WLAN 802.1X Authentication

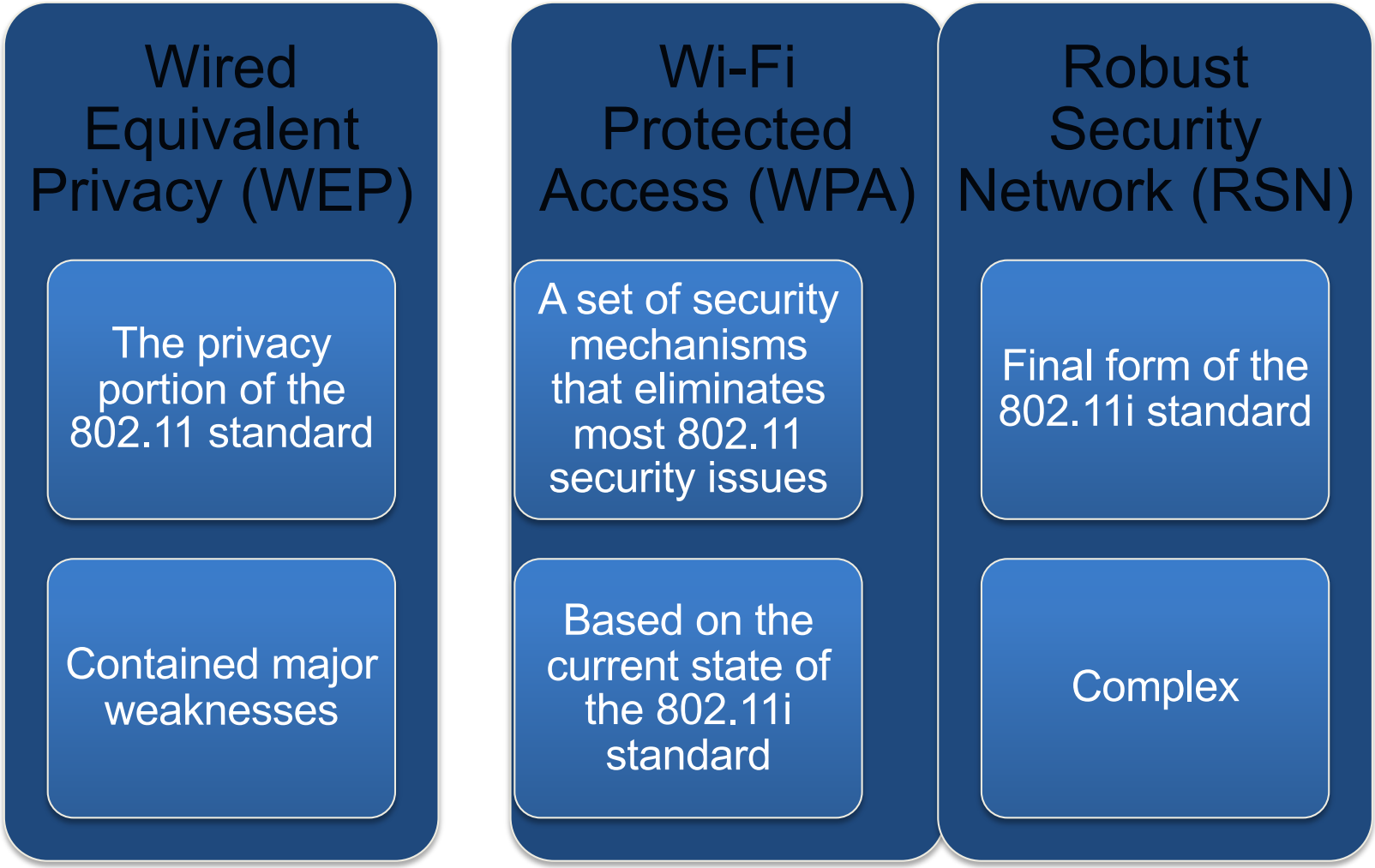
Never Stand Still

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

WLAN Security Summary



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

AAA

鉴权

- Authentication: verification of user identity and credentials
  - May be multifactor: biometric etc. 生物识别技术

授权

- 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

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)
- Wi-Fi Protected Setup (WPS) – push button/Pin
- WLAN Example of MF: A registered computer and a legitimate user which has entry in a DB e.g. A Microsoft Active Directory

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

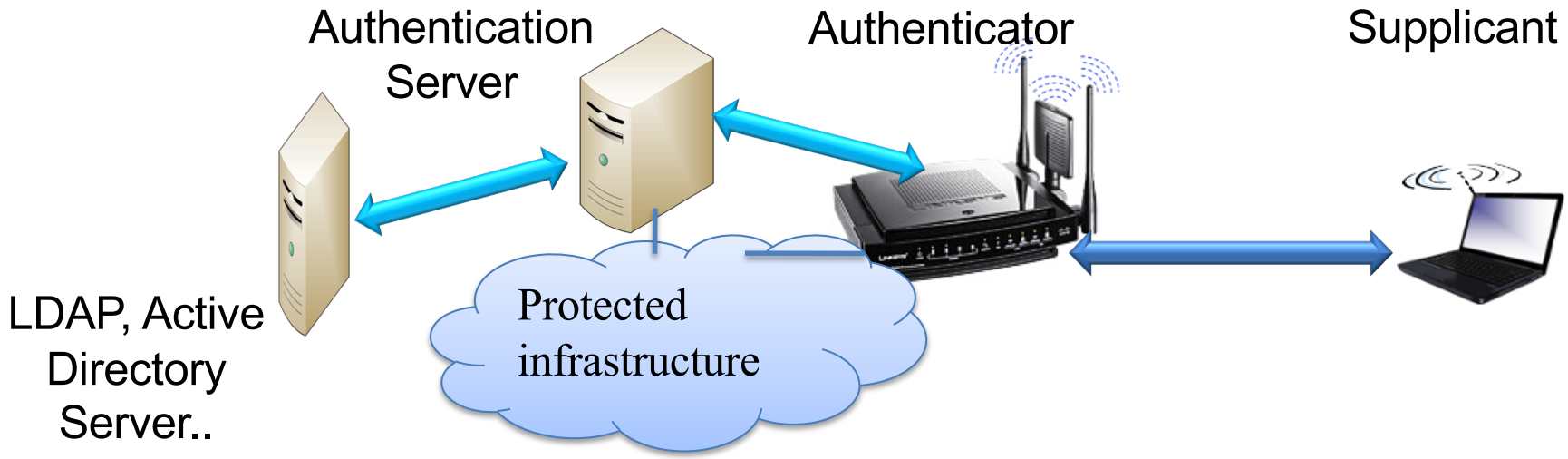
“基于端口的网络接入控制

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
    - User
  - Authenticator
    - Ethernet switch, wireless access point
  - Authentication server
    - RADIUS (Remote access dial-in user service) database, Kerberos, LDAP or AD (Can be co-located with Authenticator)

. 命名法；术语

“基于端口的网络接入控制”是指在局域网接入设备的端口这一级对所接入的用户设备进行认证和控制。



申请者（Supplicant）和验证者（Authenticator）之间

Supplicant

可扩展认证协议（Extensible authentication protocol，EAP）是一个第二层处理过程，

- 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

Authenticator (Access Point)

- For EAP, authenticator 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

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)

用MD5算出的value比对进行鉴权

- 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 hash) 只对password进行hash
  - Authentication server checks the credentials using the RADIUS server, Kerberos server, LDAP or Active Directory server
  - returns one of three responses
    - Access Accept, Access Reject, Access Challenge for extra credentials

这个flag随机生成的和nonce差不多

这个challenge就是要求supplicant给返回一个MD5(flag+username+password)

RADIUS server examples

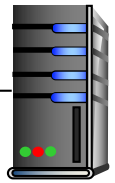
- Elektron (US$750) is an entry-level and user-friendly server
- ClearBox (US$599) is designed for small networks, but it also scales to larger networks
- FreeRADIUS (open source) is a solid and economical choice for Unix/Linux admins offering the most customization and flexibility

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)

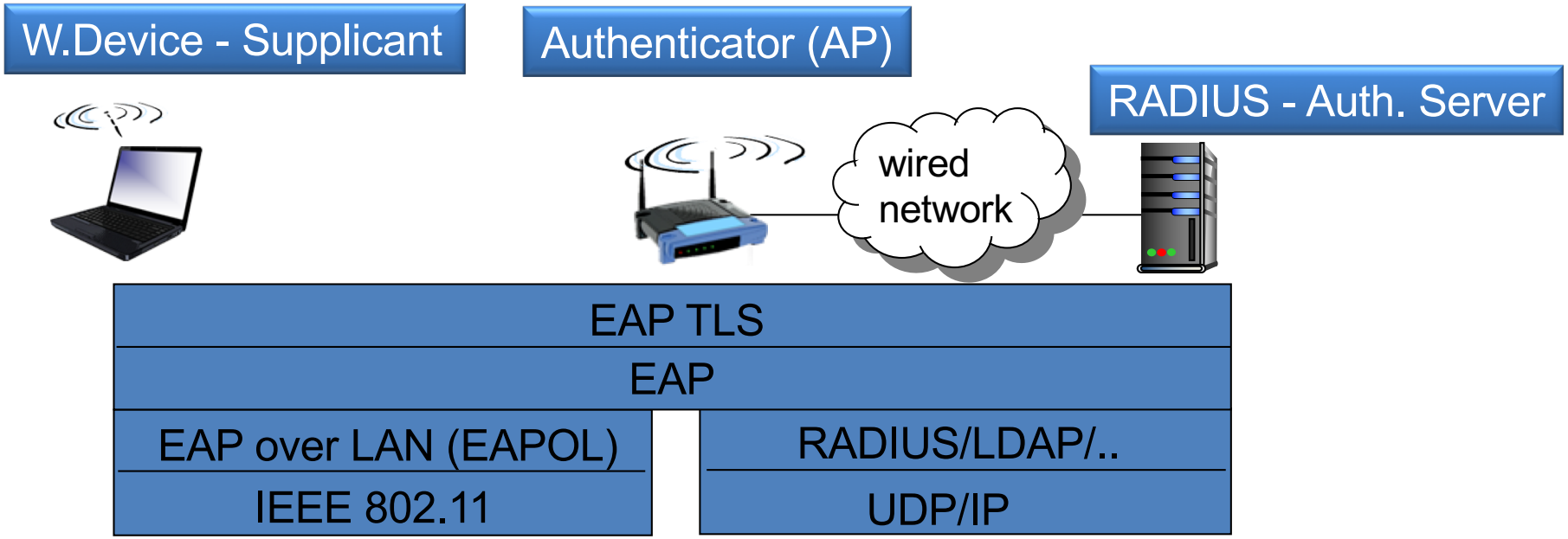
3 AS derives same PMK, sends to AP

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

déjà vu SSL/TLS ☺

EAP: extensible authentication protocol (Short Story)

- EAP: end-end client (mobile) to authentication server protocol
- EAP sent over separate “links”
  - Wireless Device-to-AP (EAP over LAN)
  - AP to authentication server (RADIUS over UDP)

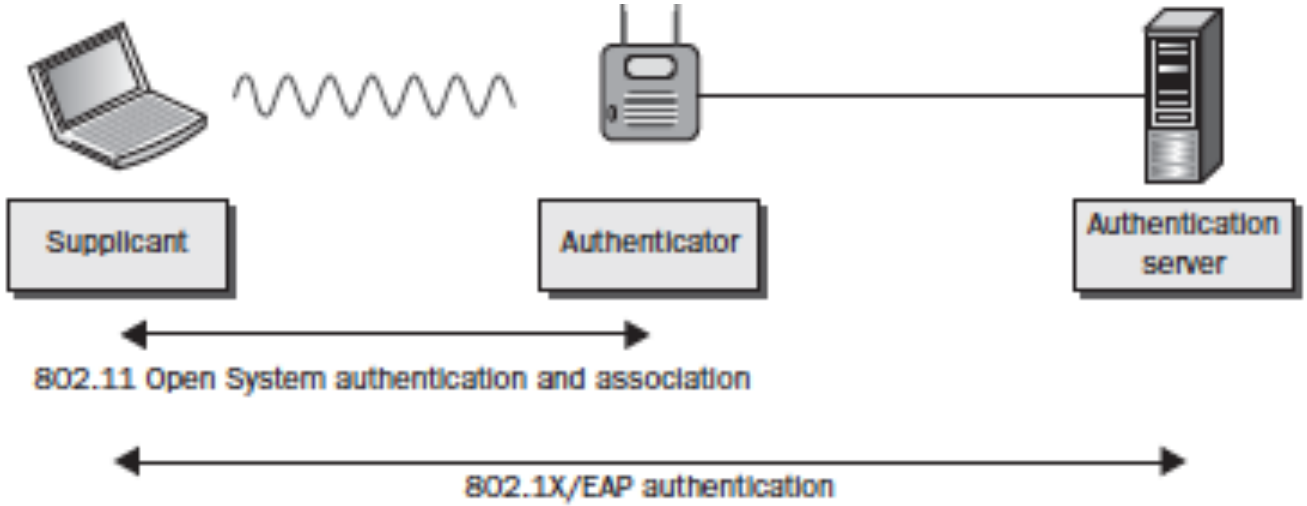


802.1X protocol - Long Story Continue

- 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

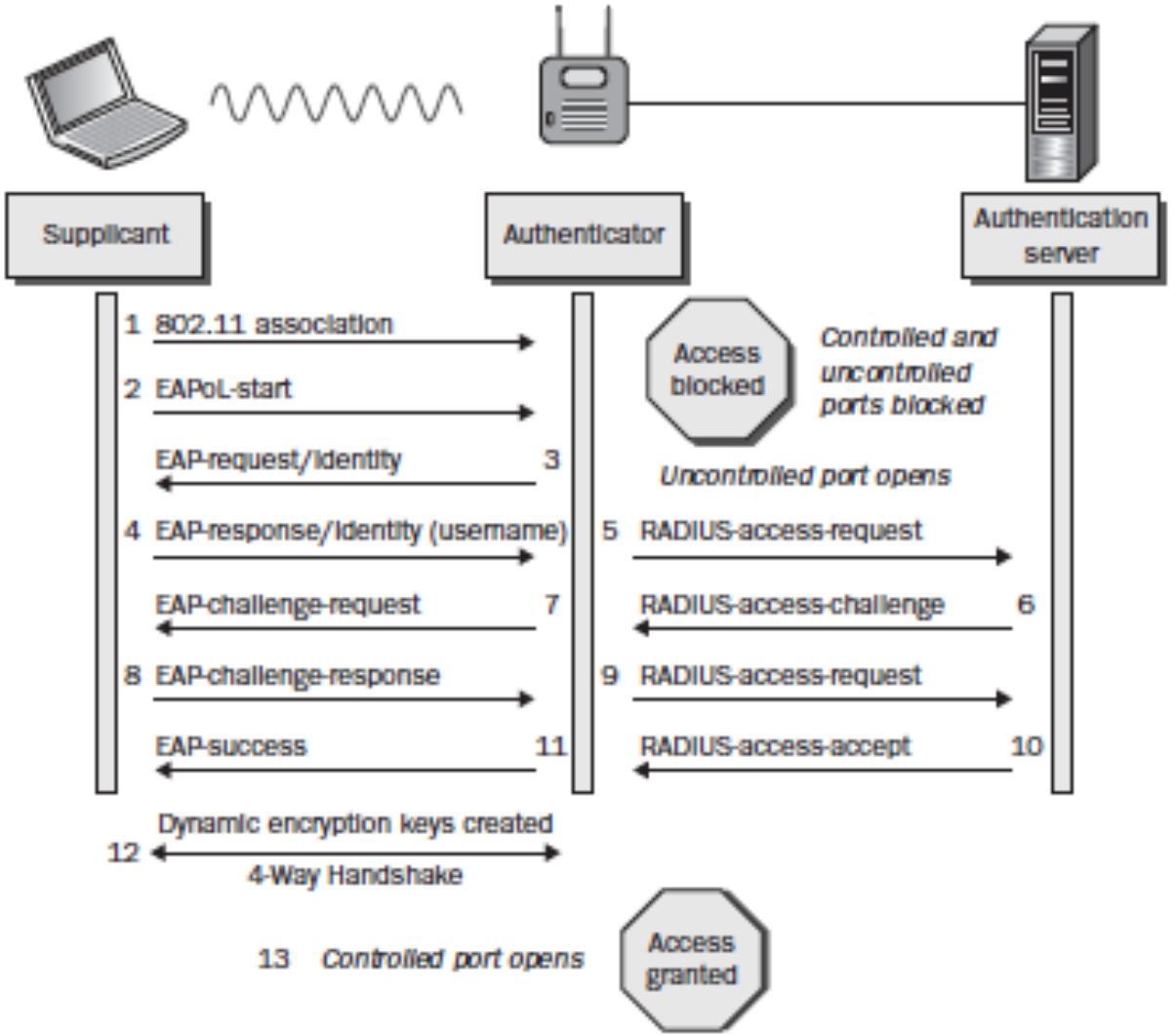
Association and EAP

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



Src: CSWP Text

Generic EAP Exchange



Src: CWSP Text

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 (see additional optional reading foils)
- 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
- No need to remember these acronyms or RFCs (some foils at then end are for optional reading

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.

EAP Tunneled Protocols

Optional reading(not examinable)

- 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.

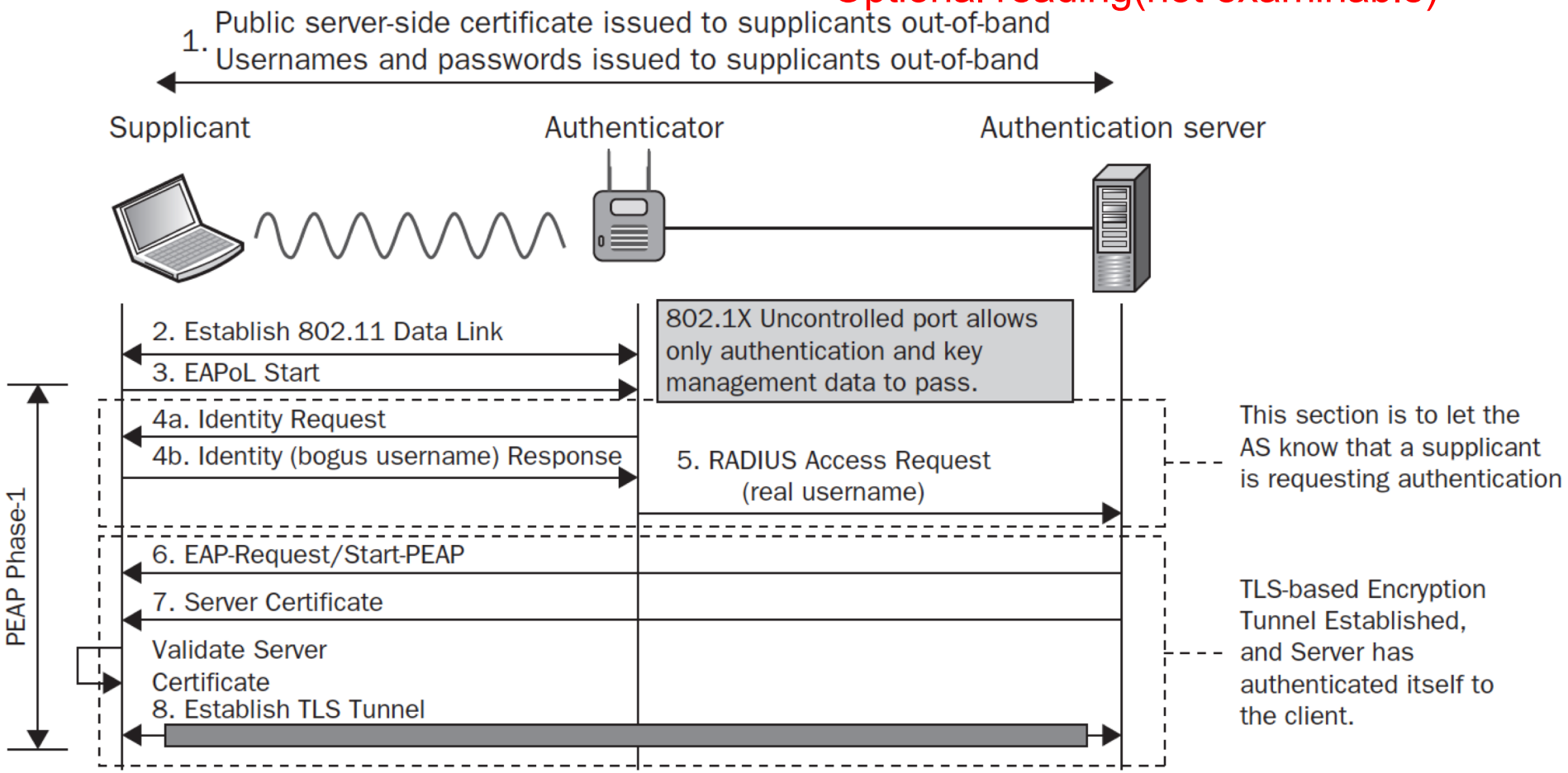
EAP - PEAP

Optional reading(not examinable)

- 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

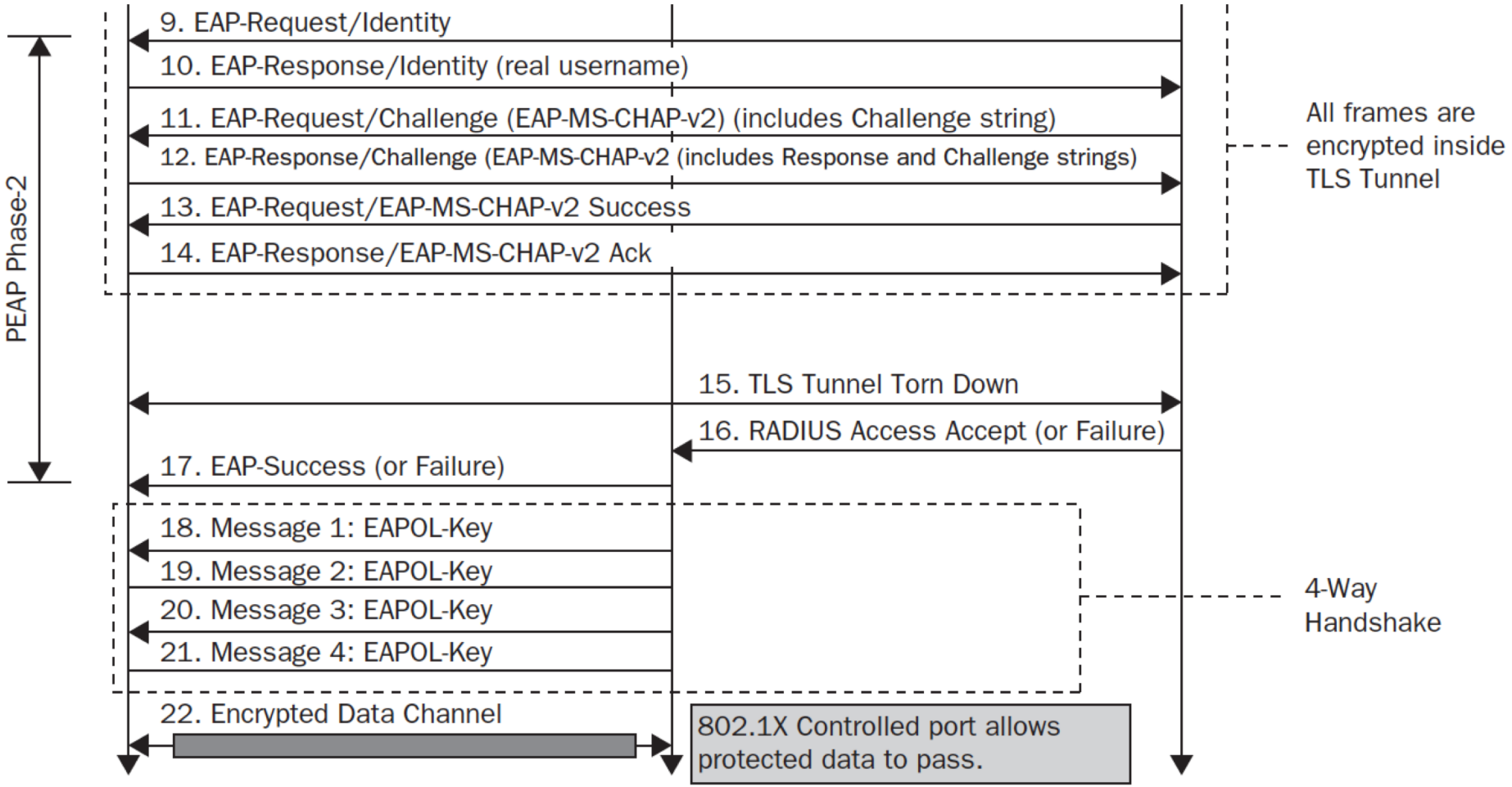
EAP-PEAP Process (Phase1)

Optional reading(not examinable)



Src: CSWP Text

EAP-PEAP (Phase2)



Src: CSWP Text

Optional reading(not examinable)

EAP-TTLS

Optional reading(not examinable)

- 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

EAP-TLS

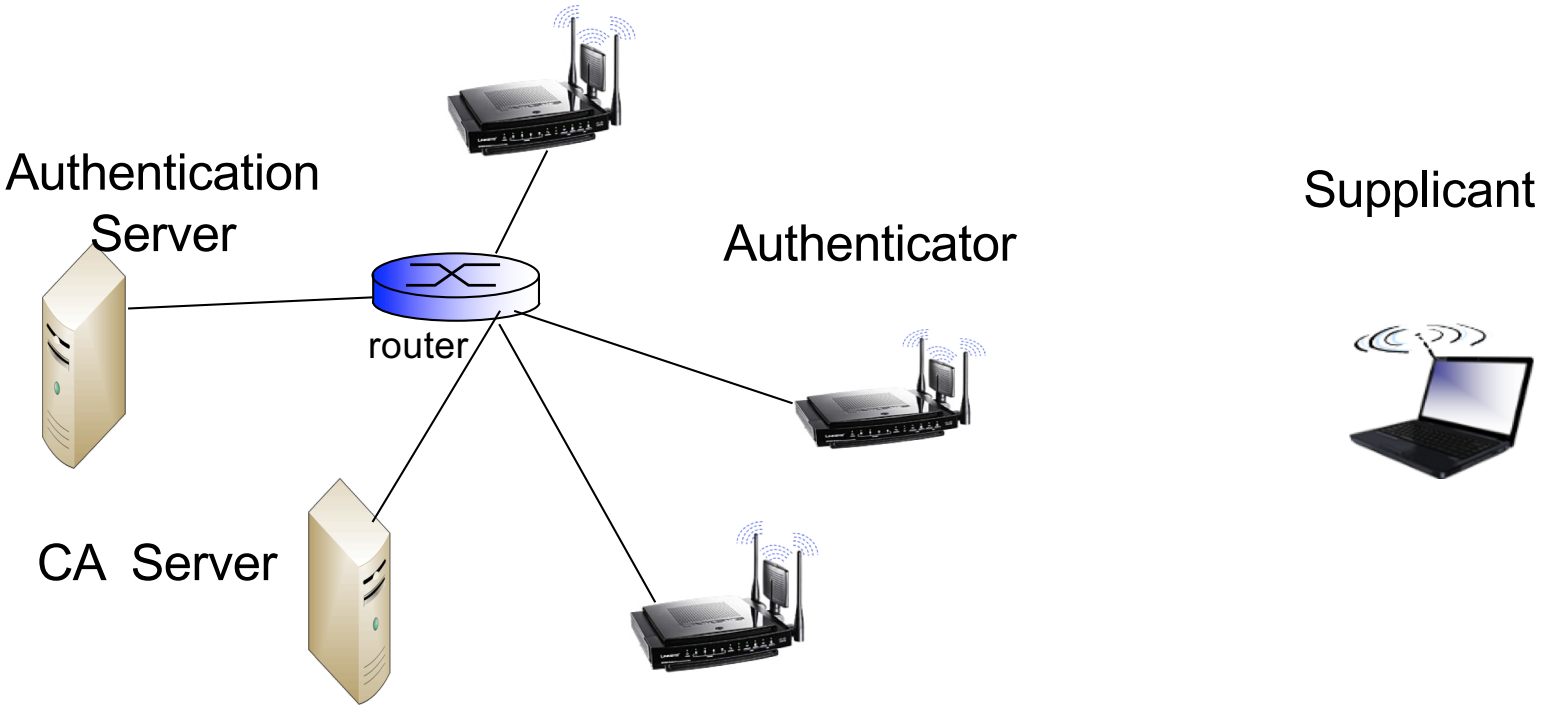
Optional reading(not examinable)

- 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

Optional reading(not examinable)

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



EAP-TLS CA configuration

Optional reading(not examinable)

- 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