WLAN 802.1X Authentication

Professor Sanjay K. Jha

Outline

- Security at Layer2

- Authentication and Authorization in WLAN

- 802.1X Extensible Authentication Protocol (EAP)

  – Authentication and Authorisation for both wired and wireless network

- Robust Security Network (RSN)/802.11i for Key Management

- Roaming

Challenges for Enterprise

- Pre Shared Key (PSK) not scalable
  - Max 64 hex characters, configure manually in each device
- E.g. 100 Employees, all share same Key.
- One leaves the company
  - Configure 99 devices with new key
- We have learnt the vulnerability with WEP/WPA – and labs.
- WPA2 provides CCMP/AES.
- We learnt about SSL and IPSec
  - Provide lot of flexibility/Option in configuring security at network and transport layers
- Advanced Authentication Methods based on "Extensible Authentication Protocol (EAP)" – topic of this lecture

UNSW
AUSTRALIA
CySPri Laboratory

AAA

- Authentication: verification of user identity and credentials
  - May be multifactor: biometric etc.
- Authorization: granting access to resources and services
  - Needs authentication first.
- Accounting: tracking network use by users
  - Important to keep log
  - Required by many industry regulators
  - Helpful for billing/charging

UNSW
AUSTRALIA
CySPri Laboratory
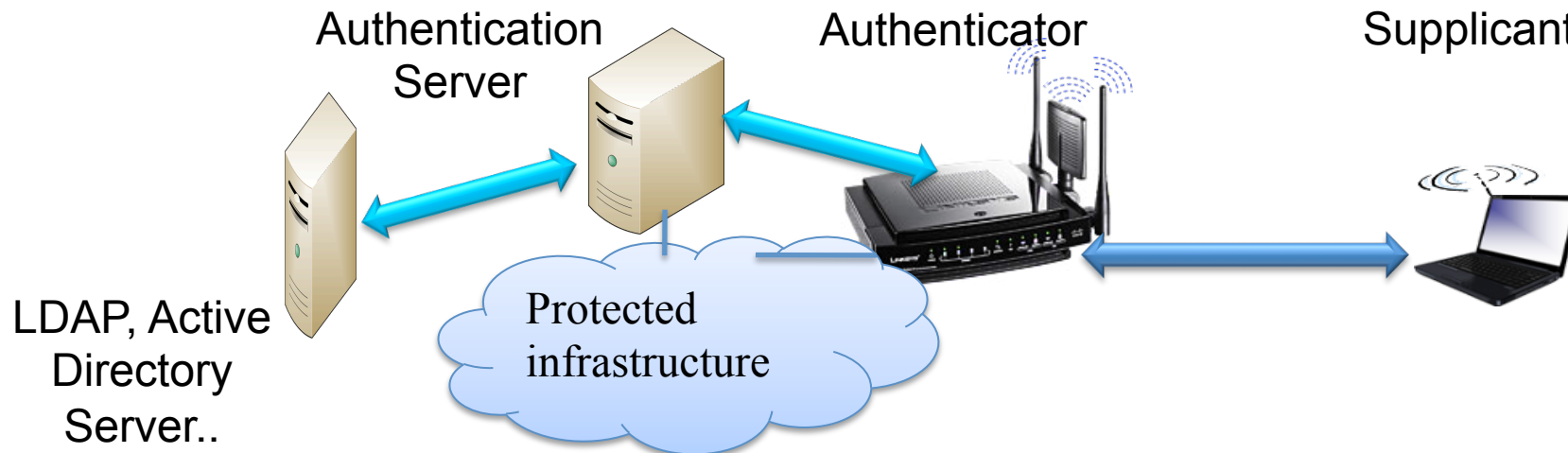
Authentication in WLAN - recap

- Username and passwords
- Digital Certificates
- Dynamic/One Time passwords
- Smartcards or credential on USBs
- Machine authentication (based on embedded identity)
- Pre-shared Keys (We saw WEP, WPA using this earlier)
- WLAN Example of MF: A registered computer and a legitimate user which has entry in a DB e.g. A Microsoft Active Directory

UNSW
AUSTRALIA
CySPri Laboratory

Authorization in WLAN

- Various applications and higher layer protocols have their own authorization schemes.

- WLAN can provide authorization via 801.X framework at Layer-2 (can be used with Robust Security Network (RSN))
  - Port based access control (more later), for both wired and wireless network

  - Lot of standard documents for various bits/pieces – not focus of this subject

- Accounting is an important part but not within scope of WSN
  - Useful for forensics though

UNSW
AUSTRALIA
CySPri Laboratory

IEEE 802.1X Port based Authentication

- Port Based: User must authenticate to switch they are physically connected to.
- Involves 3-party communications (nomenclature from 802.1X standard)
  - Supplicant
    - o User
  - Authenticator
    - o Ethernet switch, wireless access point
  - Authentication server
    - o RADIUS (Remote access dial-in user service) database, Kerberos, LDAP or AD (Can be co-located with Authenticator)

Authentication Server   Authenticator   Supplicant

LDAP, Active Directory Server..

Protected infrastructure

UNSW
AUSTRALIA
CySPri Laboratory

Supplicant

- Device to be authenticated for resource use

- Uses EAP protocol to connect to Auth. Server

- Until identity verified – can't use higher layer protocols (3 – 7)

- Can be software/app running 802.1X client

- OS based supplicants:
  - Microsoft Wireless Zero Conf – WZC
    - Known problems with supplicant software
  - Apple's airport client

- Chipset vendors may provide supplicant software
  - Intel, Atheros, Broadcom

UNSW
AUSTRALIA
CySPri Laboratory

Authenticator (Access Point)

- For EAP, acts as a relay between Supplicant and Auth. Server
- Two Virtual Ports:
  - Uncontrolled : allows EAP authentication traffic
  - Controlled: Only authenticated traffic
- With WLAN Bridging solution:
  - Root bridge (a nominated bridge) is authenticator and other connected ones are supplicant
- Configured with address of Authentication Server
  - Possible co-location of Auth. Server with Authenticator
  - Shared Secret with Auth. Server

UNSW
AUSTRALIA
CySPri Laboratory

Authentication Server: RADIUS (1)

- RADIUS provides centralized authentication, authorization and accounting management for user/host to access a network service/resource
  - Details in RFC 2865
- Supports AAA (Authentication, Authorization and Accounting) – a.k.a " Triple A"
  - RFC 3579 (AAA protocols such as RADIUS/EAP)
  - RADIUS is used to shuttle RADIUS-encapsulated EAP Packets between authenticator and an authentication server
- Most network equipment supports RADIUS
  - Wireless AP, VPN appliance, SSL, etc.
- Keeps an audit log of user's activity – accountability
- Radius Server
  - Standalone – local DB
  - Use External DB – e.g Active Directory
  - UDP Port 1812 for Auth, 1813 for Acct.
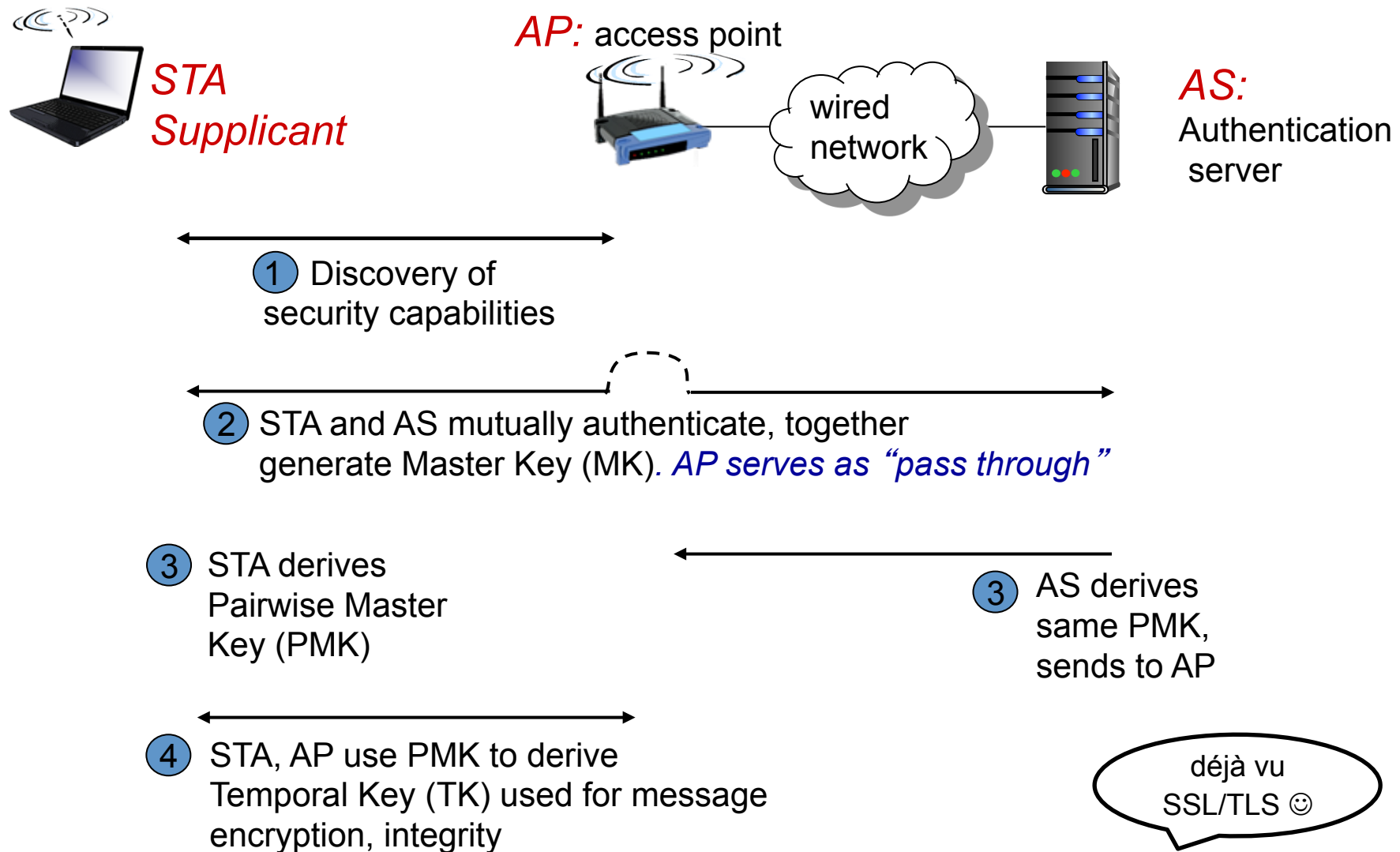- Any other server can also be directly used in place of RADIUS

RADIUS (2)

- Radius Server and Authenticator configured with a shared secret.

- Authenticator sends a RADIUS Access Request message to the RADIUS server, requesting authorization to grant access via the RADIUS protocol

  – This request includes access credentials (e.g., username and password)

  – Authentication server checks the credentials using the RADIUS server, Kerberos server, LDAP or Active Directory server

  – returns one of three responses

    o Access Accept, Access Reject, Access Challenge for extra credentials

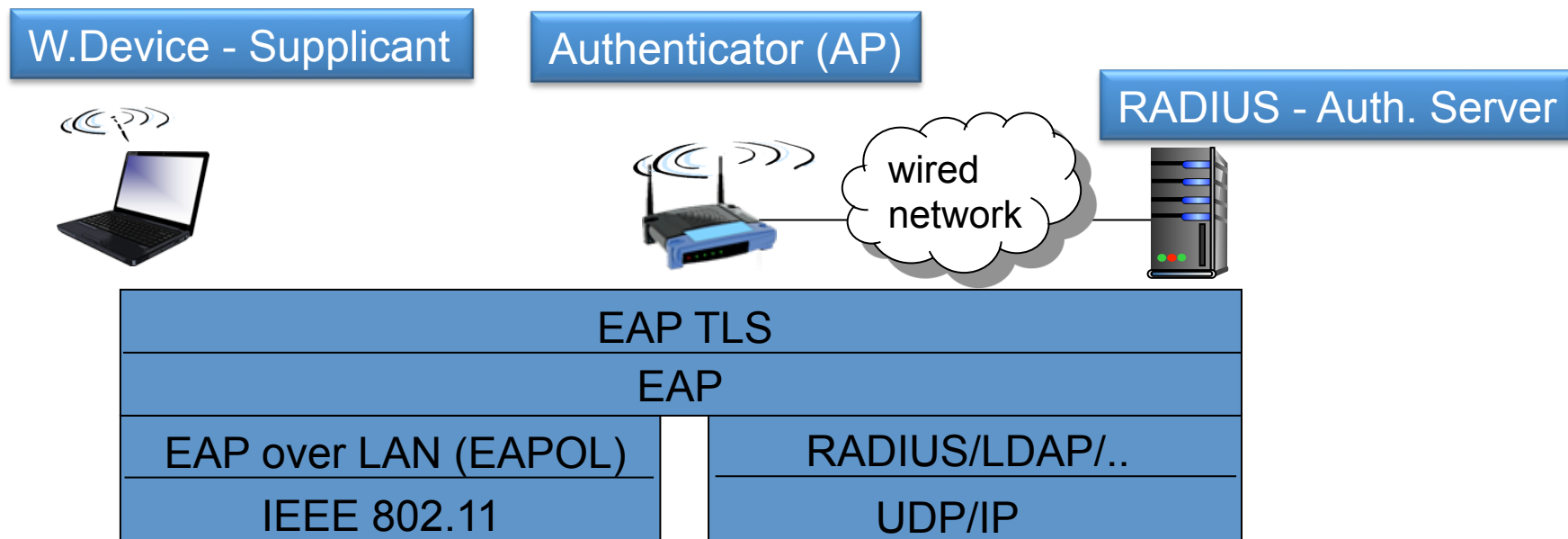UNSW
AUSTRALIA
CySPri Laboratory

RADIUS server examples

- Elektron (US$750) is an entry-level and user-friendly server

- ClearBox (US$599) is designed for small networks, but it also scales to larger networks

- FreeRADIUS (open source) is a solid and economical choice for Unix/Linux admins offering the most customization and flexibility

Four phases of operation (Short Story)

STA
Supplicant

AP: access point

wired
network

AS:
Authentication
server

(1) Discovery of
security capabilities

(2) STA and AS mutually authenticate, together
generate Master Key (MK). *AP serves as "pass through"*

(3) STA derives
Pairwise Master
Key (PMK)

(3) AS derives
same PMK,
sends to AP

(4) STA, AP use PMK to derive
Temporal Key (TK) used for message
encryption, integrity

déjà vu
SSL/TLS ☺

UNSW
AUSTRALIA
CySPri Laboratory

EAP: extensible authentication protocol (Short Story)

- EAP: end-end client (mobile) to authentication server protocol
- EAP sent over separate "links"
  - WirelessDevice-to-AP (EAP over LAN)
  - AP to authentication server (RADIUS over UDP)

| W.Device - Supplicant | Authenticator (AP) | RADIUS - Auth. Server |

EAP TLS		
EAP		
EAP over LAN (EAPOL)		RADIUS/LDAP/..
IEEE 802.11		UDP/IP

802.1X protocol - Long Story Continue

- When a new client (supplicant) is connected to an authenticator, the port on the switch/wireless AP (authenticator) is enabled and set to the "unauthorized" state
  - In this state, only 802.1X traffic is allowed
  - Other traffic, such as DHCP and HTTP, is blocked at the data link layer
  - Steps
    - Authenticator sends out the EAP-Request identity to the supplicant
    - Supplicant responds with the EAP-response packet that the authenticator forwards to the authenticating server
    - If the authenticating server accepts the request, the authenticator sets the port to the "authorized" mode and normal traffic is allowed
    - When the supplicant logs off, it sends an EAP-logoff message to the authenticator; the authenticator then sets the port to the "unauthorized" state, once again blocking all non-EAP traffic

UNSW
AUSTRALIA
CySPri Laboratory

EAP (1)

- EAP was designed for use in local network access authentication, where IP layer connectivity may not be available
  - When operating as a "pass-through authenticator" in the RADIUS/EAP scenario (RFC 3579), an authenticator performs checks on the Code, Identifier, and Length fields in accordance with EAP packet format and forwards EAP packets received from the supplicant to the authentication server

code	ID	Length	Data

- The Code field is one octet and identifies the Type of EAP packet. EAP Codes are assigned as follows:
  - 1   Request
  - 2   Response
  - 3   Success
  - 4   Failure
- EAP defines message formats in RFC 3748
- RFC 5247 specifies the EAP key hierarchy and provides a framework for the transport and usage of keying material and parameters generated by EAP authentication algorithms, known as "methods"
- *Read RFCs if interested – not examinable unless explicity requested for exam.*

UNSW
AUSTRALIA
CySPri Laboratory

EAPOL Messages

TABLE 4.2   EAPOL Messages

Packet Type	Name	Description
0000 0000	EAP-Packet	This is an encapsulated EAP frame. The majority of EAP frames are EAP-Packet frames.
0000 0001	EAPOL-Start	This is an optional frame that the supplicant can use to start the EAP process.
0000 0010	EAPOL-Logoff	This frame terminates an EAP session and shuts down the virtual ports. Hackers sometimes use this frame for DoS attacks.
0000 0011	EAPOL-Key	This frame is used to exchange dynamic keying information. For example, it is used during the 4-Way Handshake.
0000 0100	EAPOL- Encapsulated - ASF-Alert.	This frame is used to send alerts, such as SNMP traps to the virtual ports.

Src: CSWP Text

UNSW
AUSTRALIA
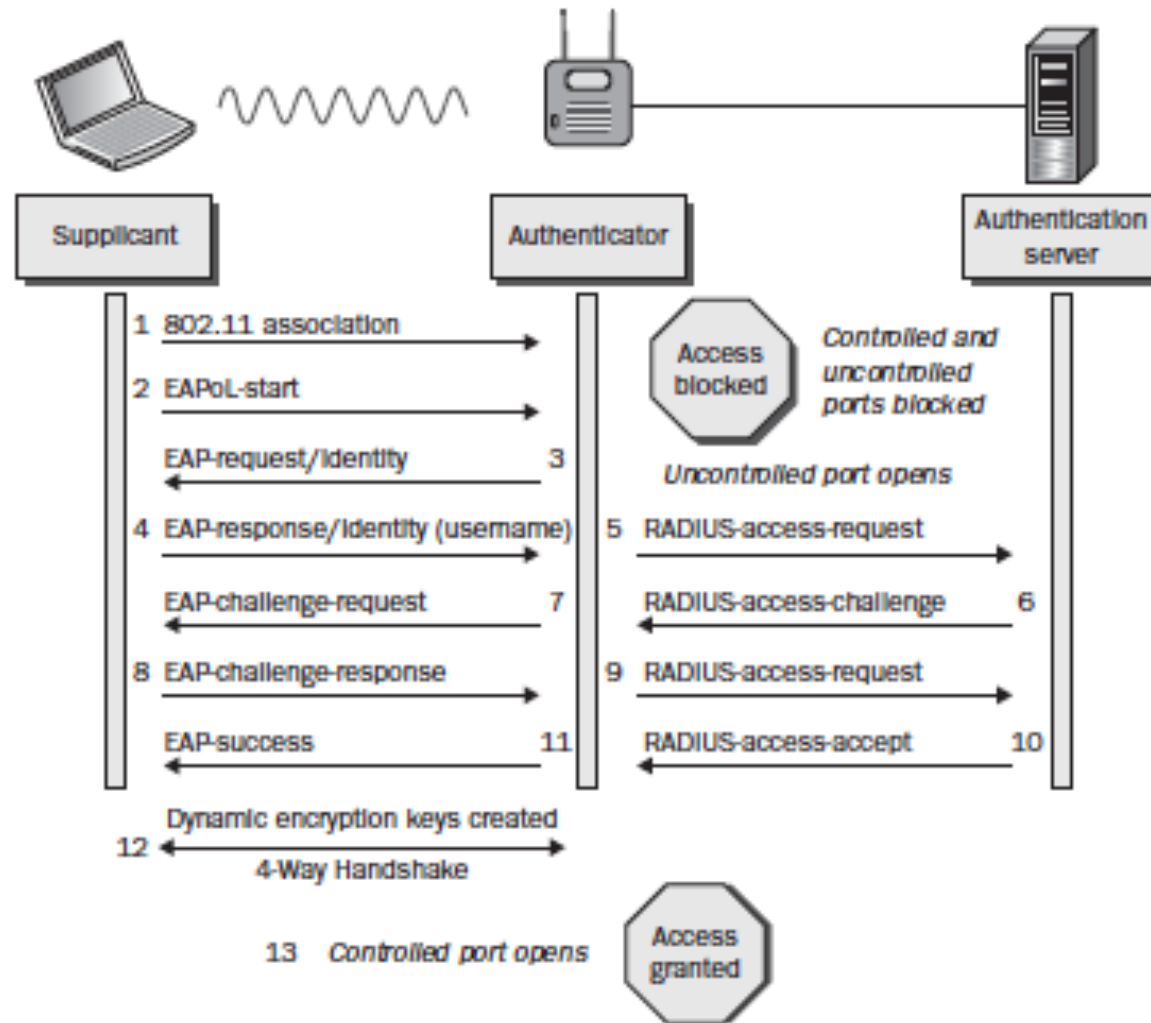MANU ET MENTE
CySPri Laboratory

Association and EAP

- First step is usual 802.11 association to establish L2 connection
- If 802.1X framework used, network unusable unless the show authorization process is complete.
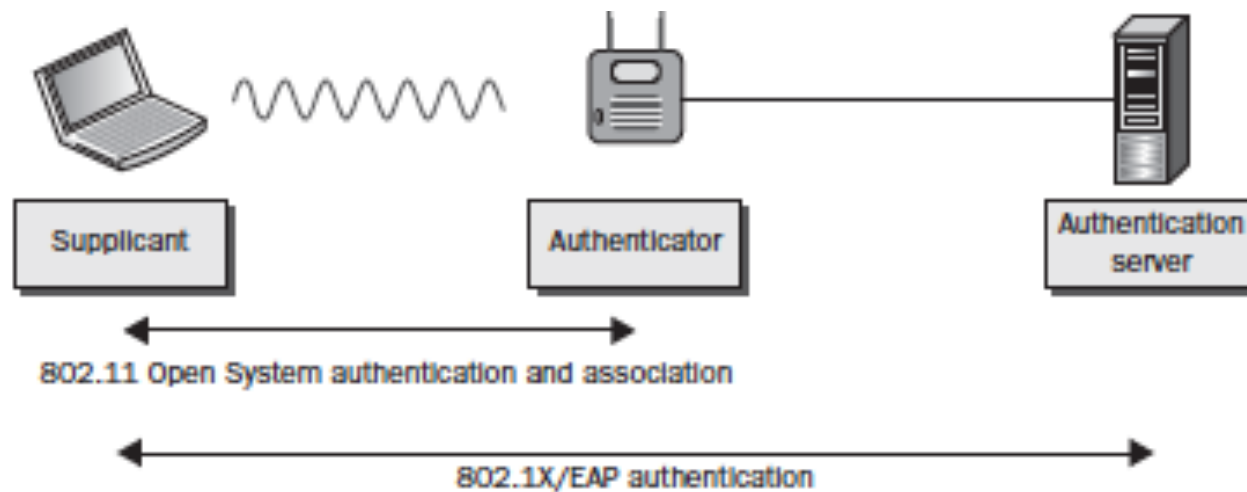
Src: CSWP Text

Generic EAP Exchange

Notes on General Exchange

- Most steps are self explanatory
- Step4: Only identity is sent to the AP in clear text
  - This allows for uncontrolled port to open
- Step8: Supplicant doesn't send password, just MD5 (or other hash of password)
- Step12: A complex process to generate dynamic encryption key
  - uses 4 way handshake (discussed later)
- Step13: Controlled port is unblocked for the user.
  - Proceeds to obtain an IP address using DHCP
- Note: Step4 and 8 create security risk,
  - hash algorithms can be cracked
  - Dictionary attack possible
  - Would it help to have an encrypted tunnel for these steps 4 -9?
- Most schemes use tunneled authentication to pass identity credentials

Tunneling of EAP

- EAP Methods defined in commonly used modern EAP standards include
  - EAP-TLS (EAP-Transport Layer Security)
    - RFC 5216
  - EAP-SIM (EAP for GSM Subscriber Identity)
    - RFC 4186
  - EAP-AKA (EAP for UMTS Authentication and Key Agreement)
    - RFC 4187
  - PEAP (Protected Extensible Authentication Protocol)
    - RFC 3748, (Microsoft Windows MS-CHAPv2
  - EAP-FAST (Flexible Authentication via Secure Tunneling)
    - RFC 4851
  - EAP-TTLS (EAP-Tunneled Transport Layer Security)
    - RFC 5281
- <u>No need to remember these acronyms or RFCs</u>
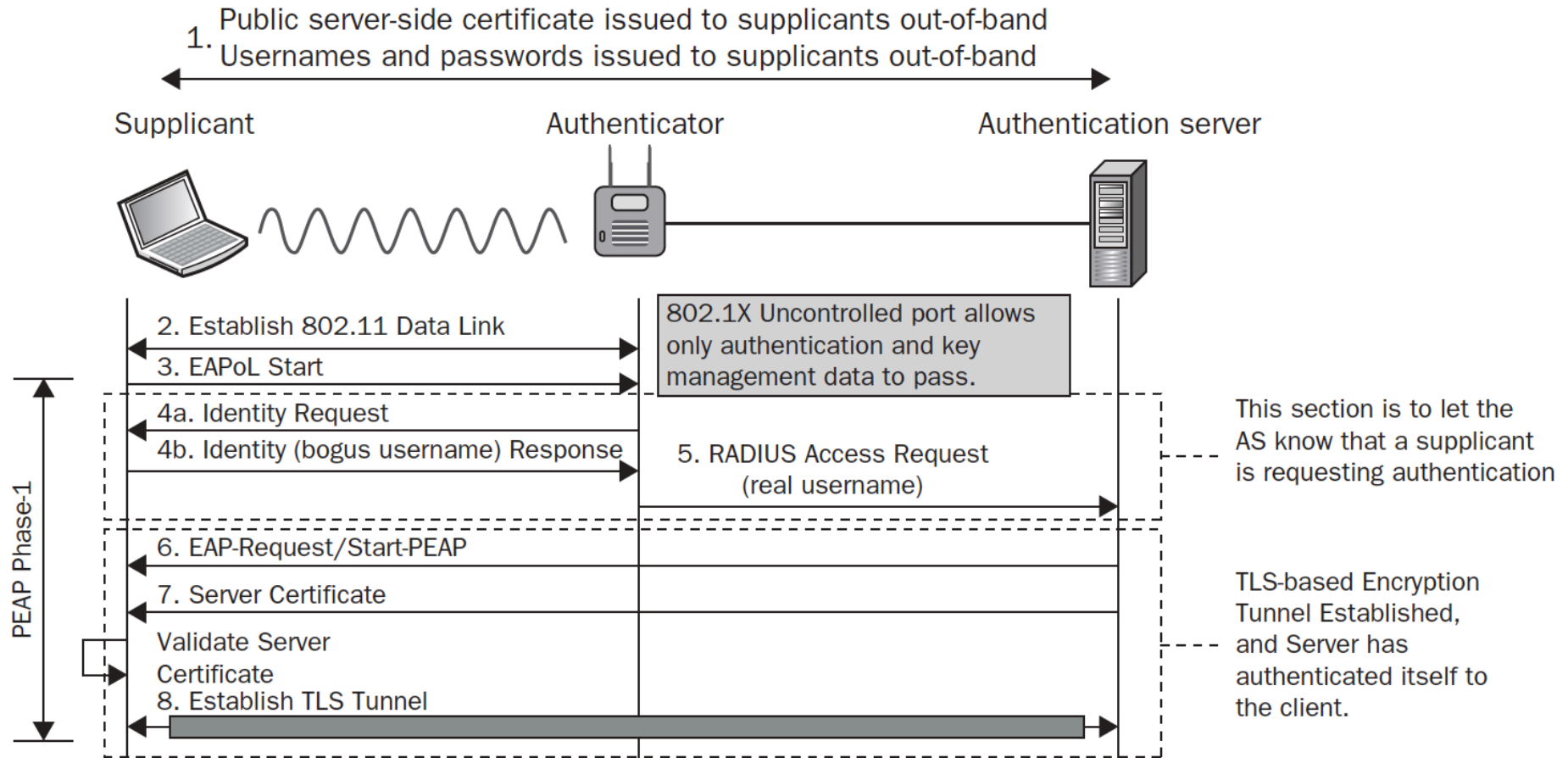
UNSW
AUSTRALIA
CySPri Laboratory

EAP Tunneled Protocols

- Two supplicant identities used
  - Outer identity: clear text (e.g. anonymous) to satisfy EAP standard (Step4 earlier), a bogus entity
  - Inner identity: true identity that goes inside the encrypted TLS tunnel
- Point to Note:
  - EAP Tunnel only for authentication and authorization to save identity
    - not for encrypting payload
    - Exists for few millisecond
  - Payload encrypted using negotiated key
- Honeypot can be set by using a fake employee name in outer identity
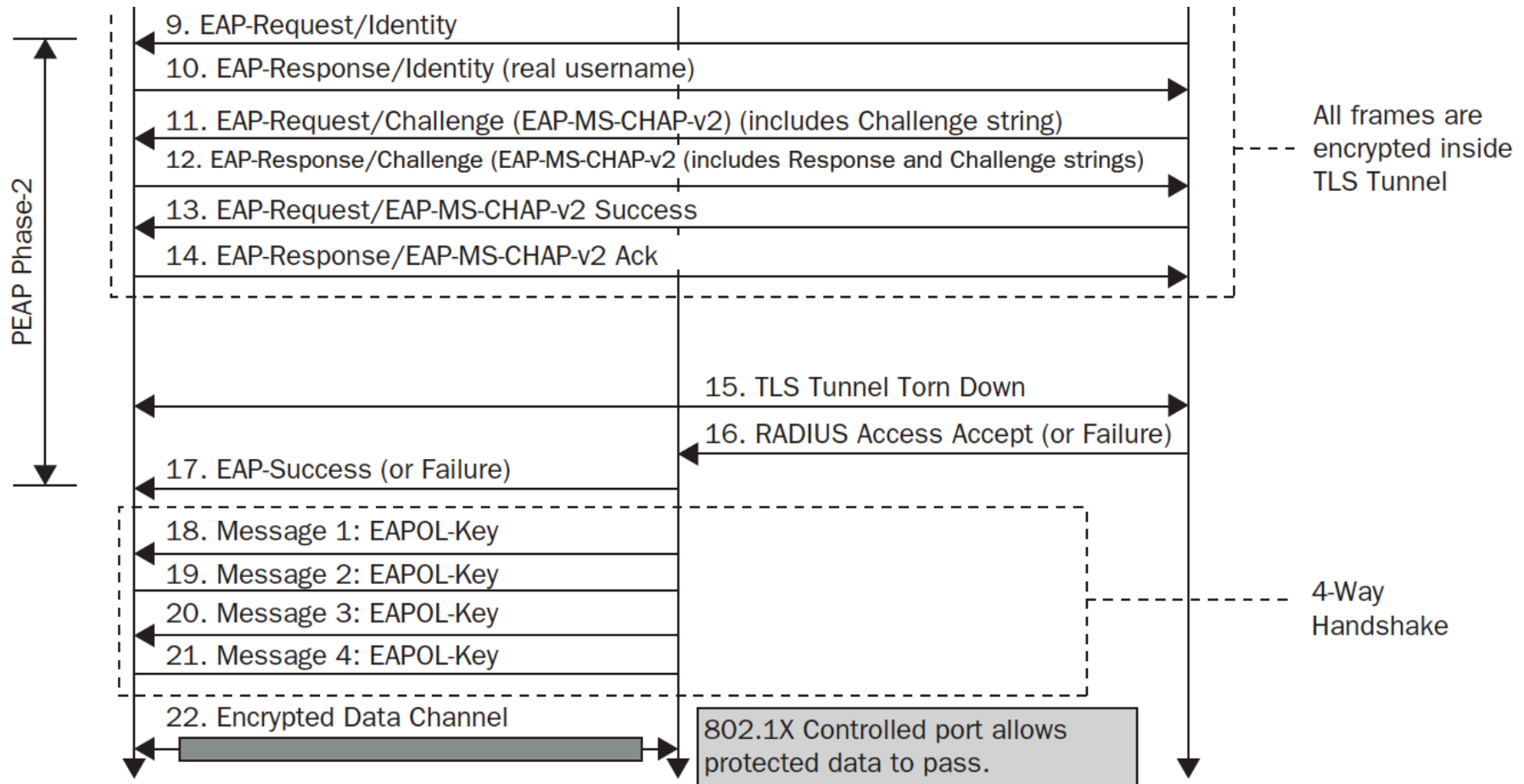 - employees can inform if they see any activity with this fake name.

EAP - PEAP

- EAP- Protected Authentication Protocol (EAP-PEAP): most popular, aka "EAP inside EAP"

- Three flavors of this protocol based on inner EAP.

  – Variants from vendors e.g. Microsoft, Cisco – politics of disagreement

  – All need at to establish TLS tunnel

  – Difference in hash algorithms, whether credentials use, tokens, username/password, client-side certificate etc.

  – Read if interested.

- A server side certificate is required for all flavors

UNSW
AUSTRALIA
CySPri Laboratory

EAP-PEAP Process (Phase1)

Src: CSWP Text

UNSW AUSTRALIA | CySPri Laboratory

EAP-PEAP (Phase2)

9. EAP-Request/Identity

10. EAP-Response/Identity (real username)

11. EAP-Request/Challenge (EAP-MS-CHAP-v2) (includes Challenge string)

12. EAP-Response/Challenge (EAP-MS-CHAP-v2 (includes Response and Challenge strings)

13. EAP-Request/EAP-MS-CHAP-v2 Success

14. EAP-Response/EAP-MS-CHAP-v2 Ack

All frames are encrypted inside TLS Tunnel

PEAP Phase-2

15. TLS Tunnel Torn Down

16. RADIUS Access Accept (or Failure)

17. EAP-Success (or Failure)

18. Message 1: EAPOL-Key

19. Message 2: EAPOL-Key

20. Message 3: EAPOL-Key

21. Message 4: EAPOL-Key

4-Way Handshake

22. Encrypted Data Channel

802.1X Controlled port allows protected data to pass.

Src: CSWP Text

UNSW AUSTRALIA

CySPri Laboratory

EAP-TTLS

- EAP – Tunneled TTLS
  - Juniper networks mostly deploy this, less popular than PEAP
  - Very similar to PEAP with minor differences
  - Supports many more inner authentication methods, Supplicant credentials normally username and password
  - Optional support for client-side certificates
- Read details if interested

UNSW
AUSTRALIA
CySPri Laboratory

EAP-TLS

- EAP – Transport Layer Security (TLS)
  - Major differentiator – Client-side certificate
  - Unique digital certificate for each client needs planning, infrastructure
  - Certificate store must be always available and highly secure
- Due to additional cost burden, not a method of choice
- We will skip the details of protocol exchange which has similarity to other methods besides mutual authentication between Supplicant and Server using certificates.

EAP-TLS Infrastructure

- Deploy Enterprise CA
- Configure Authentication Server (RADIUS)
- Configure Access Point

Authentication Server

Authenticator

Supplicant

router
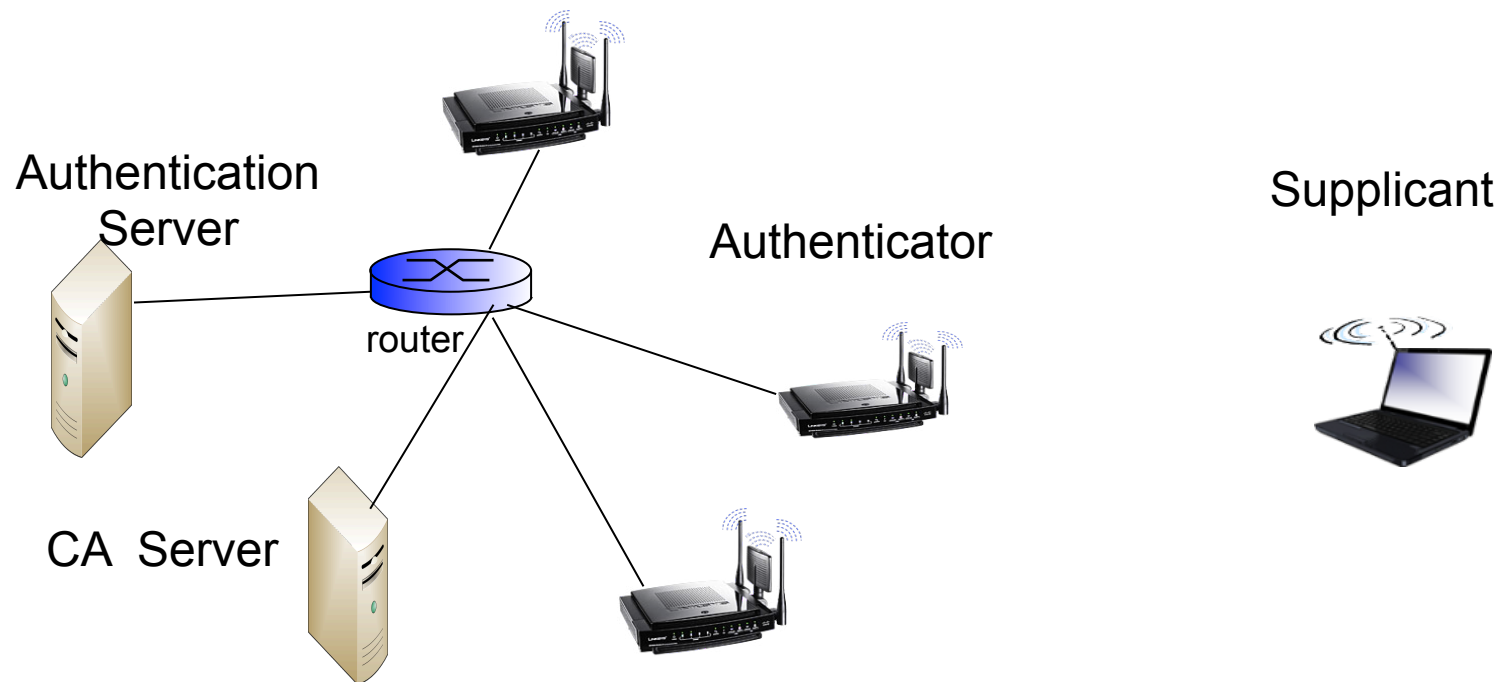
CA Server

EAP-TLS CA configuration

- Clients must be configured via wired (or authenticated Wireless net) before accessing a new network
  - Downloads CA certificate
  - Gets User's certificate
- Configure Radius server
  - Client for Radius is Authenticator (Access point)
  - Setup to accept request from each Access point (including shared secret)
- Configure Access Point
  - Setup Authenticator to the IP address of RADIUS server
  - WPA algorithm e.g. AES
  - Shared secret with Radius
- Operational details/interface etc will vary based on products you use. We are interested in basic architecture

UNSW
AUSTRALIA
CySPri Laboratory

References

- Kurose/Ross: Chapter-8, good for short story

- Wu/Irwin: Ch21 and Ch25, Good summary of standards but too much information

- CWSP – Certified Wireless Security Professional Official Study Guide: Chapter 4, Excellent coverage. Only a subset used in lecture to capture basic ideas. Details vary between vendors/implementation methods.

- Acknowledgment: Foils and figures from authors and the three text books above.

UNSW
AUSTRALIA
CySPri Laboratory