Aalto University

Network Security: Threats and Goals

Tuomas Aura, Aalto University

CS-E4300 Network security

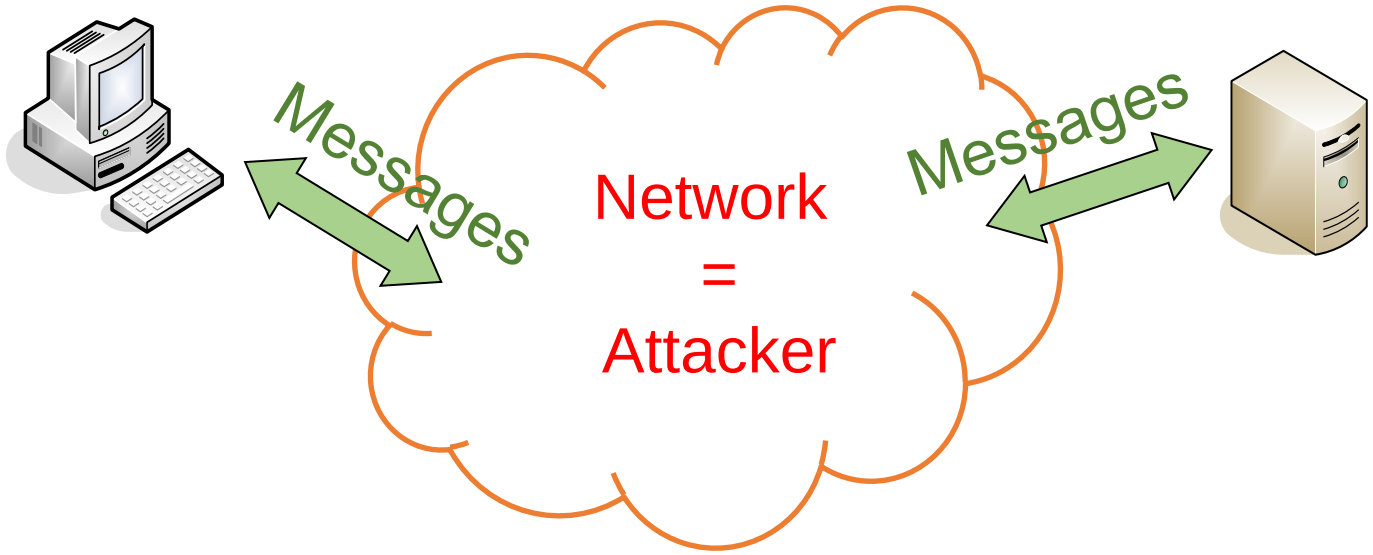
Outline

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, computer networks, wireless networks, personal-area networks, IoT devices
  - Application-level protocols, overlays, P2P, content distribution and protection, payment, etc.
  - Inter-process communication, APIs and message busses
  - Human protocols (“ceremonies”), physical security tokens, letters, paper certificates

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



- End are nodes trusted, the network is unreliable
- End nodes send messages to the network and receive messages from it
- Network will deliver some messages but can read, delete, modify and replay them

Basic network security threats

- Traditional major threats:
  - Sniffing = attacker listens to network traffic
  - Spoofing = attacker sends unauthentic messages
  - Data modification, man in the middle
    = 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
- Where might sniffers be?
  - Wireless access links, fake access points
  - Ethernet socket or compromised host for wired LAN
  - Firewalls, proxies, routers
  - Internet routing can be manipulated

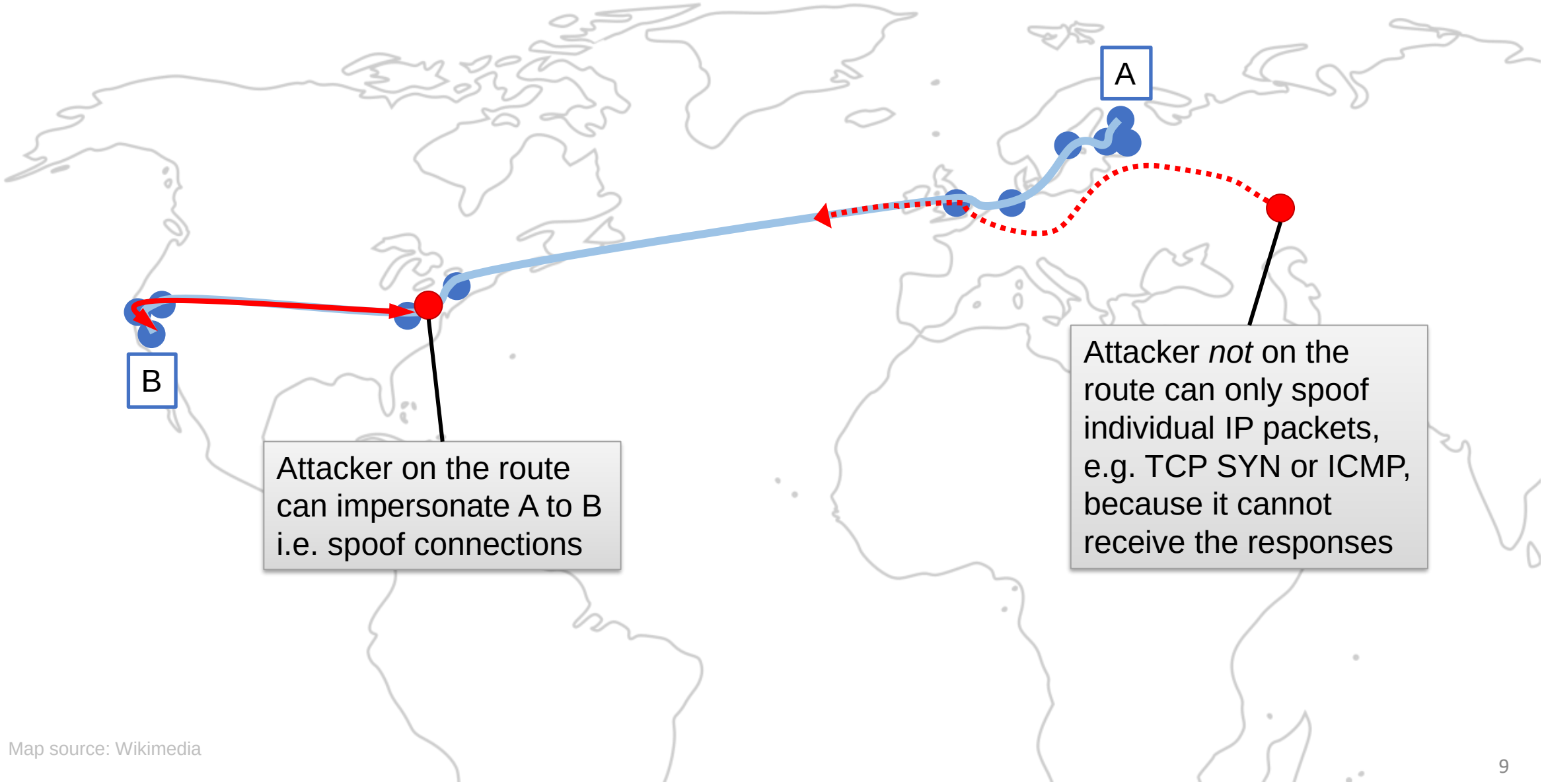
Spoofing

- 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 BU spoofing: false location information
  - False telephone caller id or SMS sender number

Example: IP spoofing

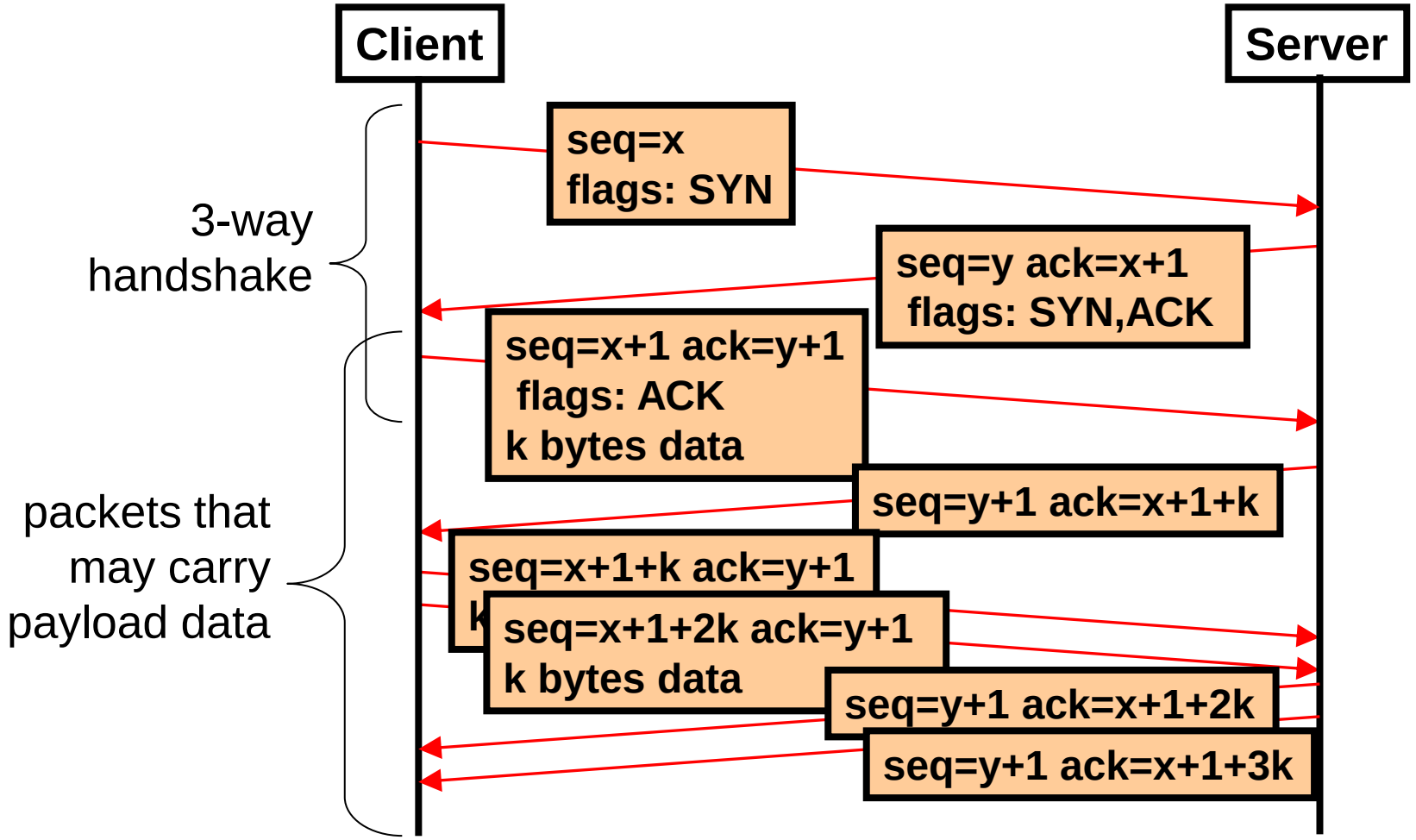
- Attacker sends IP packets with false source IP address
  - Anyone can write software to do this with raw sockets
  - Attacker may be anywhere on the Internet
- Spoofing a connection between A and B is more difficult:
  - Attacker must sniff replies from B in order to continue the conversation → Attacker must be on the route between A and B

IP routing and spoofing



Map source: Wikimedia

TCP handshake and spoofing

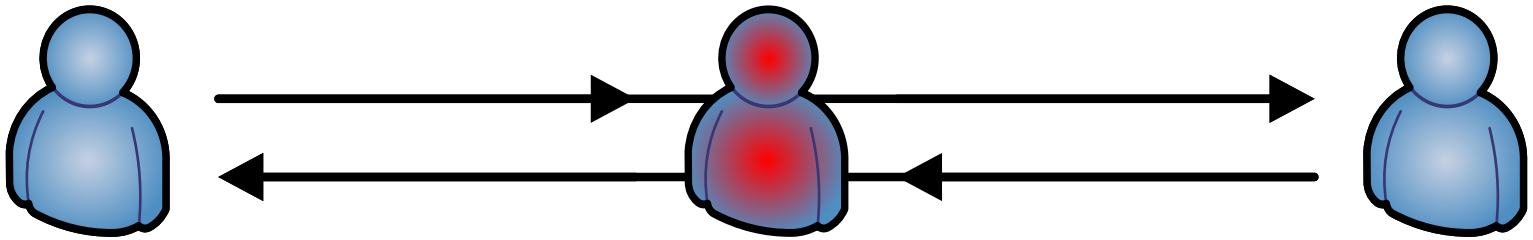


TCP sequence numbers are initialized to random values.

To inject a spoofed packet into an existing connection, the attacker must know the sequence numbers.

Man in the middle (MitM)

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



- Attacker can intercept and modify data → sniffing + spoofing
- On the Internet, a MitM attacker could
  - be at the local network of one of the end points
  - be at a link or router on the route between them, or
  - change the routing to redirect the packets via its own location

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
- 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 issues.
- Other threats:
  - Integrity of signaling and communications metadata
  - Spam and other unwanted traffic
  - Traffic analysis and location tracking
  - Lack of privacy (unwanted monitoring of behavior)
  - Tunneling attacks for spoofing location
  - Software security flaws
  - Unauthorized resource use (vs. access control)
  - Billing too much or avoiding payment
  - Liability for malicious use
- Not captured well by the traditional network-security model