University of BRISTOL

CyBOK

Cyber Security Body of Knowledge: Network Security

Professor Sanjay Jha
The University of New South Wales

bristol.ac.uk

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

Roadmap

CyBOK

- Introduction
- Internet Architecture
- Network Protocols and Vulnerabilities
- Application Layer Security
- Transport Layer Security
- Network Layer Security
- Link Layer Security
- Wireless LAN Security
- Network Defence Tools
- Advanced Network Security topics

Introduction

CyBOK

- Internet connectivity is essential but is vulnerable to threats
- Our heavy reliance on networking technology, that provides unprecedented access to a whole range of applications and services anytime, anywhere, makes it an attractive target for malicious users
  - Malicious users attempt to compromise the security of our communications and/or cause disruption to services
- Certain original protocols are either designed without bearing security in mind, or with poor security design decisions
  - Not merely of historical interest: contemporary designs are often constrained by their predecessors for pragmatic reasons

Introduction

- We explore
  - The challenges in securing a network under a variety of attacks
  - Widely used security protocols
  - Emerging security challenges and solutions

- A basic understanding of networking protocol stack and TCP/IP suite is assumed

Internet Architecture

- A complex system such as distributed applications running over a range of networking technologies is best understood when viewed as layered architecture

- Figure 1 (next slide) shows the 7-layer ISO OSI protocol stack and the interaction between various layers
  - TCP/IP protocol stack uses only five layers from OSI model i.e., layers 1- 4 and 7
  - Presentation and Session layers (shown in dotted box) are optional and their functionality can be offloaded to the application layer

- The model also allows us to understand the security issues on each layer and the interplay between them.

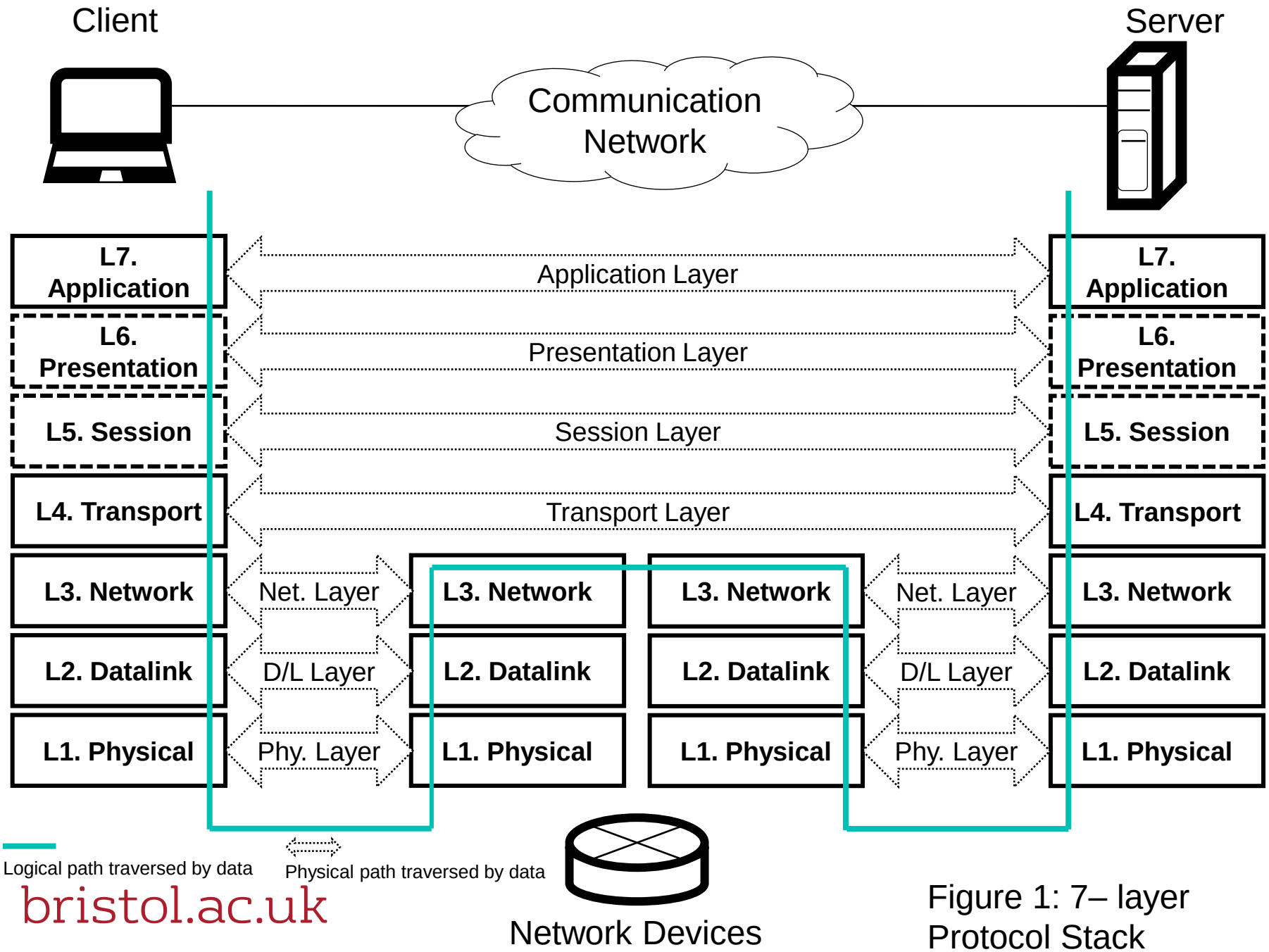


Figure 1: 7– layer Protocol Stack

Network Vulnerabilities

CyBOK

- Security research literature use Dolev-Yao (DY) adversarial formal model for formal analysis of security protocols
  - DY model describes the worst possible adversary that has complete control over the entire network allowing it to read any message, prevent delivery of any message, duplicate any message or otherwise synthesize any message for which the adversary has the relevant cryptographic keys (if any).
  - Real adversaries may have limited capabilities

Network Security Attacks

CyBOK

- We will use the popular network security characters Alice, Bob, Eve and Mallory

- Alice and Bob want to exchange messages securely while Eve (an eavesdropper) and Mallory (a malicious attacker) are waiting to compromise their communications
  - In real world Alice and Bob can be replaced with Webservers and clients, two email clients, DNS servers etc.

- Eve can capture (eavesdrop) the traffic and extract confidential information such as passwords, credit card details etc. , while Mallory can launch a man in the middle (MiTM) attack by placing himself between Alice and Bob
  - Real world Eve and Mallory could be compromised gateways/routers/access-points, or malware present in the user's device or server.

Network Security Attacks

CyBOK

- Denial of Service (DoS) attack is launched by an attacker by sending an avalanche of bogus packets to a server to keep the server constantly busy or clog up the access link with the aim of disrupting the service for the legitimate users

- In distributed DoS (DDoS) attacks, a large number of compromised devices (bots) are used.
  - Mirai is an example of DDoS attack launched in 2016 by compromising Linux-based Internet of Things (IoT) devices such as IP cameras, utility meters, home routers and others
  - Done by exploiting weak authentication configurations including use of default passwords

- In IP spoofing attacks, an attacker can impersonate as an authorised user by crafting a packet with forged IP address and adjusting certain other fields to make it look legitimate

Desirable properties of secure communication

- *confidentiality:* only sender, intended receiver should "understand" message contents
- *authentication:* sender, receiver want to confirm identity of each other
- *message integrity:* sender, receiver want to ensure message not altered (in transit, or afterwards) without detection
- *non-repudiation:* *no one (including the sender) can deny that message was sent by the sender*
- *access and availability:* services must be accessible and available to users

Application Layer Security

CyBOK

- Assume Alice and Bob want to use email

A. They decide to use a symmetric key encryption algorithm such as AES with a 256 bit key. Alice encrypts the message and send it to Bob who can decrypt using the same shared key.

- What have they achieved?
  - Message can only be decrypted by Alice and Bob achieving confidentiality
  - No message integrity and origin authentication. Additional measures required for integrity and origin authentication
  - Requires secure key distribution

Application Layer Security

CyBOK

- Assume Alice and Bob want to use email

B. Suppose Alice and Bob do not care about confidentiality but want assurance that messages will not be tampered with in transit. Alice calculates the message hash using SHA-3 algorithm and send it to Bob. Bob can recalculate the hash and verify it matches

- What have they achieved?
  - No confidentiality and origin authentication
  - What about message integrity? An attacker can easily replace the genuine message with a forged one and a matching hash. Bob cannot detect the message alteration
  - Additional measures still required for achieving message integrity

Application Layer Security

CyBOK

- Assume Alice and Bob want to use email

C. Alice calculates the message hash using SHA-3 algorithm and additionally use a pre-negotiated symmetric key to encrypt the hash. Bob now decrypts this hash using the pre-negotiated symmetric key.

- What have they achieved?
  - No confidentiality as message still sent in plain text
  - What about message integrity? Bob can verify the integrity of the received message
  - This also authenticates that the message was sent by someone who shares a key with Bob, in this instance Alice
  - Does not provide non-repudiation

Application Layer Security

CyBOK

D. Alice uses public key cryptography and calculates the message hash using SHA-3 algorithm and uses her private key to encrypt the hash (forming digital signature). Bob now decrypts this hash using the Alice's public key

- What have they achieved?
  - No confidentiality as message still sent in plain text
  - This allows for an integrity check and authentication at the same time, as no one other than Alice knows her private key.
  - Also achieves non-repudiation as well
  - We avoided pre-negotiation or sharing of keys

- How does Bob get Alice's public key and trust that Eve or Mallory are not using a forged public/private key to perform MiTM?

Application Layer Security

CyBOK

- Public Key Infrastructure (PKI) provides a solution for registering and managing a trustworthy public key
- Government agencies or standard organisations appoint or recognise registrars who issue keys, and keep track of the public certificates of entities (individuals, servers, routers etc.)
  - The registrars themselves have a registered public/private key pair
- Typically, a user's identity, public-key and CA information are used as an input to the hash function. The hash is then signed with the CA's private key to produce a Public Key Certificate (PKC)
  - The fields on the certificate include a unique identifier/serial number, a signature algorithm used by the CA and the period of validity.
- Bob can get the PKC for Alice from a CA and apply CA's public key to retrieve Alice's authentic public key

Application Layer Security

CyBOK

- The web of trust is an alternative scheme where users can create a community of trusted parties by mutually signing certificates without needing a registrar
- Alice and Bob can sign each other certificates certifying their public keys. Other entities if they trust on Alice, can use Bob's certificate duly certified by Alice
- Pretty Good Privacy (PGP) was one of the earliest email systems to propose the security approach using the web of trust for certificates

Application Layer Security

CyBOK

- The PKI model has faced several challenges
  - Certificate Authorities issued certificates in error, or under coercion, or through their own infrastructure being attacked
- Recent years have seen many partial solutions such as certificate pinning and public immutable logs of issued certificates being implemented to prevent the PKI trust model from being undermined

Application Layer Security

CyBOK

- Various original application layer protocols lacked security features

Protocol Name	Functionality	Security Attacks
Simple Mail Transfer Protocol (SMTP) & Multipurpose Internet Mail Extensions (MIME)	Exchanging messages between mail servers, MIME for content formatting in SMTP	DoS, Impersonation
Domain Name System (DNS)	Translation between a host name and the corresponding IP address	MiTM, DNS cache poisoning, DNS exfiltration
Hyper Text Transfer Protocol (HTTP)	Interaction between web servers and web clients	Various forms of DoS
Network Time Protocol (NTP)	Synchronize devices to Coordinated Universal Time (UTC)	Replay, MiTM, Spoofing, DoS

Application Layer Security

CyBOK

Protocol Name	Security extension	Usage
SMTP	SMTPS (RFC 3207 / 7817)	Uses security services from transport layer
MIME	S/MIME (RFC 5751)	Integrity check and certificates validation automatically performed by the respective mail agents
DNS	DNSSEC (RFC 4033-35)	Provides authenticity and data integrity by using public key cryptography
HTTP	HTTPS (RFC 2818)	Uses security services from transport layer
NTP	Ntpd compliance with RFC 7384	Authentication, authorisation using cryptographic keys

Transport Layer Security

CyBOK

- Security services at the transport layer could relieve each application from the burden of taking care of security itself
  - This would also provide compatibility across platforms/vendors
- Provide a shim layer between the application and the transport layers in the form of Secure Socket Layer (SSL)
  - API provided by SSL enable applications to bootstrap secure connections and send/receive data securely
- IETF developed Transport Layer Security (TLS) taking ideas from SSL 3.0 protocol
  - Current version is TLS 1.3 (standardised in 2018)

- TLS protocol has 3 phases:
  Handshake, key-derivation and data transfer

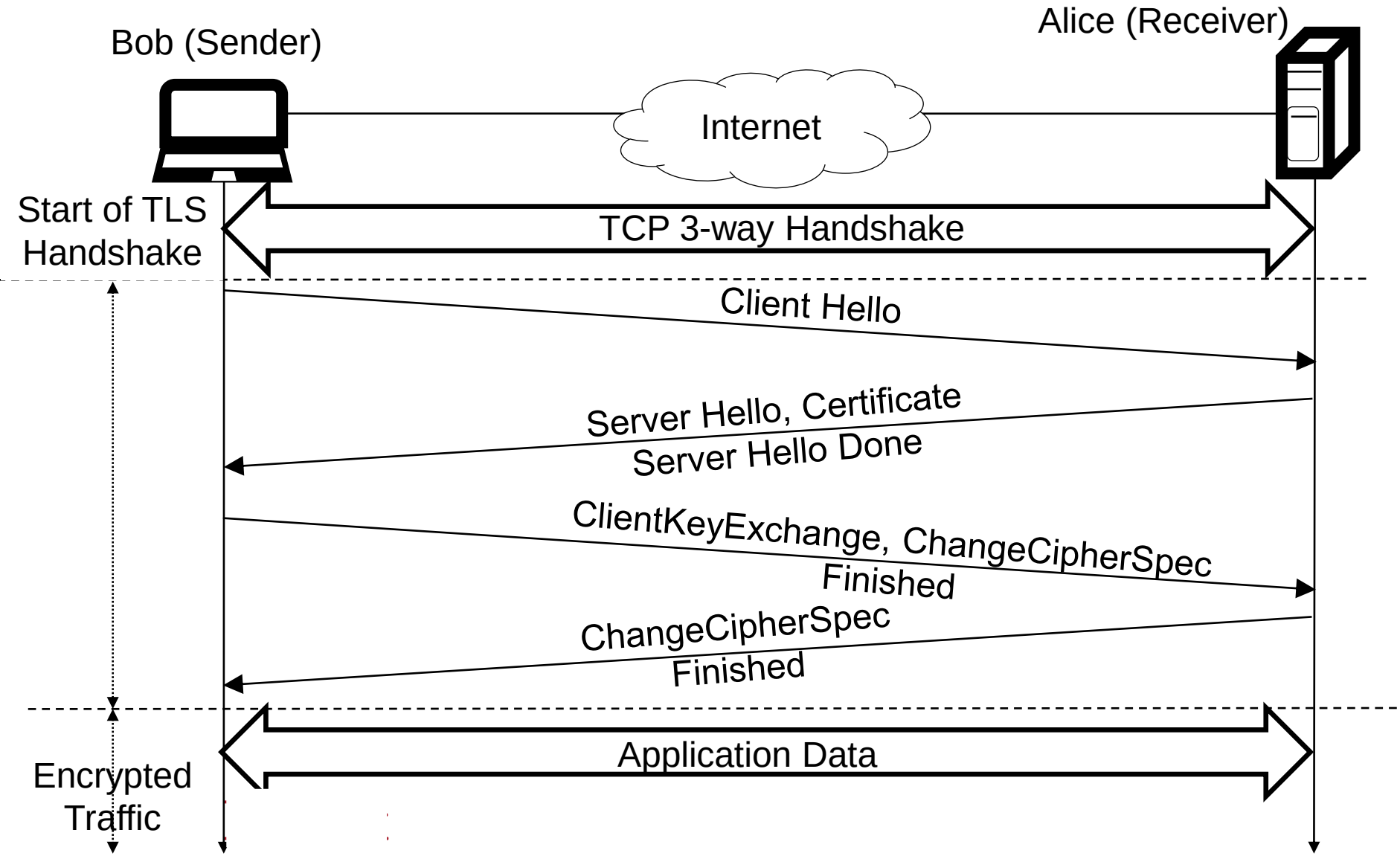


Figure No 2

TLS Protocol Handshake

CyBOK

- After TCP connection establishment
  - Bob sends a ClientHello message to Alice containing available ciphers, hash functions and a large random number (nonce)
  - Alice responds with a ServerHello message along with her choice of ciphers and hashes (e.g., AES for confidentiality, RSA for public key, SHA3 for Message Authentication Code (MAC), Deffie Hellman for key exchange), her public key certificate and a nonce.
  - Bob checks validity of Alice's certificate and initiates ClientKeyExchange message
  - Bob sends a ChangeCipherSpec and a finished message to indicate that key generation and authentication are complete
  - Alice also has the shared key now and responds with ChangeCipherSpec and finished message
  - Bob decrypts message with symmetric key and check integrity

TLS Protocol Key Derivation

CyBOK

- A pseudorandom function produces a Master Secret (MS) using client nonce, server nonce and Pre-Master Secret (PMS)

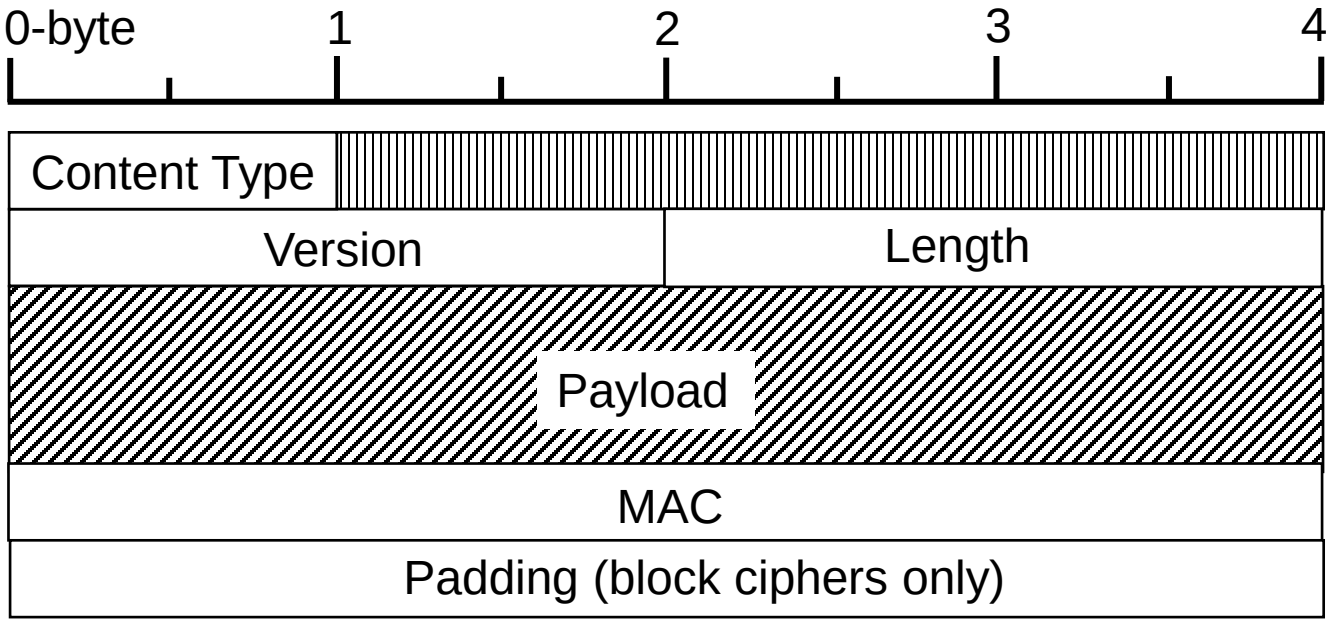
- Following four keys are derived using MS and additional parameters
  - Client encryption key: Session key for data sent from Bob to Alice
  - Server encryption key: Session key for data sent from Alice to Bob
  - Client MAC key: session MAC key for data sent from Bob to Alice
  - Server MAC key: Session MAC key for data sent from Alice to Bob

- Separate ephemeral keys for encryption and Integrity in each direction provides perfect forward secrecy (avoids replay attacks)

TLS Protocol Data Transfer

CyBOK

- TLS defines a record format to keep track of the data being sent



  - Length of data sent in each record is indicated along with the type of record (data or control). A MAC is also appended at the end of each record
  - Data plus MAC are encrypted using the session encryption key and it then passed on to TCP

bristol.ac.uk

Transport Layer Security

CyBOK

- Various attacks on Transport layer

Attack	Functionality	Counter measure
TCP SYN Flooding	Client sends SYN, Server replies with SYN/ACK, Client never replies back	TCP SYN Cookies [RFC 4987]
Connection Replay	Eve capture communication and repeat the sequence later on	TLS (and PMS generation algorithm) uses session specific nonce
Various attacks on SSL/TLS itself	SSL stripping, BEAST, Lucky thirteen attacks [RFC 7457]	[RFC 7366] Encrypt before MAC, Counter measures in latest version of TLS 1.3 [RFC 8446]

QUIC

CyBOK

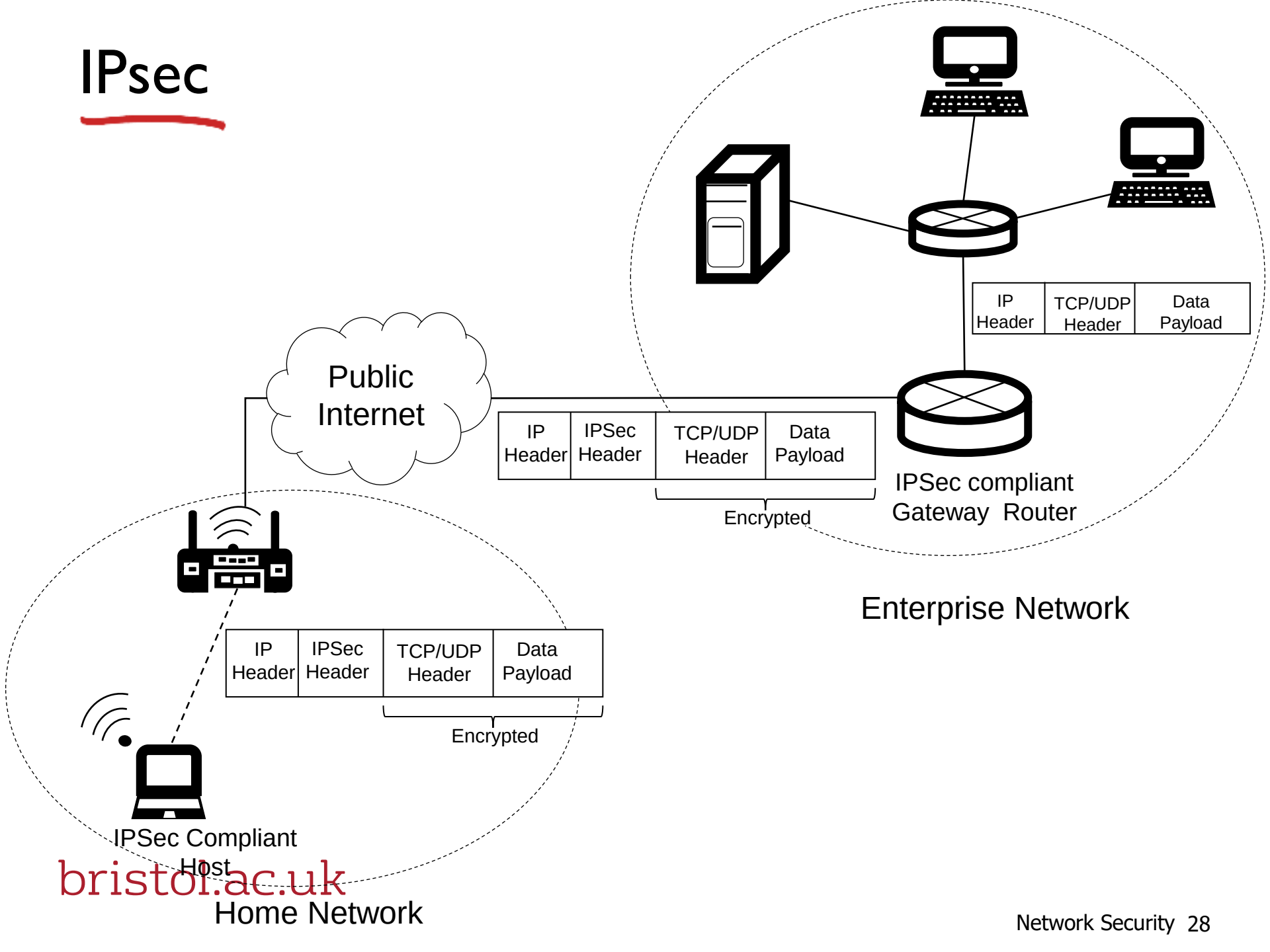
- QUIC is a new transport protocol designed by Google for faster web-browsing using UDP instead of HTTP over TCP
  - The protocol currently uses proprietary encryption and authentication
- Although QUIC uses the standard HTTP ports, security devices such as Firewalls and IDS do not track this application layer protocol at present
- Since the standardisation work is already in progress, it is likely to use TLS1.3 for secure transport

Network Layer Security

CyBOK

- Why do we need security mechanisms at the network layer?
- Higher layer security mechanisms do not necessarily protect an organisation's internal network links from malicious traffic
  - If and when malicious traffic is detected at the end-hosts, it is too late, as the bandwidth has already been consumed
- Higher-layer security mechanisms (e.g., TLS) do not conceal IP headers
  - This makes the IP addresses of the communicating end-hosts visible to eavesdroppers
- Security mechanism at the network layer supports Virtual Private Networks (VPN) over the Internet

IPsec



IPsec

CyBOK

- IPsec provides data confidentiality, integrity, origin authentication and replay attack prevention
- It supports Tunneling and Transport modes of operation (Figure shown in previous slide is the transport mode)
- In tunneling mode, the endpoint of tunnels could be a source or a edge router at either end, with edge devices the more popular choice
  - Edge devices performs encapsulation of every header including the IP hiding the communicating IPs to create a tunnel
  - Edge devices participating in IPsec reduces the key management and obliterates the need for end host implementing IPsec

IPsec

CyBOK

- IPsec supports a set of formats to implement security
- The Encapsulation Security Payload (ESP) format supports confidentiality using encrypted IP packets, data integrity using hash functions, and source authentication
- If an application does not require confidentiality, it may simply use the Authentication Header (AH) format, which supports data integrity and source authentication
  - The IETF RFC2410 defines the NULL Encryption algorithm with ESP to achieve the same outcome
- In total, we get four different options for communication: Transport mode with ESP, Transport mode with AH, Tunnel mode with ESP and Tunnel Mode with AH
  - Since VPN tunnels are fully encrypted, the Tunnel mode with ESP remains the protocol of choice

IPsec

- IPsec maintains a Security Association (SA) for each direction of the link in SA database (SAD) for lookup
  - Type of encryption, integrity check, authentication key etc.
- Uses Internet Key Exchange Protocol (IKEv2) for key exchange
  - Establishes SKEYSEED used to generate keys for the session

Network Layer Security

CyBOK

- Other important aspects to consider at the network layer are:
- NAT devices providing IP Masquerading
- IPv6 proliferation
  - 128 bit addresses increases the searchable address space
  - IPv6 L3 addresses are derived directly from L2 addresses without the need to do ARP
  - Allows cryptographically generated addresses (CGA) binding addresses to a public signature key
  - IPsec initially mandated but now recommended

Network Layer Security

CyBOK

- Routing protocols security
  - Important aspect to ensure routers do not act on malicious routing exchange control messages
- Interior Gateway protocols (IGP) that work within the Autonomous Systems (AS) support no security by default
  - Can be configured to support plain text-based or MD5-based authentication
  - Routers exchange message digest and key-id to indicate which key to use from a previously shared list of passwords

Network Layer Security

CyBOK

- Border Gateway Protocol (BGP) is the de-facto exterior gateway protocol that advertises the reachability information within and across ASs
- BGP also lacks integrity and authentication mechanisms by default and hence subject to attacks such as
  - BGP route hijacking attack
    - Divert all traffic to flow through your AS or another AS
  - BGP DoS attack
    - Attacking the BGP border router
- BGPSec
  - Utilises PKI to verify the signatures of the BGP peers
    - Signature verification comes at a cost
  - Can use IPsec for point to point security for exchanging update messages

Link Layer Security

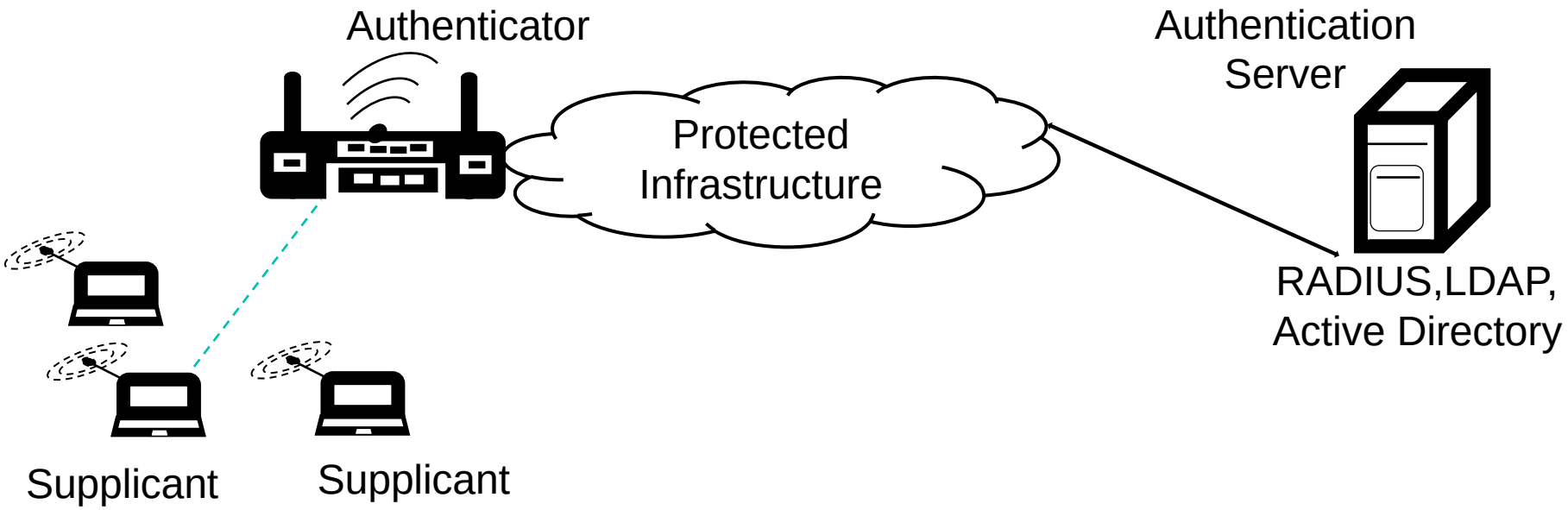
CyBOK

- 802.1X Port based Authentication
- Security issues in Ethernet switched LAN
- Security issues in Wireless LAN

Link Layer Security

CyBOK

- 802.1X Port based Authentication
  - For both wired and wireless networks
  - A station (supplicant) must authenticate with the switch or Access Point (AP) (Authenticator) before connecting
  - The AS and authenticator can be co-located or if separate preconfigured with a shared secret

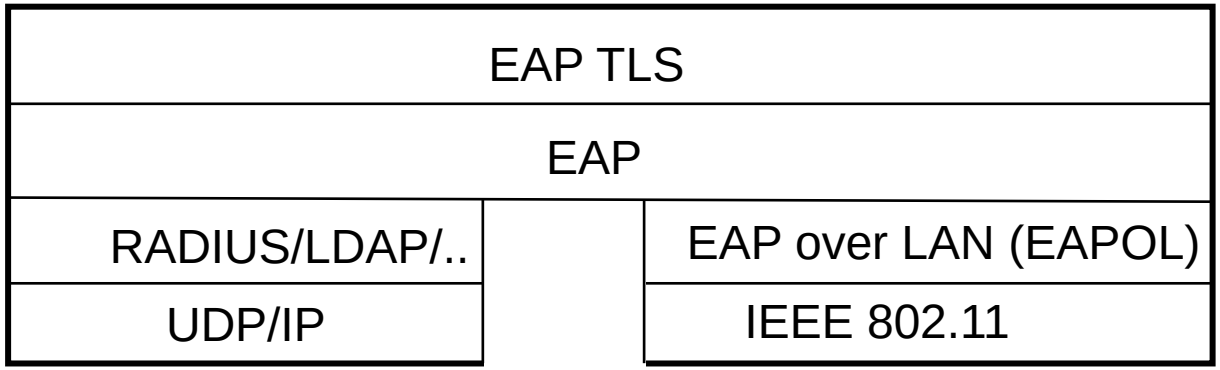


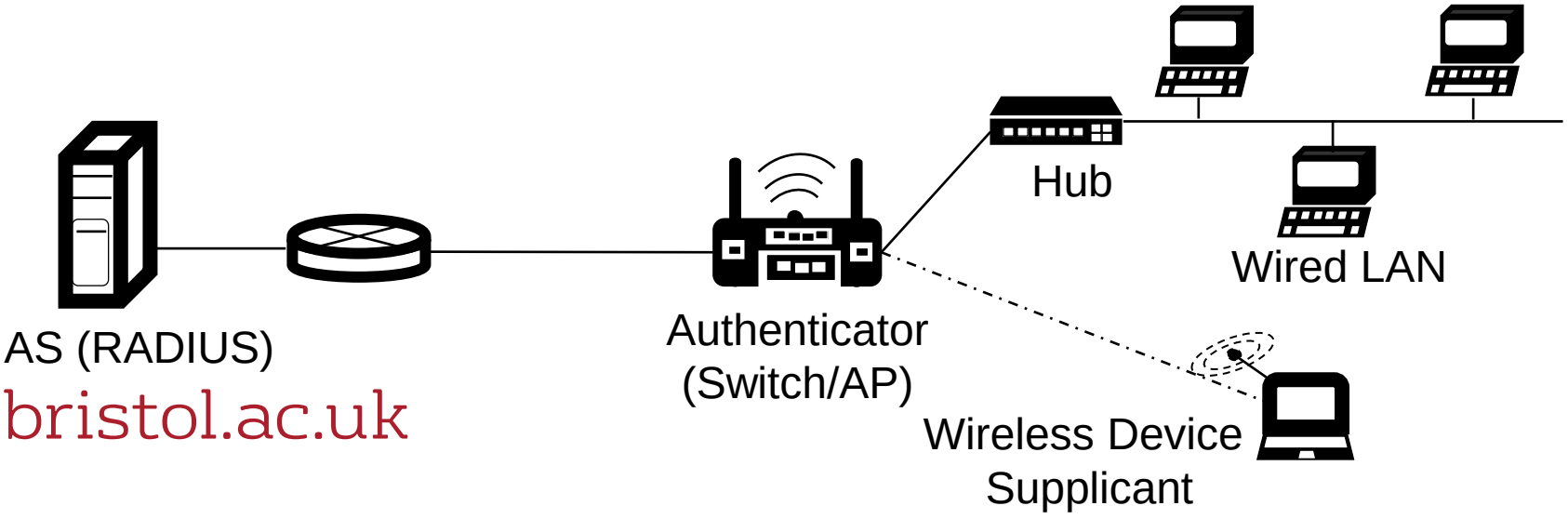
bristol.ac.uk

Link Layer Security

CyBOK

- Supplicant uses Extensible Authentication Protocol (EAP) for authentication by AS through the Authenticator
  - Uses L2 protocol between supplicant and authenticator and higher layer protocol between the authenticator and AS





EAP in action

CyBOK

- When a new client (supplicant) is connected to an authenticator, the port on the authenticator is set to the 'unauthorised' state, allowing only 802.1X traffic
- The authenticator sends out the EAP-Request identity to the supplicant. The supplicant responds with the EAP-response packet, which is forwarded to the AS.
  - This typically includes the supplicant's credentials (username and hash of password).
- Upon verification, the AS returns one of the following responses: Access Accept, Access Reject, Access Challenge for extra credentials. If the result is Access Accept, the authenticator unblocks the port to let higher layer traffic through.
- When the supplicant logs off, the EAP-logoff to the authenticator sets the port to block all non-EAP traffic.

EAP Tunneling

CyBOK

- To safeguard against any eavesdropping, the EAP uses a Tunnel for authentication and authorisation
  - A whole range of EAP Tunneling protocols are available. EAP-Transport Layer Security (EAP-TLS), EAP for GSM Subscriber Identity (EAP-SIM) and EAP Protected Authentication Protocol (EAP-PEAP) are some of the examples for establishing a secure tunnel.

- Once the supplicant and AS mutually authenticate, they together generate a Pairwise Master Key (PMK)
  - The AS sends this PMK to the authenticator
  - From this point on, the supplicant and authenticator use the PMK to derive the Temporal Key (TK) used for the message encryption and integrity (similar to TLS)

Ethernet Switched LANs

CyBOK

- Ethernet switched LANs operate on self-learning and configuring protocols; various attacks are possible
- Switch Poisoning Attack: The attacker fills up the switching table with bogus MAC addresses forcing the switch to broadcast all incoming data frames to all outgoing ports
  - Attacker controls a device attached to one of the port
- MAC Spoofing: Attacker uses a legitimate MAC address by snooping and flooding the network directing all traffic to itself destined for the target machine
- ARP Spoofing: Attacker sends fake ARP messages binding the target's IP address to its own MAC address
  - ARP spoofing can also be used for DoS attacks by populating the ARP table with multiple IP addresses corresponding to a single MAC address of a target server

bristol.ac.uk

Ethernet Switched LANs

CyBOK

- VLAN Hopping: VLAN hopping attacks allow an attacking host on a VLAN to gain access to resources on other VLANs that would normally be restricted
  - In a switch spoofing attack, an attacking host impersonates a trunking switch responding to the tagging and trunking protocols (e.g., IEEE 802.1Q or Dynamic Trunking Protocol) typically used in a VLAN environment.
    - The attacker can access traffic for multiple VLANs
  - In a double tagging attack, an attacker succeeds in sending its frame to more than one VLAN by inserting two VLAN tags to a frame it transmits.
    - This attack does not allow the attacker to receive a response

Link Layer Security

CyBOK

- Various attacks on Switched Ethernet LANs

Attack	Counter measure
Switch poisoning attack	Authenticating MAC addresses from some local database of legitimate addresses
MAC spoofing	802.1X based authentication
ARP spoofing	Limit number of per port addresses, Trusted binding table for verification
VLAN Hopping	Switch configurations to limit ports participation in trunking protocols, Disable automatic trunk negotiation

Wireless LANs Security

CyBOK

- Wireless Equivalent Privacy (WEP)
- Provides integrity, confidentiality and authentication using symmetric key encryption
  - A 24-bit initialisation vector (IV) is combined with 104-bit shared key and fed into a pseudo random number generator (PRNG such as RC4 stream cipher)
  - The plaintext payload and the CRC of the frame are then combined with the key sequence generated by the RC4 using bit-wise exclusive-or operation for encryption
  - A new IV is used for each frame and sent in plaintext along with the encrypted frame
  - The receiver input the received IV and shared secret key into PRNG to get the keystream, XOR the keystream with the encrypted data for decryption
  - Data integrity through 32-bit CRC and authentication using 128-bit nonce

Wireless LANs Security

CyBOK

- A number of design flaws exist in WEP
  - 24-bit IV – 16 million unique IVs can be exhausted in less than 2 hours for high speed LANs
    - Attacker can mount a known plaintext attack as IVs ae sent in plain text
  - RC4 is open to FMS (Fluhrer, Martin and Shamir) attack
    - Key can be recovered by capturing a large number of messages
  - CRC is a poor choice for detecting maliciously modified messages
    - MAC and digital signatures are preferred

Wireless LANs Security

CyBOK

- WiFi Protected Access (WPA) (2003):
  - Extends WEP IV to 48 bits which is also used as a packet sequence counter
  - Uses Temporal Key Integrity Protocol (TKIP) but maintains RC4 for compatibility
  - Pre-shared key (PSK) and a nonce are hashed to generate a temporal key
  - This temporal key plus transmitter MAC address and the sequence counter is fed in a cryptographic mixing function to generate 128 bit key for encryption and another 64 bit key for integrity
  - Every packet is thus encrypted with a unique encryption key to avoid FMS-style attacks

Wireless LANs Security

CyBOK

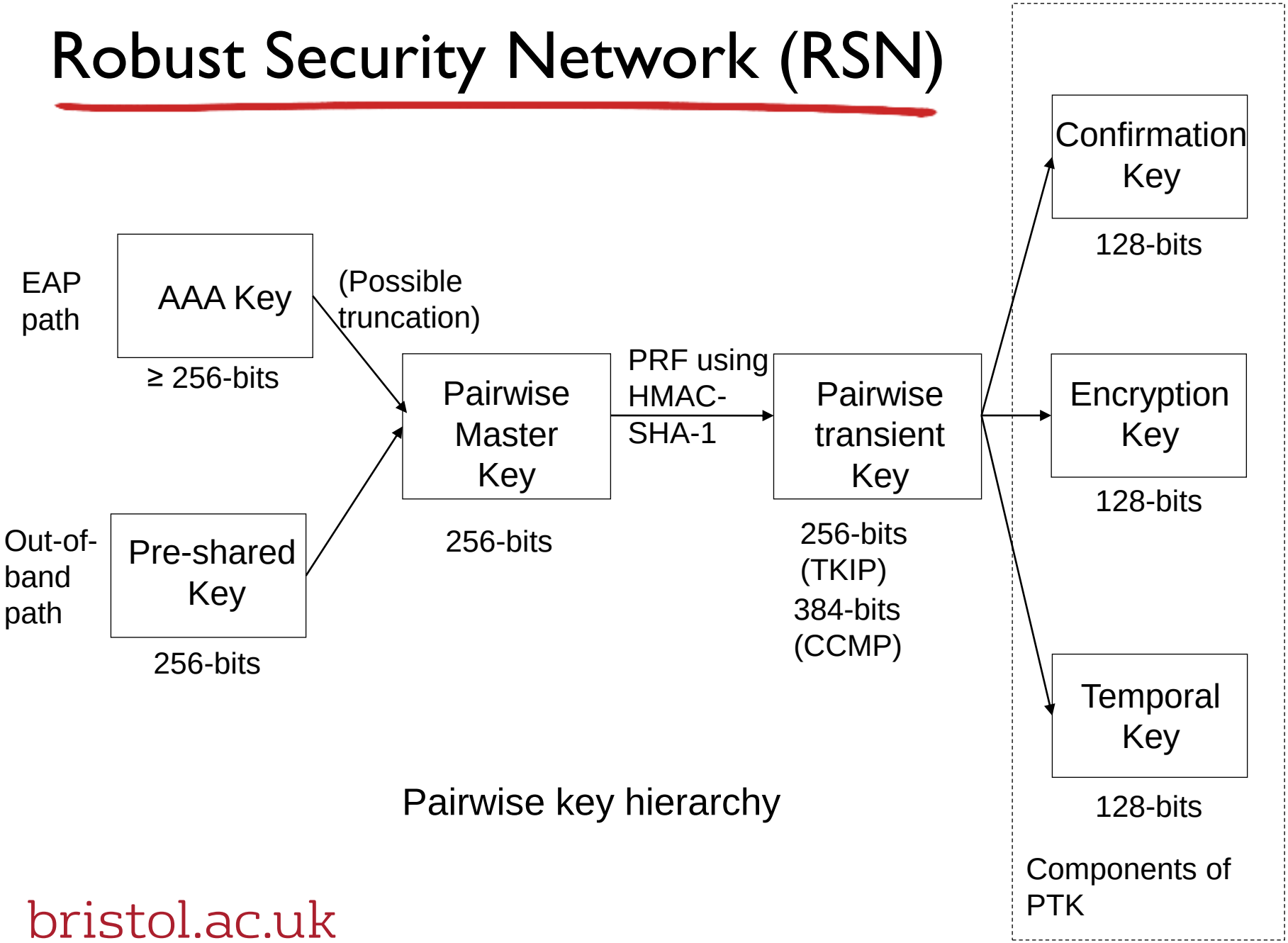
- WPA2 (2004):
  - Relies on 128 bit AES Counter Mode with the Cipher Block chaining Message Authentication Code Protocol (CCMP)
    - Improves temporal key generation
    - Improved four way handshake
- WPA3 (2018):
  - PSK is replaced with a new key distribution called Simultaneous Authentication of Equals (SAE) based on IETF Dragonfly key exchange
    - WPA3-Personal uses a 128-bit encryption
    - WPA3-Enterprise uses 192-bit encryption

Wireless LANs Security

CyBOK

- Robust Security Network (RSN):
  - 802.1X-based mechanism for access control
  - EAP for authentication and key-generation
  - TKIP and CCMP for encryption/decryption, integrity and origin authentication
- RSN key derivation
  - User device and AP have a pre-shared PSK or in enterprise solutions Master Session Key (MSK) is generated during 802.1X authentication
  - PSK can be used as a pair-wise master key (PMK) or PMK can be generated from MSK
  - Pair-wise Transient Key (PTK) is generated using Host and AP addresses, nonce and PMK
  - PTK is split three ways generating separate keys for each function

Robust Security Network (RSN)



Pairwise key hierarchy

Network Defense Tools

CyBOK

- A number of approaches that can be implemented at various layers of the protocol stack
  - Packet filters and firewalls
  - Application gateways
  - Circuit level gateway
  - Intrusion detection system (IDS)
  - Intrusion prevention system (IPS)

Network Defense Tools

CyBOK

- Packet filters and firewalls
- Two types stateless and stateful
  - Stateless filters do not retain any state information about the packets/flows/sessions
  - Stateful packet filters can track transport layer flow, a chain of packets belonging to a session

- Use a set of rules to inspect each packet and perform a matching action
  - Pass, drop, drop and generate a notification etc.
  - Packets may be filtered according to their source and destination network addresses, protocol type (TCP, UDP, ICMP), TCP or UDP source/destination port numbers, TCP Flag bits (SYN/ACK), rules for traffic from a host or leaving the network via a particular interface and so on

Network Defense Tools

CyBOK

- Application Gateway (AG) / Application Proxies can perform access control through user authentication
- Can inspect information from full 5-layers of TCP/IP stack
  - Can be co-located with a firewall or uses a firewall
  - Can create two sessions: one between the client and AG, and one between AG and the destination that goes through the firewall
  - AG can terminate a SSL connection.
    - *AG does the resource intensive encryption/decryption and passes the un-encrypted traffic to the backend servers*
    - *AGs can inspect encrypted outbound traffic where the clients are configured with corresponding certificates installed at the AG*
- AGs can slow down the connection
  - Authentication, policy checks, state maintenance

bristol.ac.uk

Network Defense Tools

CyBOK

- Circuit-level Gateway (CG)
- A proxy that functions as a relay for TCP connections
  - Allows hosts from a corporate Intranet to make TCP connections over the Internet

- The most widely used CG is SOCKS
  - It runs transparently as long as the hosts are configured to use SOCKS interface
  - Works with variety of applications

Network Defense Tools

CyBOK

- Intrusion detection systems (IDS)
- Does deep packet inspection using agents/sensors/monitors on the network or the hosts
- A copy of all incoming traffic is supplied to an IDS for analysis
- Compares the traffic against what it considers as a normal traffic and sets of alarm when it detects suspicious activity
- Two main categories based on analysis: Signature based and Anomaly based
- Two main categories based on deployment: Host based and Network based

Network Defense Tools

CyBOK

- Intrusion detection systems (IDS)
- Signature based IDS uses a database of known threat signatures similar to virus definitions to compare the monitored traffic
  - Many false negatives due to outdated database
  - Generates heavy workload
  - Cannot detect new attacks

- Anomaly based IDS uses statistical features of normal traffic to compare with the monitored traffic
  - Bandwidth, arrival rate and burstiness
  - A large number of port scans would generate an alert
  - Many false positives despite use of advanced machine learning and Artificial Intelligence techniques

Network Defense Tools

CyBOK

- Intrusion detection systems (IDS)
- Host based IDS (HIDS) runs on individual hosts
  - Can monitor host activities at the process level
  - Monitor inbound and outbound traffic for the host
- Network based IDS (NIDS) is deployed at strategic locations within the network
  - Monitors important segments of network

Network Defense Tools

CyBOK

- Intrusion prevention systems (IPS)
- An IPS can drop/block traffic as it is deployed inline on routers/switches
- Also has an IDS capability
- An IPS can proactively prevent delivery of an unsafe email on inspecting the headers/payload
  - Risk of blocking legitimate traffic due to false positives /misconfiguration

Network Security Architecture Design

CyBOK

- Network protection tools are most effective when deployed in combination
- A demilitarised zone (DMZ) is an extranet hosting an organisation external facing services such as webserver, DNS, email server etc.
- Private network is further partitioned into several security zones by the security architect
  - Each zone is managed by one or more of the IDS/IPS or AG based on the significance of the information/infrastructure to be protected

Advanced Network Security Topics

CyBOK

- Software Defined Network (SDN), Virtualisation
- SDN separates the packet forwarding functionality of the forwarding devices, i.e. the data plane from the control plane
- The routing function and other intelligence is implemented in a centralised controller
- The SDN architecture provides many new features to improve security for threat detection and attack prevention and provides innovative security services
  - A DDoS attack can be inferred by the central controller more accurately, and a threat mitigation application may dynamically reprogram switches at the network perimeter to drop malicious traffic flows

Advanced Network Security Topics

CyBOK

- SDN platform has to be secured itself
- SDN switches are prone to a timing side channel attack
  - An attacker can determine whether an exchange between an IDS and a database server has taken place or whether a host has visited a particular website based on inference
  - As a countermeasure, introduce artificial delays for first few packets of every flow even if the rule exists
- Network Functions Virtualisation (NFV) deploys network middleboxes such as firewalls, DMZs, load balancers etc. entirely as virtualized software modules called Virtual Network Functions (VNFs) managed through standard APIs
  - An attacker can compromise a VNF and spawn other new VNFs to change configuration of the network

Advanced Network Security Topics

CyBOK

- Internet of Things (IoT) security

- IoT devices are typically low powered and have limited capability for participating in advanced security protocols
- IoT vendors prefer ‘first to market’ with security being low priority
- TLS and datagram TLS are cornerstone of IoT security
  - Also use public key cryptography (PKC) or a PSK
    - PKC is resource intensive
  - DTLS is designed to be used in constrained devices but End to End communication is not scalable