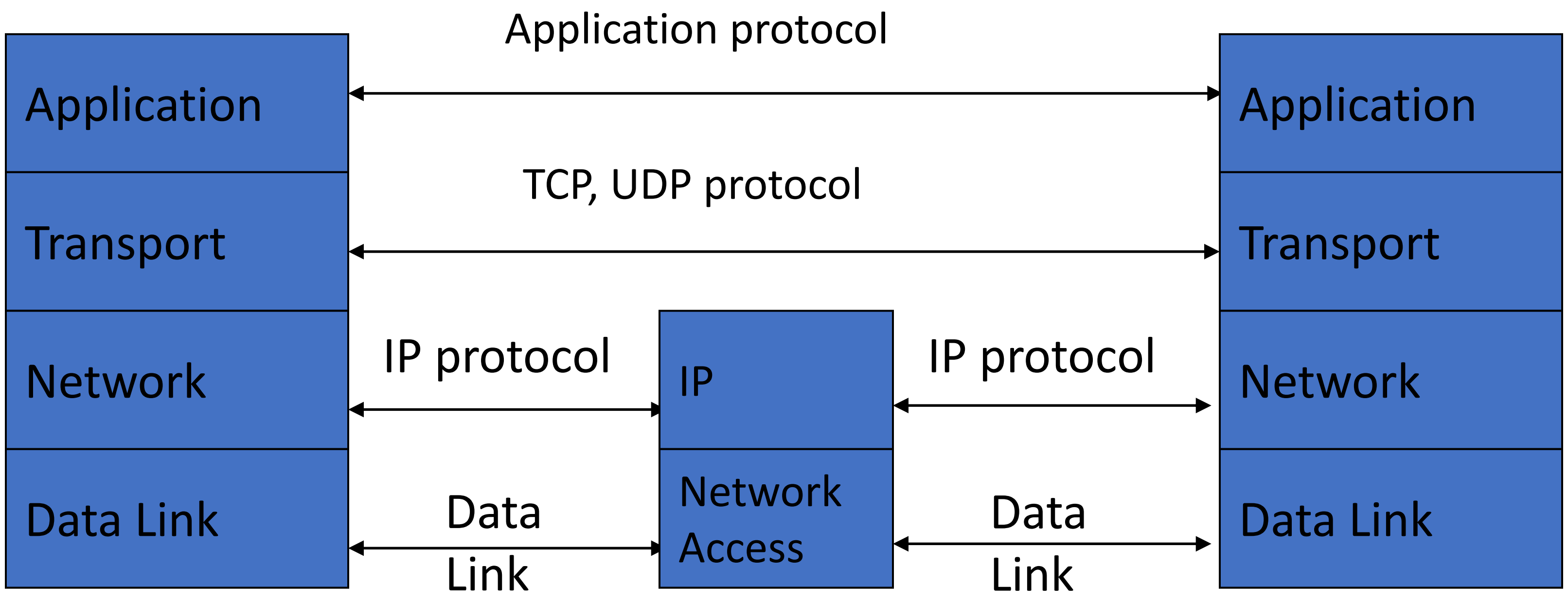
Threat, Vulnerability, Risk

- **Threat**: potential occurrence that can have an undesired effect on the system
- **Vulnerability**: characteristics of the system that makes is possible for a threat to potentially occur
- **Attack**: action of malicious intruder that exploits vulnerabilities of the system to cause a threat to occur
- **Risk**: measure of the possibility of security breaches and severity of the damage

Methods of Defense

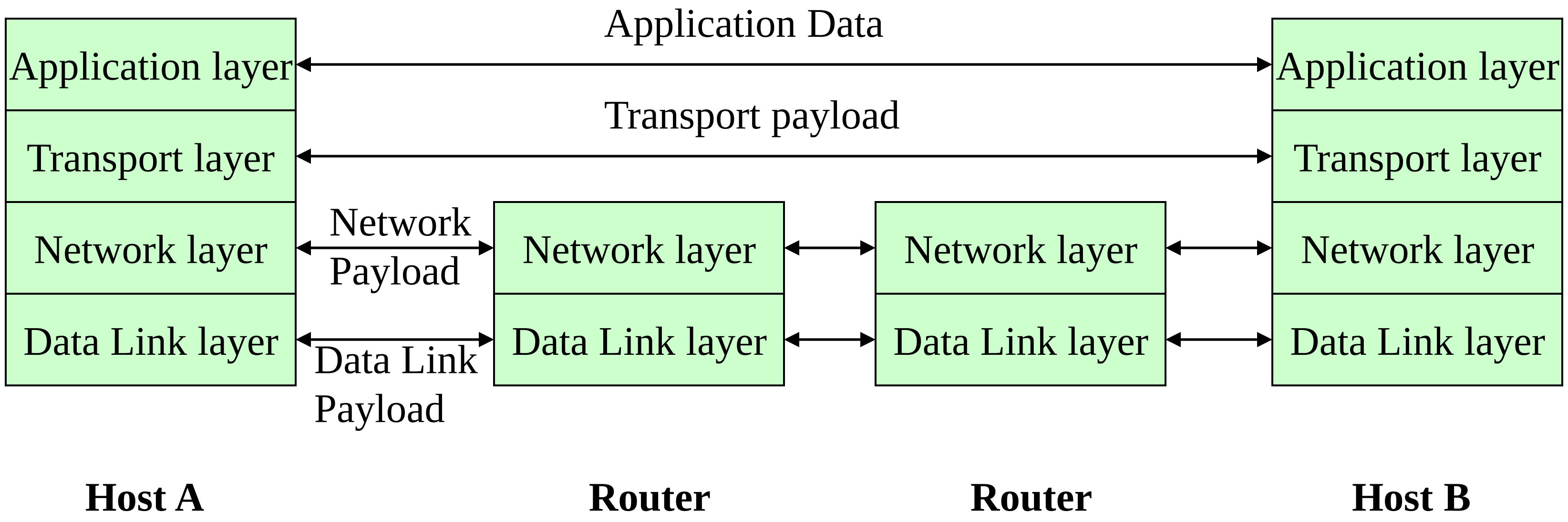
- **Prevent**: block attack
- **Deter**: make the attack harder
- **Deflect**: make other targets more attractive
- **Detect**: identify misuse
- **Tolerate**: function under attack
- **Recover**: restore to correct state
- **Documentation** and **reporting**

TCP/IP Protocol Stack



Transport layer provides *ports*, logical channels identified by number

Communication Between Layers



TCP/IP Protocol Stack …

- Application layer: the communicating processes themselves and the actual ‘content’ transmitted
- Transport layer (TCP/UDP): “end-to-end” communication; reliability; flow control
- Network layer (IP): “host-to-host” communication; routing
- Data link layer (Ethernet/WiFi): transmission of frames over a single hop

TCP/IP Layers and Vulnerabilities

- After reviewed the four communication layers used with the TCP/IP suite and can identify the information that is contained in an IP datagram, you should consider the types of attacks that might occur at each level.
- This is not meant to be a comprehensive list; rather it provides you with an understanding of the types of attacks that can occur at different levels.

Identifying Possible Data Link Layer Attacks

- Identifying Possible Data Link Layer Attacks
  - At the Data link layer, the packet of information that is placed on the wire is known as a frame.
  - The packet is comprised of three areas: the header, the payload, and the FCS.
  - Because the Data link layer is used for communications on a local network, the attacks that occur at this level would be carried out on local networks.

Data link Layer Attacks

- MAC address spoofing

  The header contains the MAC address of the source and destination computers and is required to successfully send a directed message from a source computer to a destination computer. Attackers can easily spoof the MAC address of another computer. Any security mechanism based on MAC addresses is vulnerable to this type of attack.

- Denial of service (DoS)

  A DoS attack overloads a single system so that it cannot provide the service it is configured to provide. An ARP protocol attack could be launched against a computer to overwhelm it, which would make it unavailable to support the C-I-A triad.

- ARP cache poisoning

  The ARP(**A**ddress **R**esolution **P**rotocol. A TCP/IP protocol for determining the hardware address (or physical address) of a node on a local area network connected to the Internet) cache stores MAC (**M**edia **A**ccess **C**ontrol) addresses of computers on the local network that have been contacted within a certain amount of time in memory. If incorrect, or spoofed, entries were added to the ARP cache, then the computer is not able to send information to the correct destination.

Identifying Possible Network Layer Attacks

- At the Network layer, IP datagrams are formed. The packet is comprised of two areas: the header and the payload. Some of the ways the Internet layer can be exploited to compromise the C-I-A triad include the following:
  - IP address spoofing

  If the IP header fields and lengths are known, the IP address in the IP datagram can be easily discovered and spoofed. Any security mechanism based on the source IP address is vulnerable to this attack.

  - Man-in-the-middle attacks.

  This attack occurs when a hacker places himself or herself between the source and destination computer in such a way that neither notices his or her existence. Meanwhile, the attacker can modify packets or simply view their contents.

Identifying Possible Network Layer Attacks …

- DoS

  With a DoS attack at this level, simple IP-level protocols and utilities can be exploited to overload a computer, thus breaking the C-I-A triad.

- Incorrect reassembly of fragmented datagrams

  For fragmented datagrams, the Offset field is used with packet reassembly. If the offset is changed, the datagram is reformed incorrectly. This could allow a datagram that would typically not pass through a firewall to gain access to your internal network, and could disrupt the C-I-A triad.

- Corrupting packets

  Because IP datagrams can pass through several computers between the source and destination, the information in the IP header fields is read and sometimes modified, such as when the information reaches a router. If the packet is intercepted, the information in the header can be modified, corrupting the IP datagram. This could cause the datagram to never reach the destination computer, or it could change the protocols and payload information in the datagram.

Identifying Possible Transport Layer Attacks

- At the Transport layer, either a UDP header is added to the message or a TCP header is added. The application that is requesting the service determines what protocol will be used. Some of the ways the Transport layer can be exploited to compromise the C-I-A triad include the following:
  - Manipulation of the UDP or TCP ports.

  By knowing the UDP and TCP header fields and lengths, the ports that are used for communications between a source and destination computer can be identified, and that information can be corrupted or exploited.

Identifying Possible Transport Layer Attacks …

- DoS
  - With a DoS attack at this level, simple IP-level protocols and utilities can be exploited to overload a computer, thus breaking the C-I-A triad. For instance, by knowing the steps involved in a three-way TCP handshake, a hacker or cracker might send the packets in the incorrect order and disrupt the availability of one of your servers. An example of this is a SYN flood, where a hacker sends a large number of SYN packets to a server and leaves the session half open. The server leaves these sessions half-open for a prescribed amount of time. If the hacker is successful in opening all available sessions, legitimate traffic will be unable to reach the server.
- Session hijacking.
  - This kind of attack occurs after a source and destination computer have established a communications link. A third computer disables the ability of one the computers to communicate, and then imitates that computer. Because the connection has already been established, the third computer can disrupt your C-I-A triad.

Identifying Possible Application Layer Attacks

- Application layer attacks can be some of the most difficult to protect against because they take advantage of vulnerabilities in applications and lack of end-user knowledge of computer security. Some of the ways the Application layer can be exploited to compromise the C-I-A triad include the following:
- E-mail application exploits.
  - Attachments can be added to e-mail messages and delivered to a user's inbox. The user can open the e-mail message and run the application. The attachment might do immediate damage, or might lay dormant and be used later. Similarly, hackers often embed malicious code in Hypertext Markup Language (HTML) formatted messages. Exploits of this nature might take advantage of vulnerability in the client's e-mail application or a lack of user knowledge about e-mail security concerns.

Identifying Possible Application Layer Attacks …

- Web browser exploits.
  - When a client computer uses a Web browser to connect to a Web server and download a Web page, the content of the Web page can be active. That is, the content is not just static information, but can be executable code. If the code is malicious, it can be used to disrupt the C-I-A triad.
- FTP client exploits.
  - File Transfer Protocol (FTP) is used to transfer files from one computer to another. When a client has to provide a user name and password for authentication, that information can be sent across the Internet using plain text. The information can be captured at any point along the way. If the client uses the same user name and password as they use to attach to your corporate servers, that information could be obtained by a hacker or cracker and used to access your company's information.

Building Blocks for Network Security

- Encryption and authentication algorithms are building blocks of secure network protocols
- Deploying cryptographic algorithms at different layers have different security effects
- Where should we put the security protocol in the network architecture?

Security in what layer?

- Depends on the purpose…
  - How are keys provisioned/shared?
  - Should the (human) user be involved?
  - Semantics: authenticate user-to-user, or host-to-host?

Security in what layer?

- Depends on what's available
  - E.g., consider a user connecting to a website from a café (over a wireless network)
  - End-to-end encryption might be unavailable (e.g., if website does not support encryption)
  - Eavesdropping on Internet backbone less likely than eavesdropping on wireless link in café
  - Encrypt link from user to wireless router
  - Link-layer encryption more appropriate
    - Link-layer authentication also possible

Security in what layer?

- Depends on the threat model/what threats are being addressed
  - What information needs to be protected? (Ports, IP addresses?)
  - E.g., network-layer authentication will not prevent DoS attacks at link level (e.g., ARP spoofing, replay disconnect messages, overloading access point)
  - E.g., an application-layer protocol cannot protect IP header information
  - End-to-end, or hop-by-hop?

Security in what layer?

- Security interactions with various layers
  - E.g., if TCP accepts a packet which is rejected by the application above it, then TCP will reject the “correct” packet (detecting a replay) when it arrives!
  - E.g., if higher-layer header data is used by a firewall to make decisions, this is incompatible with network-layer encryption (if it encrypts headers)

Security -- At What Level?

- Secure traffic at various levels in the network
- Where to implement security? -- Depends on the security requirements of the application and the user
- Basic services that need to be implemented:
    - Key management
    - Confidentiality
    - Nonrepudiation
    - Integrity/authentication
    - Authorization

Network Access (Data Link) Layer Security

- Dedicated link between hosts/routers → hardware devices for encryption
- Advantages:
    - Speed
- Disadvantages:
    - Not scaleable
    - Works well only on dedicates links
    - Two hardware devices need to be physically connected

Internetwork (Network) Layer Security

IP Security (IPSec)

- At the IP layer, implementation is quite complicated since every device must be enabled.
- It also provides services to many other protocols like OSPF, ICMP, IGMP, etc.
- IP Security (IPSec) is a protocol that provides security at the IP layer.

- Advantages:
  - Overhead involved with key negotiation decreases <-- multiple protocols can share the same key management infrastructure
  - Ability to build VPN and intranet
- Disadvantages:
  - Difficult to handle low granularity security, e.g., nonrepudiation, user-based security,

Transport Layer Security

Transport Layer:

  - Quite complicated.
  - New layer glues with the transport layer to provide security at this layer.

- <u>Advantages:</u>
  - Does not require enhancement to each application
- <u>Disadvantages:</u>
  - Obtaining user context gets complicated
  - Protocol specific --> need to be duplicated for each transport protocol
    - Implemented for each protocol
    - Must maintain context for a connection
  - Implemented on an end system (Transport Layer Security)

Application Layer Security

Application Layer:

  - Simplest. It concerns the client and the server.

- <u>Advantages:</u>
  - Executing in the context of the user --> easy access to user's credentials
  - Complete access to data --> easier to ensure nonrepudation
  - Application can be extended to provide security (do not depend on the operating system)
  - Application understand data --> fine tune security
- <u>Disadvantages:</u>
  - Implemented in end hosts
  - Security mechanisms have to be implemented for each application -->
    - expensive
    - greated probability of making mistake

Application Example

- E-mail client using PGP
- Extended capabilities
  - Ability to look up public keys of the users
  - Ability to provide securiy services such as encryption/decrytion, nonrepudation, and authentication for e-mail messages

Security in what layer?

- Generally…
  - When security is placed at lower levels, it can provide automatic, “blanket” coverage…
    - …but it can take a long time before it is widely adopted
    - Can be inefficient to encrypt everything
  - When security is placed at higher levels, individual users can choose when to use it…
    - …but users who are not security-conscious may not take advantage of it
    - Can encrypt only what is necessary

Example: PGP vs. SSL vs. IPsec

- PGP is an application-level protocol for “secure email”
  - Can provide security over insecure networks
  - Users choose when to use PGP; user must be involved
  - Alice’s signature on an email proves that Alice actually generated the message, and it was received unaltered; also non-repudiation
    - In contrast, SSL secures “the connection” from Alice’s computer; would need additional mechanisms to authenticate the user
  - Communication with off-line party (i.e., email)

Example: PGP vs. SSL vs. IPsec …

- SSL sits at the transport layer, “above” TCP
  - Packet stream authenticated/encrypted
  - End-to-end security, best for connection-oriented sessions (e.g., http traffic)
  - User does not need to be involved
  - The OS does not have to change, but applications do if they want to communicate securely

Example: PGP vs. SSL vs. IPsec …

- IPsec sits at the network layer
  - Individual packets authenticated/encrypted
  - End-to-end or hop-by-hop security
  - Need to modify OS
  - All applications “protected” by default, without requiring any change to applications or actions on behalf of users
  - Only authenticates hosts, not users
  - User can be completely unaware that IPsec is running