Aalto University

Network Security: Threats and Goals

Tuomas Aura, Aalto University

CS-E4300 Network security

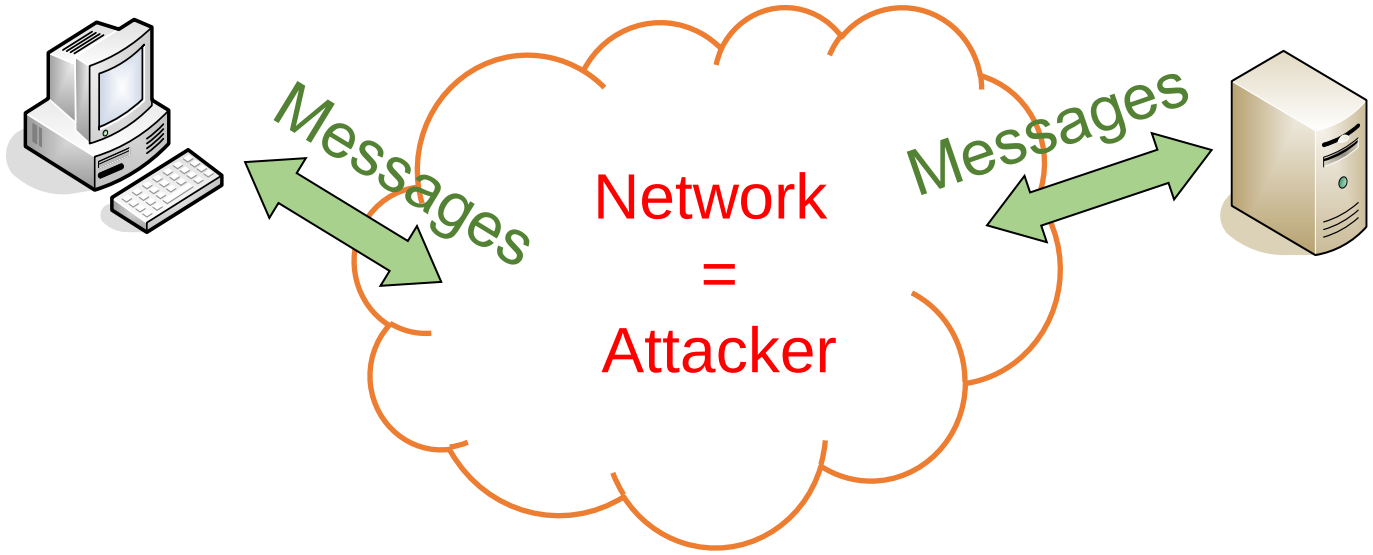
Outline

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, mobile networks, computer networks, wireless networks, personal-area networks, IoT devices
  - Application-level protocols, overlays, P2P, content distribution and protection, VPN, service mesh
  - 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)



- 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?

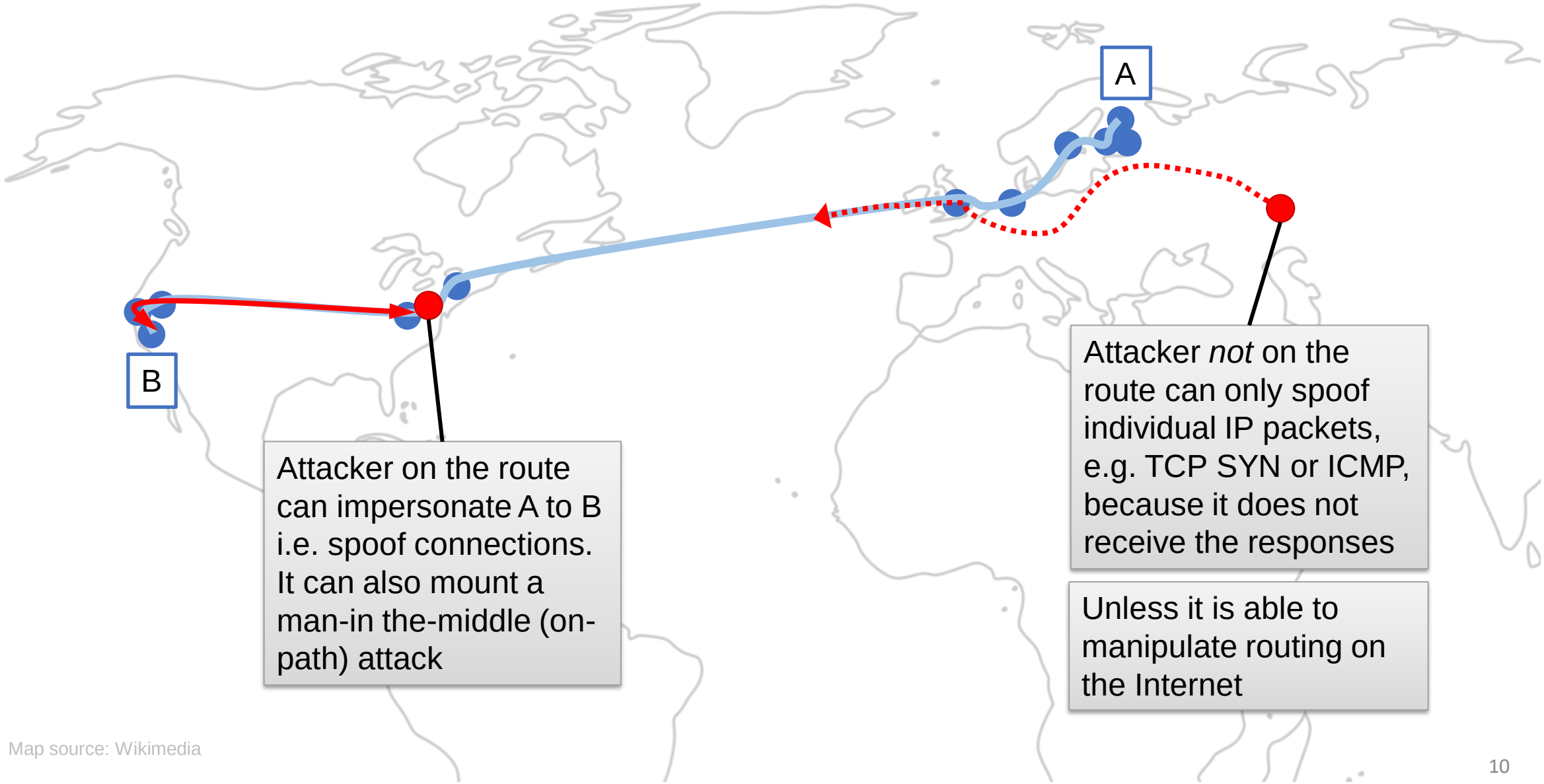
- Provide free wireless access, or spoof SSIDs
- DNS poisoning
- Pretend to be the target on the local link
  - ARP poisoning
  - IPv6 ND spoofing
- Advertise better route to the destination
  - BGP prefix hijacking
  - Intra-domain routing protocol may be similarly vulnerable
- Topology spoofing on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

WiFi Pineapple

Spoofing

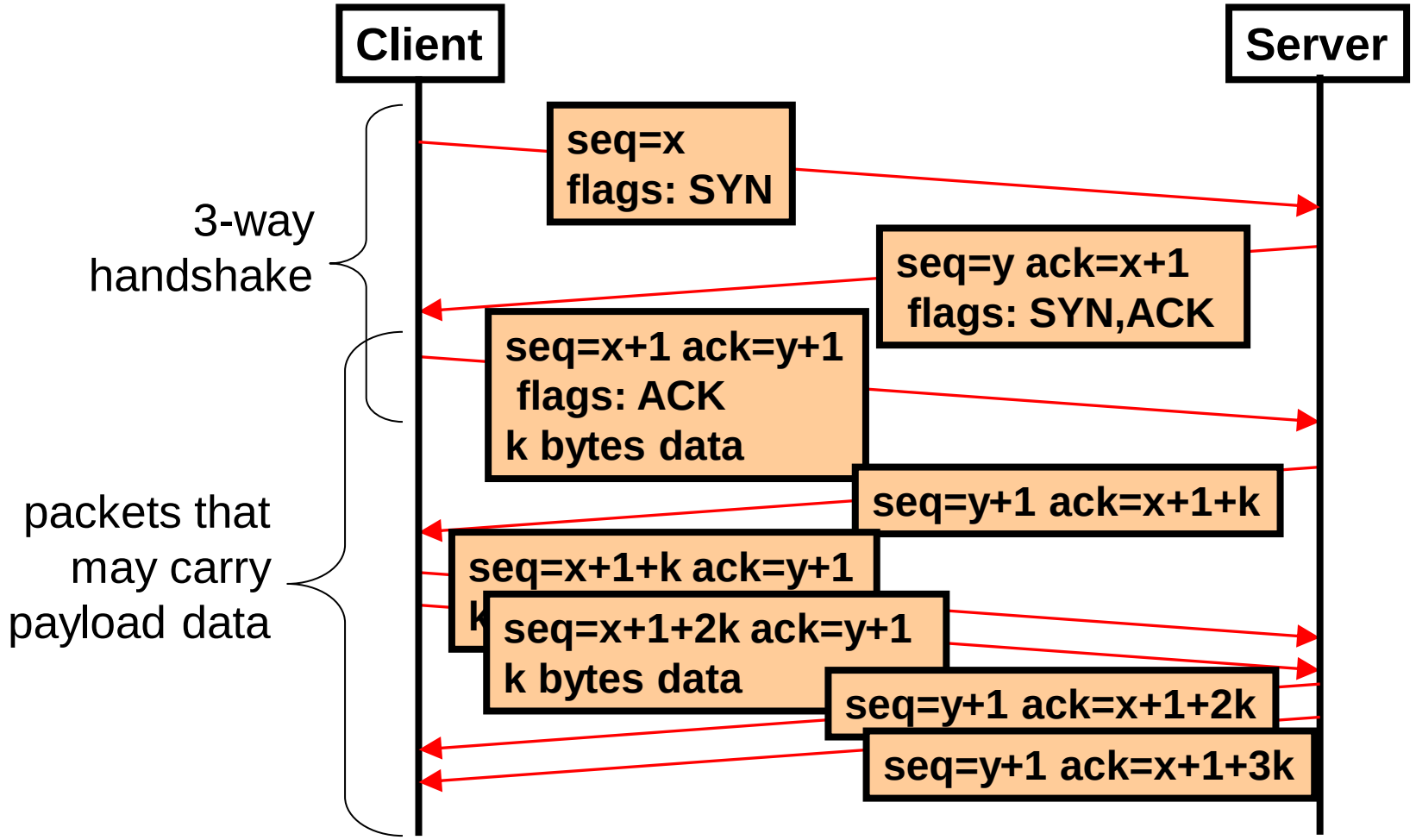
- Spoofing = sending unauthentic/false/counterfeit messages = using false sender address or identifier = impersonation
- Examples:
  - Email spoofing: false From field
  - IP spoofing: false source IP address
  - DNS spoofing: false DNS responses
  - Mobile-IP BU spoofing: false location information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

IP routing and spoofing



Map source: Wikimedia

TCP handshake and spoofing

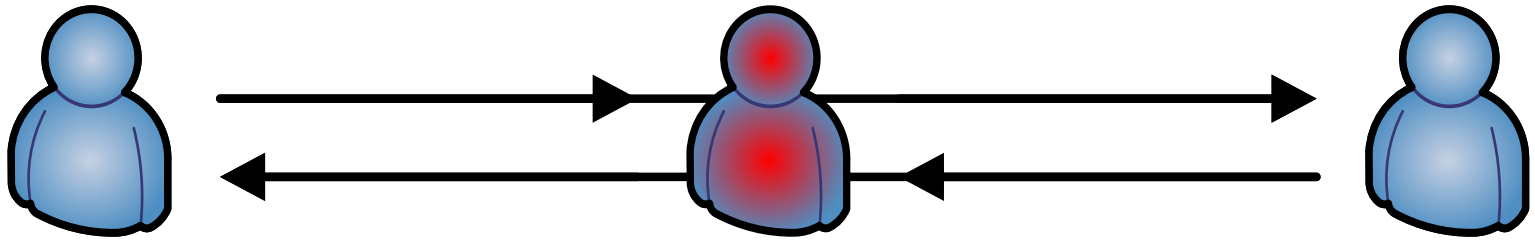


TCP sequence numbers are initialized to random values.

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

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

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 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