CPE5021
Advanced Network Security

-- Advanced Wireless Network Security---

Lecture 8

Outline

- Wireless LAN Security Enhancements
  - TKIP
  - LEAP
  - EAP-TLS
  - PEAP
- Broadband Wireless Networks
- Broadband Wireless Network Security

Acknowledgement:
(Many slides of this lecture are borrowed from other authors)

802.11 Standards

- 802.11: addresses two separate layers of the ISO model:
  - Physical network layer - defines the physical transmission characteristics of the signal - radio signal frequency, power levels, and type of modulation.
  - MAC - mostly made up of software-based protocols that enable devices to talk to each other.
- 802.11a: 5GHz, supports up to 54Mbps
- 802.11b (Wi-Fi): 2.4GHz, up to 11Mbps
- 802.11g: 2.4GHz, up to 54Mbps – to increase the speed of 802.11b
- 802.11i: Wireless LAN Security
  - Introduces authentication protocols (LEAP; EAP-TLS, PEAP, EAP-TTLS).
  - Introduces requirement to use Advanced Encryption Standard
  - Proposes Wi-Fi Protected Access (WPA).
- 802.15: Wireless Personal Area Network
- 802.16: Wireless Metropolitan Area Network

Wireless Network Security

- Need to provide per-packet authentication, integrity and confidentiality.
- Need to allow mutual authentication between clients and the network.
- Should allow future network expansion and additional protocols with stronger authentication and encryption.

802.11i with 802.11x: Security Goals

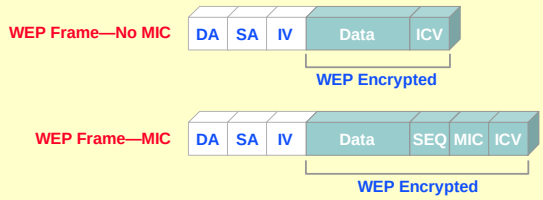
802.11x is part of 802.11i proposed to allow:

- Message Integrity Check (MIC).
- Temporal Key Integrity Protocol (TKIP).
  - Per-packet key hashing.
  - Initialization Vector sequencing.
  - Rapid re-keying.
  - Stronger encryption schemes such as AES.
- Mutual Authentication – two-way authentication.
- Dynamic Session Key.

Message Integrity Check (MIC)

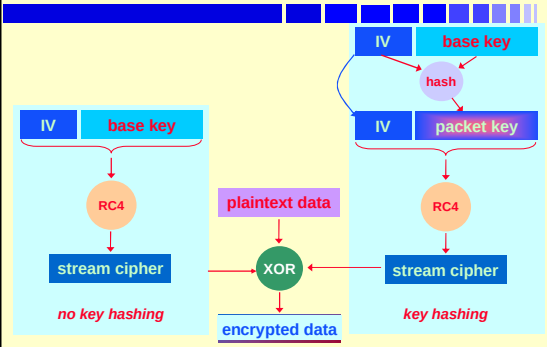
- The MIC will protect WEP frames from being tampered with.
- The MIC is based on seed value, destination MAC, source MAC, and payload.
  - Any change to these will change MIC value.
- The MIC is included in the WEP encrypted payload.

Message Integrity Check



- MIC uses a hashing algorithm to stamp frames
- If the original frame were modified, then we can detect that because MIC would be different.

TKIP: WEP Key Hashing



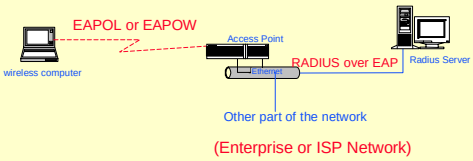
TKIP: WEP Key Hashing

- *If we append IV to the base key to form the encryption key (base key is static) we can work out the base key when IV is reused for a number of frames.*
- *Because packet key now is the hash of IV and base key, the packet key is different for every IV. This makes it harder for the attacker to work out the key when IV is reused for a number of frames.*

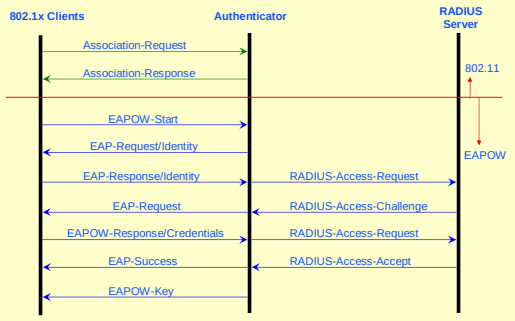
Wireless Authentication with RADIUS

- Remote Access Dial In User Service
- Allows centralised administration and accounting
- Support
  - Authentication and authorisation
  - Accounting
  - tunneling support
  - Extensions
  - support IPv6

802.?? and RADIUS



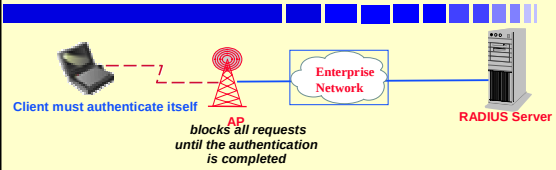
Message Flow



802.?? and Authentication Improvement

- Mutual authentication
  - A wireless network authenticates clients before providing any access, and a client should be able to authenticate the wireless network before it provides its confidential information.
  - Supports various authentication types.
- Encryption keys dynamically derived after authentication – session keys are dynamically changed.
- Centralised control – there is a central authentication server.
- Scalable – allows network expansion.

802.?? and Mutual Authentication



blocks all requests until the authentication is completed

RADIUS server authenticates client

Client authenticates RADIUS server

Mutual Authentication is required to prevent rogue clients (e.g. in the parking area) from accessing your network, AND to prevent rogue APs from stealing data from clients

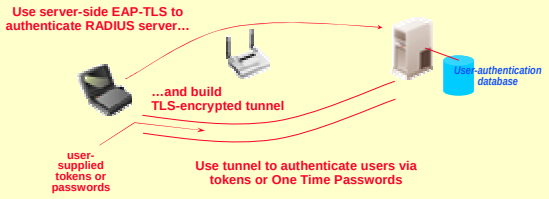
802.?? and Authentication Types

- LEAP- lightweight Extensible Authentication Protocol
  - Provides username/password-based authentication between a wireless client and a RADIUS server like Cisco ACS or Interlink AAA.
  - Supports Windows, CE, Linux and Mac OS
- EAP-TLS (EAP-Transport Layer Security)
  - Uses a TLS handshake as the basis for authentication.
  - EAP-TLS requires both the station and RADIUS server to prove their identities via public key cryptography.
  - Authentication is done using client certificate and server certificate.
  - Relying on PKI.

802.?? Authentication Types

- PEAP (Protected EAP) and EAP-TTLS (tunnel TLS) are similar in structure. They make use of TTLS and make it possible to authenticate wireless LAN clients without requiring them to have certificates.
  - Establish security in stage one.
  - Exchange authentication in stage two.
- PEAP and EAP-TTLS
  - Use server-side TLS which requires only server certificate.
  - Client authentication via user ID and password or token.

EAP & PEAP Authentication with RADIUS: Eg.



PEAP sets up a secure, encrypted tunnel between a client and RADIUS server

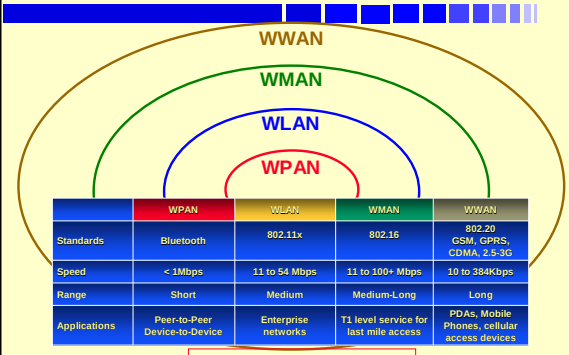
Wi-Fi Protected Access

- WPA = 802.1X + TKIP
  - WPA requires authentication & encryption
  - 802.1X authentication choices include LEAP, PEAP, SSL or TLS
- Industry suppliers are strong supporters of WPA
  - Built on 802.1X and TKIP as an extension of WEP.
  - Widespread adoption of WPA will hopefully make it possible to have one standard for WLAN.

WLAN Security Summary

- **IEEE 802.1x – Attempt to provide** network protocols that make wireless networking as secure as wired.
- **Encryption –** Enhancements to WEP with TKIP will secure transmitted data
  - Dynamic Session Keys
  - Key hashing to prevent weak IV
  - Message Integrity Check to prevent frame tampering
- **Authentication –** Network access is blocked until mutual authentication is completed
  - Selection of authentication type derived from mobile application and devices (LEAP, EAP-TLS, PEAP, EAP-TTLS)
- **WPA –** Wi-Fi Protected Access
  - Standard encryption architecture based on TKIP and authentication based on (LEAP, EAP-TLS, PEAP,TTLS, RADIUS)

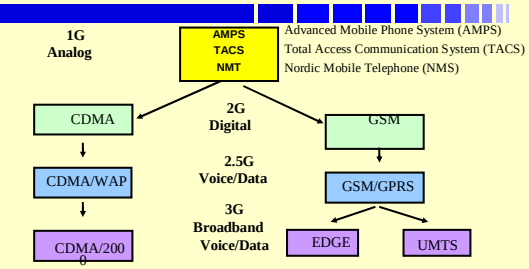
Wireless Technologies



	WPAN	WLAN	WMAN	WWAN
Standards	Bluetooth	802.11x	802.16	802.20 GSM, GPRS, CDMA, 2.5-3G
Speed	< 1Mbps	11 to 54 Mbps	11 to 100+ Mbps	10 to 384Kbps
Range	Short	Medium	Medium-Long	Long
Applications	Peer-to-Peer Device-to-Device	Enterprise networks	T1 level service for last mile access	PDAs, Mobile Phones, cellular access devices

Borrowed from another university

Wireless Technologies



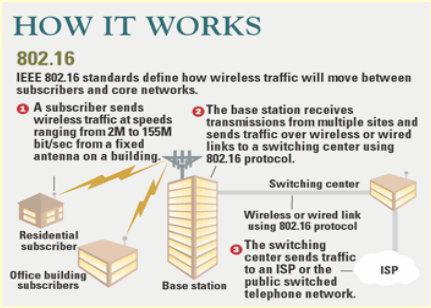
Advanced Mobile Phone System (AMPS)
Total Access Communication System (TACS)
Nordic Mobile Telephone (NMS)

Code Division Multiple Access (CDMA)
Wireless Access Protocol (WAP)

Global System for Mobile Communication (GSM)
General Packet Radio Service (GPRS)
Enhanced Data Rate for GSM Evolution (EDGE)
Universal Mobile Telecommunication System (UMTS)

Borrowed from another university

802.16 – How it works



Borrowed from William Stallings

802.16: Broadband Wireless Networks

- **Provides PHY and MAC of single-point-to-multipoint broadband wireless access system**
- **Enables transport of data, video and voice.**
- **Provide connection-oriented communication.**
- **Supports difficult requirements.**
  - **High bandwidth - hundreds of users per channel.**
  - **Continuous and burst traffic.**
  - **Very efficient use of spectrum.**
- **Allow protocol-independent (ATM, IPv, Ethernet, …)**
- **Supports multiple 802.16 PHY**

802.16: Broadband Wireless Networks

- **An 802.16 wireless service provides a communications path between a subscriber site and a core network such as the Internet.**
- **802.16 standard is concerned with the air interface between a subscriber's transceiver station and a base transceiver station.**
- **The standard protocols defined specifically for wireless transmission address issues related to the transmission of data over a network.**
- **It is organised into a three-layer architecture.**
  - **The lowest layer, the physical layer, specifies the frequency band, the modulation scheme, error-correction techniques, synchronisation between transmitter and receiver, data rate and the time-division multiplexing (TDM) structure.**
  - **Right above the physical layer is media access control (MAC) layer. The layer contains functions associated with services provided to subscribers. These functions include transmitting data in frames and controlling access to the shared wireless medium.**
  - **Above the MAC layer is a layer that provides functions specific to the service being provided (services including digital audio/video multicast, digital telephony, ATM, Internet access, etc.).**

802.16: Broadband Wireless Networks

- **The standard uses the Demand Assignment Multiple Access-Time Division Multiple Access (DAMA-TDMA) technique for transmission from subscribers to a base station.**
  - **DAMA is a capacity assignment technique that adapts as needed to respond to demand changes among multiple stations.**
  - **TDMA is the technique of dividing time on a channel into a sequence of frames, each consisting of a number of slots, and allocating one or more slots per frame to form a logical channel.**

802.16: Broadband Wireless Networks

- **The MAC protocol defines how and when a base station or subscriber station may initiate transmission on the channel.**
  - **Some of the layers above the MAC layer, such as ATM, require quality of service, the MAC protocol must be able to allocate radio channel capacity to satisfy service demands.**
  - **The MAC protocol for communications from a base station to a subscriber station is simple since there is only one transmitter. However, from subscribers to a base station, subscriber stations have to compete for access, resulting in a more complex MAC protocol.**

802.15: WPAN

- Data rates of 250 kb/s, 40 kb/s and 20 kb/s.
- Star or Peer-to-Peer operation.
- CSMA/CA channel access.
- Dynamic device addressing.
- Fully hand shake protocol for transfer reliability.
- Low power consumption.
- Frequency Bands of Operation
  - 16 channels in the 2.4GHz ISM band
  - 10 channels in the 915MHz ISM band
  - 1 channel in the European 868MHz band.

WPA, WMAN and WWAN Security

- **Use WPA hardware with more advanced crypto algorithms.**
  - **Plan for AES and ECC with 802.11i**
- **Authentication with 802.1X / RADIUS**
  - **Secure AP using authentication servers**
  - **Set re-authentication key refresh every short period of time, e.g 5 minutes.**
- **Use strong authentication**
  - **E.g: Certificates and/or Smartcards/tokens and/or one-time passwords.**
- **Always monitor for rogue APs and unauthorised users.**

WPA, WMAN and WWAN Security

- **Physical isolation protection is no longer very important.**
- **All signals are available to anyone.**
- **Dynamic key schemes become extremely important to protect against crypto analysis attacks.**
- **Need to apply different security schemes for different services.**

Future Trends

- **Enterprise wireless applications begin to explode**
  - **Availability of notebooks with imbedded wireless interfaces.**
  - **PDAs, Web Pads, Cell Phones with 802.11.**
  - **Support dual band (802.11a.,b.,g.).**
- **Widespread availability of 802.11 access.**
  - **Organisations employing virtual LAN's in common areas.**
  - **Organisations offering wireless access.**
  - **Service providers offering wireless access in the public venue.**
- **Mobile workers staying connected at work, home and on the move.**
- **Multiple Authentication types will be supported.**
- **Wireless MAN is spreading rapidly.**
- **Wireless WAN will be accepted for certain services.**
- **Total wireless communications with full authentication and encryption.**