THE UNIVERSITY OF BRITISH COLUMBIA

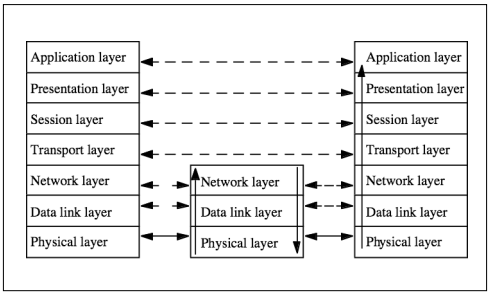
Network Security

EECE 412

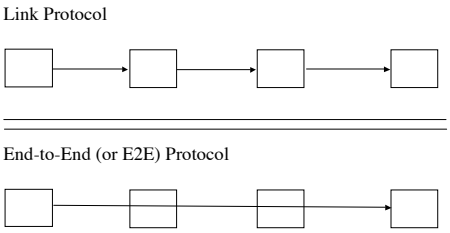
Outline

- Link & end-to-end protocols
- SSL/TLS
- WPA

Networks



Link and End-to-End Protocols



Examples

- Telnet protocol
  - Messages between client, server enciphered, and
    - encipherment/decipherment occur only at these hosts
  - End-to-end protocol
- PPP Encryption Control Protocol
  - Host gets message, deciphers it
    - Figures out where to forward it
    - Enciphers it in appropriate key and forwards it
  - Link protocol

Link vs. End-to-end protection

Link encryption

- Can protect headers of packets
- Possible to hide source and destination
  - Note: may be able to deduce this from traffic flows

End-to-end encryption

- Cannot hide packet headers
- Attacker can read source, destination

Example Protocols

- Privacy-Enhanced Electronic Mail (PEM)
  - Applications layer protocol
  - Bishop
- Secure Socket Layer (SSL)/Transport Layer Security (TLS)
  - Transport layer protocol
- IP Security (IPSec)
  - Network layer protocol
  - Bishop
- Wi-Fi Protected Access (WPA)
  - Data layer protocol
  - Today session

7

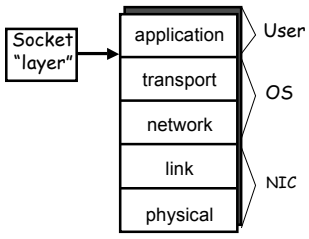
Secure Socket Layer

From "Information Security: Principles and Practice" by Mark Stamp

8

Socket layer

- "Socket layer" lives between application and transport layers
- SSL usually lies between HTTP and TCP



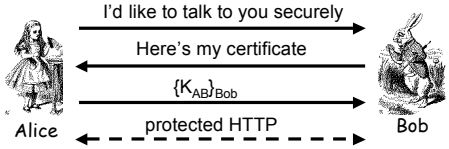
9

What is SSL?

- SSL is the protocol used for most secure transactions over the Internet
- For example, if you want to buy a book at amazon.com…
  - You want to be sure you are dealing with Amazon (**authentication**)
  - Your credit card information must be protected in transit (**confidentiality** and/or **integrity**)
  - As long as you have money, Amazon doesn't care who you are (authentication need not be mutual)

10

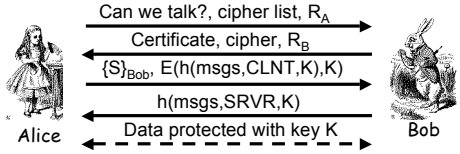
Simple SSL-like Protocol



- Is Alice sure she's talking to Bob?
- Is Bob sure he's talking to Alice?

11

Simplified SSL Protocol



- S is **pre-master secret**
- $K = h(S,R_A,R_B)$
- msgs = all previous messages
- CLNT and SRVR are constants

12

SSL Keys

- 6 "keys" derived from $K = hash(S,R_A,R_B)$
  - 2 encryption keys: send and receive
  - 2 integrity keys: send and receive
  - 2 IVs: send and receive
  - Why different keys in each direction?
- **Q:** Why is $h(msgs,CLNT,K)$ encrypted (and integrity protected)?
- **A:** It adds no security…

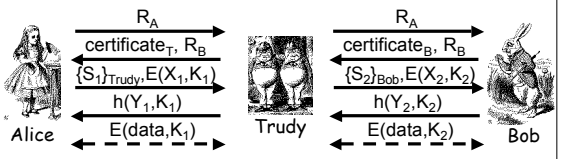
13

SSL Authentication

- Alice authenticates Bob, not vice-versa
  - How does client authenticate server?
  - Why does server not authenticate client?
- Mutual authentication is possible: Bob sends **certificate request** in message 2
  - This requires client to have certificate
  - If server wants to authenticate client, server could instead require (encrypted) password

14

SSL MiM Attack



- **Q:** What prevents this MiM attack?
- **A:** Bob's certificate must be signed by a certificate authority (such as Verisign)
- What does Web browser do if sig. not valid?
- What does user do if signature is not valid?

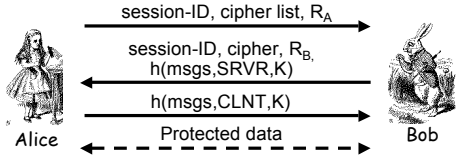
15

SSL Sessions vs Connections

- SSL **session** is established as shown on previous slides
- SSL designed for use with HTTP 1.0
- HTTP 1.0 usually opens multiple simultaneous (parallel) **connections**
- SSL session establishment is costly
  - Due to public key operations
- SSL has an efficient protocol for opening new connections given an existing session

16

SSL Connection



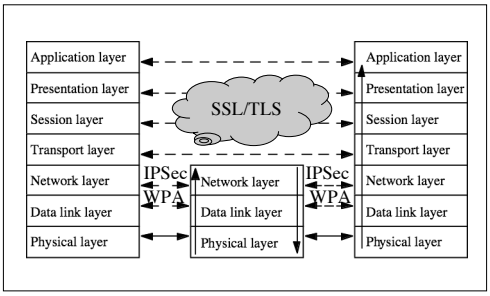
- Assuming SSL **session** exists
- So S is already known to Alice and Bob
- Both sides must remember session-ID
- Again, $K = h(S,R_A,R_B)$
  - **No public key operations!** (relies on known S)

17

THE UNIVERSITY OF BRITISH COLUMBIA

Wi-Fi Protected Access (WPA)

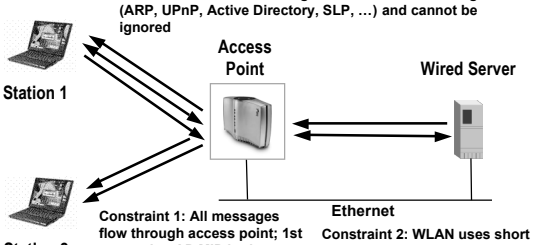
Where is WPA?



19

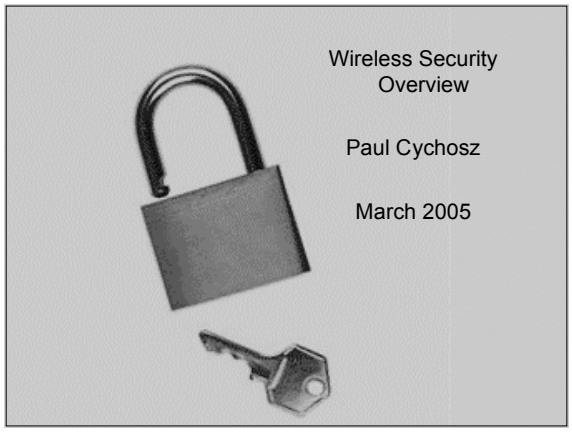
Design Constraints

Constraint 3: Multicast integral to modern networking (ARP, UPnP, Active Directory, SLP, …) and cannot be ignored



Constraint 1: All messages flow through access point; 1st generation AP MIP budget = 4 Million instructions/sec

Constraint 2: WLAN uses short range radios, so APs must be ubiquitous, so lowest cost



Wireless Security Overview

Paul Cychosz

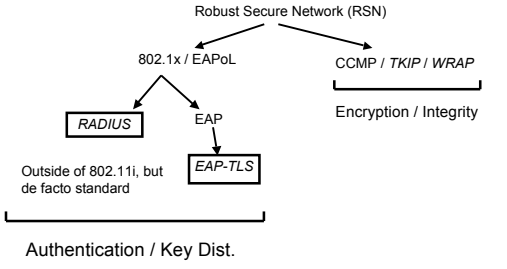
March 2005

802.11i

Terms:

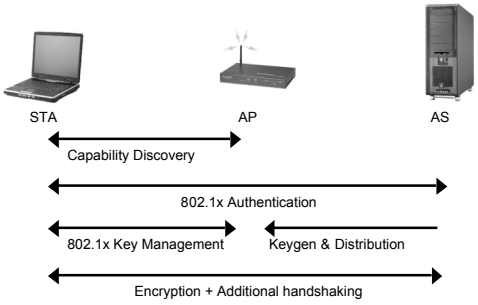
- 802.1x: Authentication standard
- RADIUS: Authentication Server
- EAP: Extensible Authentication Protocol
- CCMP: Encryption based on AES counter mode with CBC-MAC

802.11i Parts



23

802.11i – First half

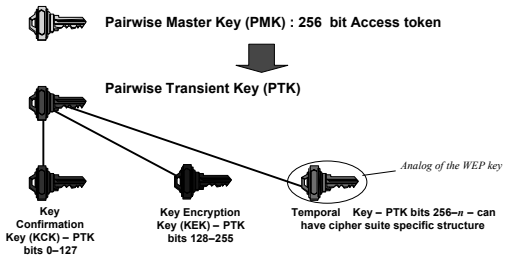


24

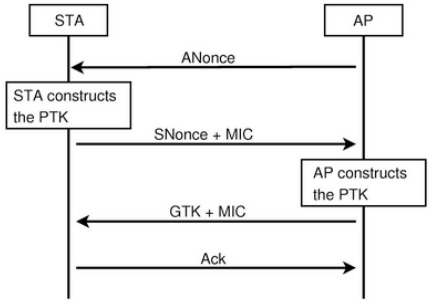
THE UNIVERSITY OF BRITISH COLUMBIA

WPA Key Managment

802.11i Pairwise Key Hierarchy

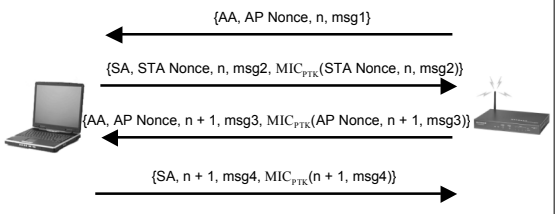


Session Key Establishment



27

Handshake Details



28

Message 1

- not protected, doesn't matter though

AP → STA: {AA, AP Nonce, n, msg1}

AA: MAC Address of AP

AP Nonce: random value

n: sequence identifier

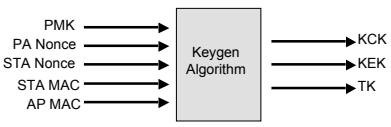
msg1: PMKID = HMAC-SHA1-128(PMK, "PMK Name" || AA || SPA).

•Client uses AP Nonce and PMK to compute PTK

PTK = 802.11i-PRF(
PMK,
min(AP Nonce, STA Nonce) || max(AP nonce, STA Nonce) ||
min(AP MAC Addr, STA MC Addr) || max(AP MAC Addr, STA MAC Addr))

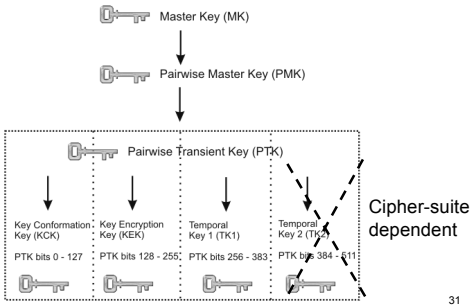
29

802.11i – What's PTK?



30

802.11i – Key Heirarchy



31

Message 2

STA → AP: {SA, STA Nonce, n, msg2, MIC_{PTK}(STA Nonce, n, msg2)}

SPA: MAC Address of STA

SNonce: random value

n: sequence identifier, matches msg1

msg2: RSN IE of STA

- AP uses STA Nonce and PMK to compute PTK

32

Message 3

AP → STA: {AA, AP Nonce, n + 1, msg3, MIC_{PTK}(AP Nonce, n + 1, msg3)}

AA: MAC Address of AP

AP Nonce: random value again

n: sequence identifier, to match msg4

msg3: Informs STA that TK ready to use, RSN IE of AP.

MIC: to verify the above. Silently discarded if MIC fails.

Verifies no MITM attack happening

33

Message 4

STA → AP: {SPA, n + 1, msg4, MIC_{PTK}(n + 1, msg4)}

SPA: MAC Address of STA

n: sequence identifier, to match msg3

MIC: to verify the above. Silently discarded if MIC fails.

- This message dropped in some implementations.
- Only kept for convention

34

WPA Data Protection

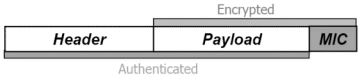
35

AES-CCMP

- New encryption based on AES

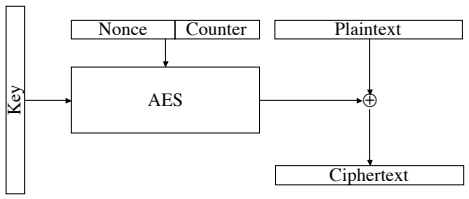
" NIST estimates that a machine that can break 56-bit DES key in 1 second would take about 149 trillion years to crack a 128-bit AES key (unless someone is very lucky)"

- CCMP: Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
  - Confidentiality protection: counter mode
  - Authenticity and integrity protection: CBC-MAC



36

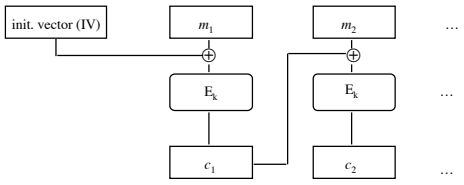
AES-CCMP: Counter Mode Encryption



37

Cipher Block Chaining (CBC)

$M = m_1 \mid m_2 \mid \ldots \mid m_n$



$C = IV \mid c_1 \mid c_2 \mid \ldots \mid c_n$

38

Integrity and authenticity Protection

MIC: CBC-MAC / per packet algorithm

- 128-bit generation, but only take first 64-bits
- XOR blocks, hence "block-chaining"
- MIC computed on packet header
- MIC then encrypted (using IV = 0, CTR mode) and appended to payload

39