University of BRISTOL

CyBOK

Network Security Knowledge Area

Prof. Christian Rossow
CISPA Helmholtz Center for Information Security

Prof. Sanjay Jha
University of New South Wales

University of BRISTOL

CyBOK

The CyBOK project would like to understand how the CyBOK is being used and its uptake. The project would like organisations using, or intending to use, CyBOK for the purposes of education, training, course development, professional development etc. to contact it at contact@cybok.org to let the project know how they are using CyBOK.

bristol.ac.uk

Security Goals

What does it mean to be secure?

- Most common security goals: “CIA triad”
  - **Confidentiality**: untrusted parties cannot infer sensitive information
  - **Integrity**: untrusted parties cannot alter information
  - **Availability**: service is accessible by designated users all the time
- Additional security goals
  - **Authenticity**: recipient can verify that sender is origin of message
  - **Non-Repudiation**: anyone can verify that sender is origin of message
  - **Sender/Recipient Anonymity:** communication cannot be traced back to sender/recipient, respectively
  - Further privacy goals in Privacy & Online Rights CyBOK Knowledge Area

Attacker Models

What attackers are we secure against?

- worst case: **Dolev-Yao** attacker model
  - Attacker has complete control over the network
    - Sometimes referred to as person-in-the-middle (PITM) attacker
    - read, drop, and inject arbitrary messages
- Attacker characterization
  - **Capabilities:** ***Active*** (can drop & manipulate messages)
    Passive (can eavesdrop only)
  - **Location:** ***On-path*** (placed between communicating parties)
    Off-path (cannot see direct communication)
  - **Trust:** ***Insider*** (part of trusted domain)
    Outsider (outside of trusted domain)
  - **Resources**: Individual Internet user, rogue ISP, state actor, ...

Networking Applications

Networking Applications

Local Area Networks (LANs)

- **Local Area Networks** (**LAN**s) connect systems within an internal environment
- **Local does not imply trustworthy or secure** (typical fallacy!)
  - Without further measures, *all* LAN clients can access each other
    - Internal services can be exposed unintentionally
  - Not all local clients can be trusted
    - Especially in Bring-Your-Own-Device (BYOD) settings
    - Untrusted clients can expose entire network to the outside world
  - Attackers may impersonate other (trusted) LAN clients
    - Hardware addresses (e.g., Ethernet MAC addresses) can be cloned

Networking Applications

Connected Networks and the Internet

- External connections are often necessary, but introduce additional security issues
  - **LAN-to-LAN**
    - join corporate networks across multiple locations
    - Internal/confidential traffic has to traverse the untrusted Internet
  - **LAN-to-Internet**
    - allow local clients to access the Internet, but expose only selected services to the Internet
- The Internet itself is a network of **Autonomous Systems** (ASs)
  - ASs can eavesdrop and manipulate traffic passing through their systems
  - ASs can hijack Internet routes and reroute other systems' traffic

Networking Applications

Bus Networks

- Cyber-physical systems often use a bus network architecture
  - Common examples:
    - *Modbus* – industrial control systems
    - *Konnex Bus (KNX)* – home automation
    - *Controller Area Network (CAN)* – vehicular networks
- Local networks similar to LANs with additional constraints
  - Real-time guarantees (e.g., brake systems)
  - Limited computing resources (cost efficiency)
  - Shared central bus (all clients can see all messages)
  - Standardized protocols often predate security best practices

Networking Applications

Wireless Networks

- Wireless LAN conceptually similar to cable-connected LAN
- Wireless medium increases attack opportunities
  - Attacking a cable-connected LAN requires access to cable or network port
  - Attacking a wireless LAN only requires physical proximity to access points or clients
- Requires increased focus on access control and secure communication

Networking Applications

Fully-Distributed Networks

- **Fully-distributed networks** (peer-to-peer (P2P) networks) provide **scalability** and **resilience *by design***
- Lack of central party or peer authentication introduces new security challenges
- **Structured P2P**: messages follow a routing scheme in overlay
  - Distributed Hash Tables (e.g., *Kademlia*, *Freenet*)
  - Attacker may attempt to disrupt message routing
- **Unstructured P2P**: use gossip protocols to spread messages
  - Gossip networks
  - Attacker may attempt to flood network with uncalled-for data

Networking Applications

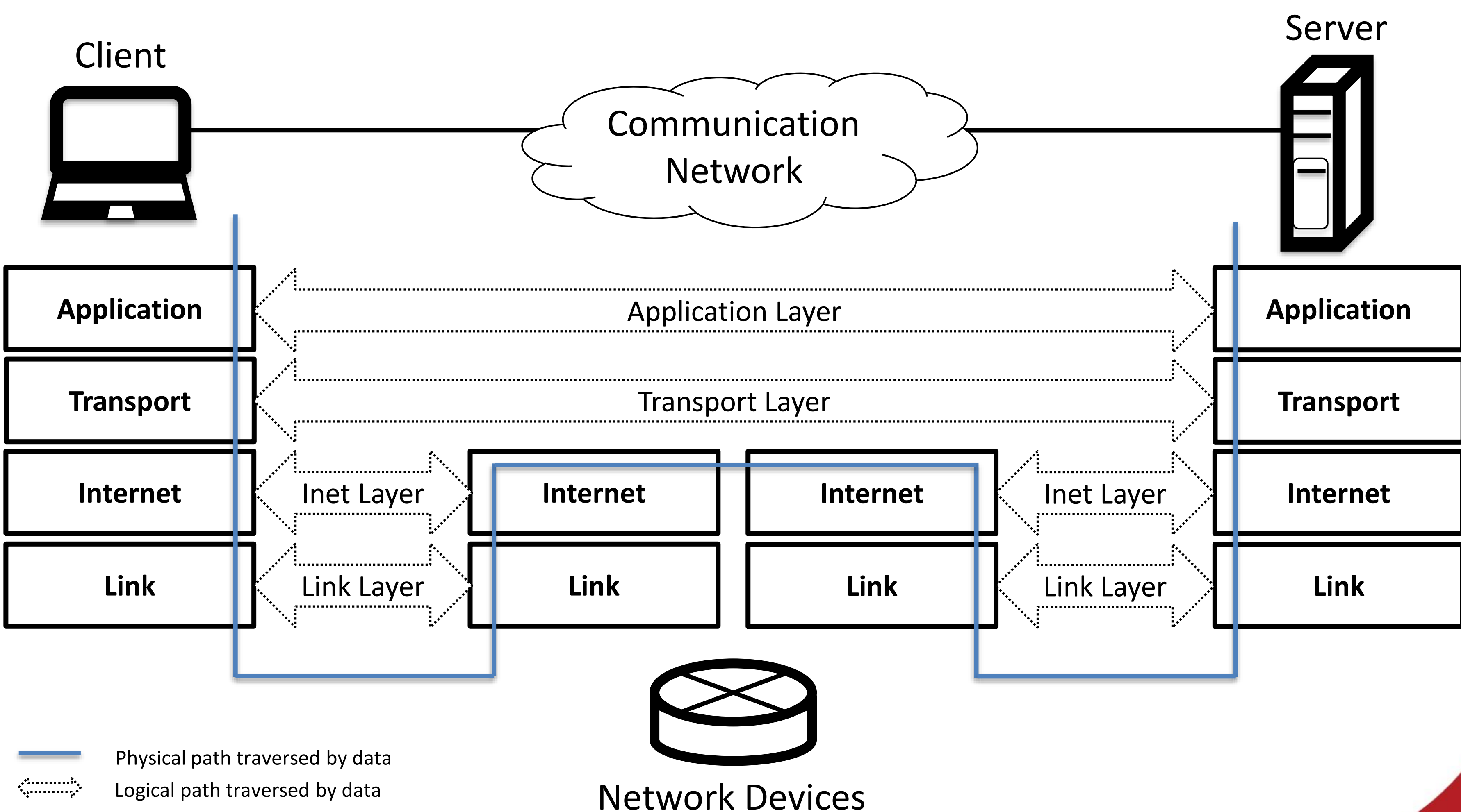
SDN & NFV

- **Software-Defined Networking (SDN)** enables dynamic and efficient network configuration by decoupling
  - **Data Plane** (***forwarding*** of network packets)
  - **Control Plane** (***routing*** of network packets)
- **Network Function Virtualization (NFV)** allows to virtualize network node functions, e.g.,
  - Virtual load balancers
  - Virtual firewalls
- Both can help to achieve security goals in a network, but also introduce new attack targets (e.g., central controllers)

Network Protocols and Their Security

Networking Protocols

and their Security



Security at the Application Layer

Hypertext Transfer Protocol Secure (HTTPS)

- Most prominent application-layer protocol: the **Hypertext Transfer Protocol (HTTP)** for accessing web content
  - Provides no security guarantees
- HTTP on its own does not provide the following desirable goals:
  - **Confidentiality** (only user should see content of webpage, only server should receive inputs from user)
  - **Integrity** (content may not be altered in transit in both directions)
- Especially relevant for e-commerce and online banking
- Can be achieved through the **Hypertext Transfer Protocol Secure (HTTPS)**, which wraps HTTP in a TLS session
- See Web & Mobile Security CyBOK Knowledge Area for more details on HTTPS

Security at the Application Layer

Email and Messaging Security

- Emails are sent using the **Simple Mail Transfer Protocol (SMTP)**
  - Provides no security guarantees
- Desirable security goals
  - **Confidentiality** (only recipient may read message)
  - **Integrity** (message may not be altered in transfer)
- Mechanisms to achieve end-to-end security
  - **Pretty Good Privacy (PGP)** and **Secure Multipurpose Internet Mail Extensions (S/MIME)**
  - Assign private/public keypair to both parties and
    - Encrypt message under recipient's public key (-> confidentiality)
    - Sign (hash of) message using sender's private key (-> integrity)

Security at the Application Layer

DNS Security

- **Domain Name System (DNS)** translates domain names to IP addresses
- DNS provides no **Authenticity** or **Integrity**
- An attacker can divert traffic for a domain to its own servers by
  - Impersonating a resolver and returning bogus DNS records
  - Forging responses from an authoritative server and poison a resolver's DNS cache
- **DNS Security Extensions (DNSSEC)** allow authoritative NSs to sign DNS records with a private key
  - Clients can check authenticity and integrity of records

Security at the Application Layer

DNS Security

- DNS provides no **Confidentiality**
- DNS queries and responses are sent in plaintext
  - eavesdroppers can learn which domains a client resolves/visits
- Still holds true with DNSSEC
- Solved by **DNS over TLS (DoT)** and **DNS over HTTPS (DoH)**
  - Wrap DNS communication in a secure channel (TLS or HTTPS)
  - DoH enabled by default in modern Web browsers
- Unfortunately leads to a massive centralization of resolvers
  - Can be alleviated by adding trusted proxies between DNS clients and their resolvers (Oblivious DoH, ODoH)

Security at the Application Layer

Distributed Hash Table (DHT) Security

- De-facto standard for structured Peer-to-Peer (P2P) networks
- Building block for many distributed systems
- Two main attacks:
  - **Eclipse attack:** Poison routing tables to isolate target nodes from the rest of the network
  - **Sybil attack:** Inject large number of (attacker-controlled) nodes to subvert protocol redundancy
- Current countermeasures reduce generality/introduce central component
- Still active field of research
- See Distributed Systems Security CyBOK Knowledge Area for more details

Security at the Application Layer

Anonymous Communication

- **The Onion Router (Tor)** is the de facto standard of **Anonymous Communication Networks (ACNs)**
  1. Select three nodes: entry, middle, exit
  2. Create end-to-end encrypted channel with next node via channel with previous node
  3. Connect to server via resulting *circuit*
- **Sender Anonymity**
  - Only entry node knows client, only exit node knows server
  - Onion services also achieve **Recipient Anonymity** (using 2 circuits)
- Not fully immune against powerful adversaries
  - Traffic correlation between entry & exit node can leak endpoints
  - Packet sizes/timing can leak visited website

Security at the Transport Layer

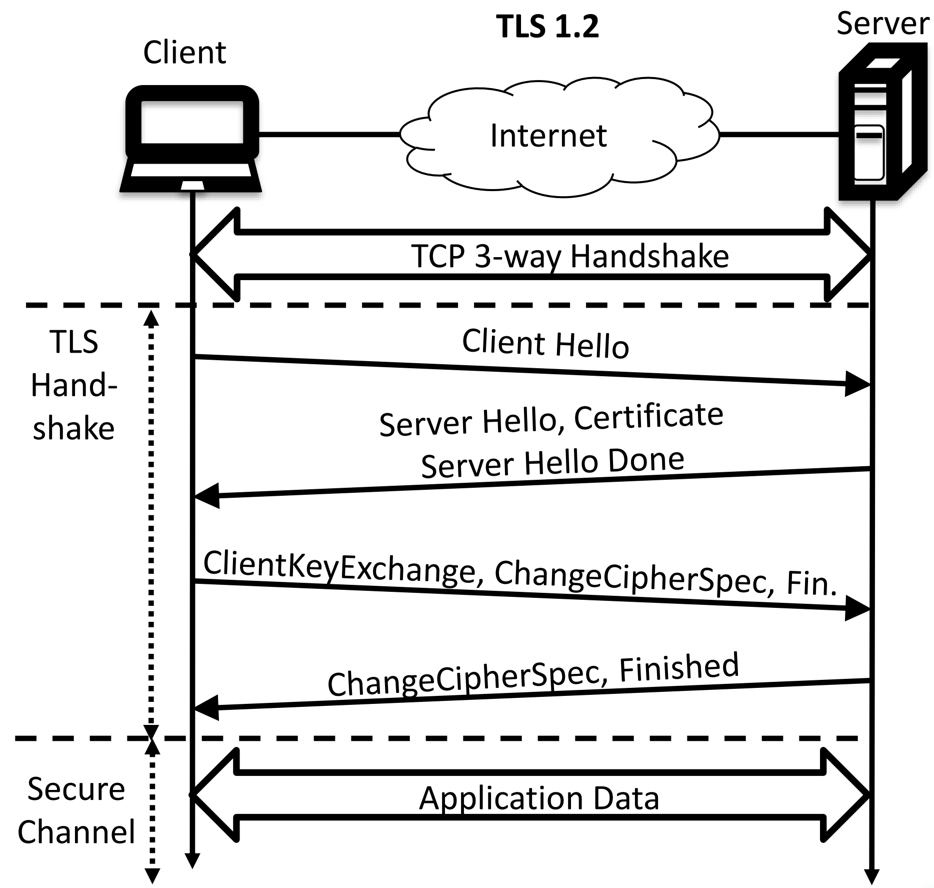
TLS (Transport Layer Security)

- Provide general **confidentiality**, **integrity**, and **authentication** mechanisms for application-layer protocols via a shim layer *between* the application and transport layer
  - Encrypting user data achieves **confidentiality**
  - Message Authentication Codes (MACs) or authenticated encryption provide **integrity**
  - Certificates can be used to **authenticate** endpoints
- Most recent versions: TLS 1.2 and 1.3
- Next slides shows (simplified) TLS 1.2 and TLS 1.3 handshake
- See Applied Cryptography Security CyBOK Knowledge Area for in-depth discussion

Security at the Transport Layer

TLS (Transport Layer Security) – TLS 1.2

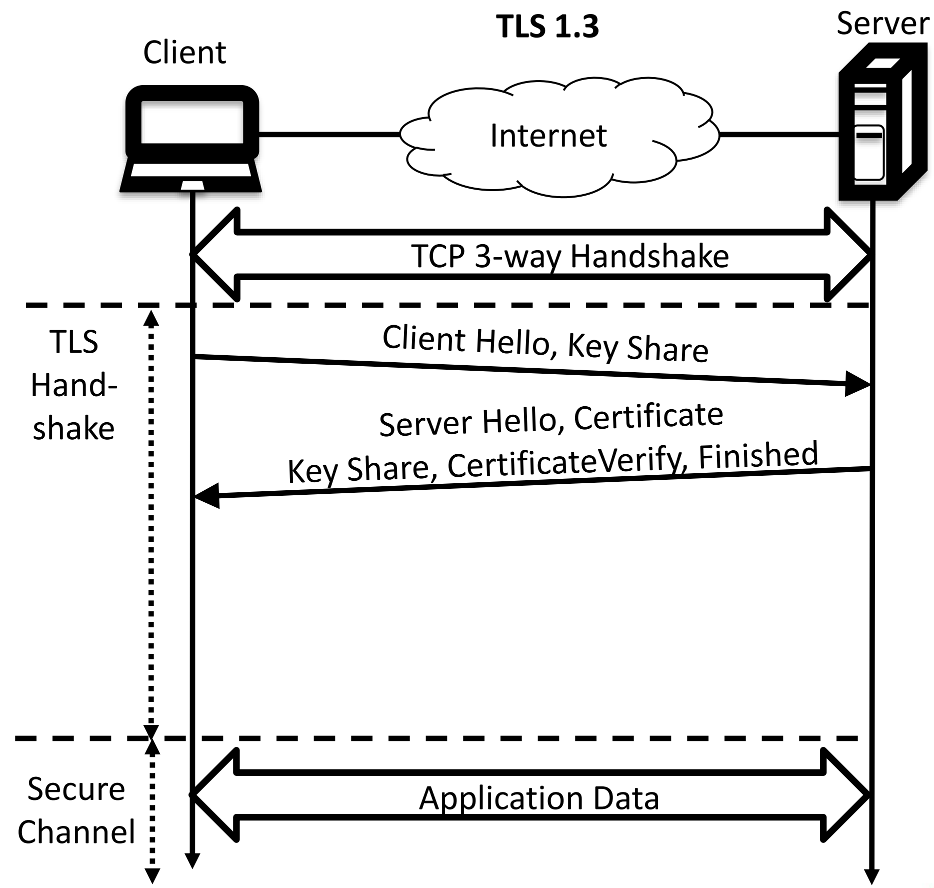
1. Client and Server negotiate TLS version and cipher suites to use
2. Server and Client exchange certificates for authentication
3. Client and Server derive a symmetric encryption key
   – Option 1: Client chooses key, sends key to server encrypted under server's RSA public key
   – Option 2: Client and Server use a Diffie-Hellman Key Exchange for perfect-forward secrecy
4. Client and Server validate handshake integrity
5. Secure Channel is ready to use



Security at the Transport Layer

TLS (Transport Layer Security) – TLS 1.3

- Reduce communication to single round-trip (1-RTT)
- Drop support for RSA-based key exchange in favour of DHKE
- Support for 0-RTT handshake after initial connection



Security at the Transport Layer

Public Key Infrastructure (PKI)

- How can public keys sent via insecure channels be trusted?
- **Public Key Infrastructure (PKI)** allows to manage *trustworthy* public keys via certificates
  - Uses appointed certificate authorities (CAs) as trust anchors
- Enrolment process:
  1. Create private/public key pair
  2. Create certificate signing request (CSR) for public key
  3. Send CSR to a CA & prove identity to CA (e.g., personal ID for S/MIME, possession of domain name for HTTPS)
  4. CA signs certificate (including user's public key and identity)
     - can be validated by anyone under the CA's public key
  - Format standardized in RFC 1422 and ITU-X.509

Security at the Transport Layer

TCP Security

- TLS only protects application layer data, but not TCP headers
- **TCP reset attack:** Spoof TCP segment with RST flag to terminate connection
  - Use strong randomness for initial sequence number generation
  - Deny RST segments within TCP sliding window
- **SYN Flood attack:** Send many TCP SYN segments to exhaust server resources with half-opened TCP connections
  - SYN Cookies
    - Derive Initial Sequence Number (ISN) from hash over IP addresses, ports, current timestamp, and server secret
    - Recompute for SYN/ACK segments, check against sequence number
    - Only allocate connection resources if check succeeds

Security at the Transport Layer

UDP Security

- Lack of implicit verification of endpoint IP addresses allows **IP spoofing** (unless handled at application layer)
  - Attacker can craft UDP packets with arbitrary source addresses

- **Reflection attacks:** spoof requests to UDP servers with address of DDoS victim
  - Servers overload DDoS victim with undesired replies
  - Large responses provide attacker with multiplied attack bandwidth (**amplification attack**)
  - Countermeasures: Modify application layer protocols or limit per-IP request rate

Security at the Transport Layer

QUIC Security

- Popular transport-level protocol Designed by Google, standardized by IETF in 2021
- Goal: Increase communication performance via multiplexed connections
- Designed with security in mind, provides TLS-like security at the transport layer
- Based on UDP + TLS1.3-like handshake
- Handshake also prevents reflection/amplification attacks

Security at the Internet Layer

IPv4 Security – IP Spoofing and Fragmentation

- **IP Spoofing**
  - IP clients can send traffic with arbitrary IP source addresses
  - Internet Layer defences:
    - **Egress Filtering** – provider drops traffic from outside of their domain
    - **Unicast Reverse Path Forwarding (uRPF)** – on-path routers drop traffic receive on unexpected interfaces
- **Fragmentation Attacks**
  - Packets beyond the network's Maximum Transmission Unit (MTU) are split into multiple fragments
  - Defragmentation non-trivial, allows attackers to e.g.,
    - Perform DoS using large overlapping fragments (*Teardrop Attack*)
    - Evade defence mechanisms by splitting their payload into fragments

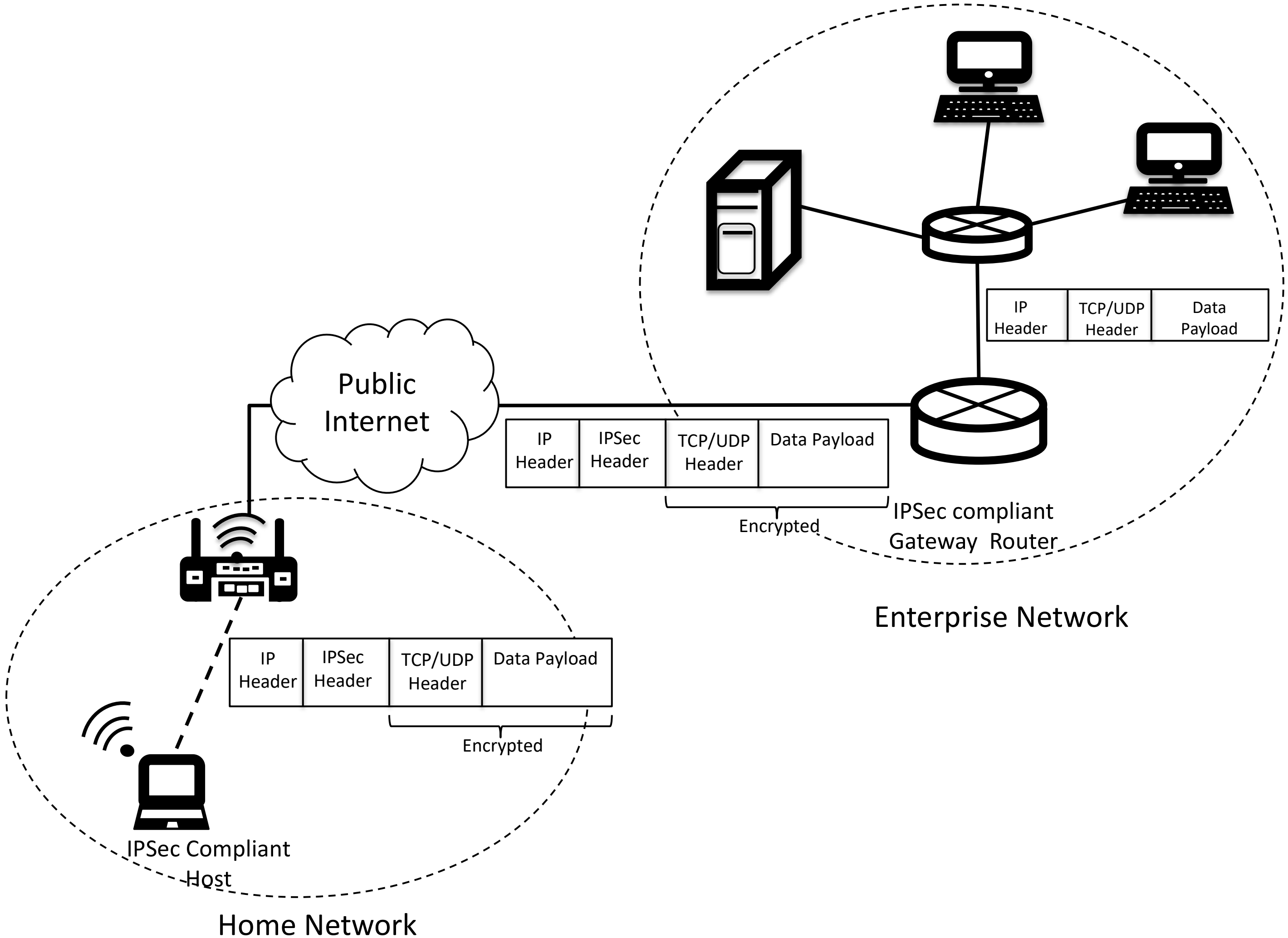
Security at the Internet Layer

IPv4 Security – VPNs and IPSec

- **Virtual Private Networks (VPNs)** connect multiple separate networks via a (secure) tunnel
- Can be implemented with many protocols, e.g.
  - ~~**Point-to-Point Tunneling (PPTP)**~~ (deprecated!)
  - **TLS** (used by, e.g., OpenVPN)
  - **Secure Socket Tunneling Protocol (SSTP)**
  - **Internet Protocol Security (IPSec)** protocol suite

Security at the Internet Layer

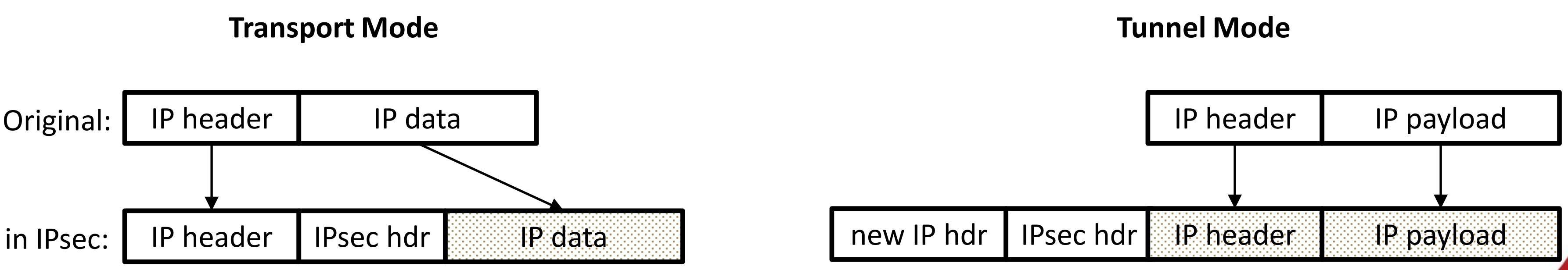
IPv4 Security – VPNs and IPSec



Security at the Internet Layer

IPv4 Security – VPNs and IPSec

- IPSec suite offers multiple protocols:
  - Encapsulation Security Payload (ESP) protocol provides confidentiality, integrity and origin authentication (and more)
  - Authentication Header (AH) protocol provides integrity only
- IPSec suite offers multiple modes of operation:
  - Tunnel Mode: encapsulate entire IP packet, including header
  - Transport Mode: encapsulate IP *payload* only



Security at the Internet Layer

IPv6 Security

- **Internet Protocol version 6 (IPv6)** is the successor to IPv4
  - Large address space: 128-bit (IPv6) vs 32-bit (IPv4)
  - IPSec integration (not mandatory, but recommended)
  - No additional header options
- Obsoletes NAT
  - Firewall necessary to prevent reachability of devices
  - Large address space allows to rotate IP addresses frequently, complicates IP address-based tracking
- Transition phase still ongoing, many devices dual-stacked (simultaneous IPv4 + IPv6)
  - Both IPv4 and IPv6 security aspects need to be considered

Security at the Internet Layer

Routing Security – IGPs

- **Interior Gateway Protocols (IGPs)** are used for routing within an autonomous system
- Popular with IPv4: **Routing Information Protocol v2 (RIPv2)** and **Open Shortest Path First v2 (OSPFv2)**
- **RIPng** and **OSPFv3** add IPv6 support
- No security by default, but mutual authentication supported
  - Can prevent bogus route insertion or rogue neighbour injection
- Older protocols (e.g., **RIPv1**, **IGRP**) provide no authentication mechanisms and should be used with care

Security at the Internet Layer

Routing Security – BGP

- **Border Gateway Protocol (BGP) hijacking attack**
  - Attacker advertises routes for foreign prefixes to redirect traffic
  - Redirecting to attacker network enables eavesdropping
  - Redirecting to other networks enables volumetric DoS
- **Resource Public Key Infrastructure (RPKI)** maintains per IP-prefix **Route Origin Authorization (ROA)**
  - **Route Origin Validation (ROV):** check ROA for origin AS
  - Does not prevent bogus advertisements with correct origin AS
- **BGPsec** attempts to address remaining security concerns
  - Full AS path integrity
  - Requires support by all on-path BGP routers

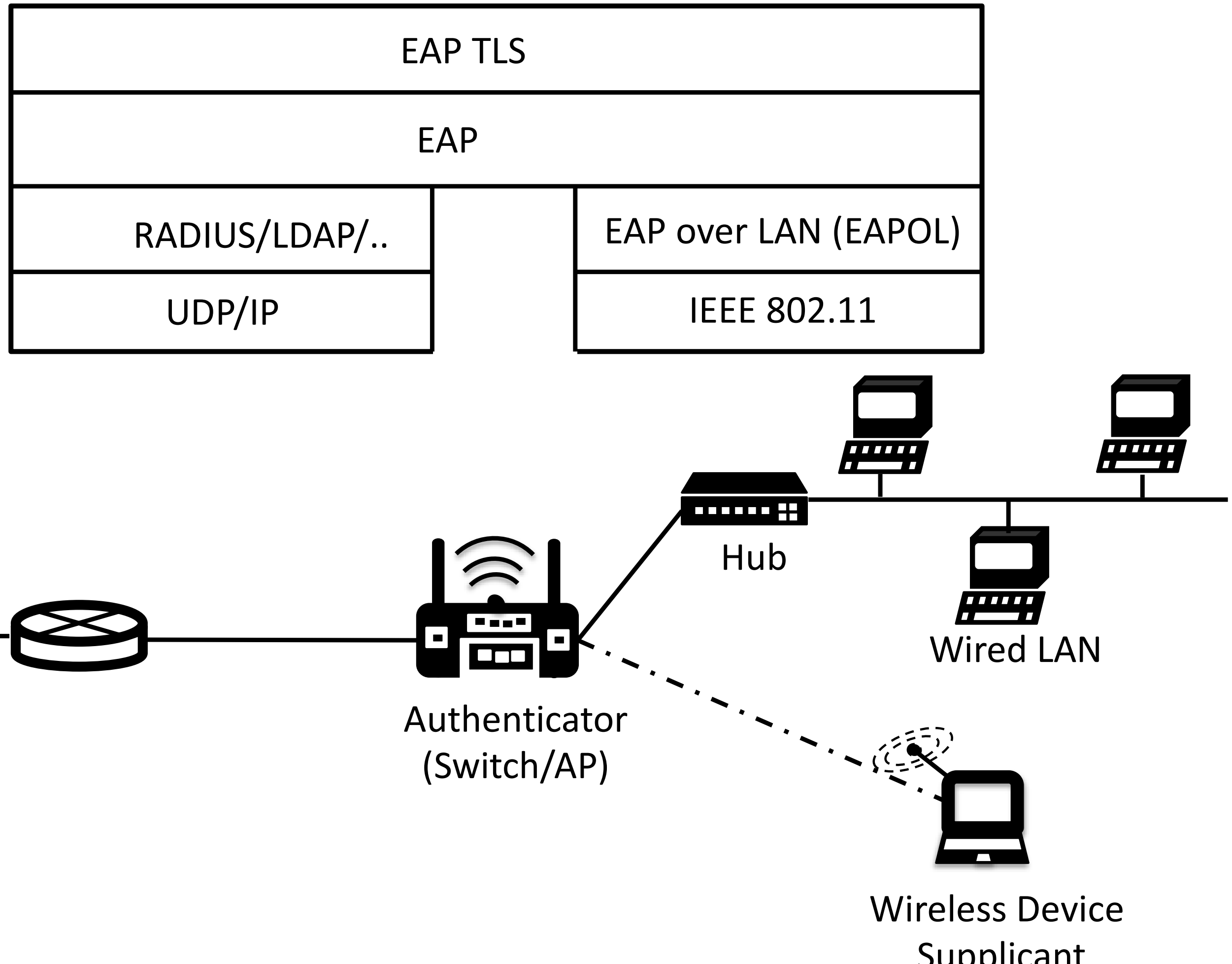
Security on Link Layer

Port-based Network Access Control (IEEE 802.1X)

- **IEEE 802.1X** provides port-based authentication for wired and wireless (local) networks
  1. New client (*supplicant*) initially unauthorized, only 802.1X traffic permitted by *authenticator* (switch/AP)
  2. *Authenticator* sends **Extensible Authentication Protocol (EAP)** request to supplicant
  3. *Supplicant* answers with EAP response to *authenticator*, which unblocks port if authentication successful
- TLS-based **EAP-TLS** or **Protected EAP (PEAP)** recommended
  - Other EAP modes can be prone to PITM (esp. wireless) or dictionary attacks
- Next slide shows typical 802.1X deployment

Security on Link Layer

Port-based Network Access Control (IEEE 802.1X)



Security on Link Layer

Attacks on Ethernet Switches

- **Ethernet switches** map link-layer addresses (MAC addresses) to physical ports for forwarding
- Mapping stored in **Content Addressable Memory (CAM)**
- Attackers can spoof MAC address in unauthenticated networks in order to
  - Flood the entire CAM with bogus entries, causing the switch to send all network packets to *all* ports (including attacker)
  - Overwrite target's CAM entry with attacker address, causing switch to forward target's traffic to attacker
- Attacks can be mitigated by IEEE 802.1X authentication

Security on Link Layer

ARP and NDP

- **Address Resolution Protocol (ARP)** maps IPv4 addresses to MAC addresses
  - Attackers can (re-)bind a target IP to another MAC address by sending fake ARP messages (**ARP spoofing**)
    - Enables PITM attack
- **Neighbor Discovery Protocol (NDP)** is the IPv6 ARP-successor
  - NDP spoofing still possible
  - Direct correspondence between MAC and IPv6 address in basic autoconfiguration scheme
    - Enabled user/device tracking
  - Both issues mitigated by **Secure Neighbor Discovery (SEND)**, which uses public-key based **Cryptographically Generated Addresses (CGA)** instead

Security on Link Layer

Wireless Security

- Wireless networks use broadcast medium
  - Additional protocols required for **Integrity** & **Confidentiality**
- **Wire Equivalent Privacy (WEP)**
  - Shared key between client and access point (AP)
  - **Broken** (short 24-bit IVs + weak RC4 encryption)
- **Wi-Fi Protected Access (WPA)**
  - Encryption with temp. key derived from **Pre-Shared Key (PSK)** using the **Temporal Key Integrity Protocol (TKIP)**
  - IVs extended to 48 bits, RC4 kept for backwards compatibility
  - Considered insecure

Security on Link Layer

Wireless Security

- **Wi-Fi Protected Access 2 (WPA2)**
  - Successor to WPA standardized in 2004
  - Authenticated encryption using AES with CCMP instead of RC4
  - Formally verified, still believed to be secure
- **Wi-Fi Protected Access 3 (WPA3)**
  - Successor to WPA2 standardized in 2018
  - Adds support for perfect forward secrecy
  - PSK replaced with **Simultaneous Authentication of Equals (SAE)**, based on IETF Dragonfly key exchange
- **Opportunistic Wireless Encryption (OWE)**
  - Support for client-specific encryption in open networks

Security on Link Layer

Network Segmentation

- **Network Segmentation** reduces attack surface by splitting large networks into smaller, separate networks
  - In high-security context: physical separation
  - Cost-effective using shared cables: **Virtual LANs (VLANs)**
    - Network frames tagged with VLAN-ID
- Shared physical medium can allow attacker to access other VLANs (**VLAN hopping**)
  - **Switch Spoofing:** Attacker impersonates switch
  - **Double Tagging:** Attacker adds additional VLAN tags to frames
- **IEEE 802.1Q** limited to 4096 VLAN IDs
  - **Virtual eXtensible LAN (VXLAN)** raises limit to > 16M
    - Network layer protocol, requires firewall at network edge

Security on Link Layer

Bus Security

- Bus network security challenging due to shared medium
- E.g.: **Controller Area Network (CAN)**, commonly used in cars
  - Connects Electronic Control Units (ECUs)
  - Real-time protocol with priority (e.g., brake ECU > radio ECU)
  - All ECUs trusted by design, no encryption or message authentication
    - Compromised ECUs can eavesdrop & inject arbitrary messages
  - **AUTomotive Open System ARchitecture (AUTOSAR)** is a proposed alternative design with improved security guarantees
    - Slow adoption due to long development and product life-cycles
  - Problems partially mitigated through network segmentation
    - Star topology can also mitigate issues, but increases wiring cost

Network Security Tools

Network Security Tools

Firewalling

- **Firewalls** enforce a network's security policy on incoming/outgoing traffic
- Often co-located with routers, but also available as (hardened) standalone systems
- Security policies defined as rules over network packet fields
  - IP Addresses, TCP/UDP port numbers, protocol flags, ...
- **Stateful firewalls** can further group packets into flows
  - Enables filtering on communication state
- Manual specification of complete and coherent policies typically hard
  - Automated tools available (Firewall Builder, Capirca, ...)

Network Security Tools

Firewalling

Rule	State	Src IP	Src Port	Dst IP	Dst Port	Proto	Action
#1	NEW	172.16.0.0/24	*	*	80, 443	TCP	ACCEPT
#2	NEW	*	*	172.16.20.5	22	TCP	ACCEPT
#3	ESTABLISHED	*	*	*	*	TCP	ACCEPT
#4	*	*	*	*	*	*	DROP

- Firewalling example
  1. All internal hosts (172.16.0.0/24) are allowed to communicate to TCP ports 80/443 (HTTP/HTTPS)
  2. External hosts may connect to an internal SSH server via TCP
  3. All follow-up communication of these connections is granted
  4. Any other traffic is dropped

Network Security Tools

Intrusion Detection and Prevention Systems

- **Intrusion Detection Systems (IDSs)** monitor network traffic and raise alerts when suspicious activity is detected
  - Traffic monitoring can range from simple statistics to high-layer information captured through **Deep Packet Inspection (DPI)**
  - **Signature-based IDSs** match traffic against a pattern database
    - Large databases can cause high workloads and detection latency
  - **Anomaly-based IDSs** try to learn a model of "normal" traffic
    - Learning traffic must be clean and sufficiently representative
  - Can be deployed on individual hosts (**Host IDS, HIDS**) or on network equipment (**Network IDS, NIDS**)
- **Intrusion *Prevention* Systems (IPSs)** behave like IDSs, but can also be configured to also *block* suspicious traffic

Network Security Tools

Network Security Monitoring

- **Flow monitoring** (e.g., NetFlow or IPFIX) provides statistical aggregate information on communication streams
  - Computationally efficient, suited for long-term storage
- **Network forensics** tools (e.g., NetworkMiner or Xplico) can extract files etc. from recorded network traffic
  - Without key material limited to non-encrypted traffic
- **Network scans** allow to enumerate hosts and services in a given network range through e.g. ICMP or SYN probes
- **IP telescopes** are routed networks that host no services or clients, but monitor all incoming traffic
  - Can be used to observe network scans or infer IP spoofing attacks through backscatter

Network Security Tools

Network Security Monitoring

- **Honeypots** are intentionally vulnerable systems used to lure and trap attackers
  - Available for a wide-range of client- and server-side systems
  - Recorded attacker behaviour allows to analyse tactics/procedures
- **Network reputation** services provide trustworthiness scores of networks or IP addresses, based on their past behaviour
  - Limited accuracy for hosts in dynamic IP ranges
- **Security Information and Event Management (SIEM)** systems collect, aggregate, and analyse security-related events from multiple sources and raise incidents for further inspection
  - system log files, firewall events, IDS alerts, ...

Network Security Tools

Network Access Control and Zero Trust Networking

- **Network Access Control** enforces security policies of devices when joining networks beyond port-based authentication
  - **Trusted Network Connect (TNC)** architecture allows to enforce a trusted device configuration via remote attestation
  - See Hardware Security CyBOK Knowledge Area for more details
- In **Zero Trust Networks** all devices are assumed untrusted unless proven otherwise
  - Motivated by **Bring-your-own-device (BYOD)** settings
  - Requires authorization for every network requests
    - Usability can be ensured through single-sign-on schemes
  - Popular example implementation: BeyondCorp
    - Network access control + SSO

Network Security Tools

SDN and NFV Security

- SDN enables new detection and defense capabilities, e.g.
  - Detect DDoS at central controller, but drop traffic at switches
  - Isolate and quarantine infected hosts in near-realtime
- Unfortunately, SDN control plane is also interesting target
  - Access to SDN controller allows to reconfigure entire network
  - Attacker-advertised fake links can cause the Spanning Tree Algorithm (SPTA) topology update to block legitimate ports
  - Some SDN implementations are prone to timing side channels, which can leak sensitive information to the attacker
- **Network Functions Virtualisation (NFV)** replaces network middleboxes (e.g., firewalls) with software modules
  - Also introduces new attack surfaces

Network Security Tools

DoS Countermeasures

- **Volumetric DoS** attacks aim at bandwidth exhaustion
  - Targets range from individual hosts to entire Internet links
  - Most effective mitigation: stop traffic as early as possible
  - Commercial **scrubbing services** filter traffic by acting as a high-bandwidth provider between an organization and the Internet
  - **Null routes** or **BGP FlowSpec** can be used to instruct upstream edge routers to drop traffic
- **Application-Level DoS** aim a computation resource exhaustion
  - Defenses are application specific, e.g.
    - SYN cookies/rate limiting against TCP SYN floods
    - CAPTCHAs against excessive requests on web applications

Conclusion

Conclusion

- There is no silver bullet to network security
- Decent network defenses often combine several security best practices (“defense in depth”)
- We have proven and standardized means for many aspects of secure networking
  - Communication between endpoints can be secured with TLS
  - Communication via untrusted middle hops can be secured using application layer end-to-end encryption schemes (e.g. S/MIME)
  - Networks can be secured against external threats using firewalls, and with zero trust networking even against internal threats
  - IDS provides an additional layer for monitoring payloads