Wireless Network Security

Raj Jain
Washington University in Saint Louis
Saint Louis, MO 63130
Jain@cse.wustl.edu

Audio/Video recordings of this lecture are available at:

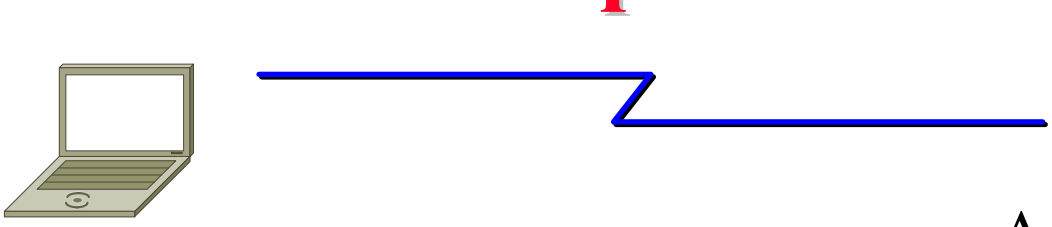
http://www.cse.wustl.edu/~jain/cse571-11/

Overview

1. IEEE 802.11 Wireless LAN Overview
2. Legacy 802.11 Security: WEP
3. IEEE 802.11i Wireless LAN Security: WPA, WPA2
4. Wireless Application Protocol (WAP) Overview
5. Wireless Transport Layer (WTLS) Security

These slides are based partly on Lawrie Brown's slides supplied with William Stallings's book "Cryptography and Network Security: Principles and Practice," 5th Ed, 2011.

Wi-Fi Operation



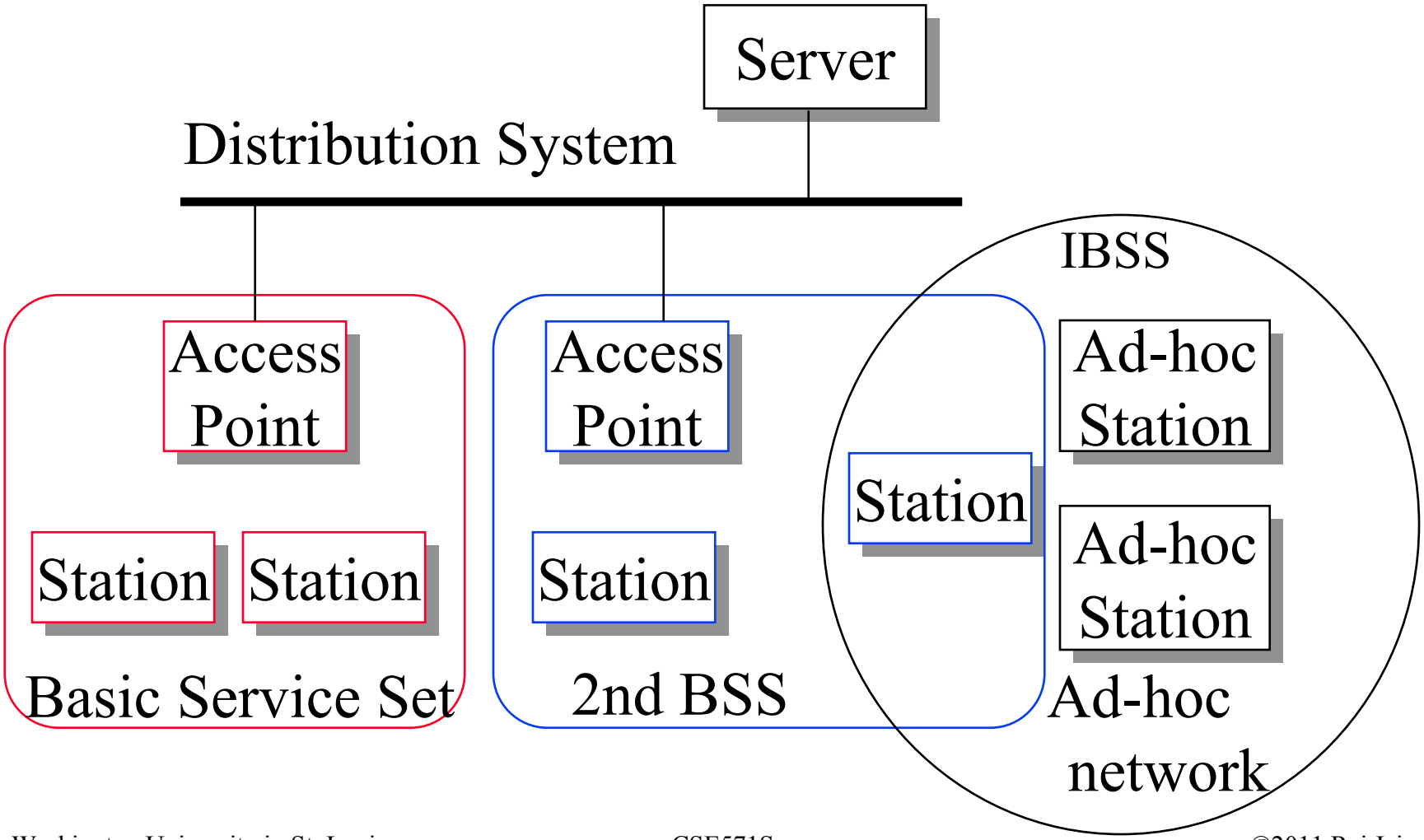
Station

Access Point

- Access Points (APs) periodically broadcast a beacon with SSID (service set ID) and security level
- Subscriber stations listen to these beacons, measure signal strength and determine which AP to join
- Subscribers can also send a "Probe" to find AP's in the neighborhood
- AP authenticates the subscriber station using shared keys
- Subscriber stations and AP exchange encrypted packets
- Subscriber station send a "Disassociate" message and log off

Ref: http://en.wikipedia.org/wiki/Service_set_%28802.11_network%29

IEEE 802.11 Architecture



IEEE 802.11 Architecture (Cont)

- Basic Service Area (BSA) = Cell
- Each BSA may have several access points (APs)
- Basic Service Set (BSS)
  = Set of stations associated with one AP
- Distribution System (DS) - wired backbone
- Extended Service Area (ESA) = Multiple BSAs interconnected via a distribution system
- Extended Service Set (ESS)
  = Set of stations in an ESA
- Independent Basic Service Set (IBSS): Set of computers in ad-hoc mode. May not be connected to wired backbone.
- Ad-hoc networks coexist and interoperate with infrastructure-based networks

IEEE 802.11 Services

- **Association**: A STA connecting with an AP.
- **Disassociation**: Termination of association.
- **Re-association**: Transfer of association from one AP to another. Mobility within BSS, within ESS, between two ESSs.
- **MSDU Delivery**: Interchange of packets between STAs
- **Distribution**: Delivery of packets between STAs possibly via the backbone distribution system
- **Integration**: Interchange of packets between STAs and wired stations connected to LANs on the distribution system
- **Authentication**: The station is authenticated
- **De-authentication**
- **Privacy**: Encryption

Wired Equivalent Privacy (WEP)

- WEP ⇒ Privacy similar to a wired network
  ⇒ Intellectual property not exposed to casual browser
  ⇒ Not protect from hacker
- First encryption standard for wireless. Defined in 802.11b
- Provides authentication and encryption
- Shared Key Authentication
  ⇒ Single key is shared by all users and access points
- Two modes of authentication: Open system and Shared Key
- Shared Key: Challenge-response verifies client has the key
- Manual key distribution
- If an adapter or AP is lost, all devices must be re-keyed

WEP Review

- Four 40-bit or 104-bit Keys are manually programmed in each subscriber station and AP
- A 24-bit IV and WEP key is used to form a 64b or 128b RC4 key
- A keystream is generated using the RC4 key
- A 32-bit CRC is added as "Integrity check value" (ICV) to the packet
- Plain text and keystream is xor'ed. A 32-bit CRC is added in clear.

Ref: http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy, http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access

WEP Problems

- No centralized key management
  Manual key distribution ⇒ Difficult to change keys
- Single set of Keys shared by all ⇒ Frequent changes necessary
- No mutual authentication
- No user management (no use of RADIUS)
- IV value is too short. Not protected from reuse.
- Weak integrity check.
- Directly uses master key
- No protection against replay

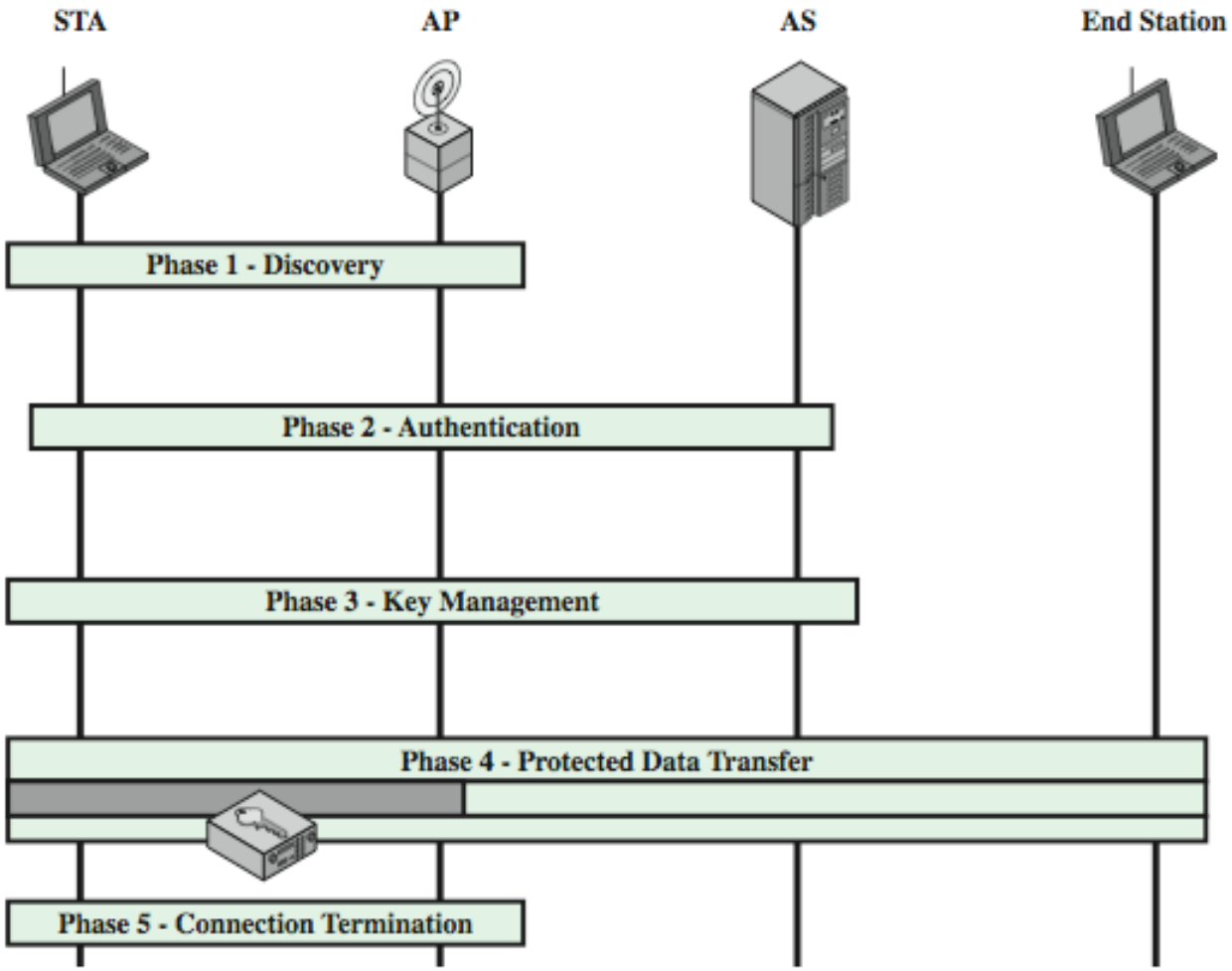
Ref: http://en.wikipedia.org/wiki/Wireless_security, http://en.wikipedia.org/wiki/Wireless_LAN_security, http://en.wikipedia.org/wiki/Cracking_of_wireless_networks

802.11i Wireless LAN Security

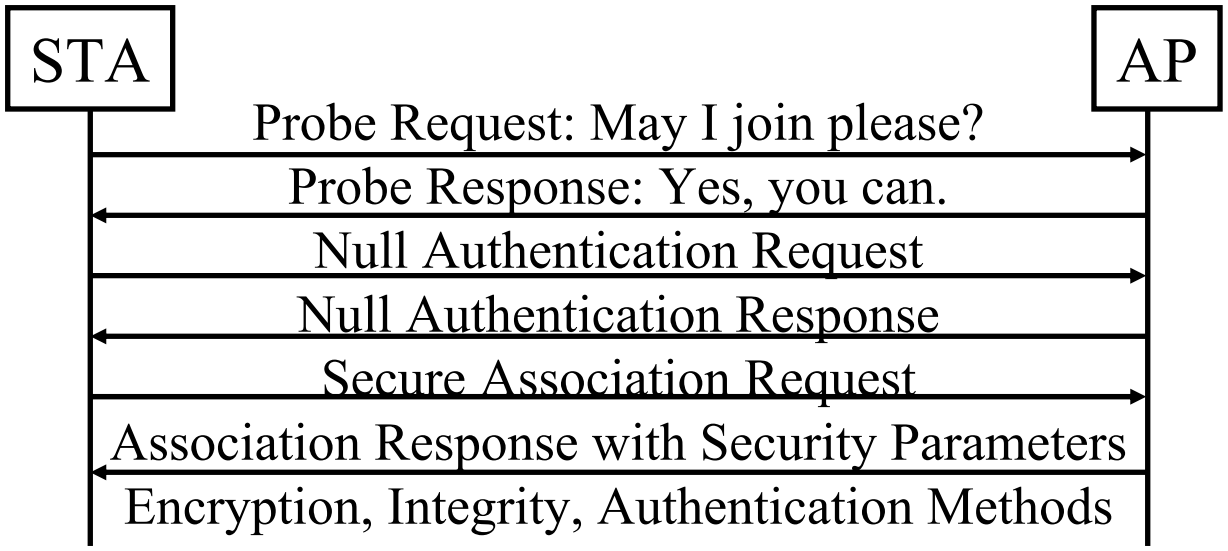
- Wi-Fi Alliance **Wi-Fi Protected Access (WPA)**
  Software modification to existing WEP systems
  - Key mixing function to generate per packet key
  - Sequence Number to protect against replay attacks
  - 64-bit message integrity check (MIC)
  - Uses the same RC4 encryption
- 802.11i **Robust Security Network (RSN) or WPA2**
  Requires hardware replacement
  - Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)
  - AES encryption with counter mode

Ref: http://en.wikipedia.org/wiki/IEEE_802.11i-2004, http://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol, http://en.wikipedia.org/wiki/CCMP

802.11i Phases of Operation



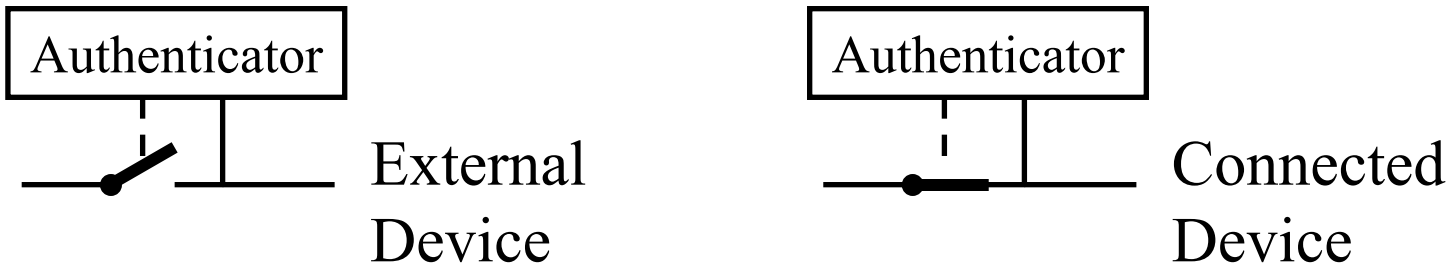
IEEE 802.11i Discovery Phase



- Capability negotiation
  - Confidentiality and Integrity: WEP, TKIP, CCMP, vendor specific
  - Authentication: 802.1x, Pre-shared key, vendor specific

802.1X

- Authentication *framework* for IEEE802 networks
- Supplicant (Client), Authenticator (Access point), Authentication server
- No per packet overhead ⇒ Can run at any speed
- Need to upgrade only driver on NIC and firmware on switches
- User is not allowed to send any data until authenticated



Ref: http://en.wikipedia.org/wiki/802.1x

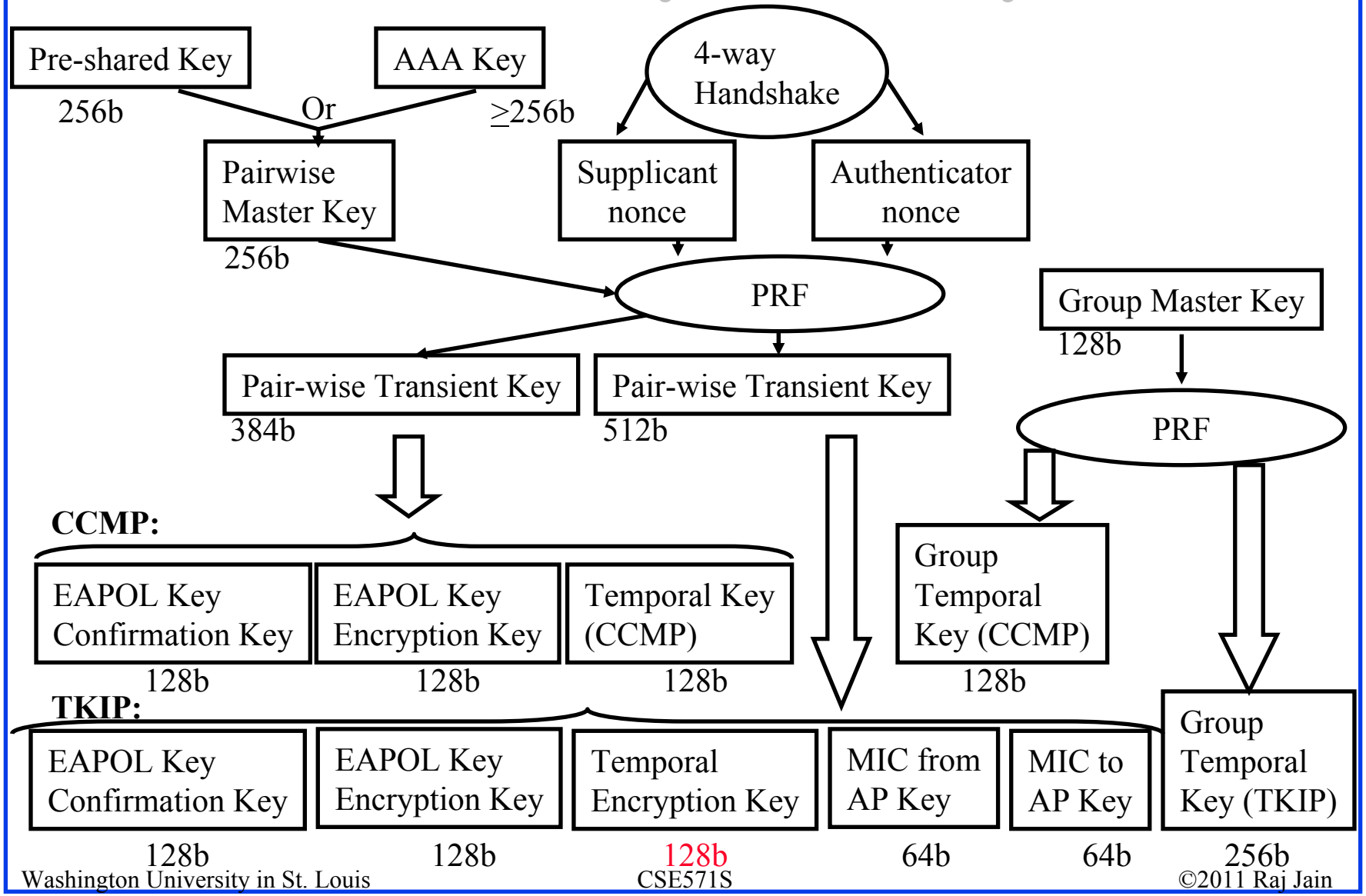
802.1X Authentication

Station | **Access Point** | **Authentication Server**

Can I connect please?	Associate	
What's your user name?	EAP Identity Request	
My user name is john	EAP Identity Response	EAP Identity Response
What's your password?	EAP Auth Request	EAP Auth Request
My password is mary?	EAP Auth Response	EAP Auth Response
You can connect!	EAP-Success	EAP-Success

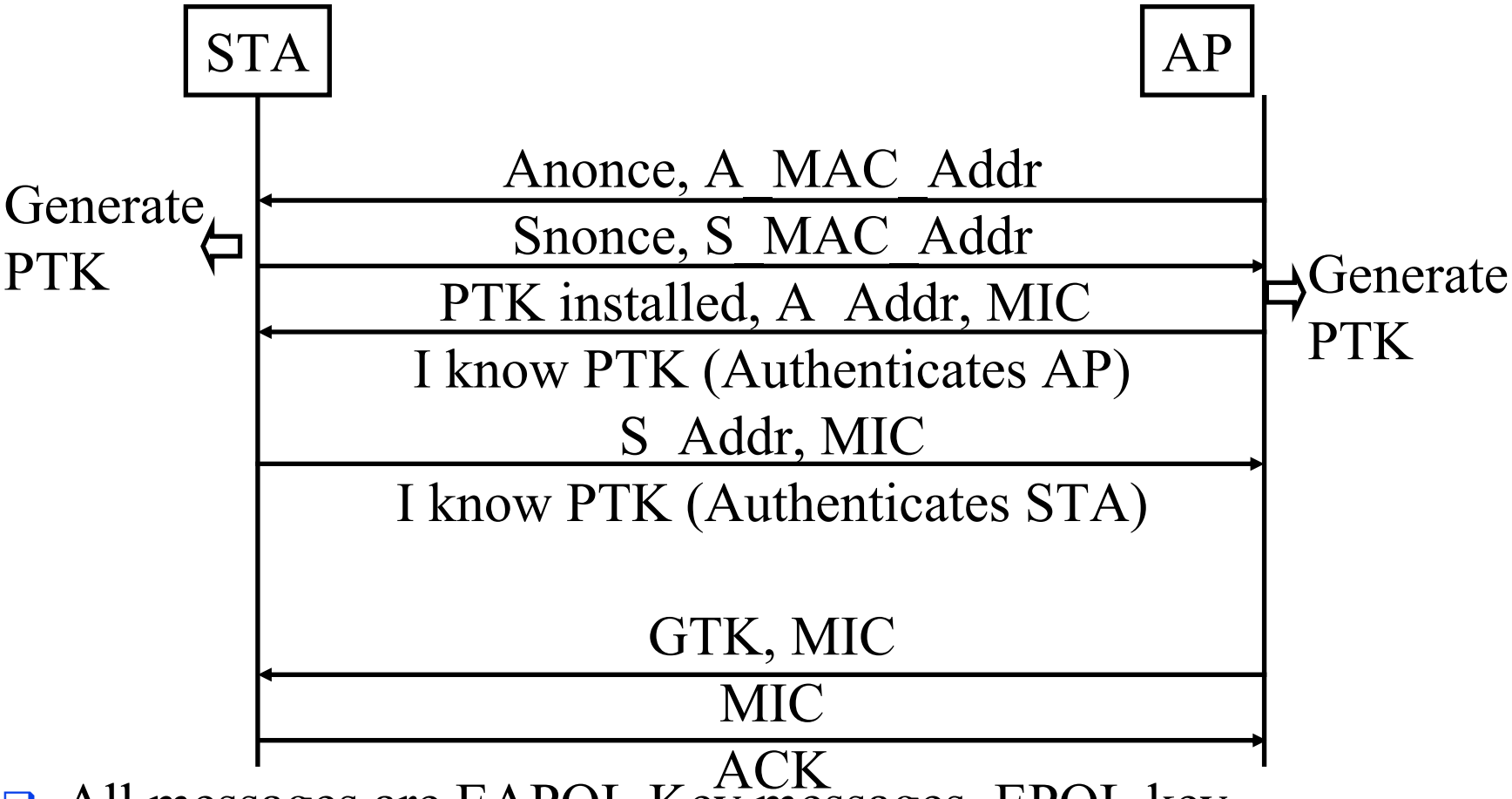
- Authentication method can be changed without upgrading switches and access points
- Only the client and authentication server need to implement the authentication method

802.11i Key Hierarchy



©2011 Raj Jain

Key Management



- All messages are EAPOL Key messages. EPOL key confirmation key is used to compute MIC for EPOL messages.

Ref: http://en.wikipedia.org/wiki/IEEE_802.11i-2004

©2011 Raj Jain

802.11i Protected Data Transfer Phase

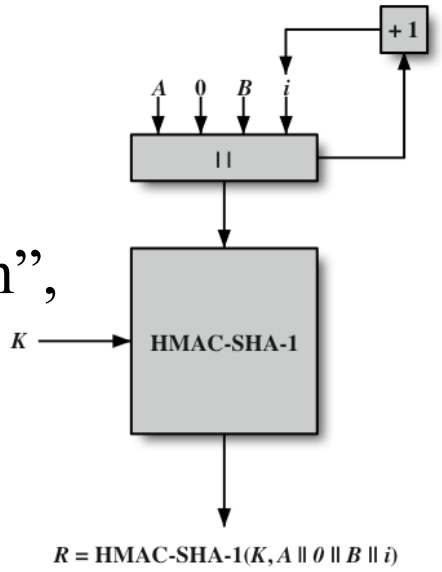
Two schemes for protecting data

- Temporal Key Integrity Protocol (TKIP)
  - S/w changes only to older WEP
  - Adds 64b Michael message integrity code (MIC) instead of 32b CRC in WEP
  - Encrypts MPDU plus MIC value using 128b RC4
- Counter Mode-CBC MAC Protocol (CCMP)
  - Uses cipher block chaining message authentication code (CBC-MAC) for integrity
  - Uses Counter mode AES for encryption

Ref: http://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol, http://en.wikipedia.org/wiki/CCMP

IEEE 802.11i Pseudo-Random Function

- PRF is required to generate nonces and keys.
- HMAC-SHA-1 is used for all
- 4 Inputs: K=Secret Key, A= Use specific text string, B= Use specific Data, length
- Set counter to 0 and take desired number of bits from the left (if less than 160)
- If more than 160 bits needed, run the function again with the next sequence number
- Example: Pair-wise Temporal Key for CCMP
  - PTK=PRM{PMK, "Pairwise key expansion", min(AP Addr, STA Addr)||max(AP-Addr, STA-Addr)||min(Anonce, Snonce)|| max(Anonce,Snonce), 384}

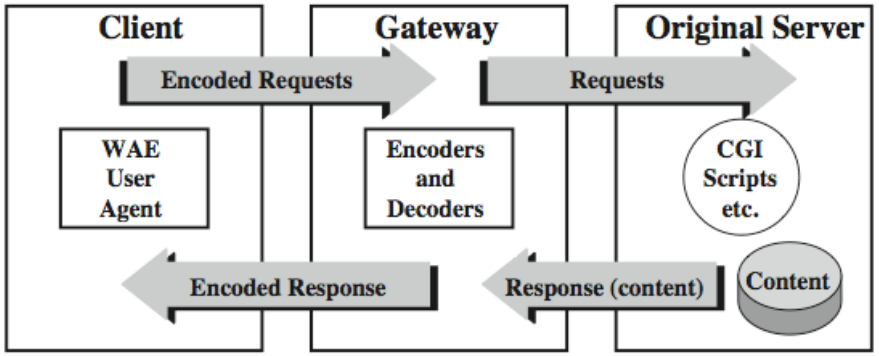


Security Problems Addressed

- No MAC address spoofing: MAC address included in both Michael MIC and CCMP MAC
- No replay: Each message has a sequence number (TSC in TKIP and PN in CCMP)
- No dictionary based key recovery: All keys are computer generated binary numbers
- No keystream recovery: Each key is used only once in TKIP. No keystream in CCMP.
- No Weak Key Attack: Special byte in IV in TKIP prevents weak keys. Also, keys are not reused.
- No rouge APs: Mutual authentication optional. Some APs provide certificates.
- **Not Addressed**: DoS attack using disassociation or deauthentication attack. Mgmt frames are still not encrypted.

Wireless Application Protocol (WAP)

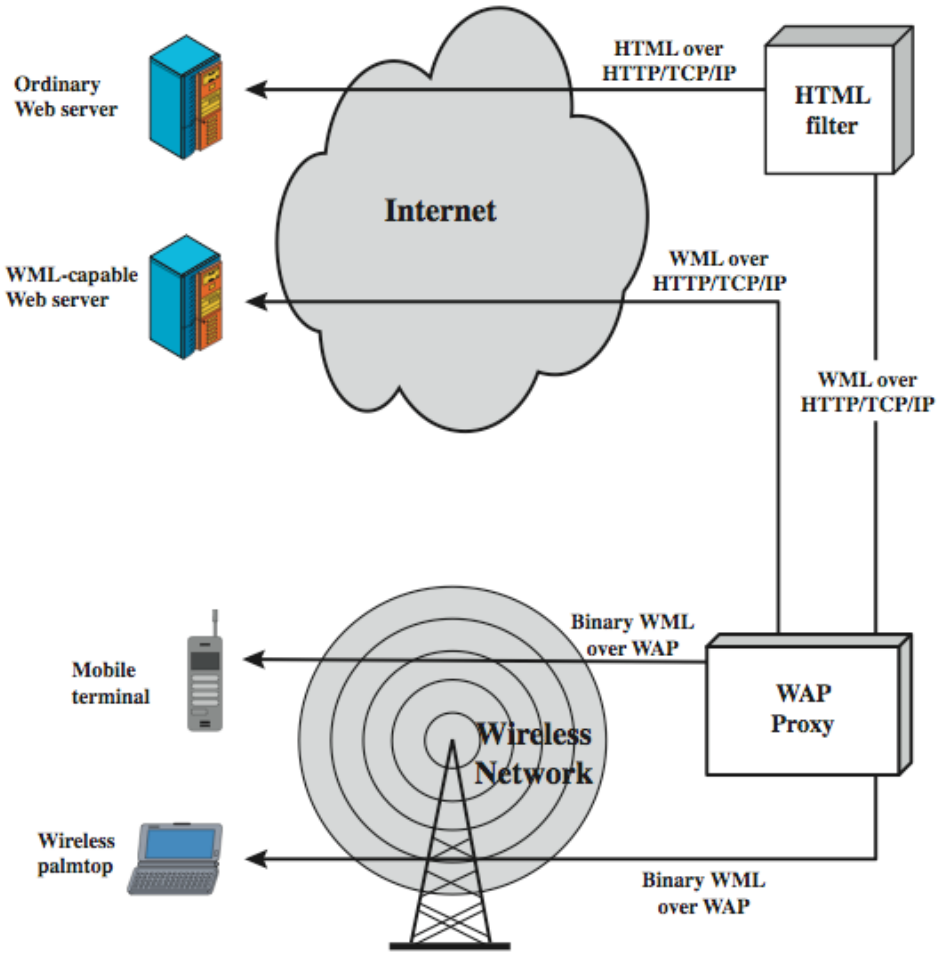
- Standard to provide mobile wireless users access to telephony and information services
- Significant limitations of devices, networks, displays with wide variations
- WAP specifications:
  - Programming model
  - Markup language
  - Small browser
  - Lightweight communications protocol stack
  - Applications framework



Ref: http://en.wikipedia.org/wiki/Wireless_Application_Protocol

WAP Infrastructure

- HTML Filter and WAP proxy may be separate or co-located
- HTML Filter converts HTML to WML
- WAP proxy converts WML to binary WML which is more compact



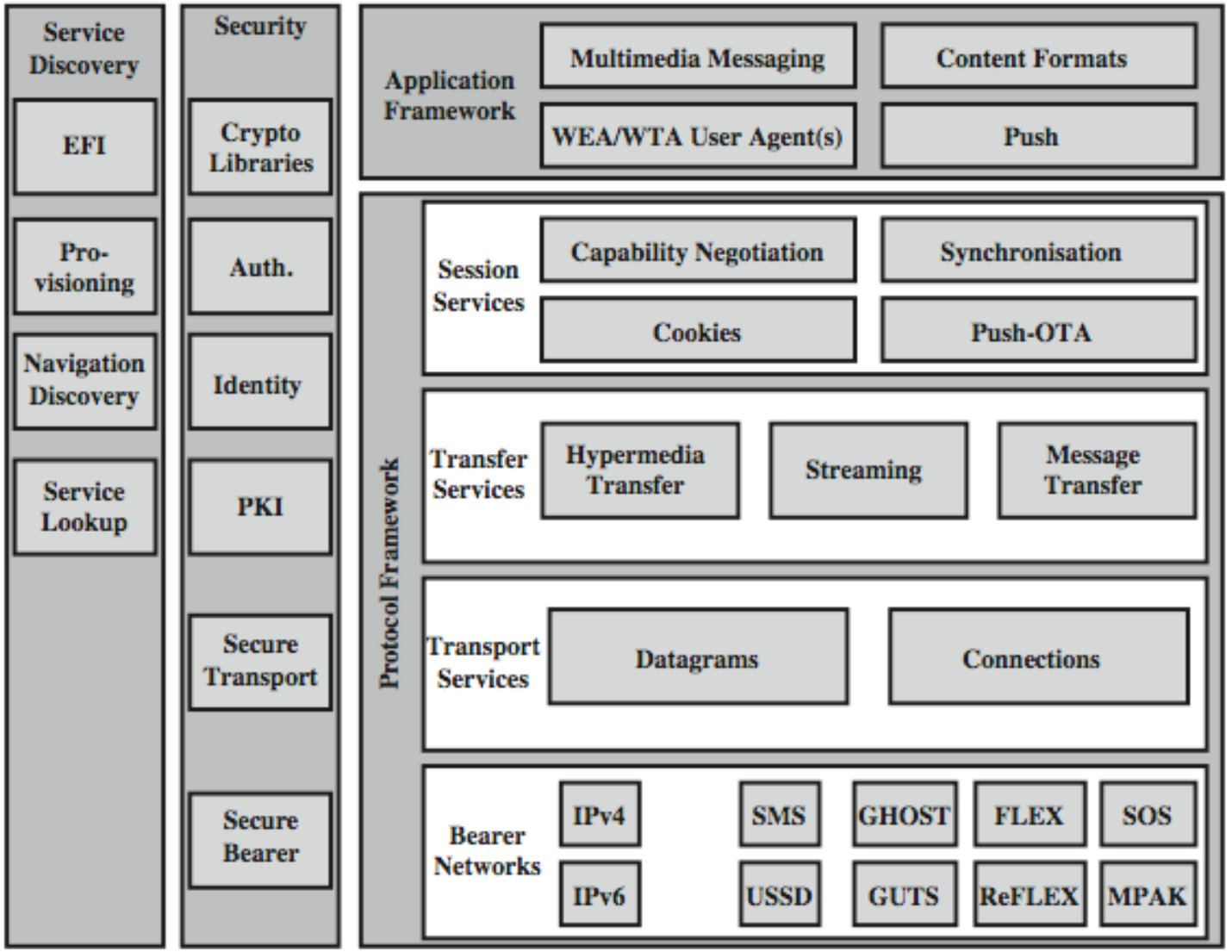
Wireless Markup Language

- Describes content and format for data display on devices with limited bandwidth, screen size, and user input capability
- Features include:
  - Text / image formatting and layout commands
  - Deck/card organizational metaphor
  - Support for navigation among cards and decks
- HTML Page = Deck = A set of interaction cards

```
<?xml version="1.0"?>
<!DOCTYPE wml PUBLIC "-//WAPFORUM//DTD WML 1.1//EN"
  "http://www.wapforum.org/DTD/wml_1.1.xml" >
<wml>
 <card id="main" title="First Card">
   <p mode="wrap">This is a sample WML page.</p>
 </card>
</wml>
```

Ref: http://en.wikipedia.org/wiki/Wireless_Markup_Language, http://en.wikipedia.org/wiki/WMLScript

WAP Architecture



WAP Architecture (Cont)

Security Services:

- Cryptographic Libraries: Integrity, Signature, Encryption
- Authentication: WTLS and TLS, HTTP Client Authentication
- Identity: WAP identity module stores user ID and secrets
- PKI: Manager Certificates
- Secure Transport: WTLS over datagrams, TLS over TCP
- Secure Bearer: Some bearers, e.g., IP provide security (IPSec)

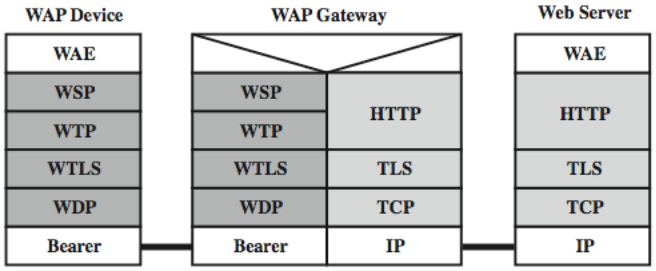
Service Discovery:

- External Functionality Interface (EFI): Allows applications to discover what functions/services are available on the device
- Provisioning: Set parameters needed to access network services
- Navigation Discovery: Find new network services
- Service Lookup: Find service's parameter using DNS

WAP Application Environment (WAE)

- Software modules and tools to eases development of applications and devices supported by WAP
- **WAP User Agents**: Software modules for various device functions, e.g., display
- **Wireless Telephony Applications**: Software modules for telephony
- **Standard Content Encoding**: Software modules for servers to generate Web content
- **Push**: A push-over-the-air (Push-OTA) service allows mobile to receive content pushed by the servers
- **Multimedia Messaging**: Email, text, MMS

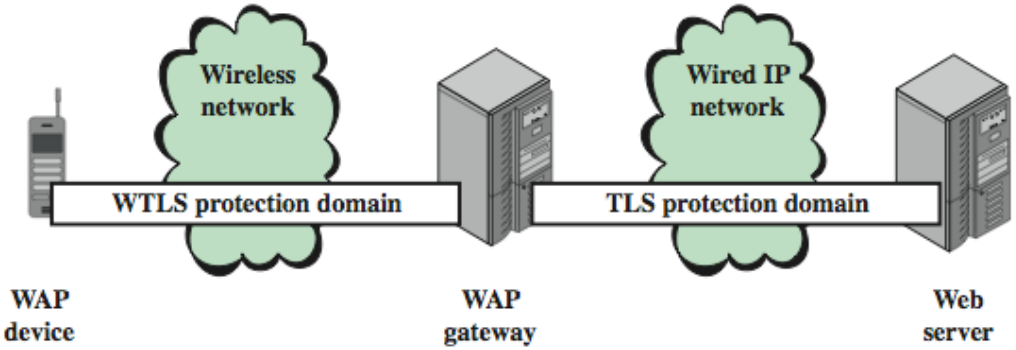
WAP Protocol Architecture



- Assumes that bearer service does not support TCP/IP
- Wireless Session Protocol (WSP): Supports connectionless and connection-oriented sessions. Allows sever Push for broadcast and alerts.
- Wireless Transaction Protocols (WTP): Lightweight TCP. Optional Acks. PDU concatenation. Transaction oriented (no connection setup). Three transaction classes:
  - Class 0: Unreliable send with no response. Used for Push.
  - Class 1: Reliable send with no response. Used for reliable push.
  - Class 2: Send with one reliable response or ack.
- Wireless Datagram Protocol (WDP): Hides the details of different bearers. May fragment.

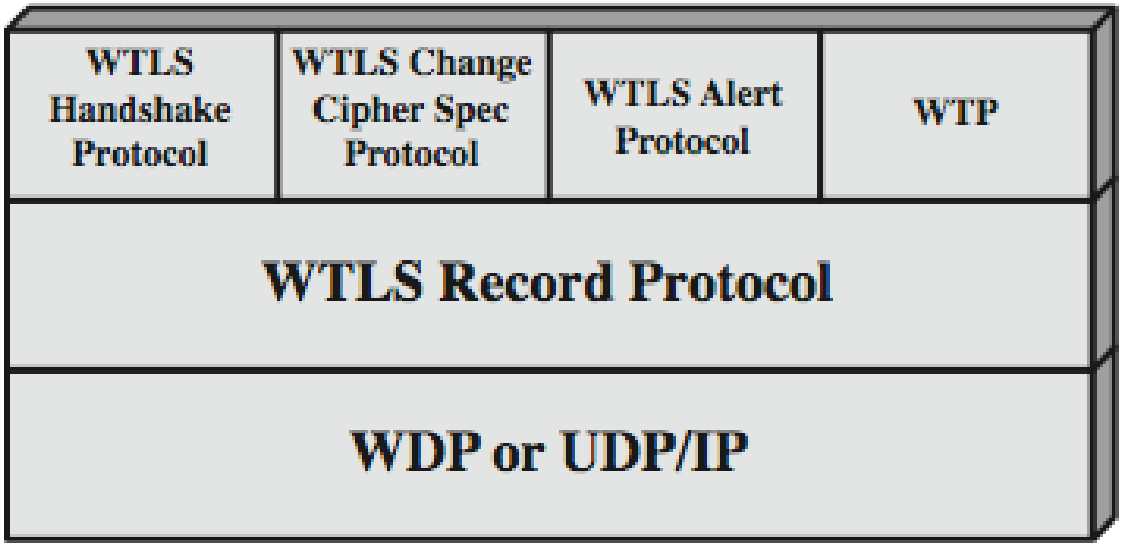
Wireless Transport Layer Security (WTLS)

- Provides security between mobile device and WAP gateway
  - Provides data integrity, privacy, authentication
- Based on TLS
  - Compressed data structures, Compressed Certificate format
  - Packet based rather than stream based design
- WAP gateway translates WTLS / TLS. Wireless may not be IP. WAP V2.0 uses TLS end-to-end



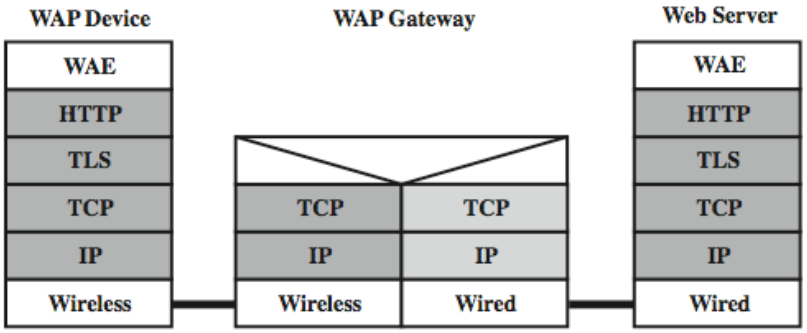
Ref: http://en.wikipedia.org/wiki/Wireless_Transport_Layer_Security

WTLS Protocol Architecture



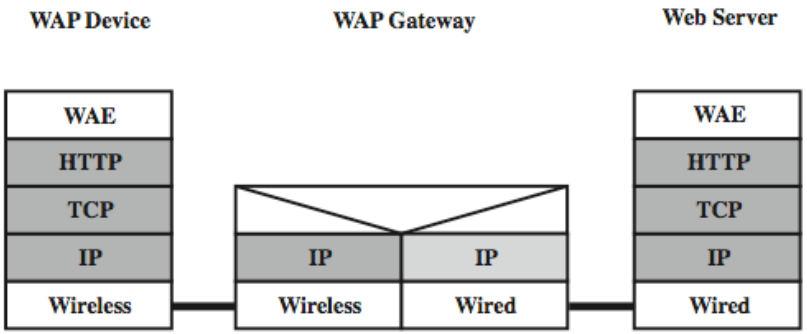
- Key Exchange and Signature: RSA, ECC (Elliptic)
  D-H to generate pre-master-secret
- Encryption: DES, 3DES, RC5
- Message Digest: MD5, SHA-1

WAP2 End-to-End Security over IP



(a) TLS-based security

1. Gateway simply forwards encrypted messages. Does not decrypt.



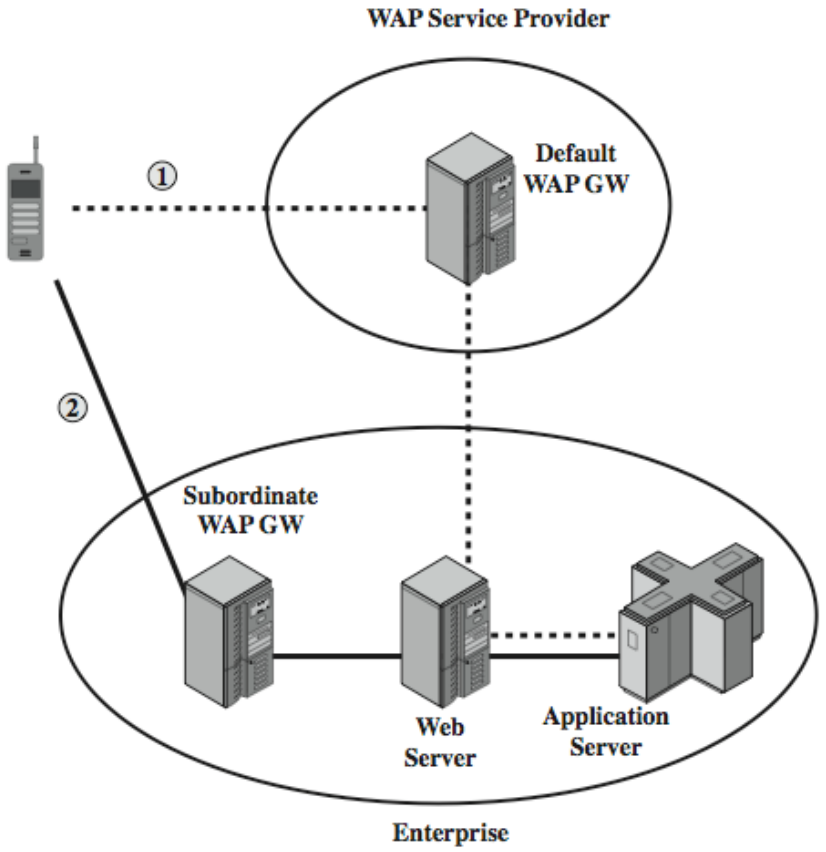
(b) IPSec-based security

2. Gateway can act as a router. Assumes both sides are IP-based.

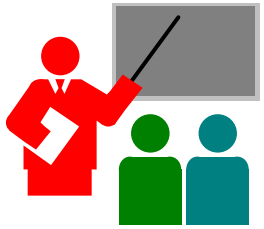
WAP2 End-to-End Security over IP (Cont)

3. WAP gateway redirection is allowed.

- Client connects through an external WAP gateway
- Application server may request that client connect through private gateway



Summary



1. 802.11 LANs consist of Basic Service Areas connected via a wired distribution system into an Extended Service Area
2. 802.11 originally used Wired Equivalent Privacy (WEP) which used RC4 for encryption and CRC-32 for MAC. Both were trivial to attack.
3. TKIP or WPA provides per-packet key and 64-bit MIC using RC4.
4. RSN or WPA2 provides stronger encryption and authentication using AES.
5. WAP allows information access via mobile devices. It consists of a session, transaction, and datagram protocol layers.
6. WTLS is used for protection over wireless links.

Homework 17

- WEP assumed all devices in the network share a secret key. The purpose of the authentication scenario is for the STA to prove that it possesses the secret key. As shown in the figure below, the STA sends a message to AP requesting authentication. The AP issues a challenge, which is a sequence of 128 random bytes sent as plain text. The STA encrypts the challenge with the shared key and returns it to the AP. The AP decrypts the incoming value and compares it to the challenge that it sent. If there is a match, the AP confirms that authentication has succeeded.

a. This authentication scheme is one-sided. How can it be made mutual?

b. What information does it provide to an attacker making it easy to attack?

c. The encryption scheme is RC4 stream cipher. How can a attacker create a valid response for any challenge after watching just one valid authentication.