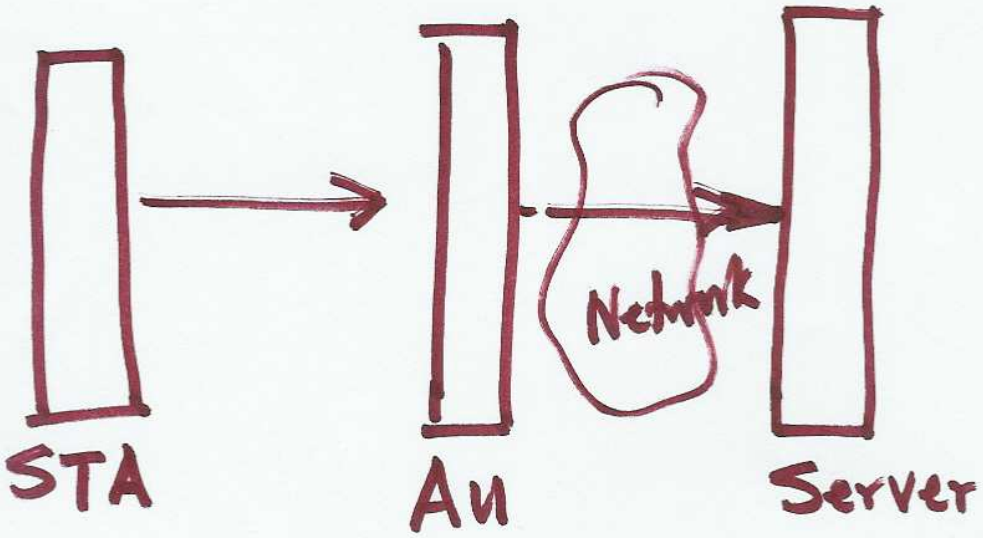
2/13/07



IEEE 802.11

Kerberos VS

Transport Layer Security (TLS)

Protected EAP (PEAP)

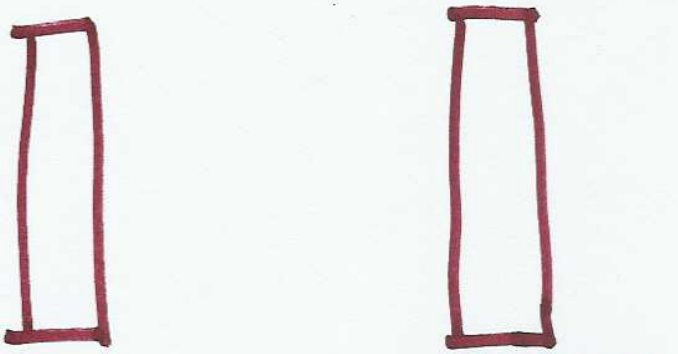
Cellular Phone Authentication

Wi-Fi Alliance

TLS

+ EAP

TLS (Server.client model)



client

Session

C → S: client Hello
List of ciphersuites,
Compression method,
C.nonce (random)

CipherSuite = { Encryption method, Type of Certificates, integrity check method }

S → C : Server Hello

S. nonce, Session ID

S → C : Server Certificate

name, public key of the server, signed by Certificate authority

C. nonce, S. nonce, Session ID

C → S : Certificate - (Optional)

(in the future - require)

C → S : Key Exchange

Create a pre-master key

Generate 48 bit random no.

encrypt with the public Key of S

client → S: client Verification

Hash (Copies of all messages)

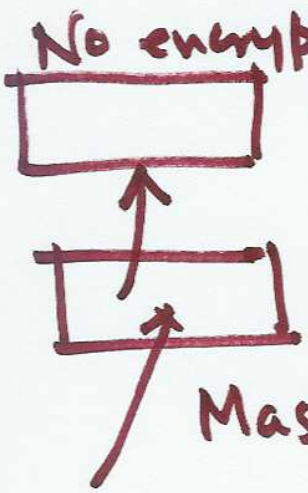
+ Signs the message

S - checks the message

Hash (C.nonce, S.nonce, 48 bit random number)

→ 384 bit number.

Master key

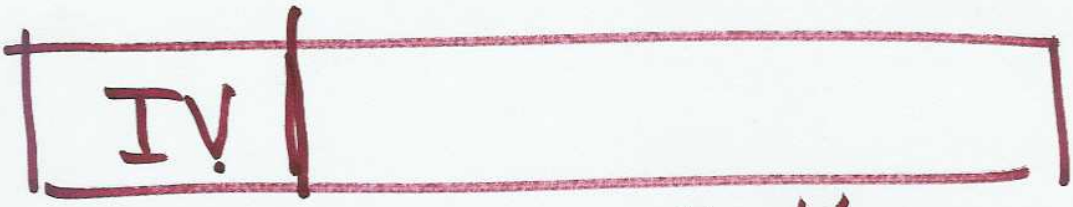


Change their state and notify each other.

Finished message.

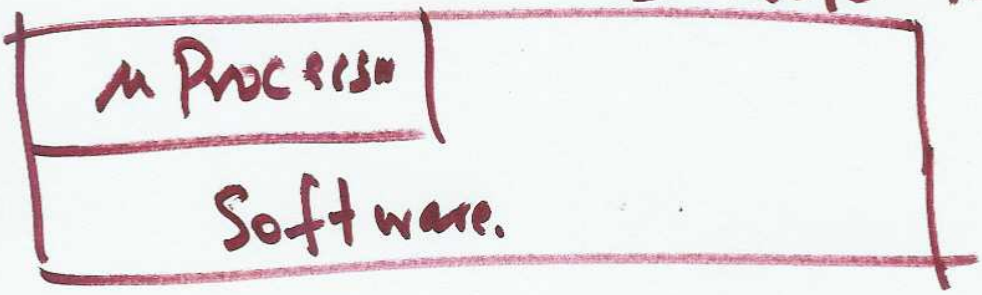
WEP

104 bit
40 bit key



24bits

4 Keys =
2 Keys for Access PT
2 Keys for Sta



WEP
TKIP
EAP
TLS

Wi-Fi LAN

|

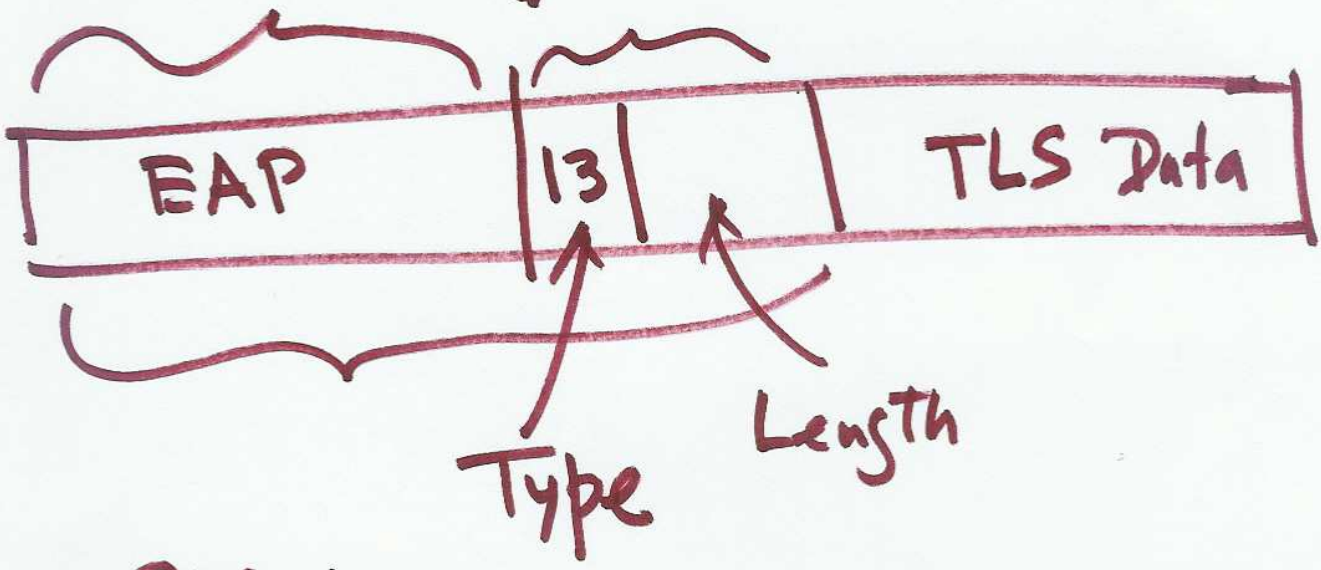
Access Control

|

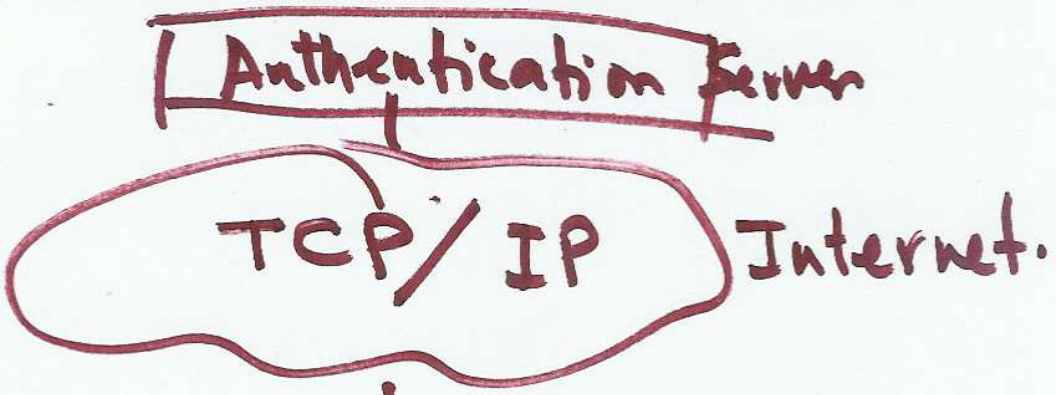
Authentication

TLS - EAP

EAPOL



802.1x



Access Control

Wireless lan

SSL

TLS. (Transport Layer Security)

Kerberos V5