Security in IEEE 802.11

FEUP
MPR

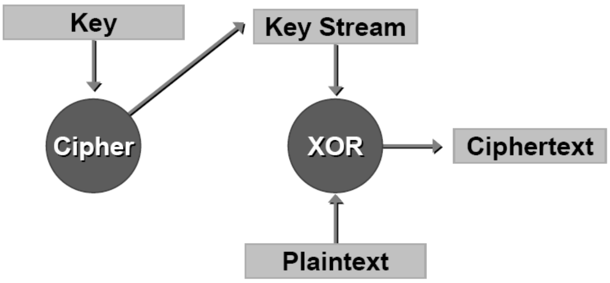
Introduction

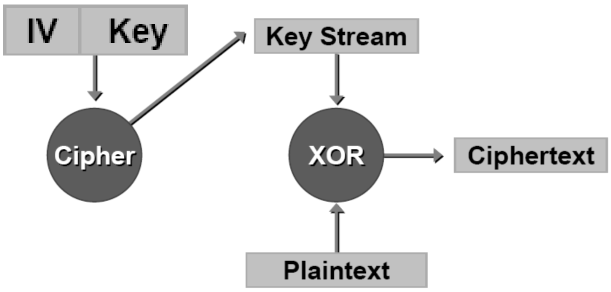
- WEP
- 802.1x
- WPA

WEP

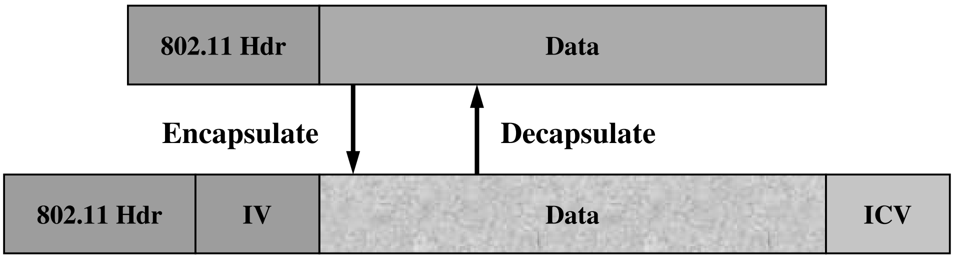
WEP - Wired Equivalent Privacy

- Based on the RC4
  symmetric stream cipher
- 40 bit or 104 bit keys
  - Static, pre-shared
  - client and access point
- Initialization Vector (IV)
  - augments the key
  - Modifies the key stream





WEP Encapsulation



802.11 Hdr | Data

Encapsulate

Decapsulate

802.11 Hdr | IV | Data | ICV

- Key stream
  - – Per packet
  - – Based on 24-bit IV and the pre-shared key
  - – IV can be reused
- 24-bit IV transported in clear
- Data integrity provided in ICV field by a CRC-32
- Data and ICV encrypted

WEP Weaknesses

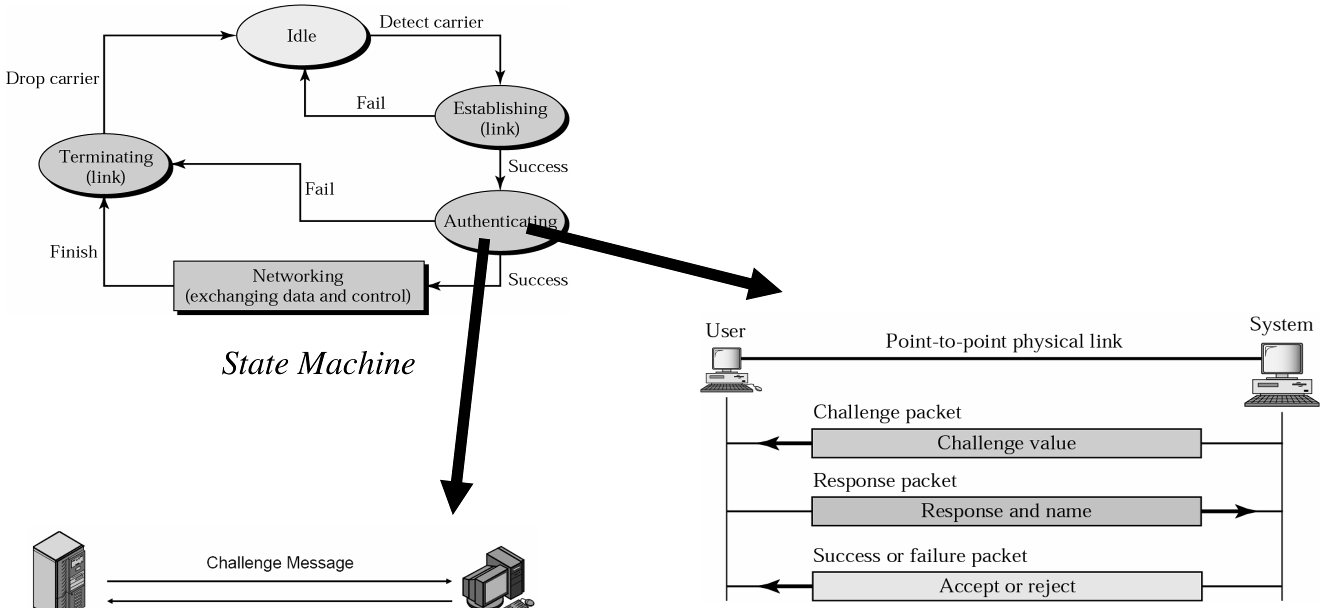
- ♦ Key management and key size are not appropriate
  - – WEP key is changed rarely
  - – WEP key size is small
- ♦ The InitializationVector (IV) is small
  - » 24 bits Ł only 16M different KeyStreams for a WEP key
  - » If *packet1* and *packet2* are encrypted with the same KeyStream
    - – They can be detected   IV values are the same and transported in clear
    - – From RC4: *packet1* xor *packet2* = *encryptedPacket1* xor *encryptedPacket2*
    - – KeyStream and WEP key can be retrieved!
- ♦ Authentication is not appropriate; messages can be forged
  - » The ICV algorithm is not appropriate; based on CRC-32
    - – Used for detecting errors in transmission
    - – Not for signing messages
  - » The well-done authentication of a message would consist of
    - – Generating an hash value of the frame, and signing it by a symmetric or asymmetric key

802.1x

IEEE 802.1x

- IEEE 802.1x depends on
  PPP, EAP and 802.1x itself
- PPP defines also an authentication mechanism
  - to identify the user before giving him access (PAP, CHAP)
  - more flexible security with the *Extensible Authentication Protocol* (EAP)
- Extensible Authentication Protocol (EAP)
  - part of the PPP authentication protocol
  - provides generalized framework for multiple authentication methods
  - Generic Request/Response messages
- IEEE 802.1x
  - transports EAP messages over wired or wireless LANs
    - EAP messages sent over 802.3 (Ethernet) and 802.11, in place of PPP
    - EAP encapsulation over LANs (EAPOL)
    - Protocol messages: EAP + EAPOL-Start, EAPOL-Logoff, EAPOL-key
  - Authentication provided by an external equipment

PPP – Point to Point Protocol



State Machine

MS-CHAP

Challenge Handshake Authentication Protocol (CHAP)

EAP – Extensible Authentication Protocol

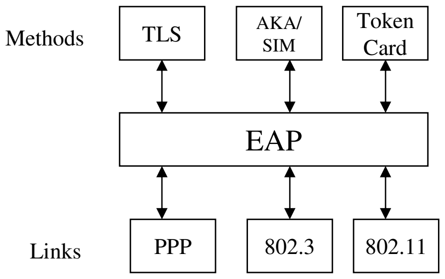
– Encapsulates authentication

– Runs over any link layer

but thought for PPP

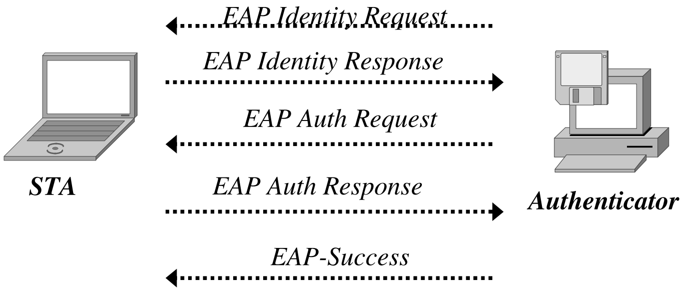
– Messages

Requests and Responses

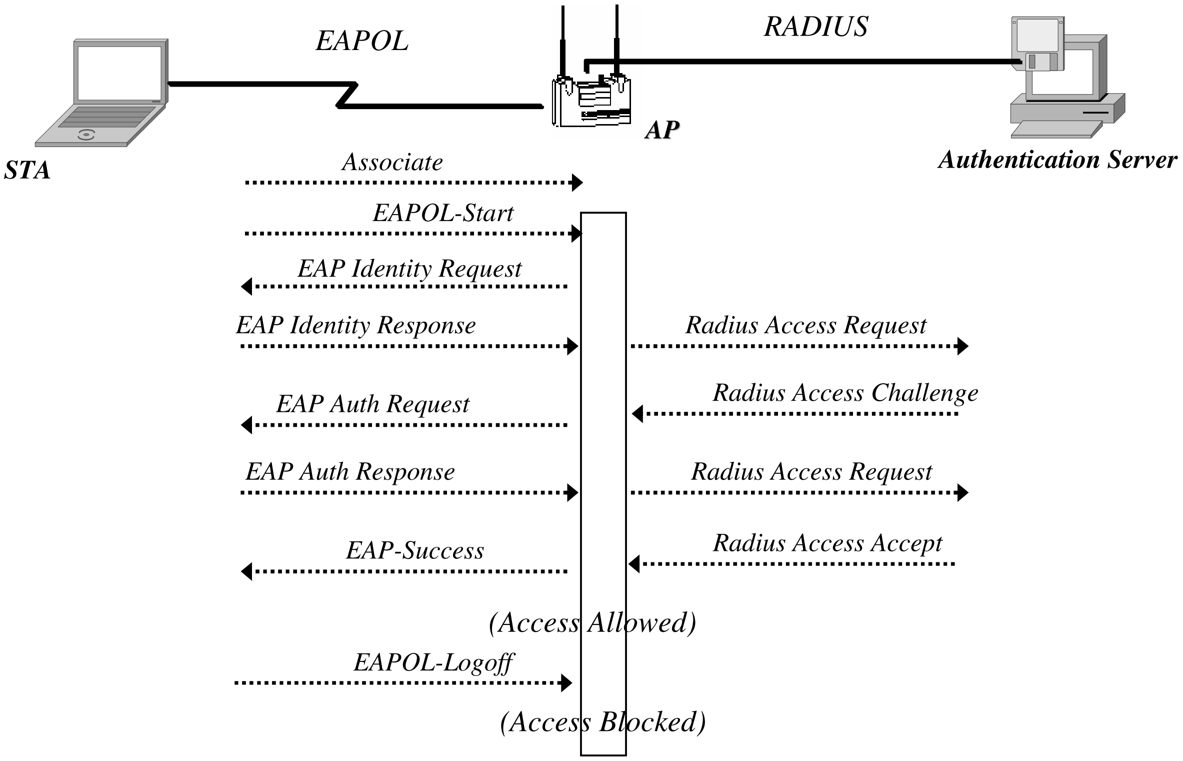


bytes	1	1	2	1	variable
	Code	Identifier	Length	Type	Type-Data

EAP – Extensible Authentication Protocol

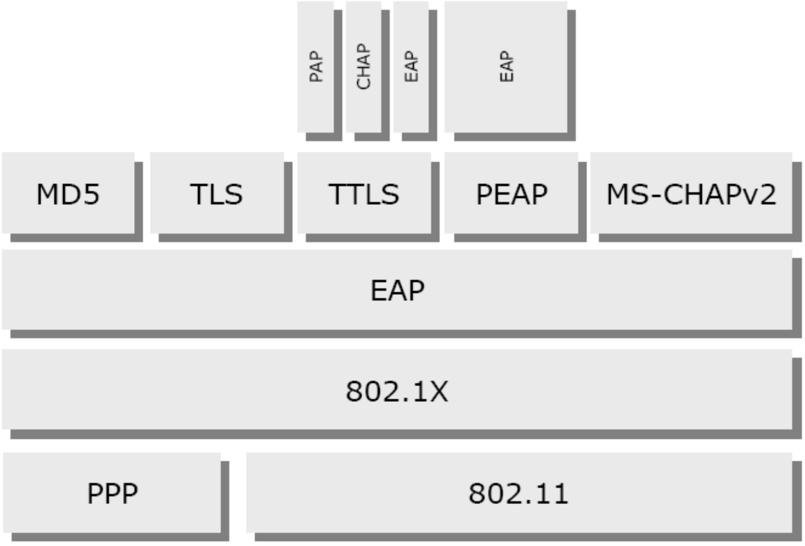


IEEE 802.1x



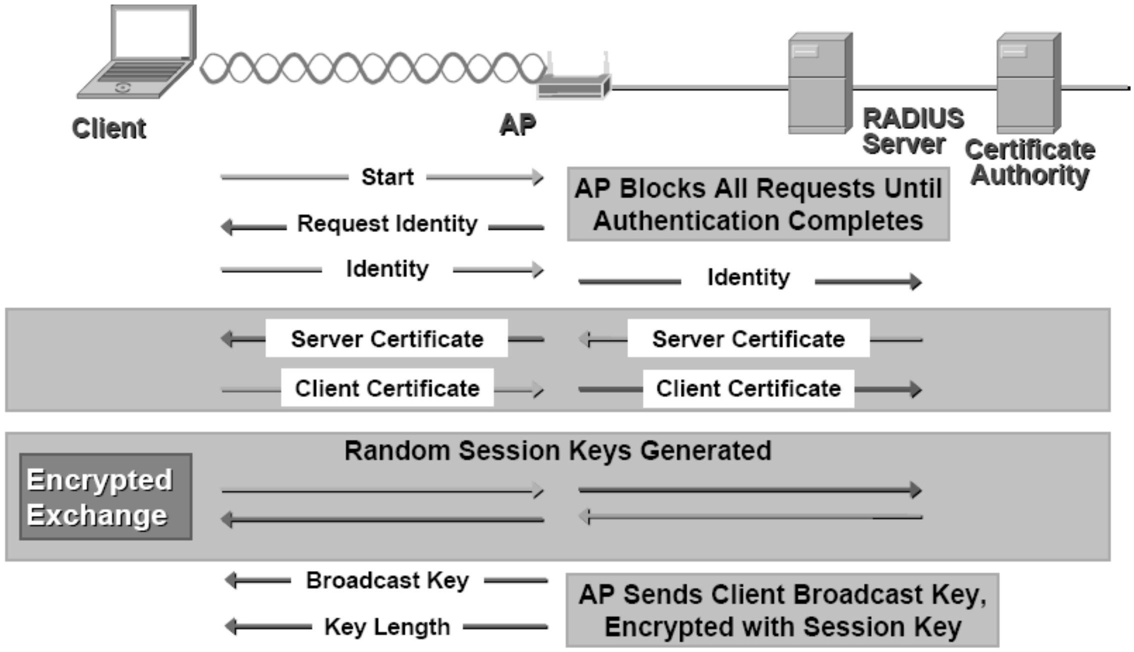
IEEE 802.1x; EAP Authentication Mechanisms

- EAP-MD5
  Username/Password
- EAP-TLSPKI
  certificates
- EAP-TTLS
  Username/Password
- MS-CHAPv2 Microsoft
  Username/Password
- PEAP tunnel
  safe transport of MS-CHAPv2



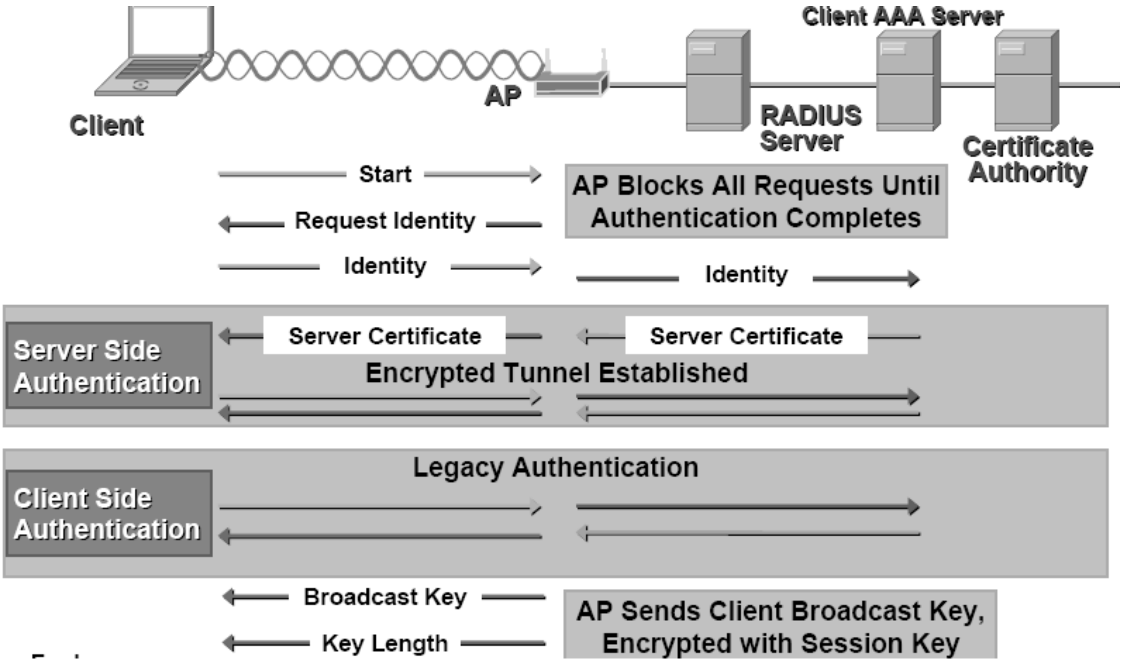
PAP
CHAP
EAP
EAP
MD5
TLS
TTLS
PEAP
MS-CHAPv2
EAP
802.1X
PPP
802.11

EAP-TLS Authentication



Start
Request Identity
Identity
AP Blocks All Requests Until Authentication Completes
Identity
Server Certificate
Server Certificate
Client Certificate
Client Certificate
Random Session Keys Generated
Encrypted Exchange
Broadcast Key
Key Length
AP Sends Client Broadcast Key, Encrypted with Session Key

EAP-TTLS Authentication



Client AAA Server

Client

AP

RADIUS Server

Certificate Authority

Start

Request Identity

Identity

AP Blocks All Requests Until Authentication Completes

Identity

Server Side Authentication

Server Certificate

Server Certificate

Encrypted Tunnel Established

Client Side Authentication

Legacy Authentication

Broadcast Key

Key Length

AP Sends Client Broadcast Key, Encrypted with Session Key

Wi-Fi Protected Access (WPA)

- Promoted by the Wi-Fi Alliance; based on 802.11i
  - Provides dynamic key encryption and mutual authentication
  - Uses
    - Temporal Key Integrity Protocol (TKIP)
    - 802.1x authentication mechanisms
- Temporal Key Integrity Protocol (TKIP)
  - uses RC4 to encrypt 802.11 frames   similar to WEP
  - uses 48-bit InitializationVectors   reduce significantly IV reuse
  - generates automatically and periodically
    - A new unique encryption key for each client
    - aimed at providing a unique key for each 802.11 frame
  - introduces a new 8 byte Message Integrity Code (MIC)
    - just before the ICV field