IEEE 802.11

Kerberos VS

Transport Layer Security (TLS)

Protected EAP (PEAP)

Cellular Phone Authentication

Wi-Fi Alliance

TLS

LEAP
TLS (Server, Client model)

Session

C → S: Client Hello
List of Ciphersuites, Compression method,
C:Nonce (random)

CipherSuite = \{ Encrypt method, Type of Certificates, integrity check method \}
$S \rightarrow C$: Server Hello
$S.nonce, Session ID$

$S \rightarrow C$: Server Certificate
name, public key of the server, signed by Certificate authority

$C.nonce, S.nonce, Session ID$

$C \rightarrow S$: Certificate (Optional)
(in the future - require)

$C \rightarrow S$: Key Exchange
Create a pre-master key
Cement 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

No encryption

Current state

pending state

Master Key

Finished message.
WEP

IV

104 bit
40 bit key

24 bits

4 Keys =

2 Keys for Access pt
2 Keys for sta

Software

WEP

TKIP

EAP

TLS
Wi-Fi Lan

Access Control

Authentication

TLS - EAP - EAPOL

EAP

802.1x
Authentication Server

TCP/IP

Internet

Access Control

Wireless Lan

SSL

TLS (Transport Layer Security)

Kerberos v5