Cryptography and Network Security
Chapter 17

Fifth Edition
by William Stallings

Lecture slides by Lawrie Brown

Chapter 17 – Wireless Network Security

Investigators have published numerous reports of birds taking turns vocalizing; the bird spoken to gave its full attention to the speaker and never vocalized at the same time, as if the two were holding a conversation

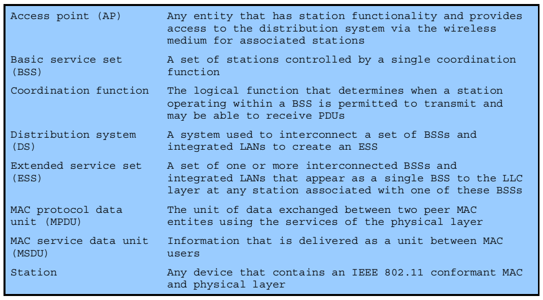
Researchers and scholars who have studied the data on avian communication carefully write the (a) the communication code of birds such has crows has not been broken by any means; (b) probably all birds have wider vocabularies than anyone realizes; and (c) greater complexity and depth are recognized in avian communication as research progresses.

—*The Human Nature of Birds*, Theodore Barber

IEEE 802.11

- IEEE 802 committee for LAN standards
- IEEE 802.11 formed in 1990's
  - – charter to develop a protocol & transmission specifications for wireless LANs (WLANs)
- since then demand for WLANs, at different frequencies and data rates, has exploded
- hence seen ever-expanding list of standards issued

IEEE 802 Terminology

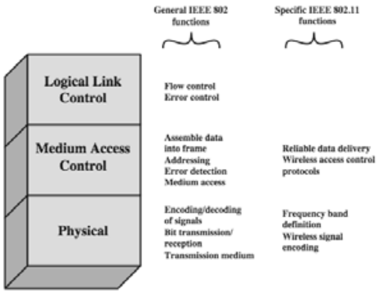


Access point (AP)	Any entity that has station functionality and provides access to the distribution system via the wireless medium for associated stations
Basic service set (BSS)	A set of stations controlled by a single coordination function
Coordination function	The logical function that determines when a station operating within a BSS is permitted to transmit and may be able to receive PDUs
Distribution system (DS)	A system used to interconnect a set of BSSs and integrated LANs to create an ESS
Extended service set (ESS)	A set of one or more interconnected BSSs and integrated LANs that appear as a single BSS to the LLC layer at any station associated with one of these BSSs
MAC protocol data unit (MPDU)	The unit of data exchanged between two peer MAC entites using the services of the physical layer
MAC service data unit (MSDU)	Information that is delivered as a unit between MAC users
Station	Any device that contains an IEEE 802.11 conformant MAC and physical layer

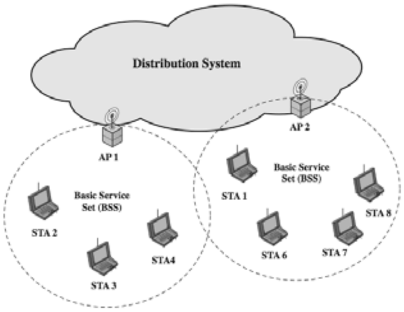
Wi-Fi Alliance

- 802.11b first broadly accepted standard
- Wireless Ethernet Compatibility Alliance (WECA) industry consortium formed 1999
  - – to assist interoperability of products
  - – renamed Wi-Fi (Wireless Fidelity) Alliance
  - – created a test suite to certify interoperability
  - – initially for 802.11b, later extended to 802.11g
  - – concerned with a range of WLANs markets, including enterprise, home, and hot spots

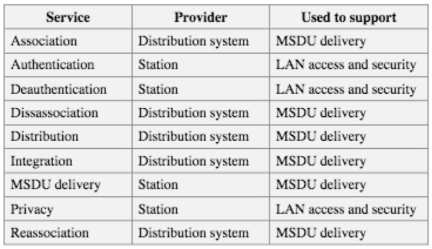
IEEE 802 Protocol Architecture



Network Components & Architecture



IEEE 802.11 Services

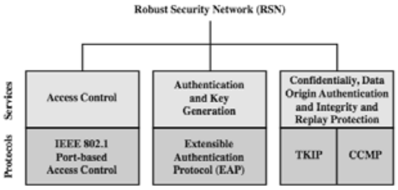


Service	Provider	Used to support
Association	Distribution system	MSDU delivery
Authentication	Station	LAN access and security
Deauthentication	Station	LAN access and security
Dissassociation	Distribution system	MSDU delivery
Distribution	Distribution system	MSDU delivery
Integration	Distribution system	MSDU delivery
MSDU delivery	Station	MSDU delivery
Privacy	Station	LAN access and security
Reassociation	Distribution system	MSDU delivery

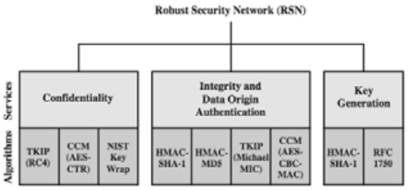
802.11 Wireless LAN Security

- wireless traffic can be monitored by any radio in range, not physically connected
- original 802.11 spec had security features
  - **Wired Equivalent Privacy (WEP)** algorithm
  - but found this contained major weaknesses
- 802.11i task group developed capabilities to address WLAN security issues
  - Wi-Fi Alliance **Wi-Fi Protected Access (WPA)**
  - final 802.11i **Robust Security Network (RSN)**

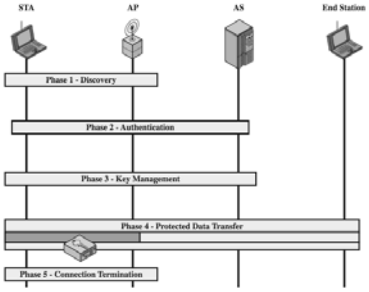
802.11i RSN Services and Protocols


Robust Security Network (RSN)
Services
Protocols
Access Control
Authentication and Key Generation
Confidentialiy, Data Origin Authentication and Integrity and Replay Protection
IEEE 802.1 Port-based Access Control
Extensible Authentication Protocol (EAP)
TKIP
CCMP

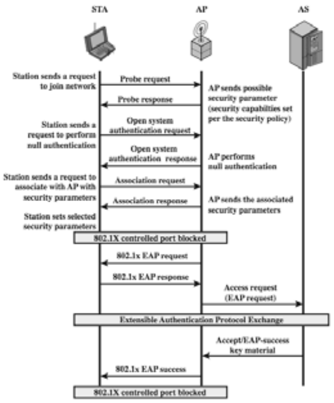
802.11i RSN Cryptographic Algorithms



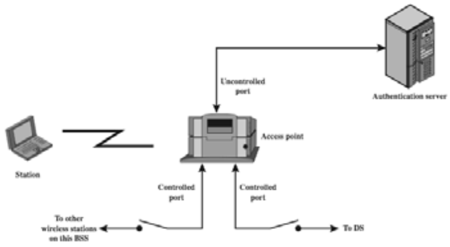
802.11i Phases of Operation



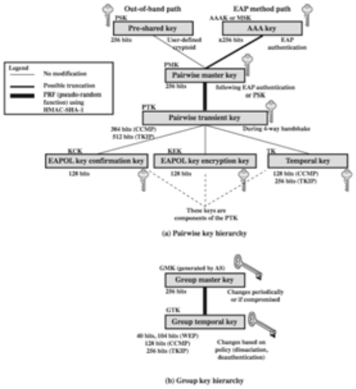
802.11i Discovery and Authent- ication Phases


STA
AP
AS
Station sends a request to join network
Probe request
Probe response
AP sends possible security parameter (security capabilties set per the security policy)
Station sends a request to perform null authentication
Open system authentication request
Open system authentication response
AP performs null authentication
Station sends a request to associate with AP with security parameters
Association request
Association response
AP sends the associated security parameters
Station sets selected security parameters
802.1X controlled port blocked
802.1x EAP request
802.1x EAP response
Access request (EAP request)
Extensible Authentication Protocol Exchange
Accept/EAP-success key material
802.1x EAP success
802.1X controlled port blocked

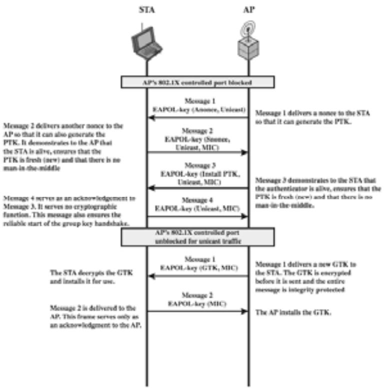
IEEE 802.1X Access Control Approach



802.11i Key Manage- ment Phase



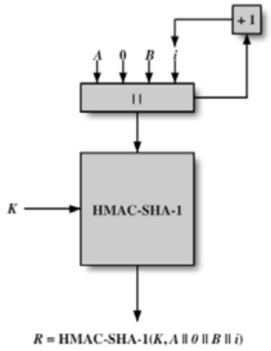
802.11i Key Manage- ment Phase


STA
AP
AP's 802.1X controlled port blocked
Message 1
EAPOL-key (Anonce, Unicast)
Message 1 delivers a nonce to the STA so that it can generate the PTK.
Message 2 delivers another nonce to the AP so that it can also generate the PTK. It demonstrates to the AP that the STA is alive, ensures that the PTK is fresh (new) and that there is no man-in-the-middle
Message 2
EAPOL-key (Snonce, Unicast, MIC)
Message 3
EAPOL-key (Install PTK, Unicast, MIC)
Message 3 demonstrates to the STA that the authenticator is alive, ensures that the PTK is fresh (new) and that there is no man-in-the-middle.
Message 4 serves as an acknowledgement to Message 3. It serves no cryptographic function. This message also ensures the reliable start of the group key handshake.
Message 4
EAPOL-key (Unicast, MIC)
AP's 802.1X controlled port unblocked for unicast traffic
Message 1
EAPOL-key (GTK, MIC)
Message 1 delivers a new GTK to the STA. The GTK is encrypted before it is sent and the entire message is integrity protected
The STA decrypts the GTK and installs it for use.
Message 2
EAPOL-key (MIC)
Message 2 is delivered to the AP. This frame serves only as an acknowledgment to the AP.
The AP installs the GTK.

802.11i Protected Data Transfer Phase

- have two schemes for protecting data
- Temporal Key Integrity Protocol (TKIP)
  - s/w changes only to older WEP
  - adds 64-bit Michael message integrity code (MIC)
  - encrypts MPDU plus MIC value using RC4
- Counter Mode-CBC MAC Protocol (CCMP)
  - uses the cipher block chaining message authentication code (CBC-MAC) for integrity
  - uses the CRT block cipher mode of operation

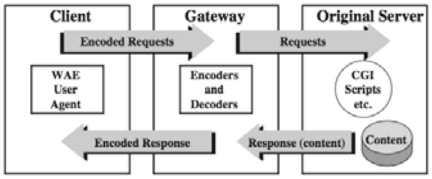
IEEE 802.11i Pseudorandom Function



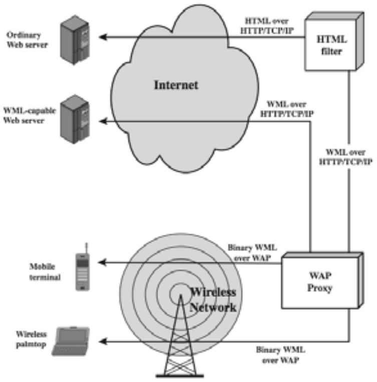
Wireless Application Protocol (WAP)

- a universal, open standard developed to provide mobile wireless users access to telephony and information services
- have significant limitations of devices, networks, displays with wide variations
- WAP specification includes:
  - programming model, markup language, small browser, lightweight communications protocol stack, applications framework

WAP Programming Model



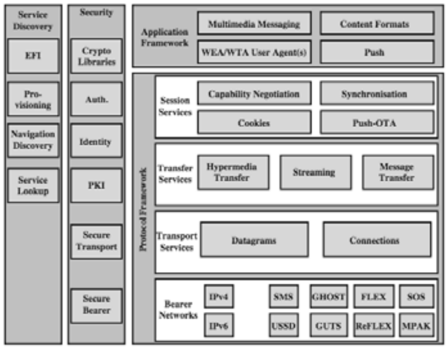
WAP Infra-structure



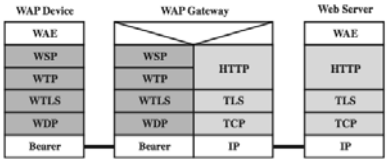
Wireless Markup Language

- 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
- a card is one or more units of interaction
- a deck is similar to an HTML page

WAP Architecture



WTP Gateway



WAP Protocols

- Wireless Session Protocol (WSP)
  - provides applications two session services
  - connection-oriented and connectionless
  - based on HTTP with optimizations
- Wireless Transaction Protocol (WTP)
  - manages transactions of requests / responses between a user agent & an application server
  - provides an efficient reliable transport service
- Wireless Datagram Protocol (WDP)
  - adapts higher-layer WAP protocol to comms

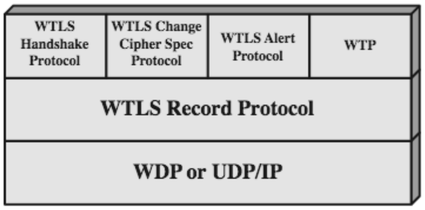
Wireless Transport Layer Security (WTLS)

- ➢ provides security services between mobile device (client) and WAP gateway
  - ● provides data integrity, privacy, authentication, denial-of-service protection
- ➢ based on TLS
  - ● more efficient with fewer message exchanges
  - ● use WTLS between the client and gateway
  - ● use TLS between gateway and target server
- ➢ WAP gateway translates WTLS / TLS

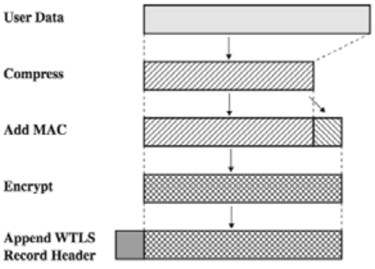
WTLS Sessions and Connections

- **secure connection**
  - a transport providing a suitable type of service
  - connections are transient
  - every connection is associated with 1 session
- **secure session**
  - an association between a client and a server
  - created by Handshake Protocol
  - define set of cryptographic security parameters
  - shared among multiple connections

WTLS Protocol Architecture



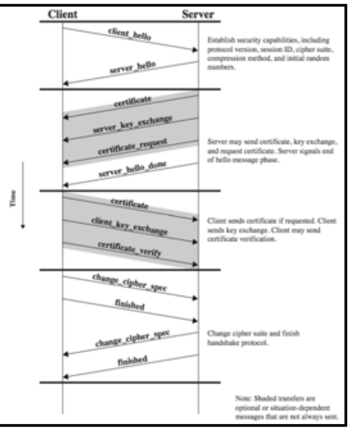
WTLS Record Protocol



WTLS Higher-Layer Protocols

- Change Cipher Spec Protocol
  - simplest, to make pending state current
- Alert Protocol
  - used to convey WTLS-related alerts to peer
  - has severity: warning, critical, or fatal
  - and specific alert type
- Handshake Protocol
  - allow server & client to mutually authenticate
  - negotiate encryption & MAC algs & keys

Handshake Protocol



Establish security capabilities, including protocol version, session ID, cipher suite, compression method, and initial random numbers.

Server may send certificate, key exchange, and request certificate. Server signals end of hello message phase.

Client sends certificate if requested. Client sends key exchange. Client may send certificate verification.

Change cipher suite and finish handshake protocol.

Note: Shaded transfers are optional or situation-dependent messages that are not always sent.

Cryptographic Algorithms

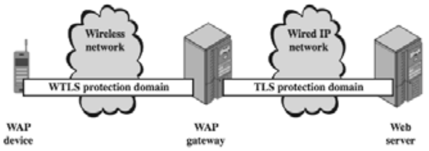
- WTLS authentication
  - uses certificates
    - X.509v3, X9.68 and WTLS (optimized for size)
  - can occur between client and server or client may only authenticates server
- WTLS key exchange
  - generates a mutually shared pre-master key
  - optional use server_key_exchange message
    - for DH_anon, ECDH_anon, RSA_anon
    - not needed for ECDH_ECDSA or RSA

Cryptographic Algorithms cont

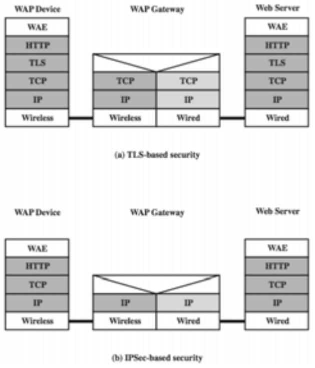
- Pseudorandom Function (PRF)
  - HMAC based, used for a number of purposes
  - only one hash alg, agreed during handshake
- Master Key Generation
  - of shared master secret
  - master_secret = PRF(pre_master_secret, "master secret”, ClientHello.random || ServerHello.random)
  - then derive MAC and encryption keys
- Encryption with RC5, DES, 3DES, IDEA

WAP End-to-End Security

- have security gap end-to-end
  - at gateway between WTLS & TLS domains



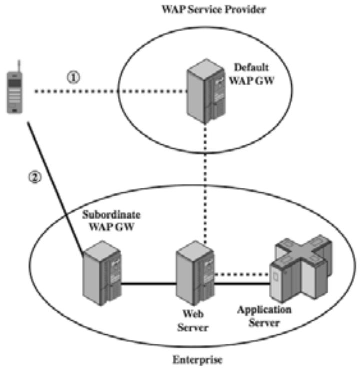
WAP2 End-to-End Security

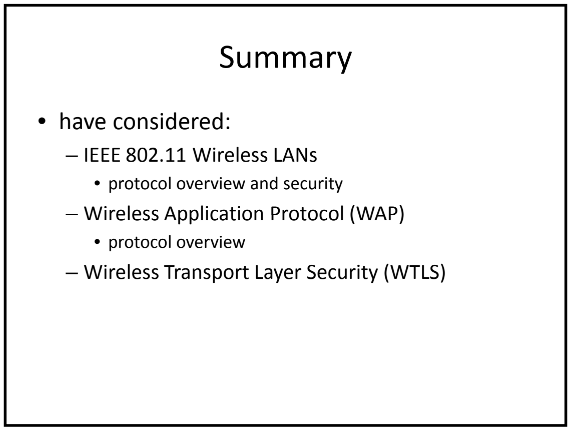


(a) TLS-based security

(b) IPSec-based security

WAP2 End-to-End Security





Summary

- have considered:
  - – IEEE 802.11 Wireless LANs
    - protocol overview and security
  - – Wireless Application Protocol (WAP)
    - protocol overview
  - – Wireless Transport Layer Security (WTLS)