Network Security: Threats and Goals

ENCS5322, NETWORK SECURITY PROTOCOLS

First Semester 2024-2025

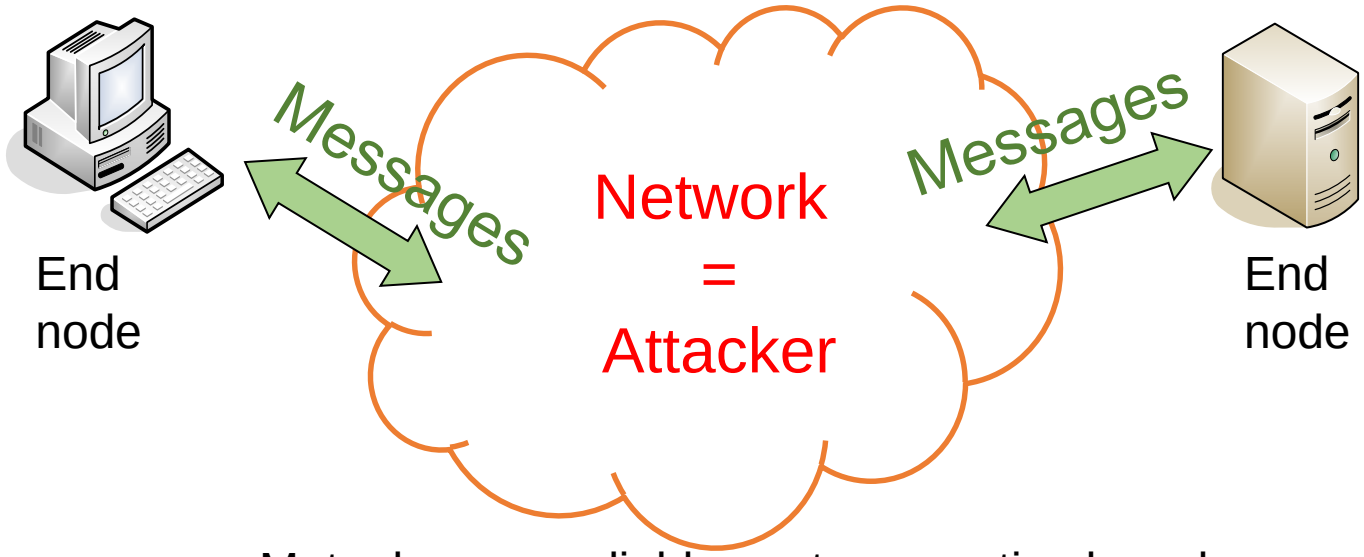
Outline

1. Network security
2. Attacker model
3. Threats
4. Sniffing and spoofing

What is network security

- Network security protects against intentional bad things done to communication
  - Protect both messages (data in transit) and the communication infrastructure
- Communication is everywhere
  - Telecommunications, mobile networks, computer networks, wireless networks, personal-area networks, IoT devices
  - Application-level protocols, overlays, P2P, content distribution and protection, VPN, service mesh (service-to-service communications)
  - Inter-process communication, APIs, events, message bus
  - Contacts, payment, value storage and transfer, distributed ledger
  - Human protocols (“ceremonies”), physical security tokens, letters, paper certificates

Traditional network-security threat model (Dolev-Yao model)



Metaphors: unreliable postman, notice board

- End nodes are trusted, the network is unreliable
- End nodes send messages to the network and receive messages from it
- Network delivers some messages but can read, delete, modify and replay
- Messages can be protected with cryptography, or sometimes with logical or physical isolation

Basic network security threats

- Traditional major threats:
  - Sniffing = attacker listens to network traffic
  - Spoofing = attacker sends unauthentic messages
  - Data modification, man in the middle = on-path attacker = attacker intercepts and modifies data
  - Denial of service
- Corresponding security requirements:
  - Data confidentiality
  - Data-origin authentication and data integrity
  - Availability

Sniffing

- Sniffing = eavesdropping = spying = snooping = unauthorized listening = monitoring = capturing = interception
- Eavesdroppers must be on the communication route
- On the Internet, a MitM attacker could
  - at the local network of one of the end points
  - at a link or router on the route between them, or
  - change the routing to redirect the packets via its own location
- Many potential eavesdroppers – but still a small minority of all internet nodes (unlike in the Dolev-Yao model)

How to capture more traffic?

- Provide free wireless access, or spoof SSIDs (service set identifiers)
- DNS poisoning
- Pretend to be the target on the local link
  - Address Resolution Protocol (ARP) poisoning
  - IPv6 Neighbor Discovery (ND) spoofing
- Advertise better route to the destination
  - Border Gateway Protocol (BGP) prefix hijacking
  - Intra-domain routing protocol may be similarly vulnerable
- Topology spoofing on switched networks and Software-defined networking (SDN)
  - Lie during topology discovery (e.g., Link Layer Topology Discovery (LLTD))
  - Create virtual shortcut links that become part of the shortest route
- Volunteer as Tor exit node or sell VPN service

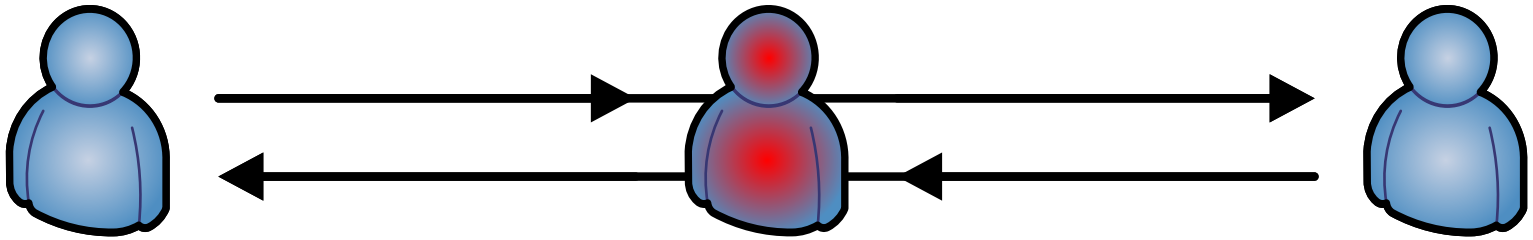
WiFi Pineapple

Spoofing

- Spoofing = sending unauthentic/false/counterfeit messages = using false sender address or identifier = impersonation
- Examples:
  - Email spoofing: false From field
  - IP spoofing: false source IP address
  - DNS spoofing: false DNS responses
  - Mobile-IP Binding Update (BU) spoofing: false location information
  - False telephone caller ID or SMS sender number

On-path attacker = man in the middle (MitM)

- In the man-in-the-middle attack, the attacker is on the communication path between the honest endpoints



- Attacker can intercept and modify data → sniffing + spoofing
  - Just forwarding data between two endpoints (like a piece of wire) is not an attack. What would the attacker gain?

Authentication and integrity

- Peer-entity authentication = verify the presence and identity of a person, device, or service at the time; e.g., car key
- Data origin authentication = verify the source of a message (sender); e.g., electronic mail
- Data integrity = verify that the data was received in the original form, without malicious modifications
- In practice, data origin authentication and integrity check always go together
- Authentication (usually) requires an entity name or identifier

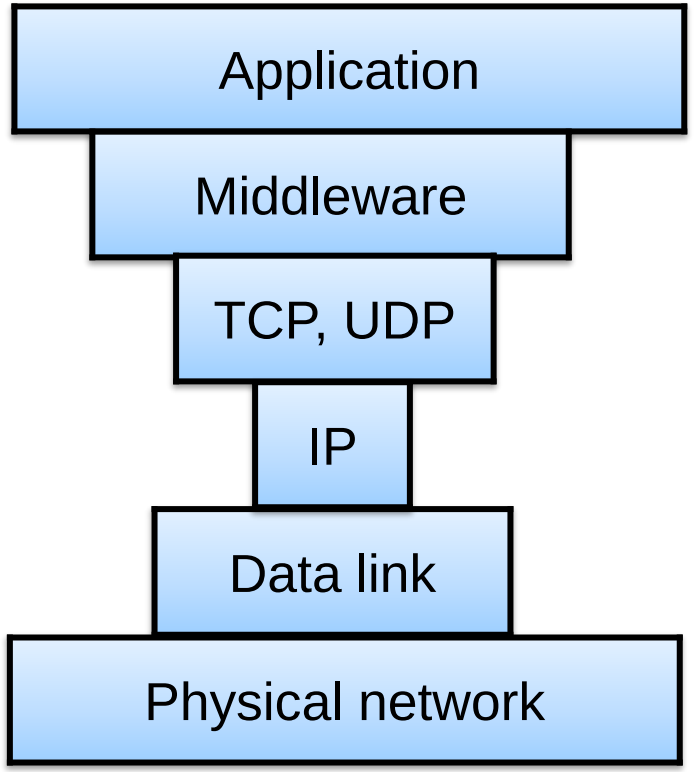
Other network threats

- Sniffing, spoofing, MitM and DoS are not the only security issues
- Other threats:
  - Integrity of signaling and communications metadata
  - Unwanted traffic like spam
  - Traffic analysis and location tracking
  - Tracking and unwanted monitoring or behavior (lack of privacy)
  - Tunneling attacks for spoofing location
  - Software security flaws
  - Unauthorized resource use (vs. access control)
  - Billing too much or avoiding payment
  - Liability for malicious actions
- Not captured well by the traditional network-security model

Network Security:
Security and the network protocol stack

ENCS5322, NETWORK SECURITY PROTOCOLS

Protocol Stack and Security



- Which layer in the protocol stack should implement security mechanisms, esp. encryption and authentication?

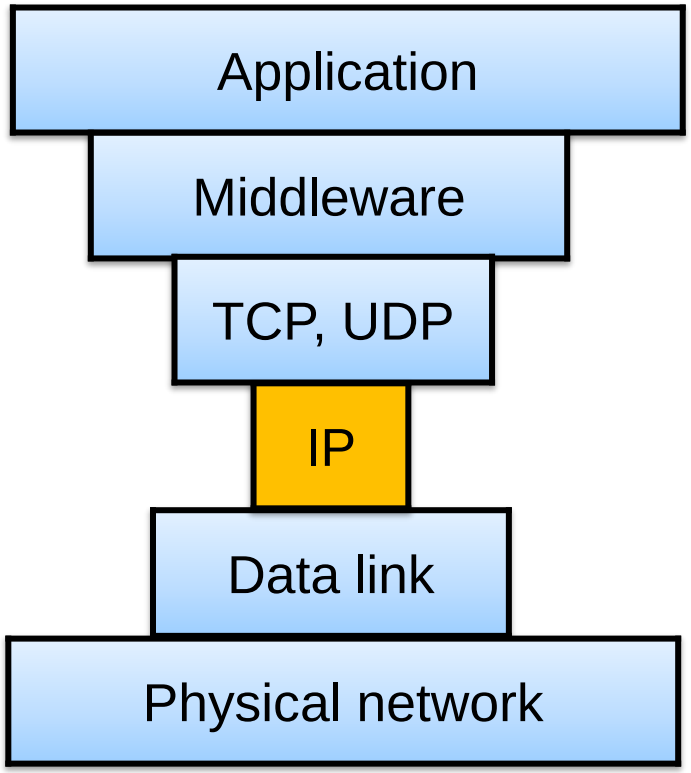
Which layer security?

- Reasons to implement cryptographic security in lower layers:
  - Security provided by physical, link or network layer is a service to the higher layers
  - Lower-layer security protects all higher-layer data: all connections, both payload and signaling or metadata
  - Security in lower layers is transparent to higher layers. No changes to applications needed
  - Lower-layer security protects the lower layer, too

Which layer security?

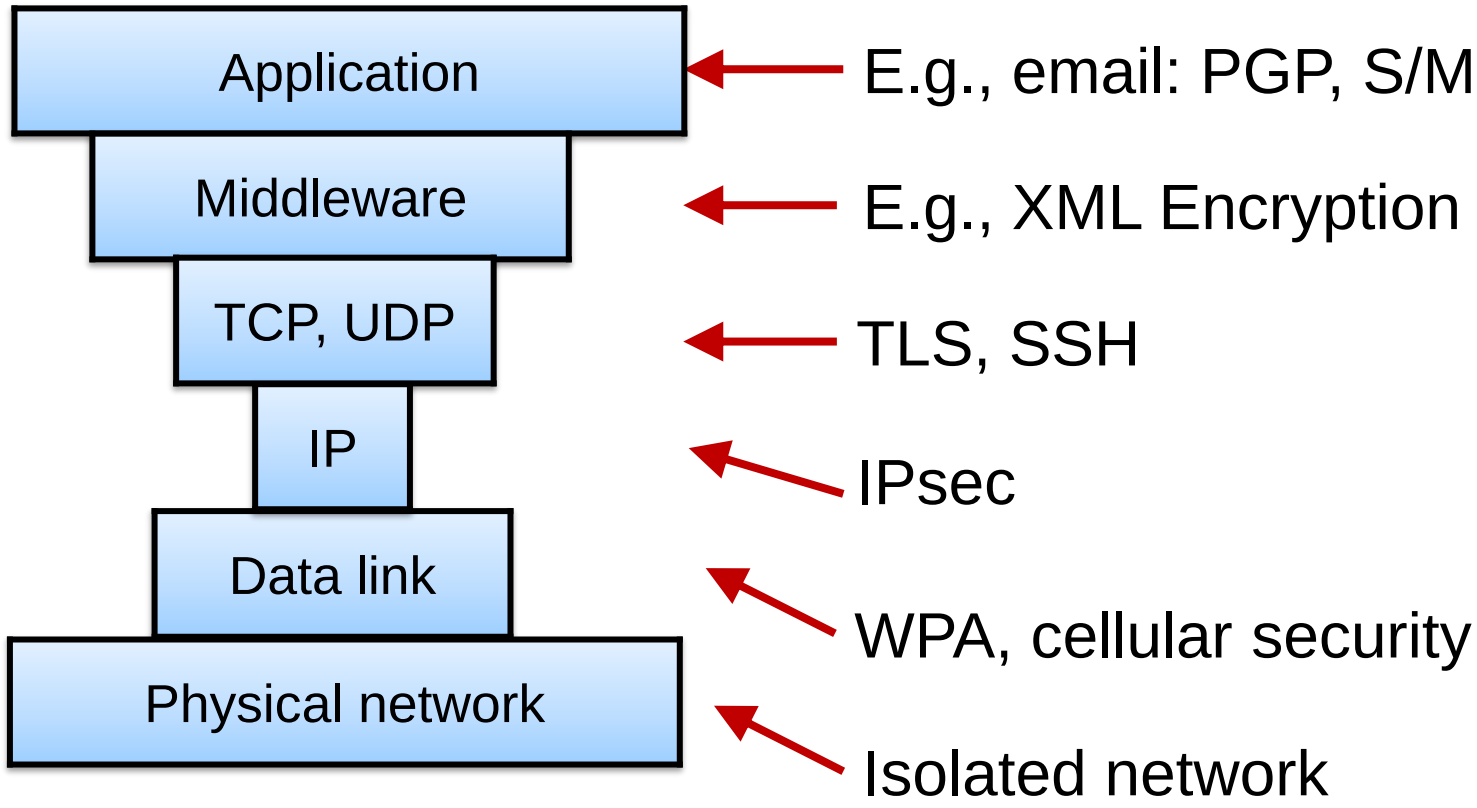
- Reason to implement security in higher layers:
  - Security implemented in the application or middleware will fit exactly to the application requirements
  - Authentication of lower-layer identifiers may not be meaningful to higher layers
  - Application developers can deploy security mechanism faster than the committees that define the lower-layer technology
  - Application developers may not trust the lower-layer service provider

IP layer



- Hourglass-shaped TCP/IP protocol stack → any service should be in the IP layer:
  - Implement only once (or twice for IPv4+IPv6)
  - Works over any data link layer
  - Works for any application

Protocol Stack and Security



S/MIME -Secure/Multipurpose internet Mail Extensions
PGP - Pretty Good Privacy
SSH - Secure Shell
IPsec- Internet Protocol Security
WPA- Wi-Fi Protected Access

- Security solutions exist for every protocol layer
- Layers have different security and performance trade-offs, trust relations and endpoint identifiers

End-to-end security

- Security should be implemented between the endpoints of communication
  - All intermediaries are part of the untrusted network
- End-to-end security only depends on the end nodes
  - Hop-by-hop (link-layer) security assumes trusted and secure intermediate nodes
  - Every business and government on the route imposes its own hop-by-hop rules
- End-to-end mechanism are independent of the link technology
  - Link-layer security is different for each link type
- Confidentiality and authentication are often user or application requirements
  - Network or link layer does not know application-level requirements or identities
- Nevertheless, link and network layer infrastructure and signalling also need protection
- Even if you agree with lawful access in one country, the traffic may be routed through another with a different political ad legal system.

Host as endpoint

- Traditionally, host = computer is the security endpoint
  - OS is trusted to isolate apps running as processes and their connections from other processes
  - OS must be trusted because it has access to software memory and controls execution
- Nowadays, increased communication inside the host:
  - Inter-process communication, VMs, containers, microservices, APIs
  - Trusted execution environments isolate software from the host
- Distributed apps and services are not at just one host