MONASH University
Information Technology

FIT3031 INFORMATION & NETWORK SECURITY

Monash University Information Technology

FIT3031 INFORMATION & NETWORK SECURITY

Lecture 6
Wireless Network Security

Unit Objectives

- ✓ OSI security architecture
  - **common security standards and protocols for network security applications**
  - **common information risks and requirements**
- ✓ operation of private key encryption techniques
- ✓ operation of public encryption techniques
- ✓ concepts and techniques for digital signatures, authentication and non-repudiation
- ✓ security threats of web servers, and their possible countermeasures
- ✓ Wireless Network Security Issues
- security threats of email systems and their possible countermeasures
- IP security
- intrusion detection techniques for security purpose
- risk of malicious software, virus and worm threats, and countermeasures
- firewall deployment and configuration to enhance protection of information assets
- network management protocol for security purpose

Review of Last Lecture

Key points from the last lecture:

- **Web security includes security of web server, client machine and security of network traffic between server and client**
- **To ensure network traffic security, 3 approaches are possible**
  - IPSec at the network layer
  - SSL/TLS protocol
  - Application specific security services embedded within the particular application, e.g., SET, Kerberos, S/MIME
- **SSL is a layer inserted between transport and application layer**
- **SSL provides: Server authentication, confidentiality, Integrity and client authentication (optional)**
- **SSL consists of 4 sub-protocols, mainly two**
  - SSL handshake protocol to negotiate cryptographic parameters between server and client
  - SSL Record Protocol actually transfers encrypted data
- **HTTPS (HTTP over SSL)**
- **Secure Shell (SSH) : secure network communications**
  - Transport layer, User Authentication & Connection protocols

Lecture 6: Objectives

- **Appreciate the IEEE 802.11 Wireless Protocol**
  – Understand the wireless security mechanisms
- **Appreciate the Wireless Applications Protocol**
- **Understand Wireless Transport Layer Security (WTLS)**
- **Appreciate end-to-end security between wireless clients and network servers**

IEEE 802.11

- **IEEE 802 committee for LAN standards**
- **IEEE 802.11 formed in 1990's**
  - charter to develop a protocol & transmission specifications for wireless LANs (WLANs)
- **since then demand for WLANs, at different frequencies and data rates, has exploded**
- **hence seen ever-expanding list of standards issued**

Table 1: IEEE 802.11 Standards

Standard	Frequency band	Bandwidth	Modulation	Maximum data rate
802.11	2.4 GHz	20 MHz	DSSS, FHSS	2 Mb/s
802.11b	2.4 GHz	20 MHz	DSSS	11 Mb/s
802.11a	5 GHz	20 MHz	OFDM	54 Mb/s
802.11g	2.4 GHz	20 MHz	DSSS, OFDM	54 Mb/s
802.11n	2.4 GHz, 5 GHz	20 MHz, 40 MHz	OFDM	600 Mb/s
802.11ac	5 GHz	20, 40, 80, 80 + 80, 160 MHz	OFDM	6.93 Gb/s
802.11ad	60 GHz	2.16 GHz	SC, OFDM	6.76 Gb/s

IEEE 802 Terminology

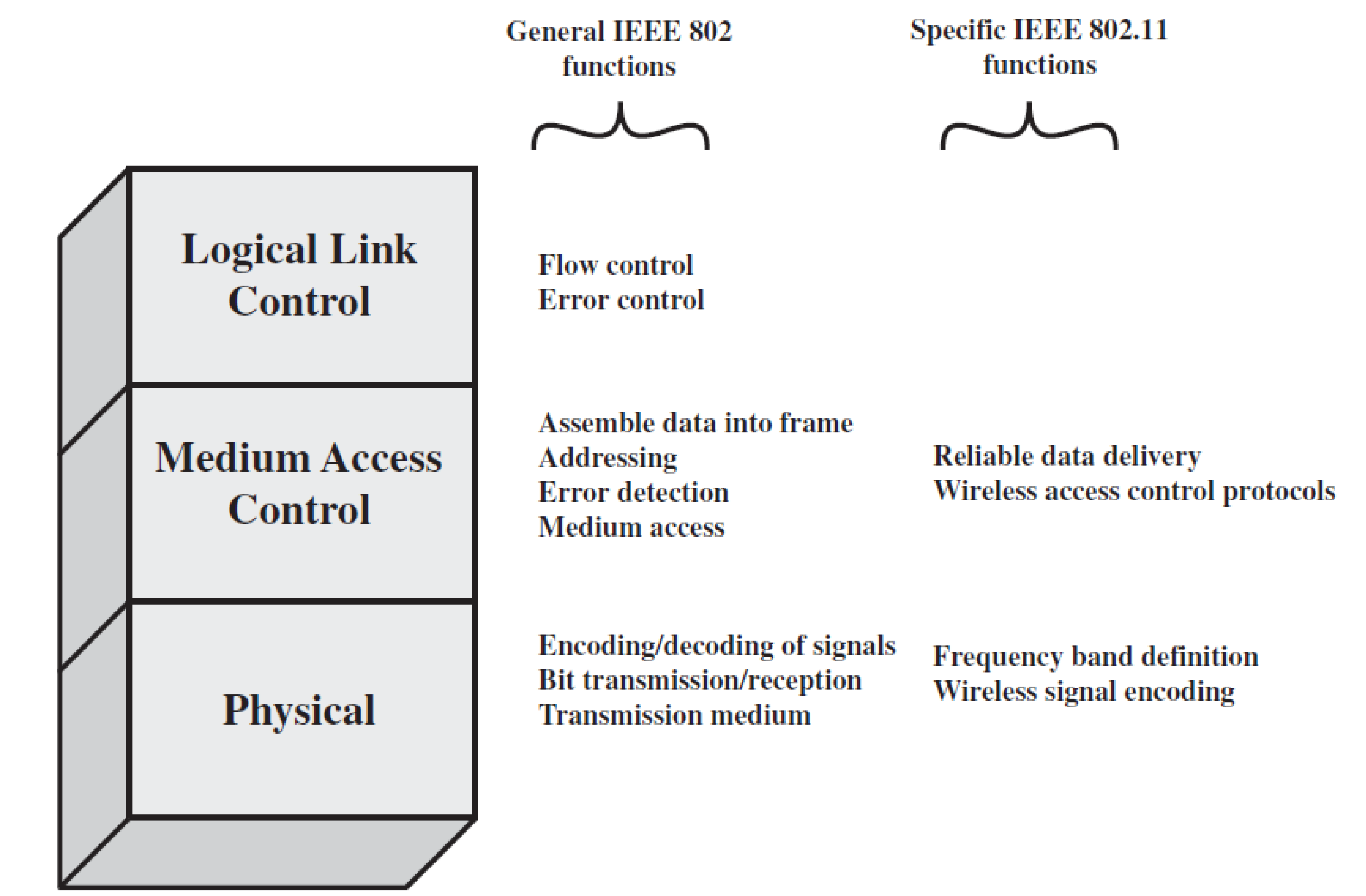
Table 6.1 IEEE 802.11 Terminology

Access point (AP)	Any entity that has station functionality and provides access to the distribution system via the wireless medium for associated stations.
Basic service set (BSS)	A set of stations controlled by a single coordination function.
Coordination function	The logical function that determines when a station operating within a BSS is permitted to transmit and may be able to receive PDUs.
Distribution system (DS)	A system used to interconnect a set of BSSs and integrated LANs to create an ESS.
Extended service set (ESS)	A set of one or more interconnected BSSs and integrated LANs that appear as a single BSS to the LLC layer at any station associated with one of these BSSs.
MAC protocol data unit (MPDU)	The unit of data exchanged between two peer MAC entities using the services of the physical layer.
MAC service data unit (MSDU)	Information that is delivered as a unit between MAC users.
Station	Any device that contains an IEEE 802.11 conformant MAC and physical layer.

Wi-Fi Alliance

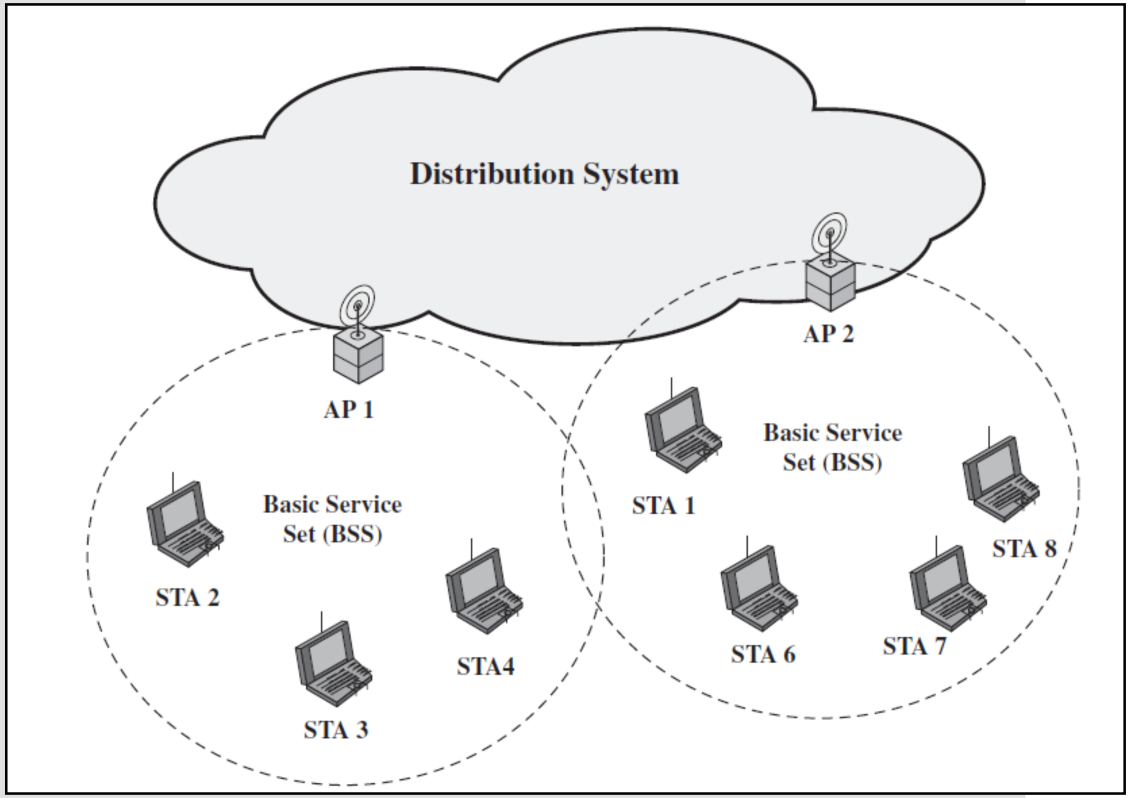
- **802.11b first broadly accepted standard**
- **Wireless Ethernet Compatibility Alliance (WECA) industry consortium formed 1999**
  - to assist interoperability of products
  - renamed Wi-Fi (Wireless Fidelity) Alliance
  - created a test suite to certify interoperability
  - initially for 802.11b, later extended to 802.11g
  - concerned with a range of WLANs markets, including enterprise, home, and hot spots

IEEE 802.11 Protocol Architecture (stack)



Network Components & Architecture

- **Basic Service Set (BSS)**
  - Smallest WLAN block
- **Distribution System (DS)**
  - Connects BSS blocks
- **Access Points (AP)**
  - Functions as a bridge or relay point
- **Extended Service Set (ESS)**
  - Two or more BSS interconnected by a DS



MONASH University
Information Technology

IEEE 802.11 Services

- **WLAN needs to provide 9 services <u>to achieve functional wired equivalence</u>**
  - Provider
    - Either a DS or Station
  - Used to Support
    - Security or Delivery

Service	Provider	Used to support
Association	Distribution system	MSDU delivery
Authentication	Station	LAN access and security
Deauthentication	Station	LAN access and security
Disassociation	Distribution system	MSDU delivery
Distribution	Distribution system	MSDU delivery
Integration	Distribution system	MSDU delivery
MSDU delivery	Station	MSDU delivery
Privacy	Station	LAN access and security
Reassociation	Distribution system	MSDU delivery

802.11 Wireless LAN Security

- **Wireless traffic can be monitored by any radio in range, not physically connected**
- **Original 802.11 spec had security features**
  - Wired Equivalent Privacy (WEP) algorithm
  - but found this contained major weaknesses
- **802.11i task group developed capabilities to address WLAN security issues**
  - Wi-Fi Alliance Wi-Fi Protected Access (WPA)
  - final 802.11i Robust Security Network (RSN)

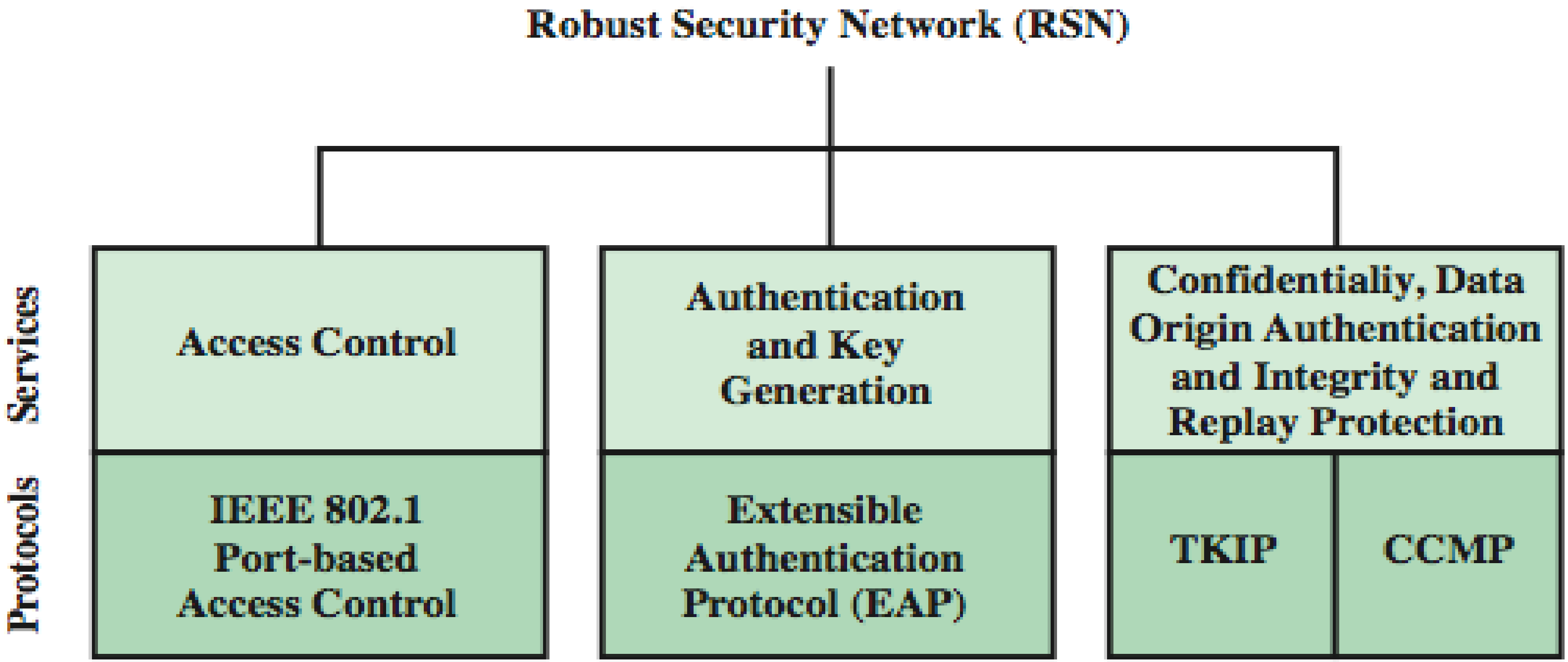
WEP Problems

- **No centralized key management**
  - Manual key distribution → Difficult to change keys
- **Single set of Keys shared by all → Frequent changes necessary**
- **No mutual authentication**
- **IV value is too short. Not protected from reuse.**
- **Weak integrity check.**
- **Directly uses master key**
- **No protection against replay**

**Bottom line:
Weakness: Key Management and Key Size**

MONASH University
Information Technology

802.11i RSN Services and Protocols

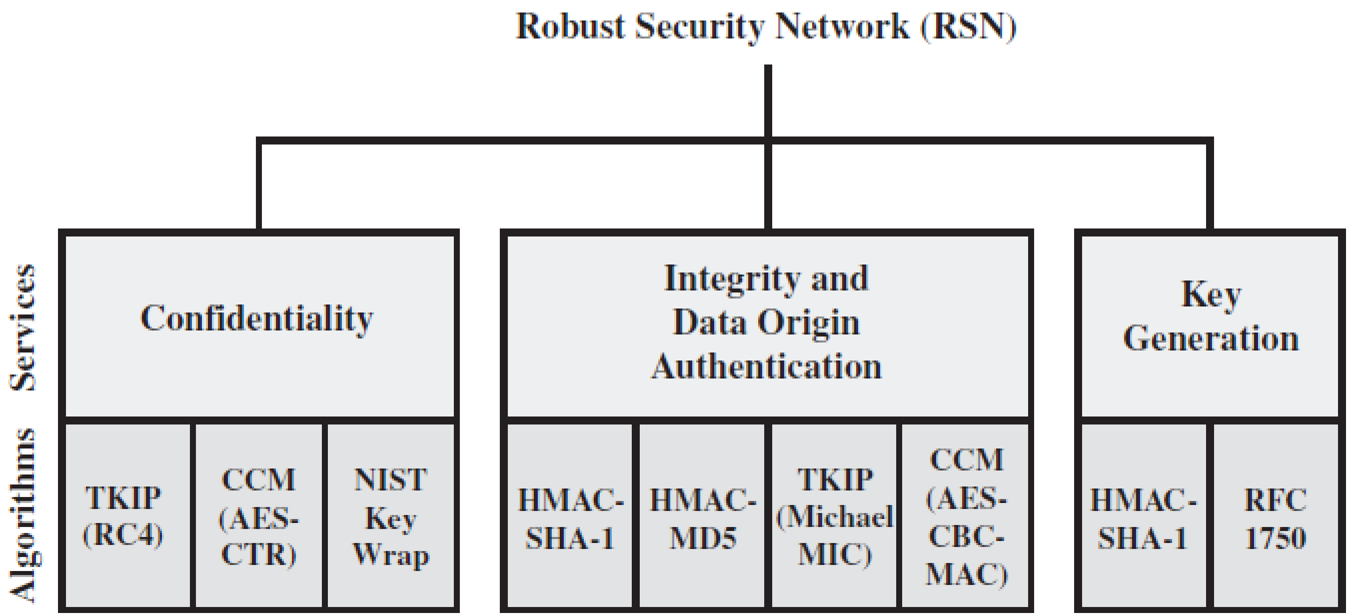


MONASH University
Information Technology

802.11i RSN Services and Protocols

- **Authentication**
  - used to define an exchange between a user and an AS that provides mutual authentication and generates temporary keys to be used between the client and the AP over the wireless link.
- **Access Control**
  - enforces the use of the authentication function, routes the messages properly, and facilitates key exchange.
- **Privacy with message integrity**
  - MAC-level encryption, message integrity code

802.11i RSN Cryptographic Algorithms

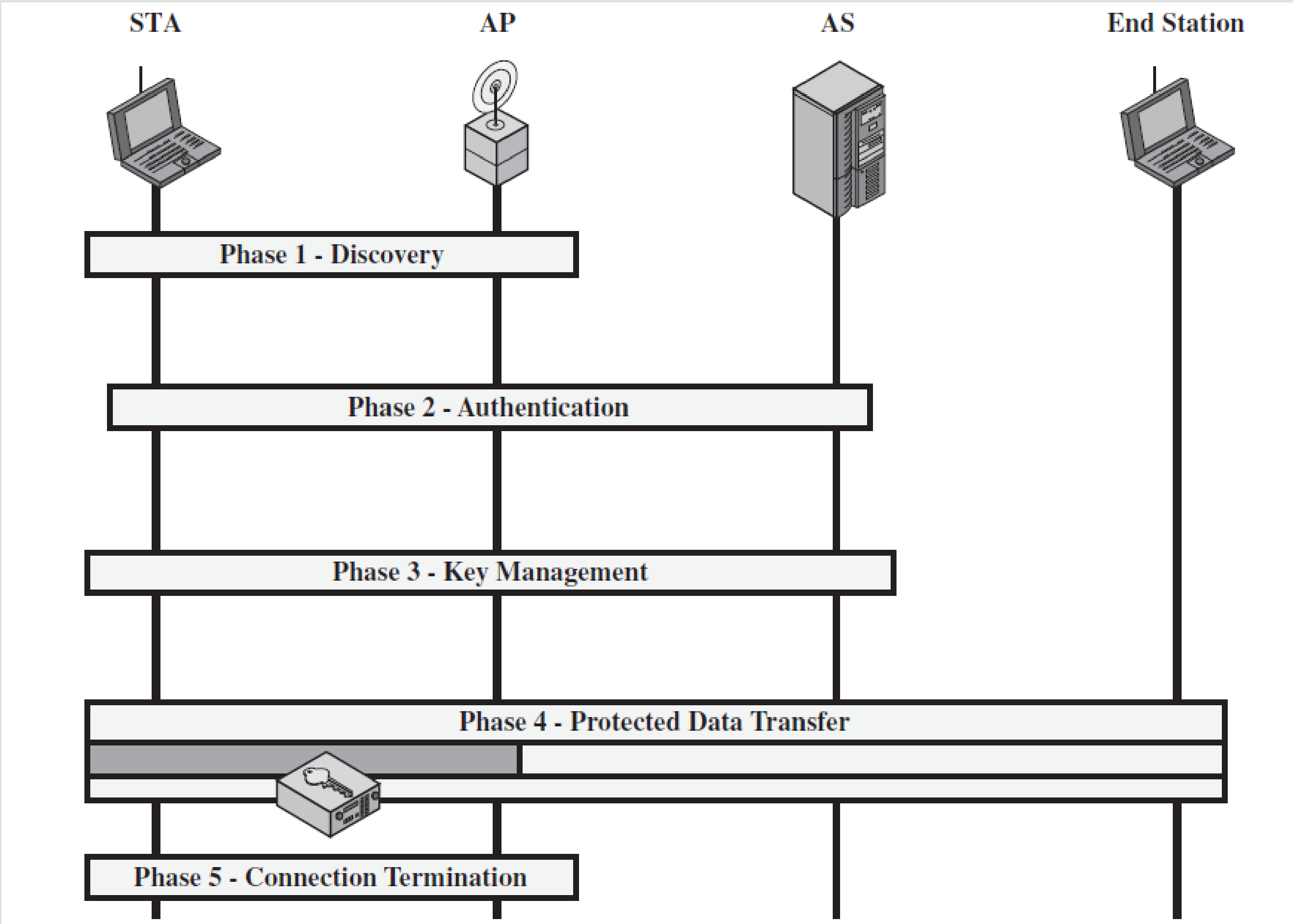


(b) Cryptographic algorithms

CBC-MAC = Cipher Block Block Chaining Message Authentication Code (MAC)
CCM = Counter Mode with Cipher Block Chaining Message Authentication Code
CCMP = Counter Mode with Cipher Block Chaining MAC Protocol
TKIP = Temporal Key Integrity Protocol

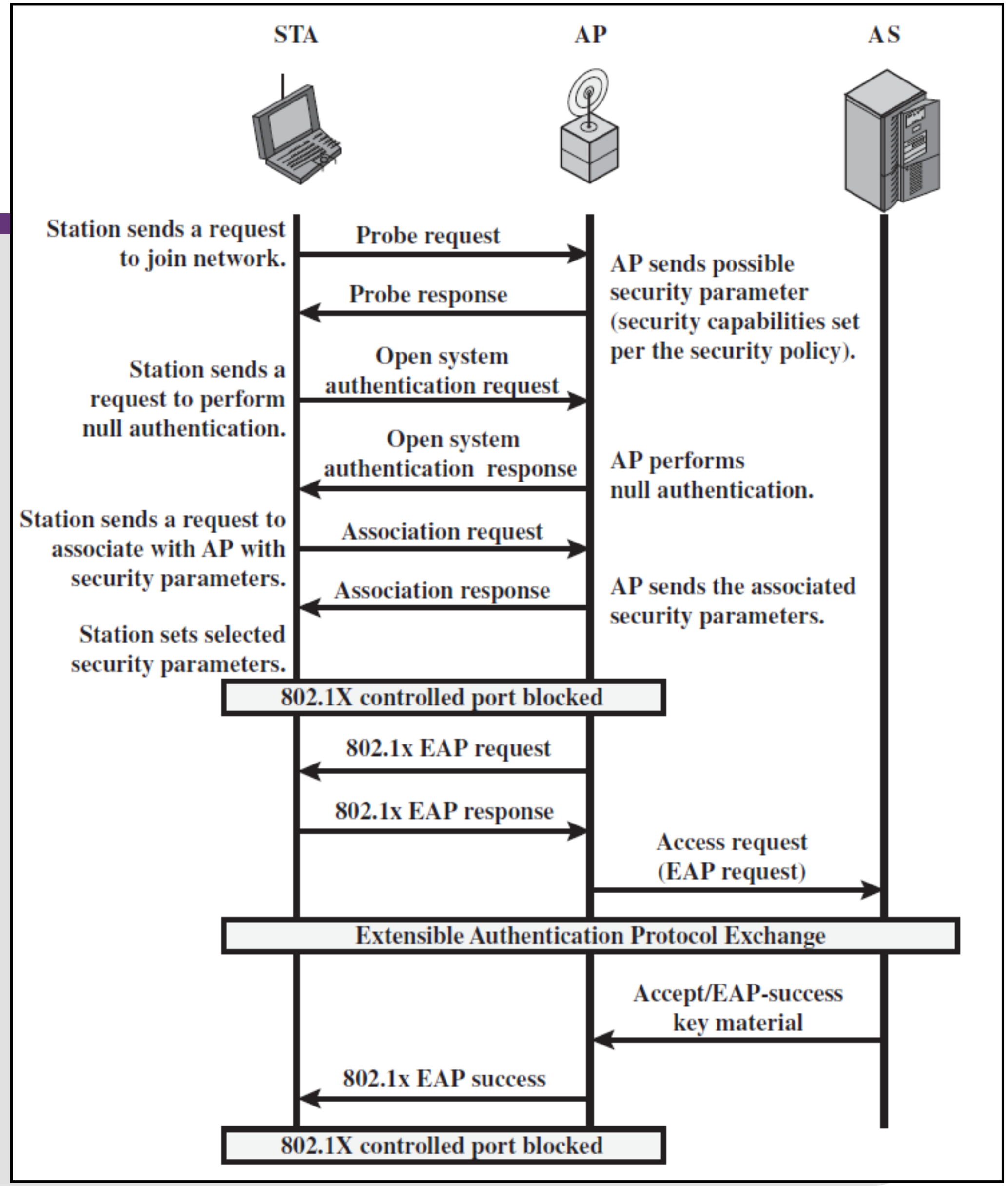
Figure 6.4 Elements of IEEE 802.11i

802.11i Phases of Operation

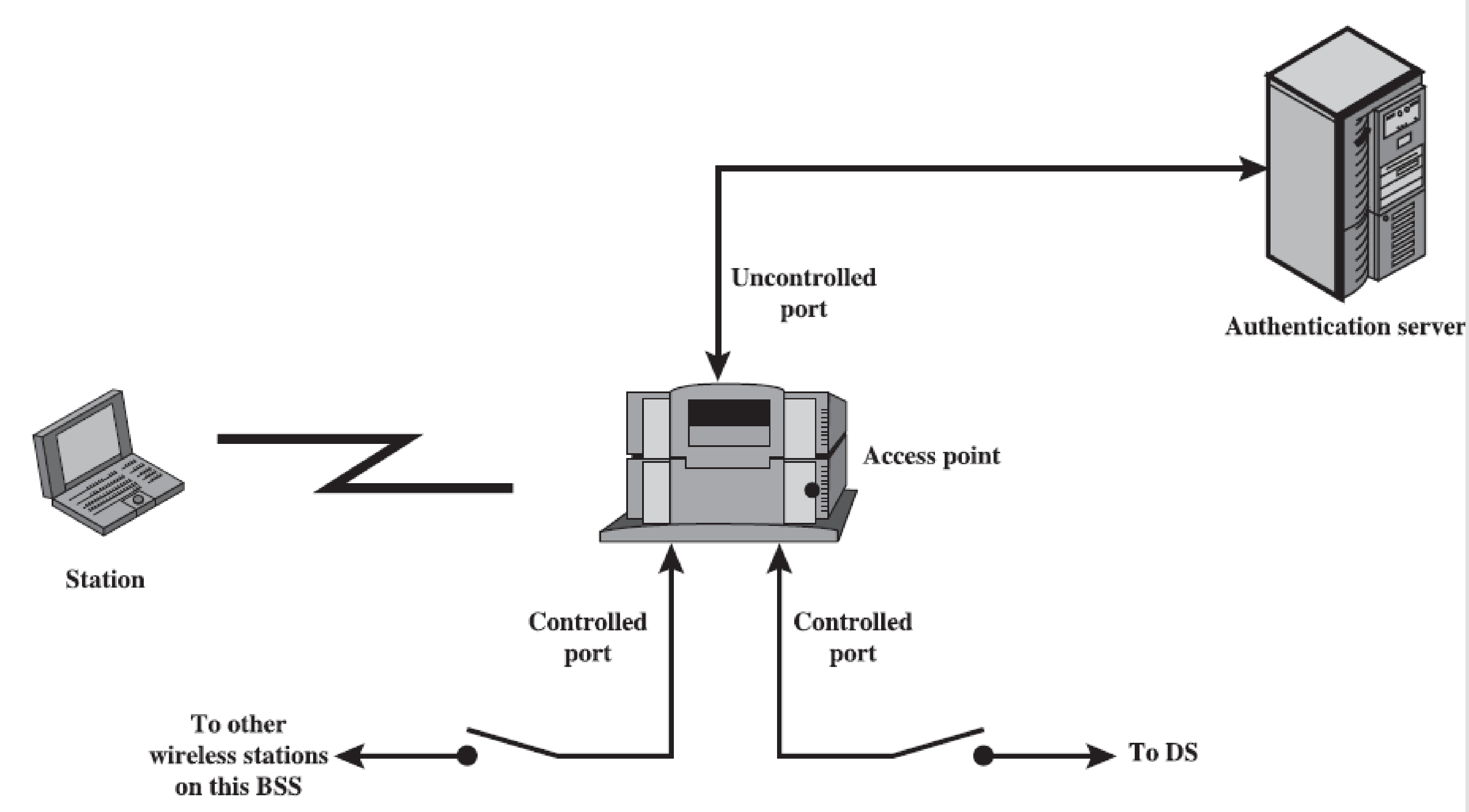


802.11i
Phases of Operation:

1. Capability Discovery,
2. Authentication, and
3. Association Phases

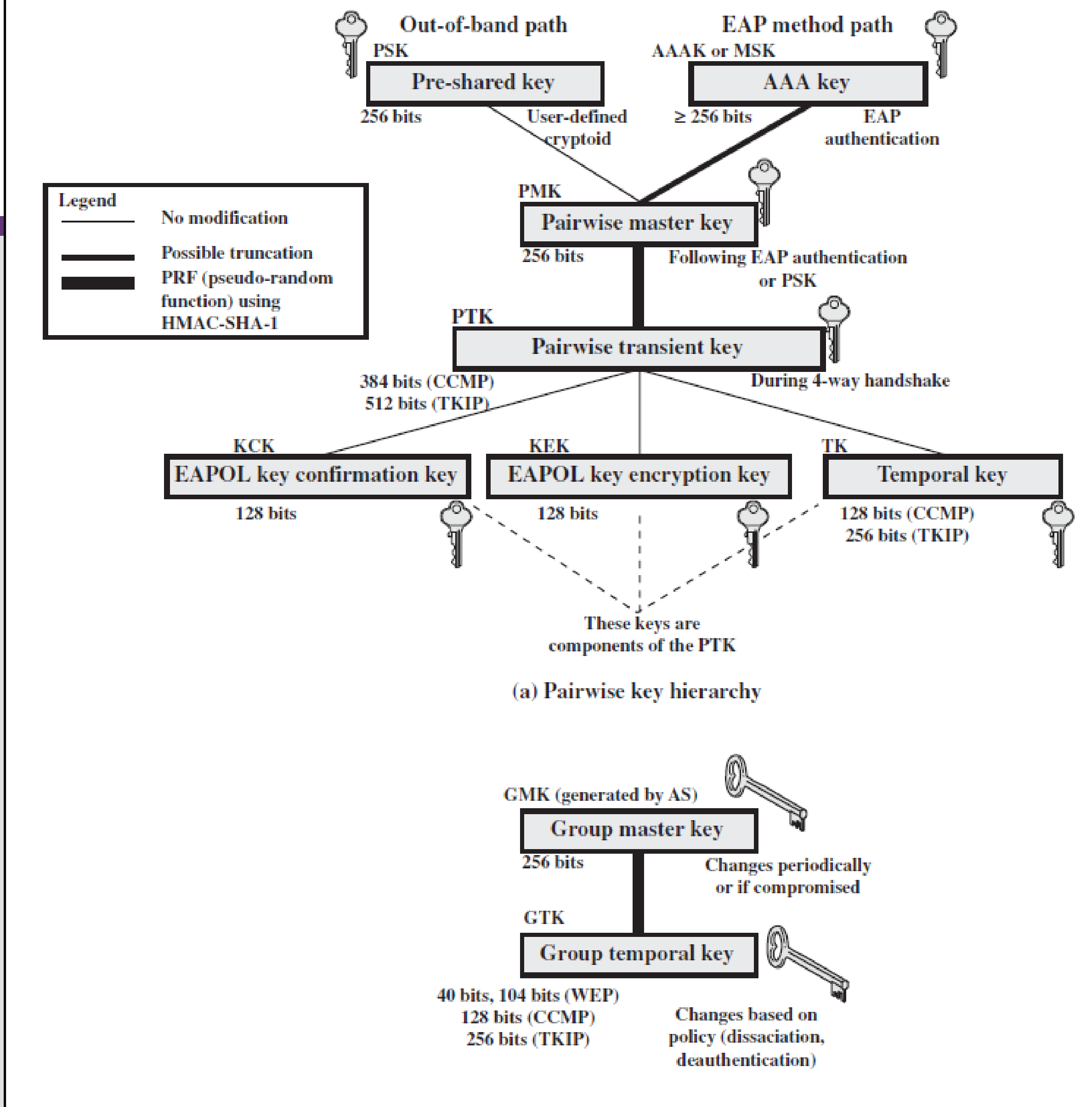


IEEE 802.1X Access Control Approach



802.11i Key Management Phase

- **A number of keys are generated and distributed to the Stations (STA)**
- **Two types of key hierarchies**
  - pairwise
    - > between STA & AP
  - group
    - > Multi cast comms

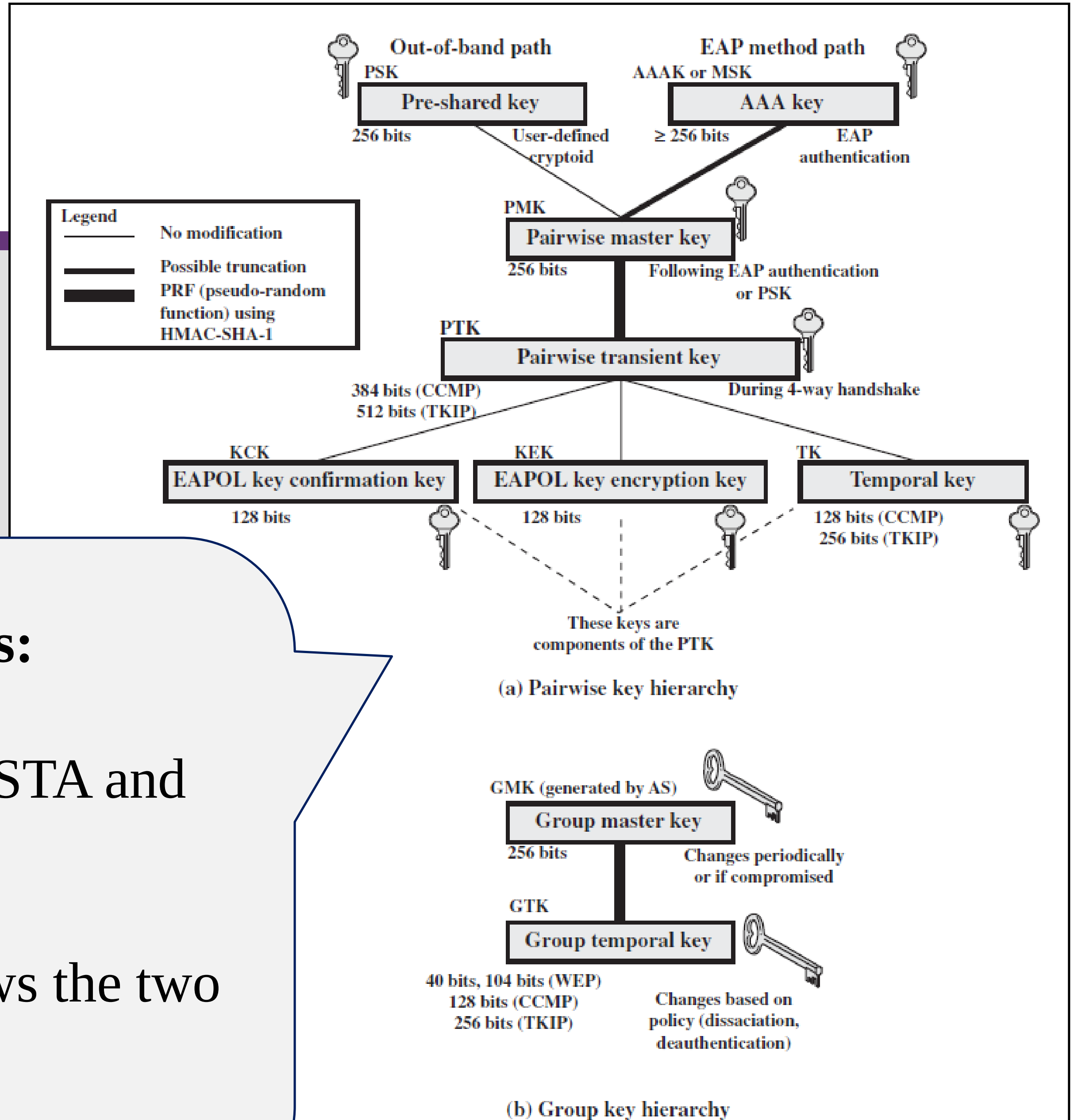


(a) Pairwise key hierarchy

(b) Group key hierarchy

MONASH University
Information Technology

802.11i Key Management Phase

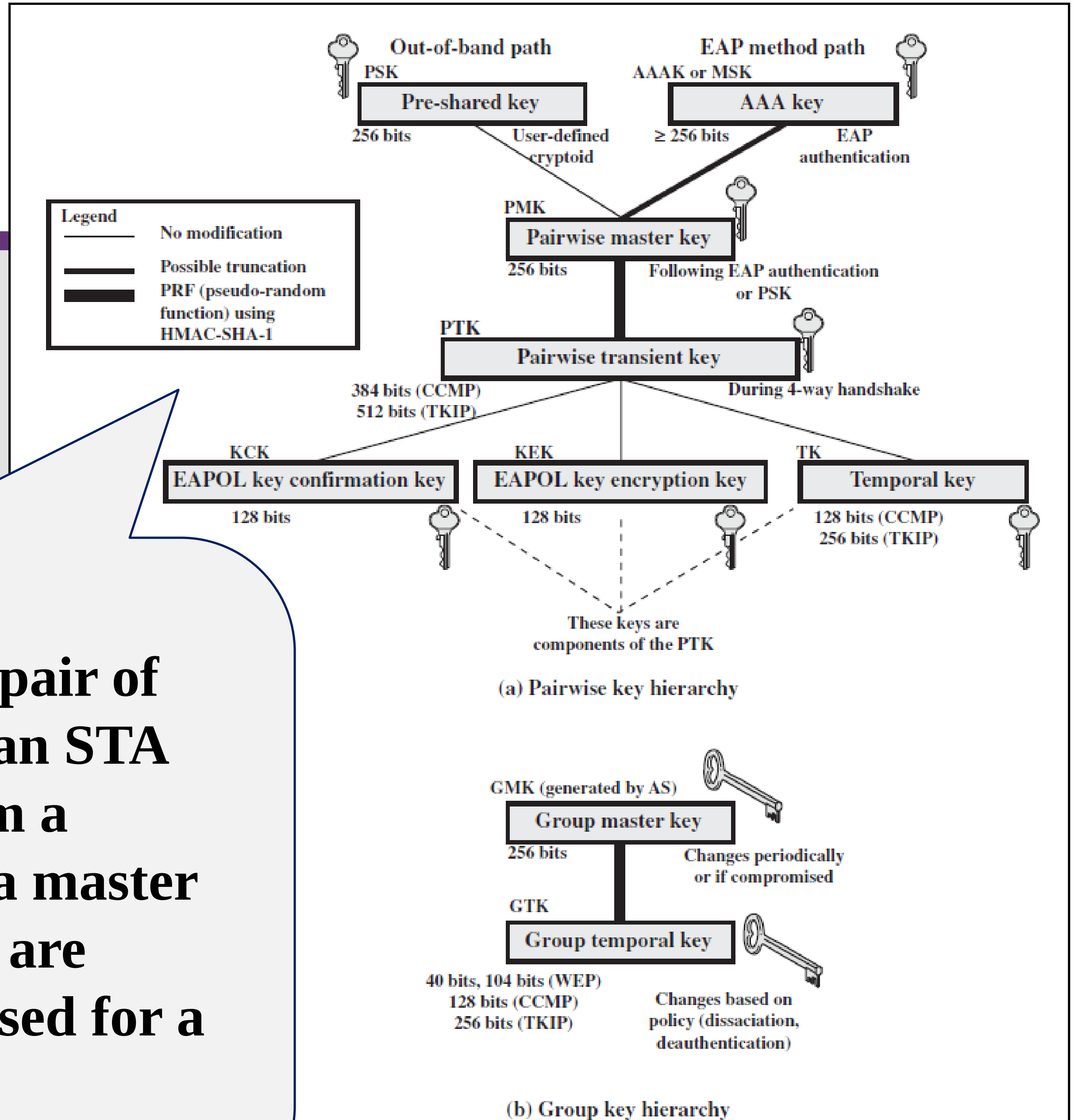


(a) Pairwise key hierarchy

(b) Group key hierarchy

There are two types of keys:
<u>pairwise keys</u>, used for communication between an STA and an AP; and
<u>group keys</u>, for multicast communication. Figure shows the two key hierarchies.

802.11i Key Management Phase



(a) Pairwise key hierarchy

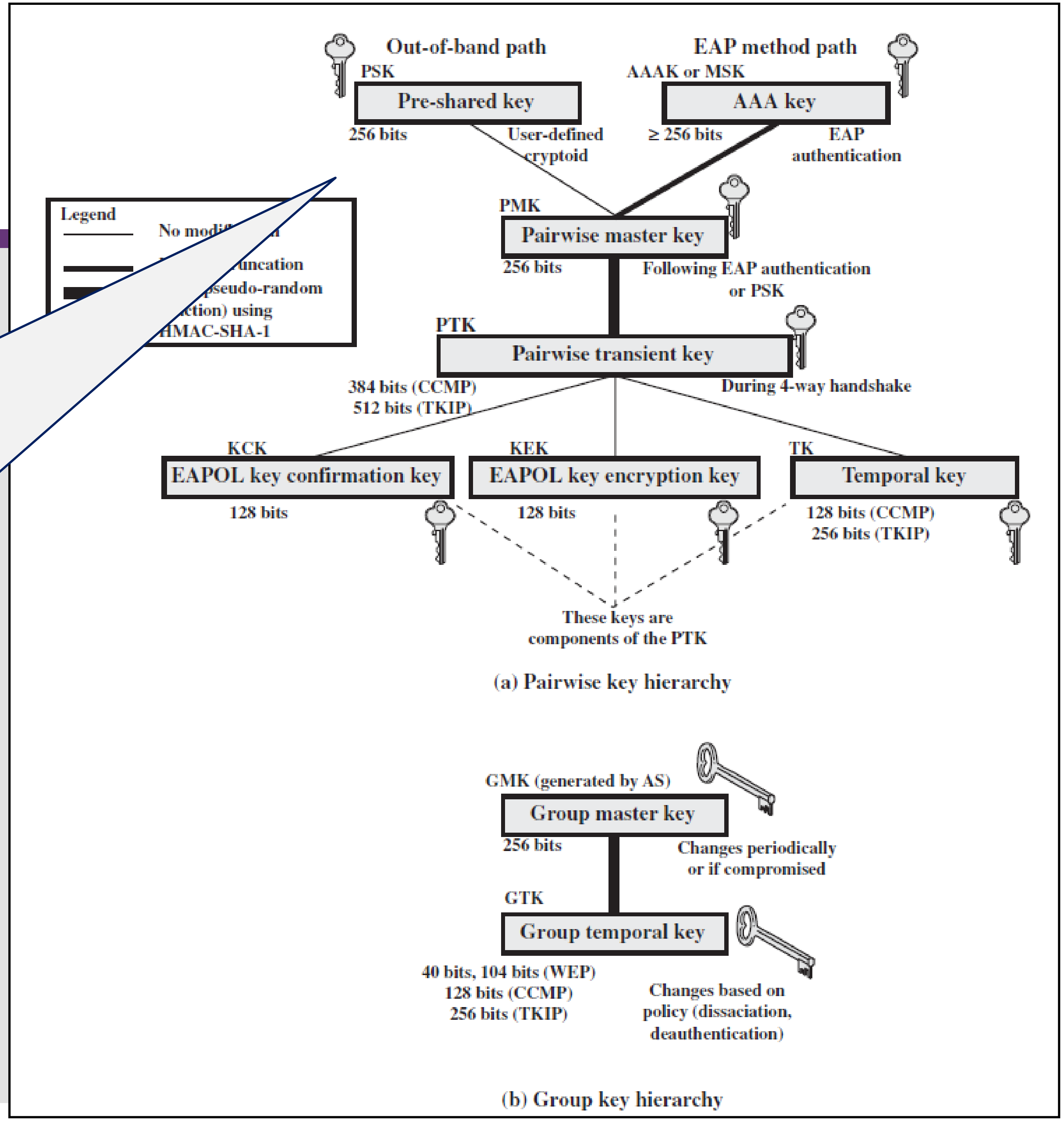
(b) Group key hierarchy

Pairwise keys are used for communication between a pair of devices, typically between an STA and an AP. These keys form a hierarchy, beginning with a master key from which other keys are derived dynamically and used for a limited period of time.

Information Technology

802.11i Key Management Phase

A pre-shared key (PSK) is a secret key shared by the AP and a STA, and installed in some fashion outside the scope of IEEE 802.11i.



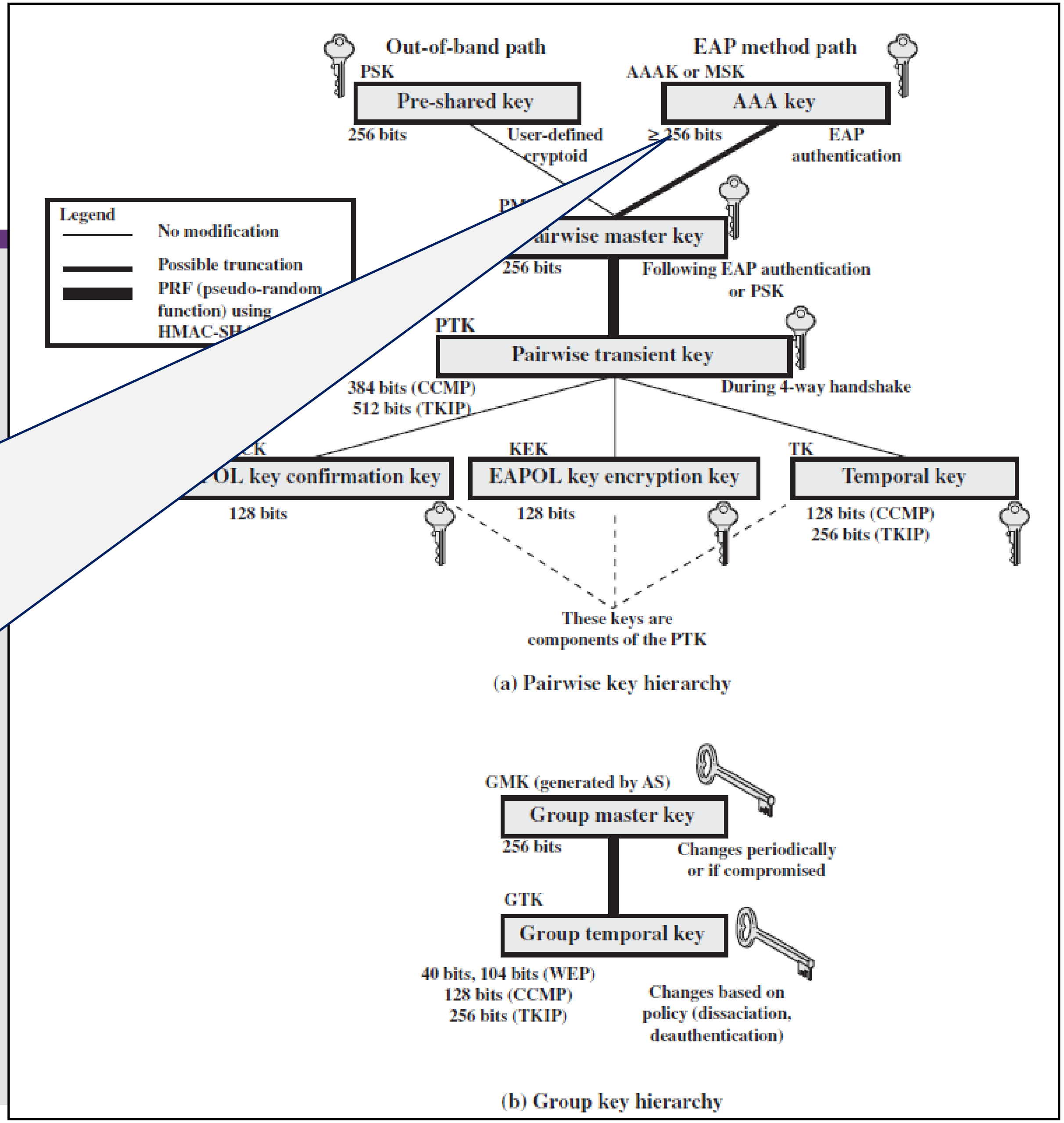
(a) Pairwise key hierarchy

(b) Group key hierarchy

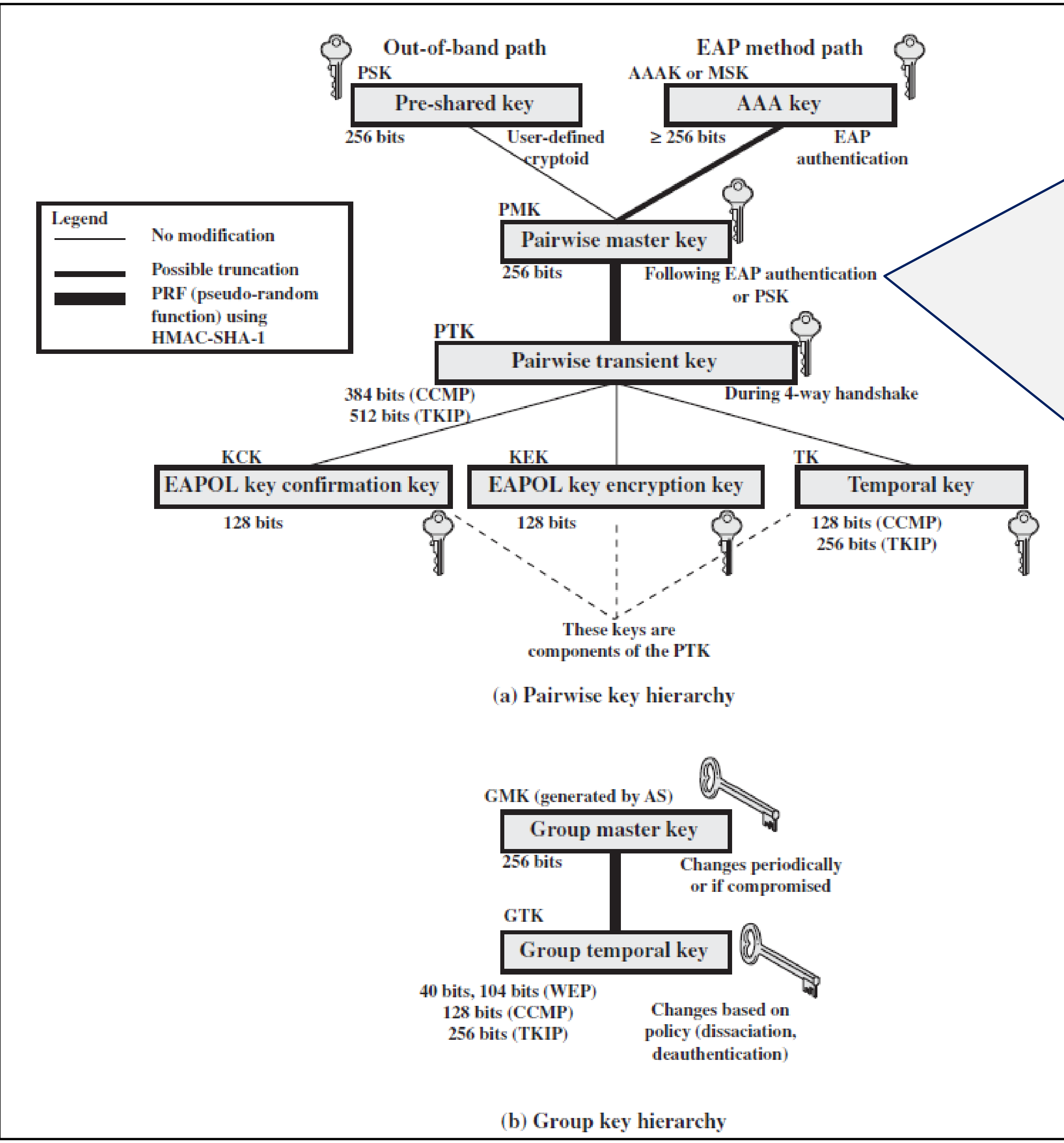
MONASH University
Information Technology

802.11i Key Management Phase

The other alternative is the master session key (MSK), also known as the AAAK, which is generated using the IEEE 802.1X protocol during the authentication phase, as stated previously.



MONASH University
Information Technology



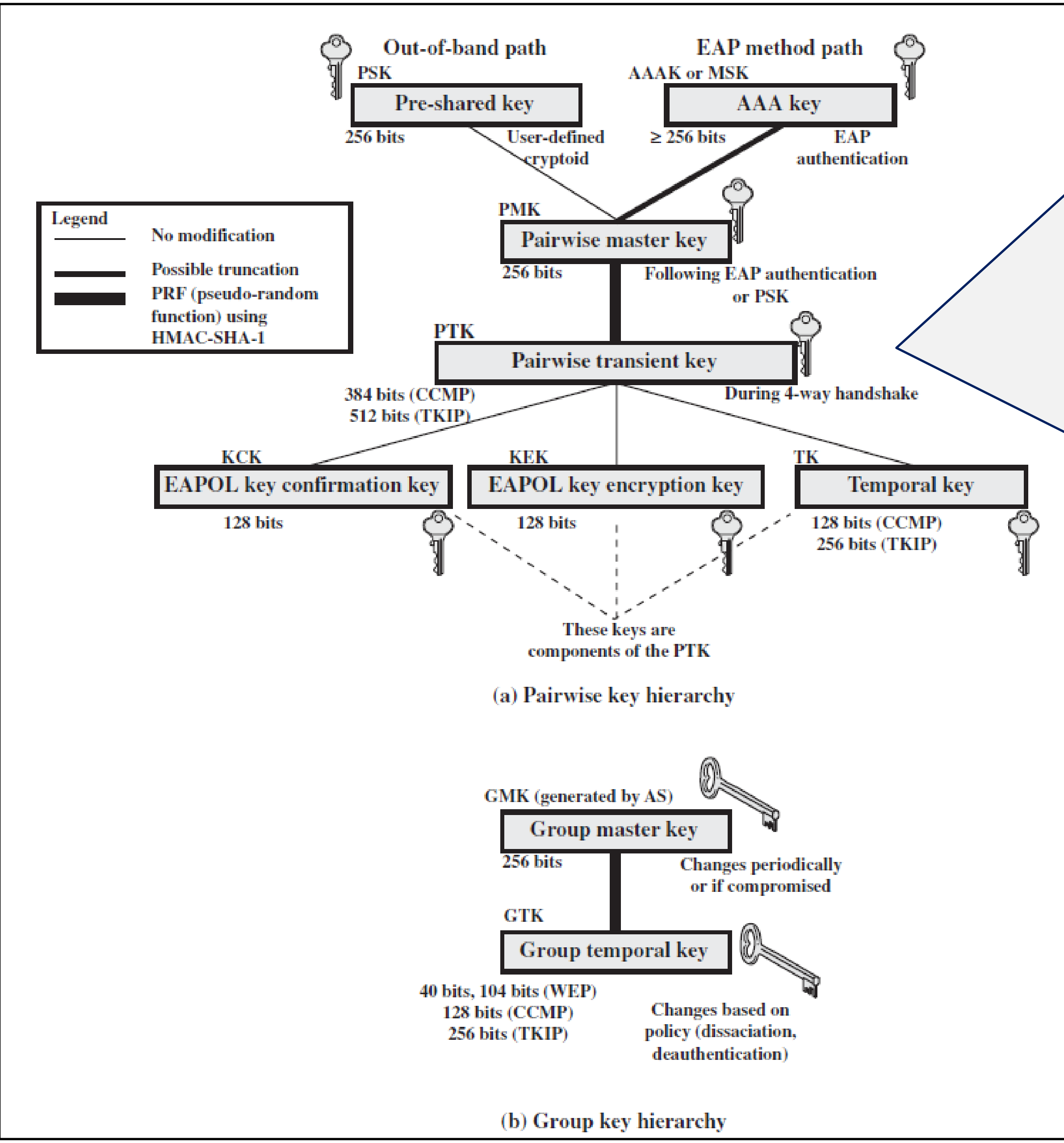
(a) Pairwise key hierarchy

(b) Group key hierarchy

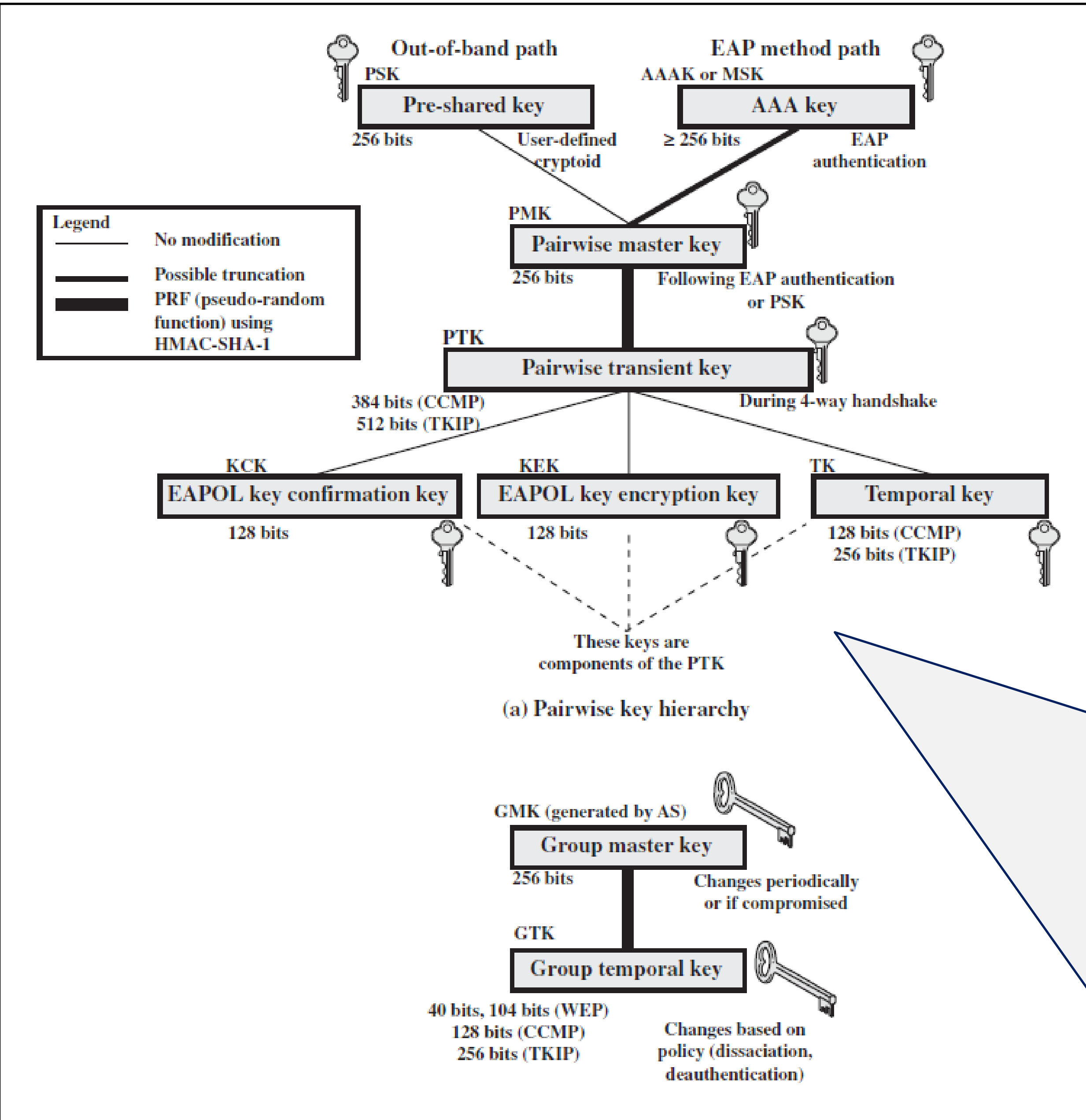
The pairwise master key (PMK) is derived from the master key .
As follows:

1. **If a PSK is used, then the PSK is used as the PMK;**
2. **if a MSK is used, then the PMK is derived from the MSK by truncation (if necessary).**

By the end of the authentication phase (on EAP Success message), both the AP and the STA have a copy of their shared PMK.



The PMK is used to generate the pairwise transient key (PTK), which in fact consists of three keys to be used for communication between an STA and AP after they have mutually authenticated.
To derive the PTK, the PMK, the MAC addresses of the STA and AP, and nonces generated when needed are all input to the HMAC-SHA-1 function.

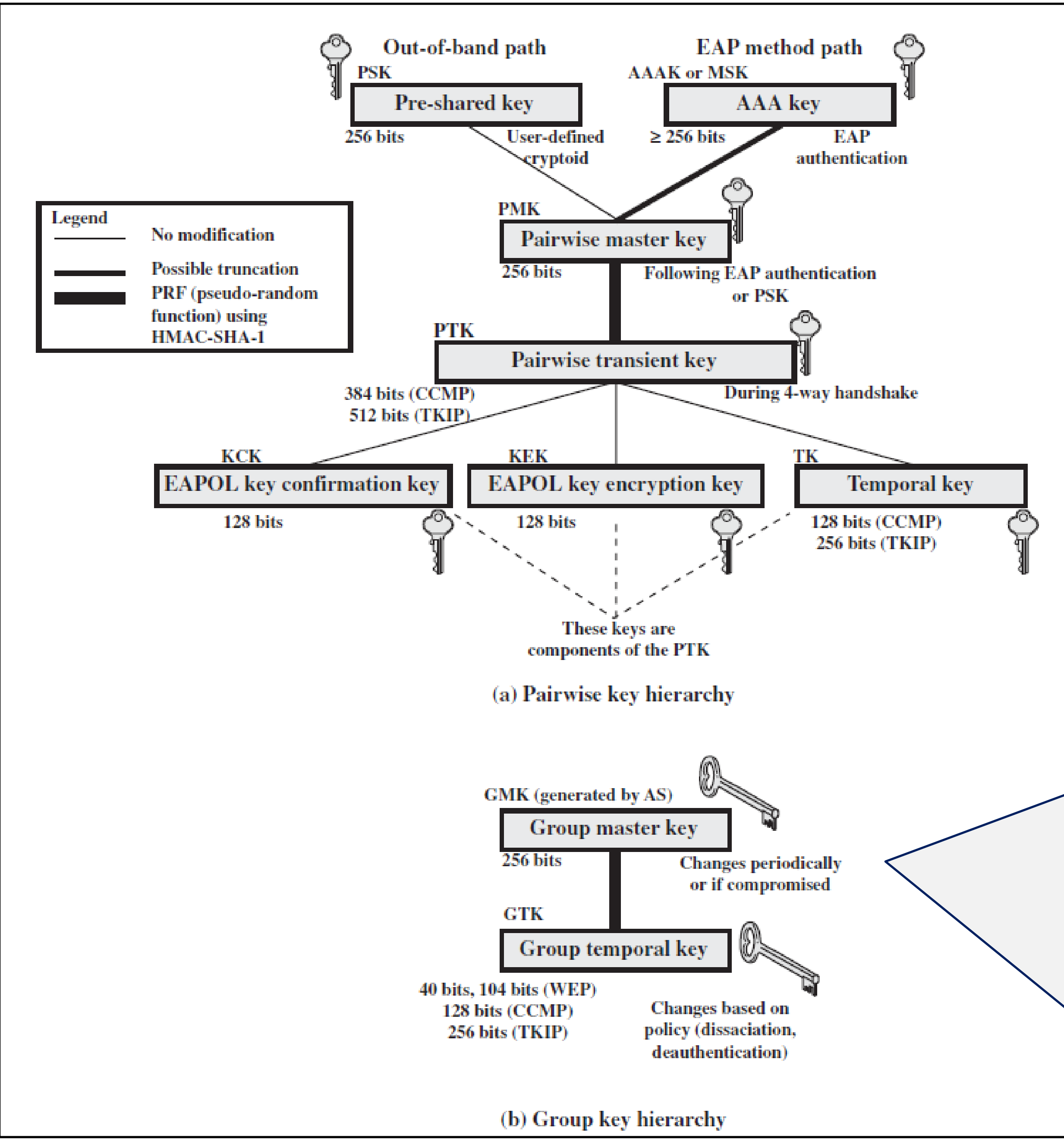


(a) Pairwise key hierarchy

(b) Group key hierarchy

The three parts of the PTK are as follows.

1. **EAP Over LAN (EAPOL) Key Confirmation Key (EAPOL-KCK):** Supports the integrity and data origin authenticity of STA-to-AP control frames . It also performs an access control function.
2. **EAPOL Key Encryption Key (EAPOL-KEK):** Protects the confidentiality of keys and other control frames.
3. **Temporal Key (TK):** Provides the actual protection for user traffic.



(a) Pairwise key hierarchy

(b) Group key hierarchy

GROUP KEYS Group keys are used for **multicast** communication in which one STA sends MPDU's to multiple STAs.

Group Master Key (GMK)
The GMK is a key-generating key used with other inputs to derive

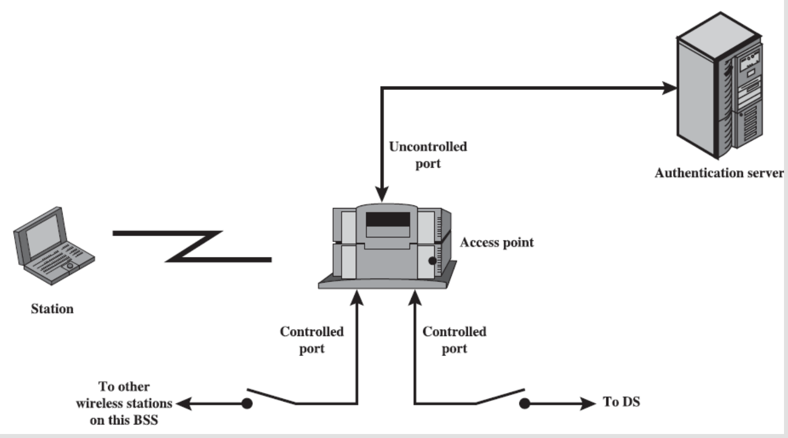
the **Group Temporal Key (GTK)**. The GTK is distributed securely using the pairwise keys that are already established. The GTK is changed every time a device leaves the network.

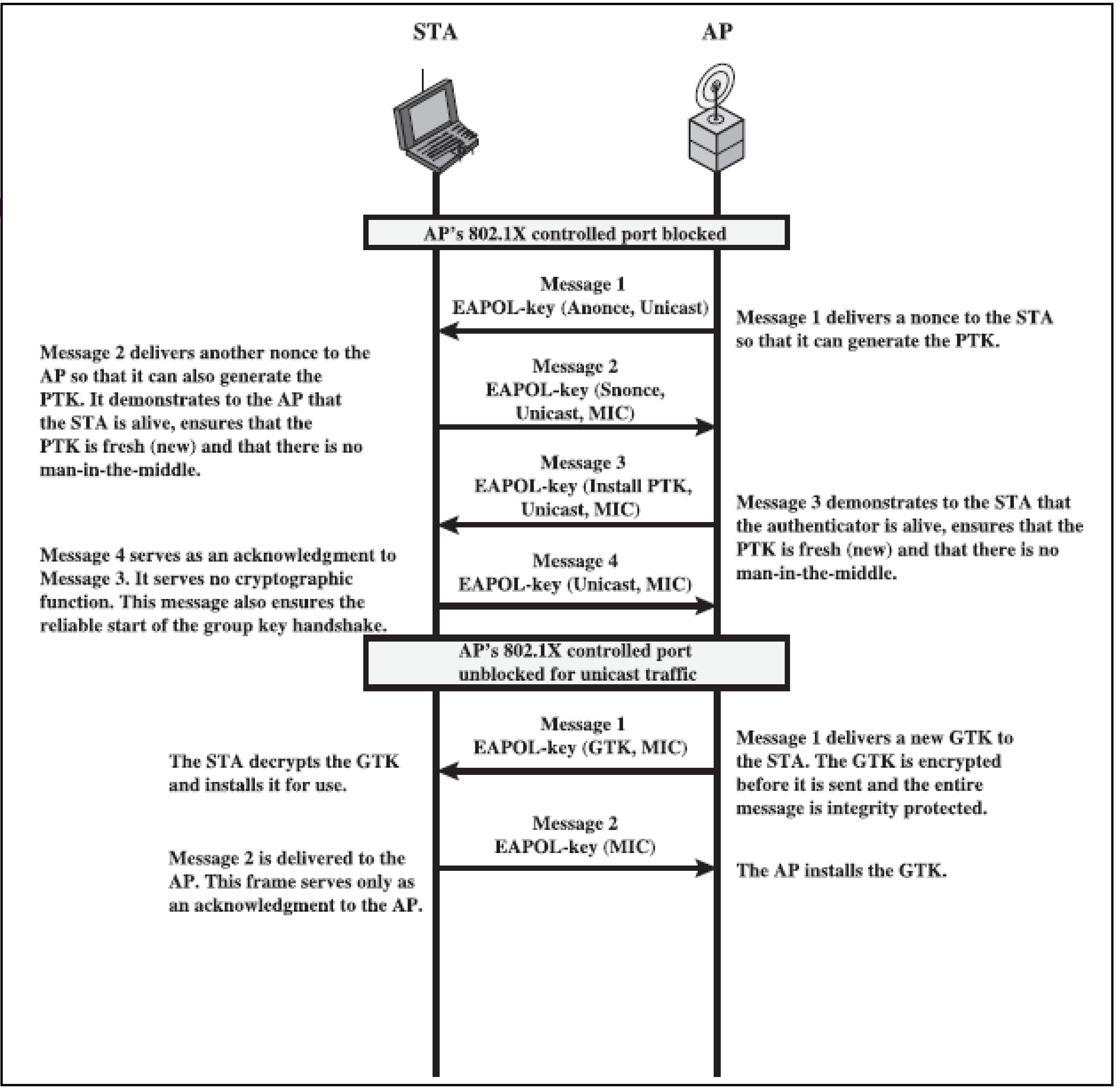
IEEE 802.11i keys for Data Confidentiality and Integrity Protocols

Abbrev-iation	Name	Description / Purpose	Size (bits)	Type
AAA Key	Authentication, Accounting, and Authorization Key	Used to derive the PMK. Used with the IEEE 802.1X authentication and key management approach. Same as MMSK.	≥ 256	Key generation key, root key
PSK	Pre-shared Key	Becomes the PMK in pre-shared key environments.	256	Key generation key, root key
PMK	Pairwise Master Key	Used with other inputs to derive the PTK.	256	Key generation key
GMK	Group Master Key	Used with other inputs to derive the GTK.	128	Key generation key
PTK	Pair-wise Transient Key	Derived from the PMK. Comprises the EAPOL-KCK, EAPOL-KEK, and TK and (for TKIP) the MIC key.	512 (TKIP) 384 (CCMP)	Composite key
TK	Temporal Key	Used with TKIP or CCMP to provide confidentiality and integrity protection for unicast user traffic.	256 (TKIP) 128 (CCMP)	Traffic key
GTK	Group Temporal Key	Derived from the GMK. Used to provide confidentiality and integrity protection for multicast/broadcast user traffic.	256 (TKIP) 128 (CCMP) 40, 104 (WEP)	Traffic key
MIC Key	Message Integrity Code Key	Used by TKIP's Michael MIC to provide integrity protection of messages.	64	Message integrity key
EAPOL-KCK	EAPOL-Key Confirmation Key	Used to provide integrity protection for key material distributed during the 4-Way Handshake.	128	Message integrity key
EAPOL-KEK	EAPOL-Key Encryption Key	Used to ensure the confidentiality of the GTK and other key material in the 4-Way Handshake.	128	Traffic key / key encryption key
WEP Key	Wired Equivalent Privacy Key	Used with WEP.	40, 104	Traffic key

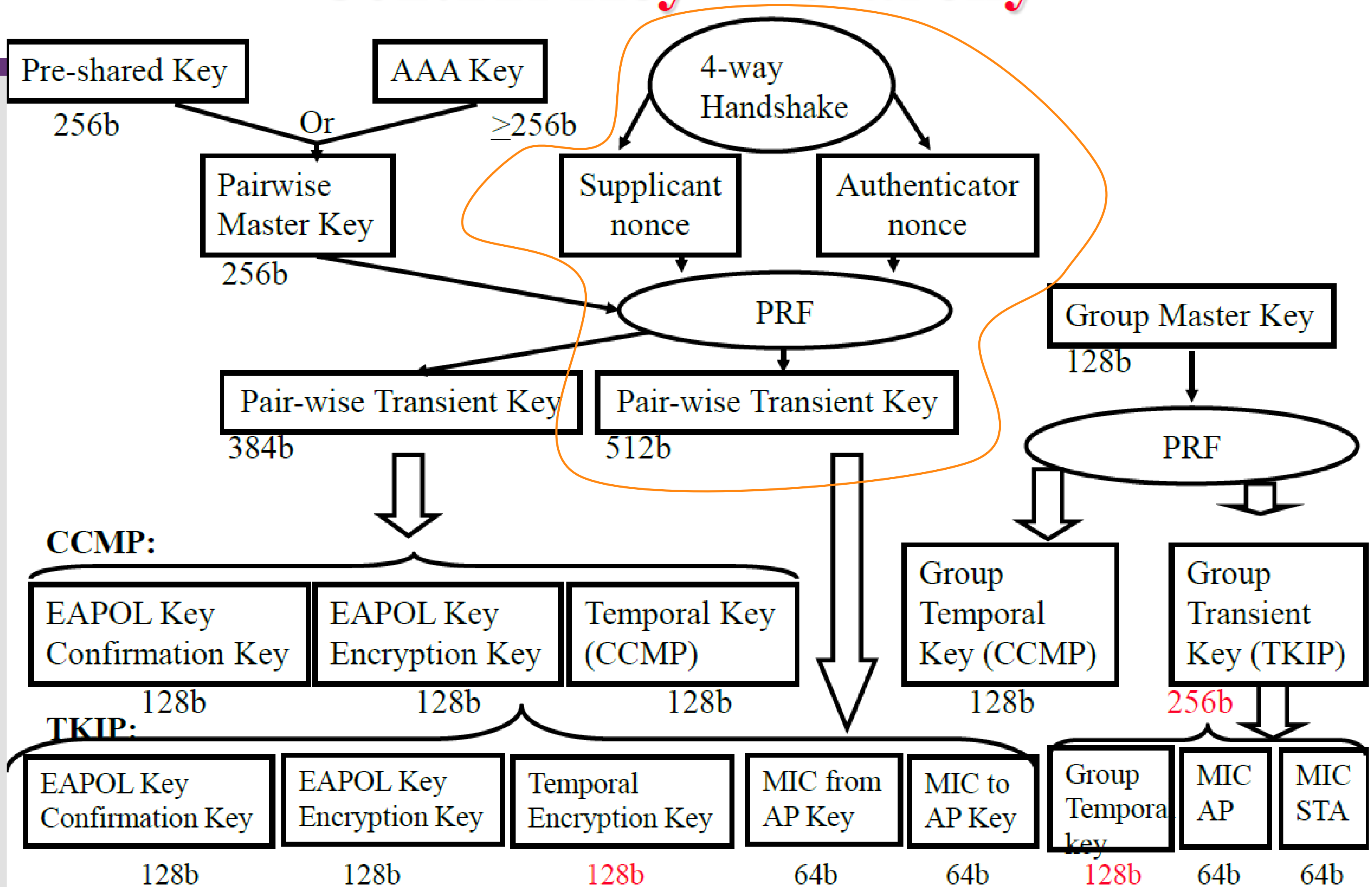
802.11i Key Management Phase

- IEEE 802.11i Phases of Operation: **Four-Way Handshake** and **Group Key Handshake**





802.11i Key Hierarchy



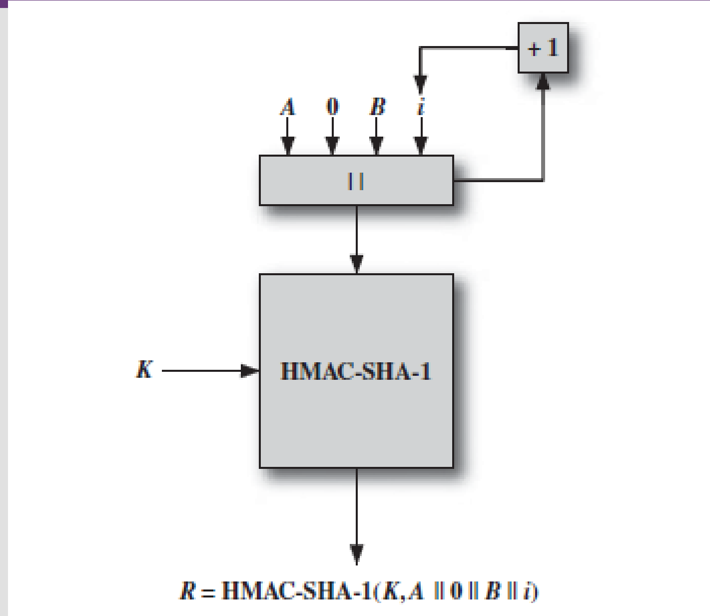
MONASH University
Information Technology

802.11i Protected Data Transfer Phase

- **have two schemes for protecting data**
- **Temporal Key Integrity Protocol (TKIP)**
  - s/w changes only to older WEP
  - adds 64-bit Michael message integrity code (MIC)
  - encrypts MPDU plus MIC value using RC4
- **Counter Mode-CBC MAC Protocol (CCMP)**
  - uses the cipher block chaining (CBC) message authentication code (CBC-MAC) for integrity
  - uses the CTR block cipher mode of operation with AES for encryption

IEEE 802.11i Pseudorandom Function

- **IEEE 802.11i scheme uses a Pseudo Random Function (PRF) in a number of places**
  - i.e. ***to generate nonce, expand pairwise keys, to generate group temporal keys (GTK)***
- **Based on HMAC-SHA-1**
  - K = Secret key
  - A = a text string specific to the application i.e. nonce, PWK expansion
  - B = some data specific to each case
  - Len – desired number of random bits
  - Output is a 160 bit message digest,
  - ***i*** is incremented counter each loop if more Len bits are required



Example: Pair-wise Temporal Key for CCMP

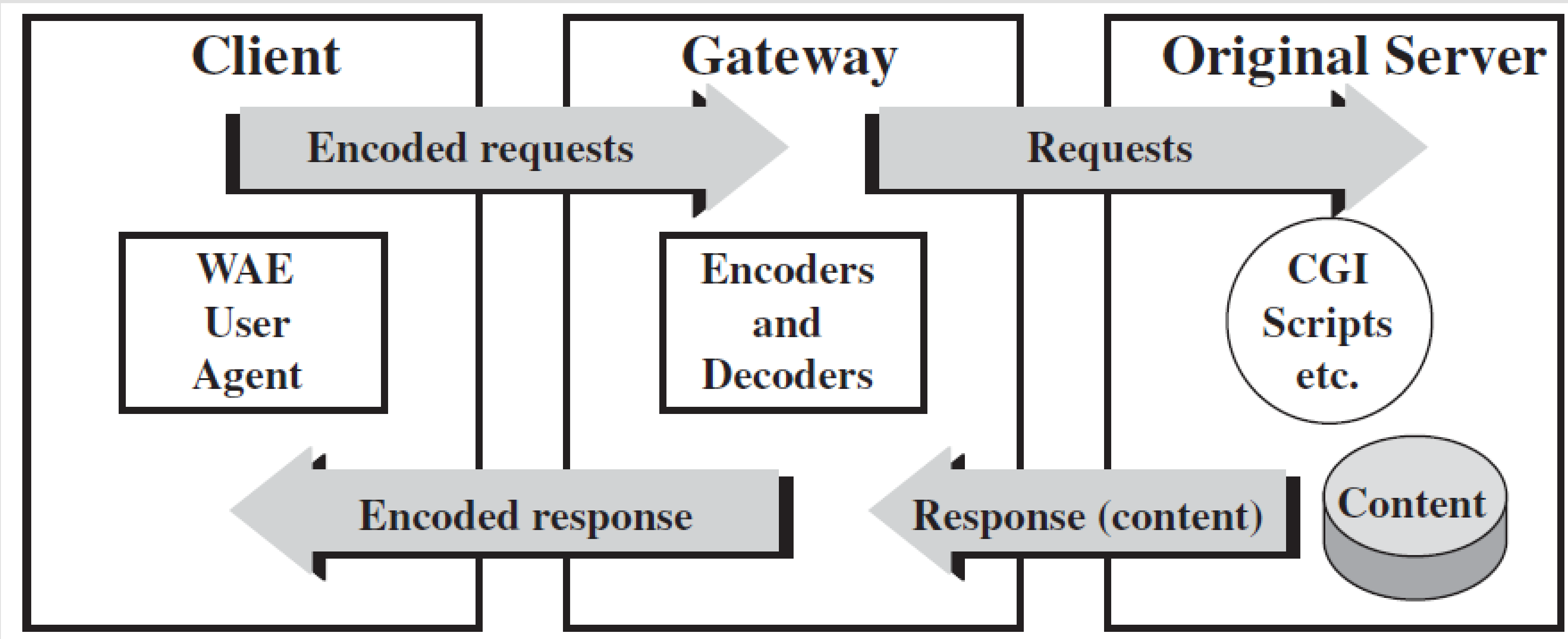
- PTK=PRM{PMK, "Pairwise key expansion", min(AP Addr, STA Addr)||max(AP-Addr, STA-Addr)||min(Anonce, Snonce)|| max(Anonce,Snonce), 384}

MONASH University
Information Technology

Wireless Application Protocol (WAP)

- **A universal, open standard developed to provide mobile wireless users access to telephony and information services**
- **Have significant limitations of devices, networks, displays with wide variations**
- **WAP specification includes:**
  - programming model, markup language, small browser, lightweight communications protocol stack, applications framework

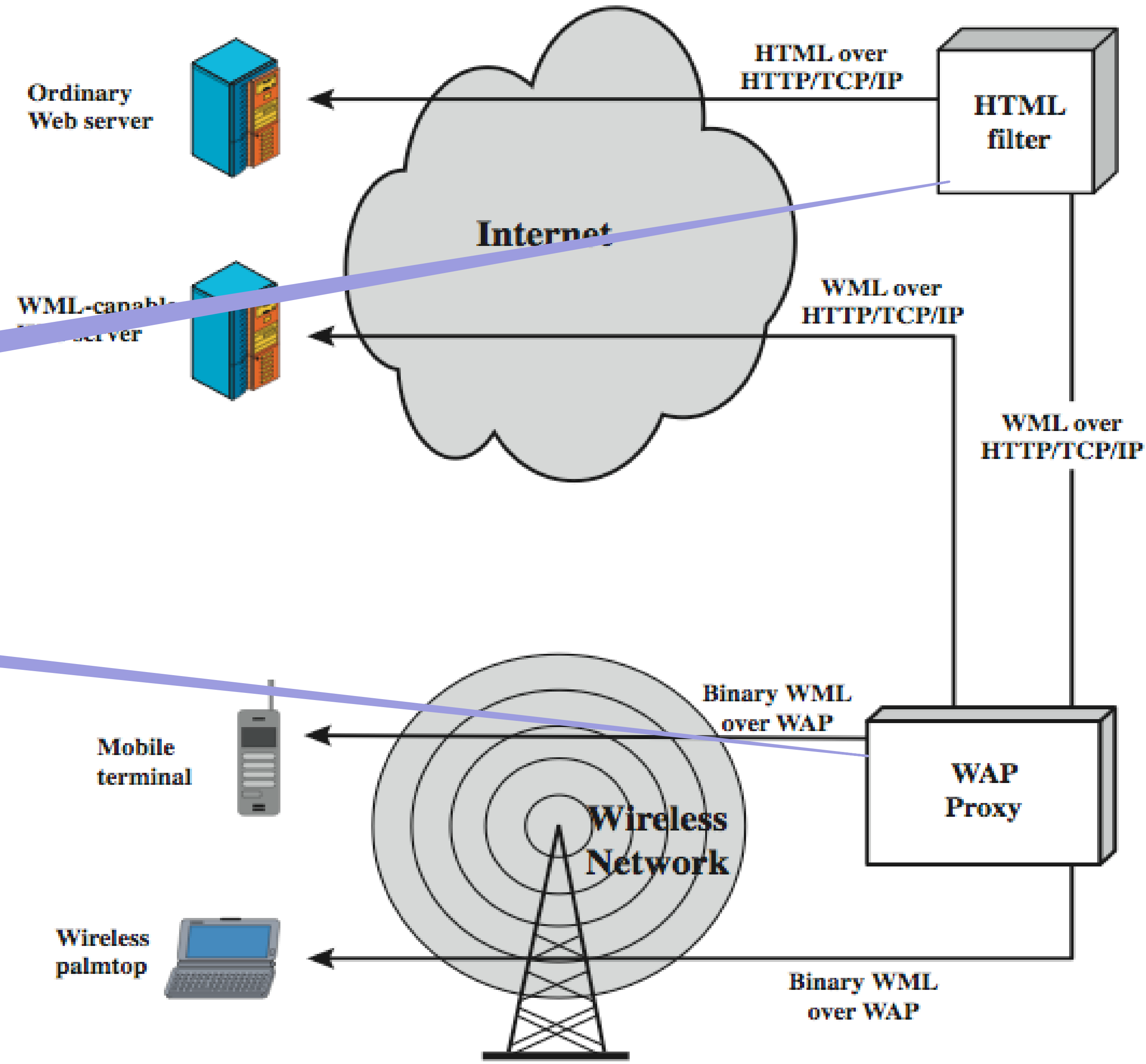
WAP Programming Model



WAP PROXY

WAP Infrastructure

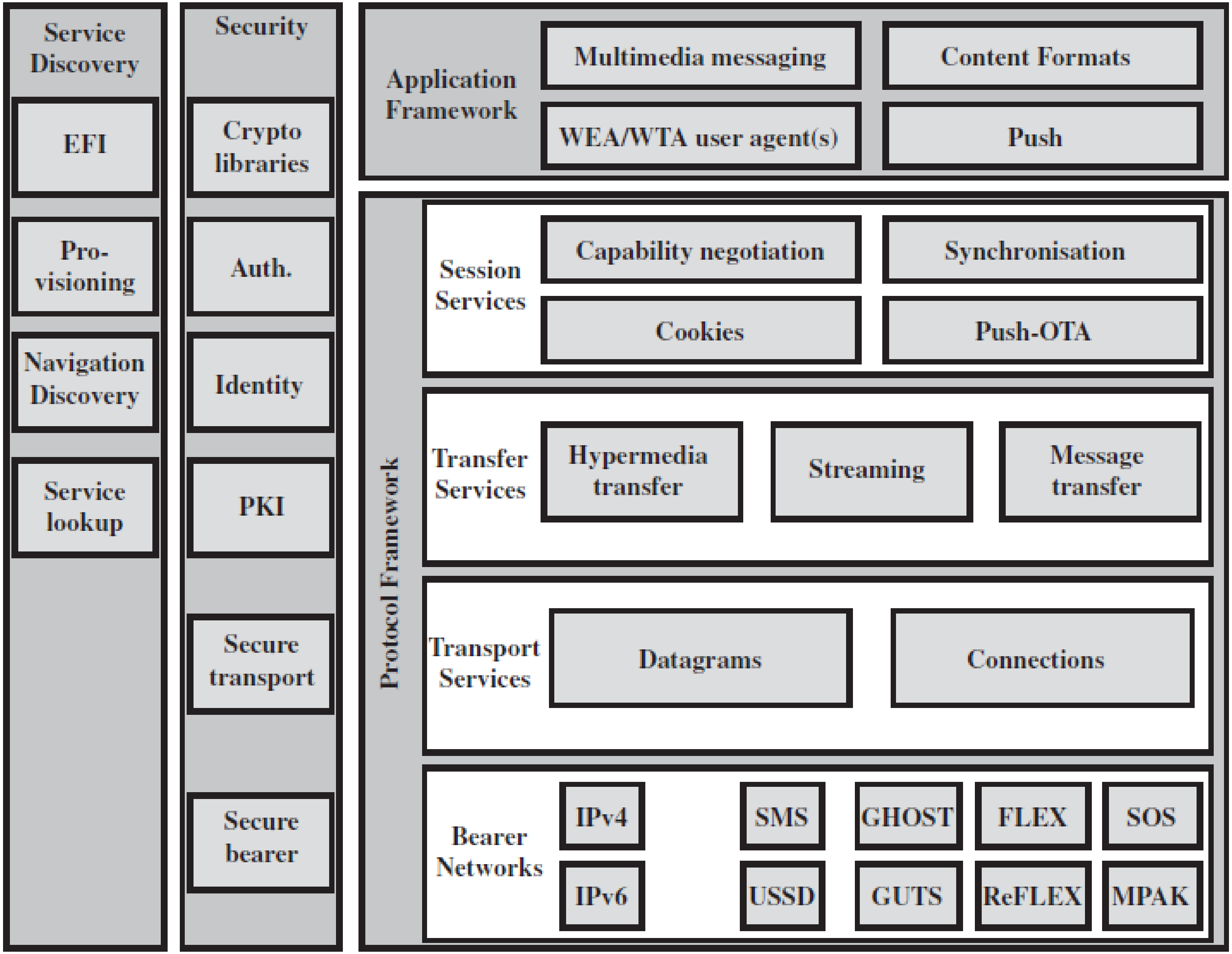
- **The HTML filter** translates the HTML content into WML content. If the filter is separate from the proxy, HTTP/TCP/IP is used to deliver the WML to the proxy.
- The **WAP proxy** converts the WML to a more compact form known as binary WML and delivers it to the mobile user over a wireless network using the WAP protocol stack.



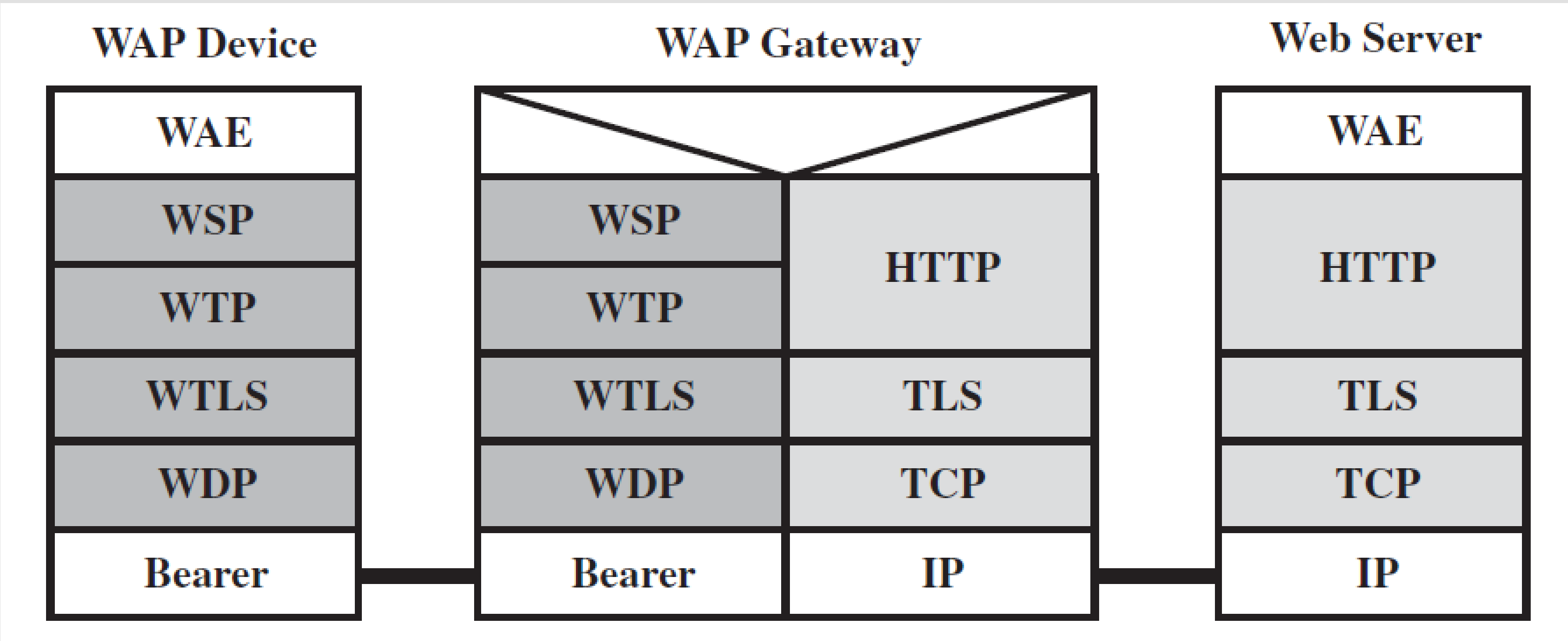
Wireless Markup Language

- **describes content and format for data display on devices with limited bandwidth, screen size, and user input capability**
- **features include:**
  - *text / image formatting and layout commands*
  - *deck/card organizational metaphor*
  - *support for navigation among cards and decks*
- **a card is one or more units of interaction**
- **A HTML Page = A Deck = a set of interaction cards**

WAP Architecture



WTP Gateway


WAP Device
WAE
WSP
WTP
WTLS
WDP
Bearer
WAP Gateway
WSP
WTP
WTLS
WDP
Bearer
HTTP
TLS
TCP
IP
Web Server
WAE
HTTP
TLS
TCP
IP

WAP Protocols

- **Wireless Session Protocol (WSP)**
  – provides applications with two session services
  – connection-oriented and connectionless
  – based on HTTP with optimizations
- **Wireless Transaction Protocol (WTP)**
  – manages transactions of requests / responses between a user agent & an application server
  – provides an efficient reliable transport service
- **Wireless Datagram Protocol (WDP)**
  – adapts higher-layer WAP protocol to comms

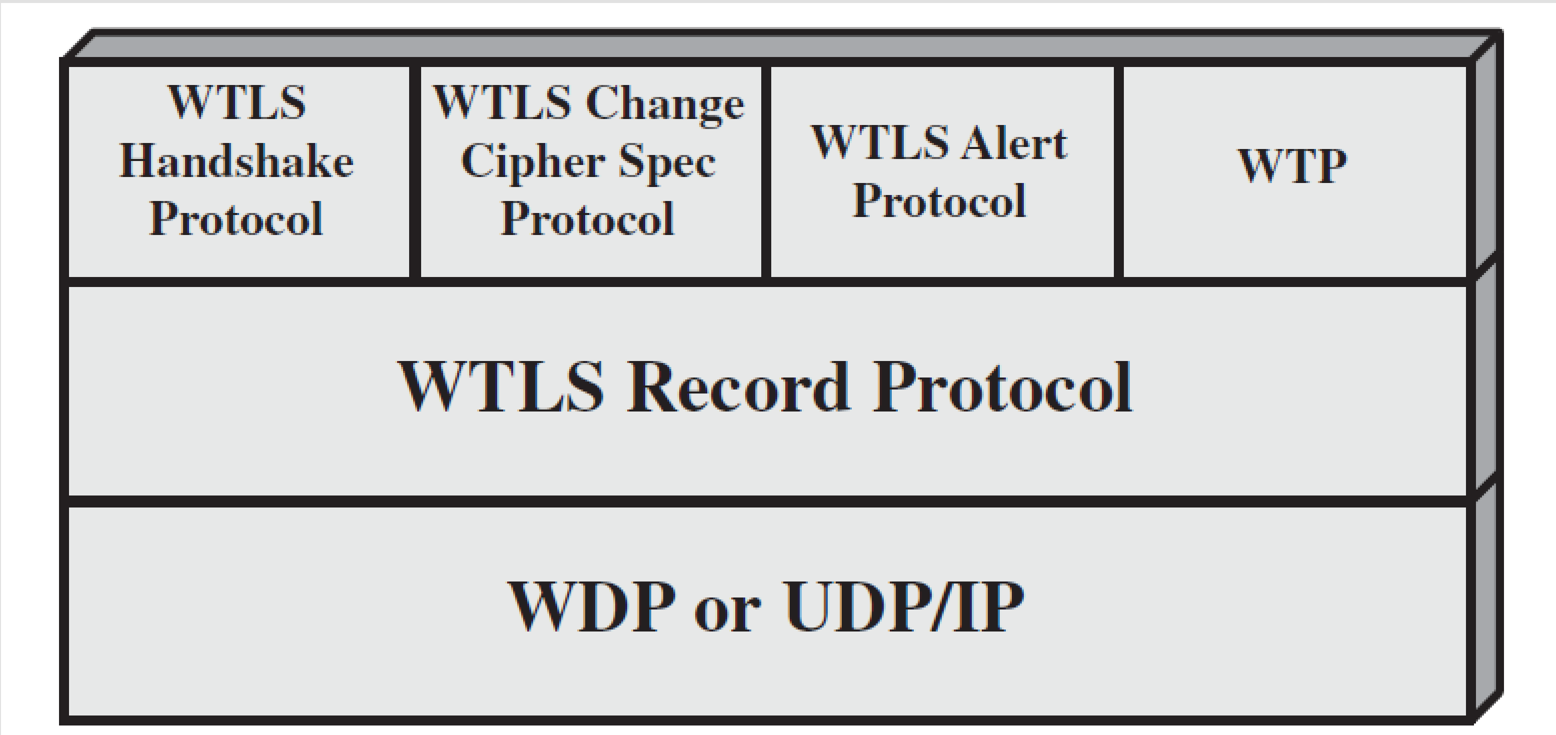
Wireless Transport Layer Security (WTLS)

- **provides security services between mobile device (client) and WAP gateway**
  - provides data integrity, privacy, authentication, denial-of-service protection
- **based on TLS**
  - more efficient with fewer message exchanges
  - use WTLS between the client and gateway
  - use TLS between gateway and target server
- **WAP gateway translates WTLS / TLS**

WTLS Sessions and Connections

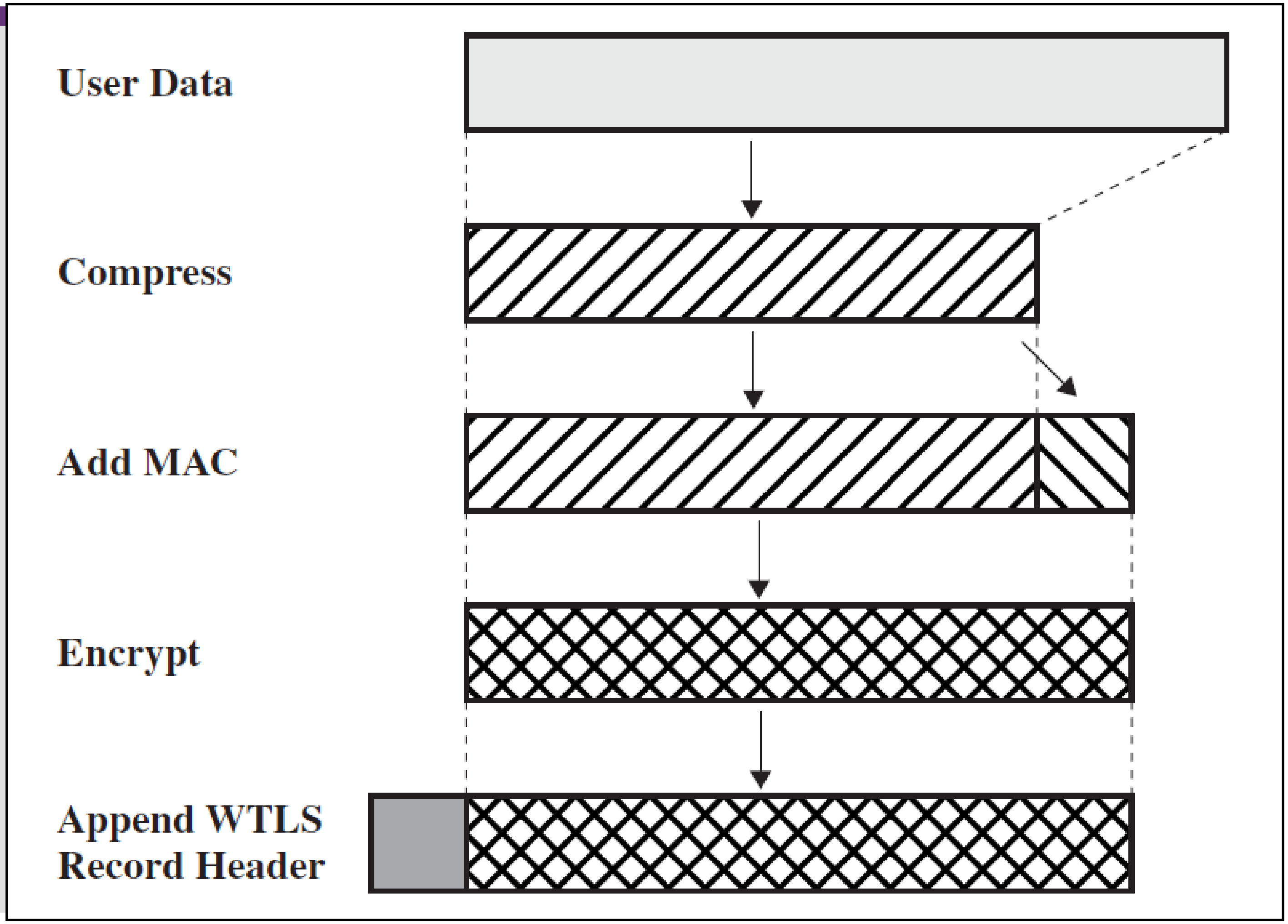
- **secure connection**
  - a transport providing a suitable type of service
  - connections are transient
  - every connection is associated with 1 session
- **secure session**
  - an association between a client and a server
  - created by Handshake Protocol
  - define set of cryptographic security parameters
  - shared among multiple connections

WTLS Protocol Architecture



Does this architecture look familiar?

WTLS Record Protocol Operation

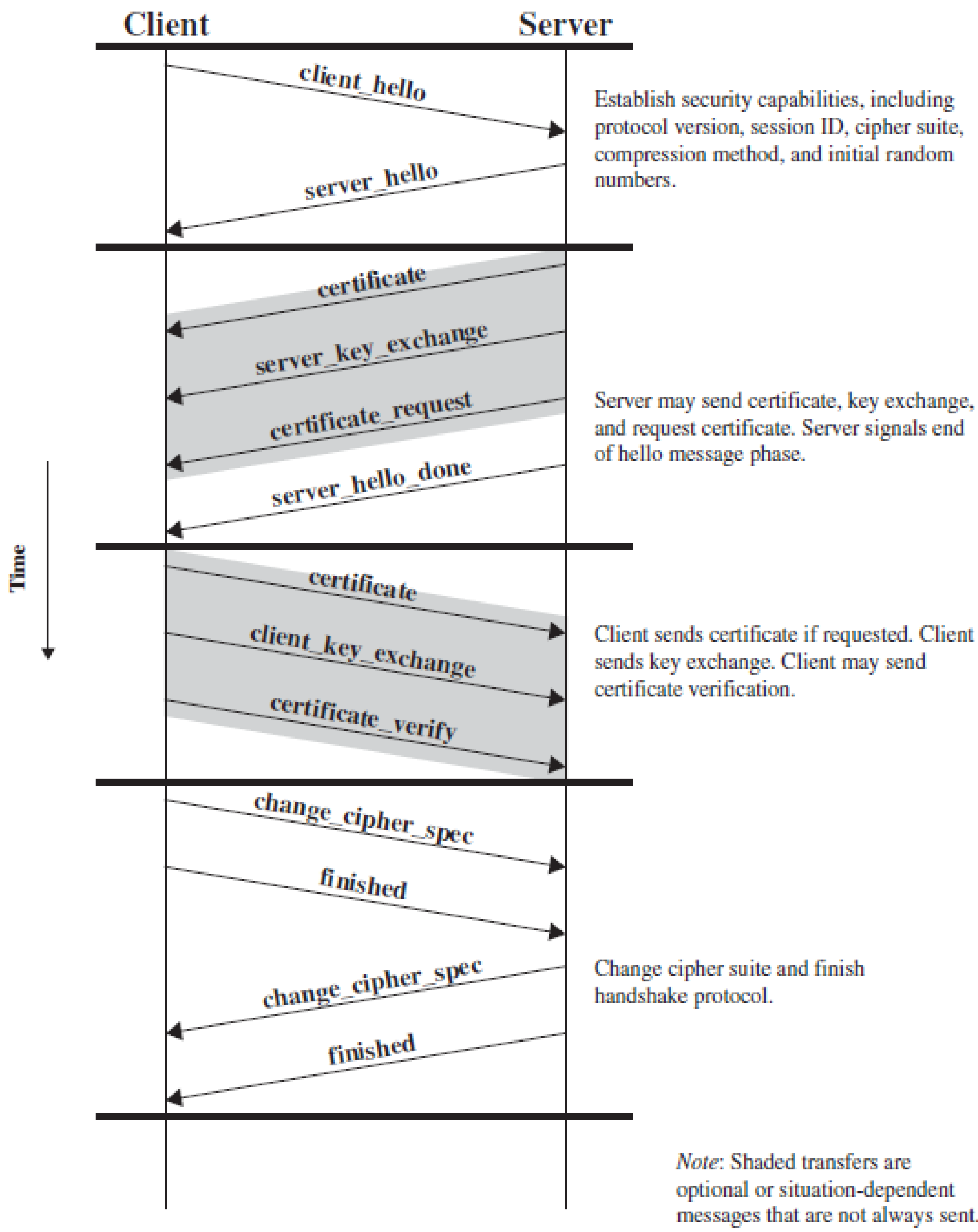


MONASH University
Information Technology

WTLS Higher-Layer Protocols

- **Change Cipher Spec Protocol**
  - simplest, to make pending state current
- **Alert Protocol**
  - used to convey WTLS-related alerts to peer
  - has severity: warning, critical, or fatal
  - and specific alert type
- **Handshake Protocol**
  - allow server & client to mutually authenticate
  - negotiate encryption & MAC algorithms & keys

WTLS Handshake Protocol operation



Cryptographic Algorithms

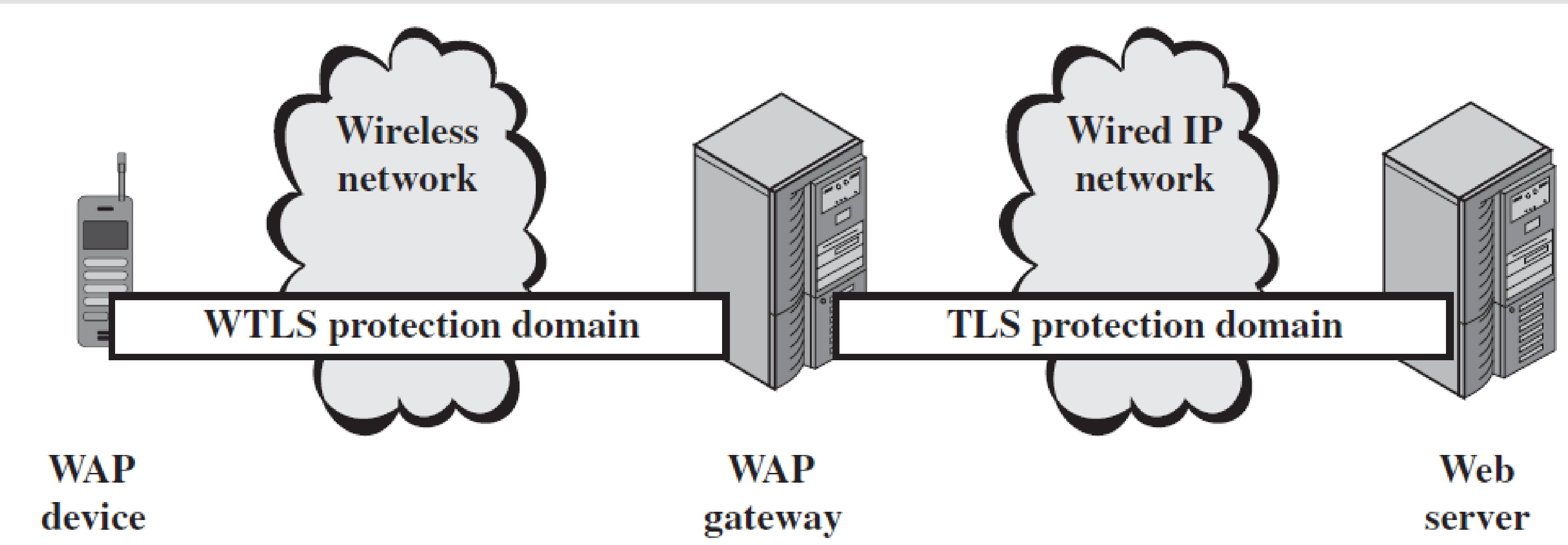
- **WTLS authentication**
  - uses certificates
    - > X.509v3, X9.68 and WTLS (optimized for size)
  - can occur between client and server or client may only authenticates server
- **WTLS key exchange**
  - generates a mutually shared pre-master key
  - optional use server_key_exchange message
    - > for DH_anon, ECDH_anon, RSA_anon
    - > not needed for ECDH_ECDSA or RSA

Cryptographic Algorithms contd.

- **Pseudorandom Function (PRF)**
  - HMAC based, used for a number of purposes
  - only one hash algorithm, agreed during handshake
- **Master Key Generation**
  - of shared master secret
  - master_secret = PRF(pre_master_secret, "master secret”, ClientHello.random || ServerHello.random)
  - then derive MAC and encryption keys
- **Encryption with RC5, DES, 3DES, IDEA**

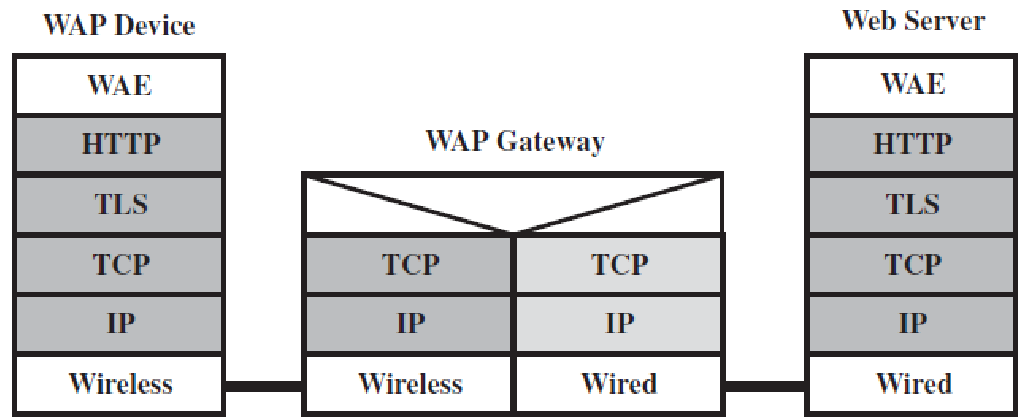
WAP End-to-End Security

- **There is an end-to-end security gap between the WTLS & TLS domains**
  - data are not encrypted within the gateway

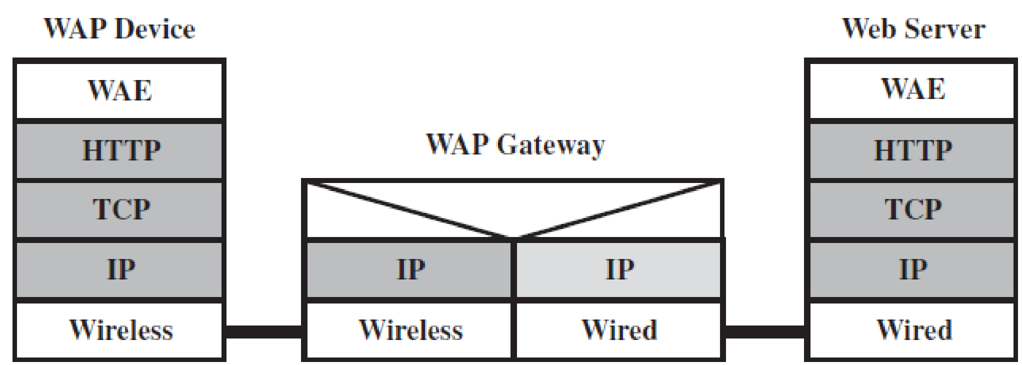


WAP2 End-to-End Security

- **Two possible solutions to this problem**
  – In both cases, devices implement TCP/IP (and HTTP)
- **First solution**
  – A secure TLS session is established between the via endpoints via the WAP gateway
  – WAP gateway acts as a TCP-level gateway and **splices together two TCP connections**
  – Traffic is carried between the two endpoints **ensuring end-to-end security** is maintained
- **Second solution**
  – Assume gateway functions as a simple IP router, and
  – Use **IPSEC**



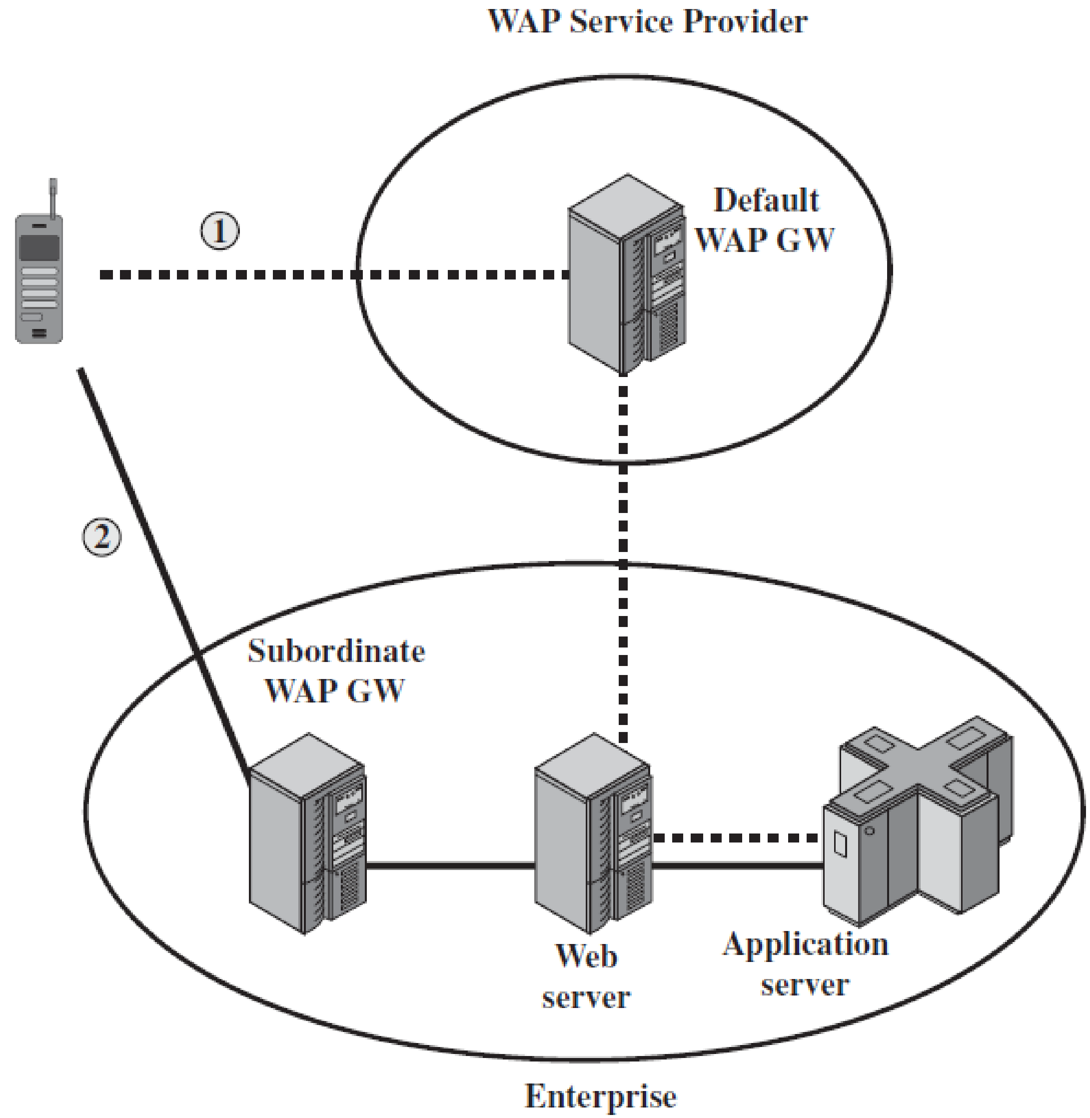
(a) TLS-based security



(b) IPSec-based security

WAP2 End-to-End Security Scheme

- **An alternative 3rd way**
  - Enterprise implements a trusted WAP gateway on the clients wireless network
    - > Initial contact is established through the default gateway
    - > Sever sends a HTTP redirect to redirect client to trusted WAP gateway within the enterprise
    - > Client established new session, but used the enterprise gateway
  - However, the enterprise must maintain their own WAP gateway



Summary

- **have considered:**
  - IEEE 802.11 Wireless LANs
    - > protocol overview and security
  - Wireless Application Protocol (WAP)
    - > protocol overview
  - Wireless Transport Layer Security (WTLS)

Further Reading

- **Study Guide 6**
- **Chapter 6 of the textbook: Network Security Essentials-Application & Standards" by William Stallings 5th Edition, Prentice Hall, 2013**
- **Additional resources for this week**

- **Acknowledgement: The materials presented in the slides were developed with the help of the Instructor's Manual and other resources made available by the author of the textbook.**