



Wireless Network Security and Mobile Commerce

Dr. Gordon B. Agnew

Electrical and Computer Engineering

University of Waterloo

gbagnew@engmail.uwaterloo.ca



Overview

1. Wireless LANS

- WLAN Standards and Characteristics
- Overview of Security Issues in Wireless

2. Security Architectures and Protocols

- WEP
- IEEE 802.1x, EAP, etc.
- Architectures – GSM, GPRS, etc.
- WAP2.0

3. Future Directions



What is the Problem?

- ◆ Until “recently”, networks were wire based connecting computers in fixed locations
 - Bandwidth not a concern
 - Computational/transmit power not a concern
 - Channel error rates small
 - Physical connection generally required for interception



What is the Problem?

- ◆ Wireless networks do not map well into wired structures
 - Bandwidth limited
 - Computation power limited
 - Battery power limited
 - Relatively large error rates (security functions require perfect fidelity!)
 - “Features” sell!



Wireless LAN's

Architectures, Standards, Operability



IEEE 802.11x

- ◆ Started in 1997 by IEEE as a method of wireless local area networking
- ◆ Objective was to provide easy to implement wireless environment over a small area (up to about 100+ m)
- ◆ Three main standards
 - 802.11a (54 Mbps)
 - 802.11b (11 Mbps)
 - 802.11g (54 Mbps)



IEEE 802.15

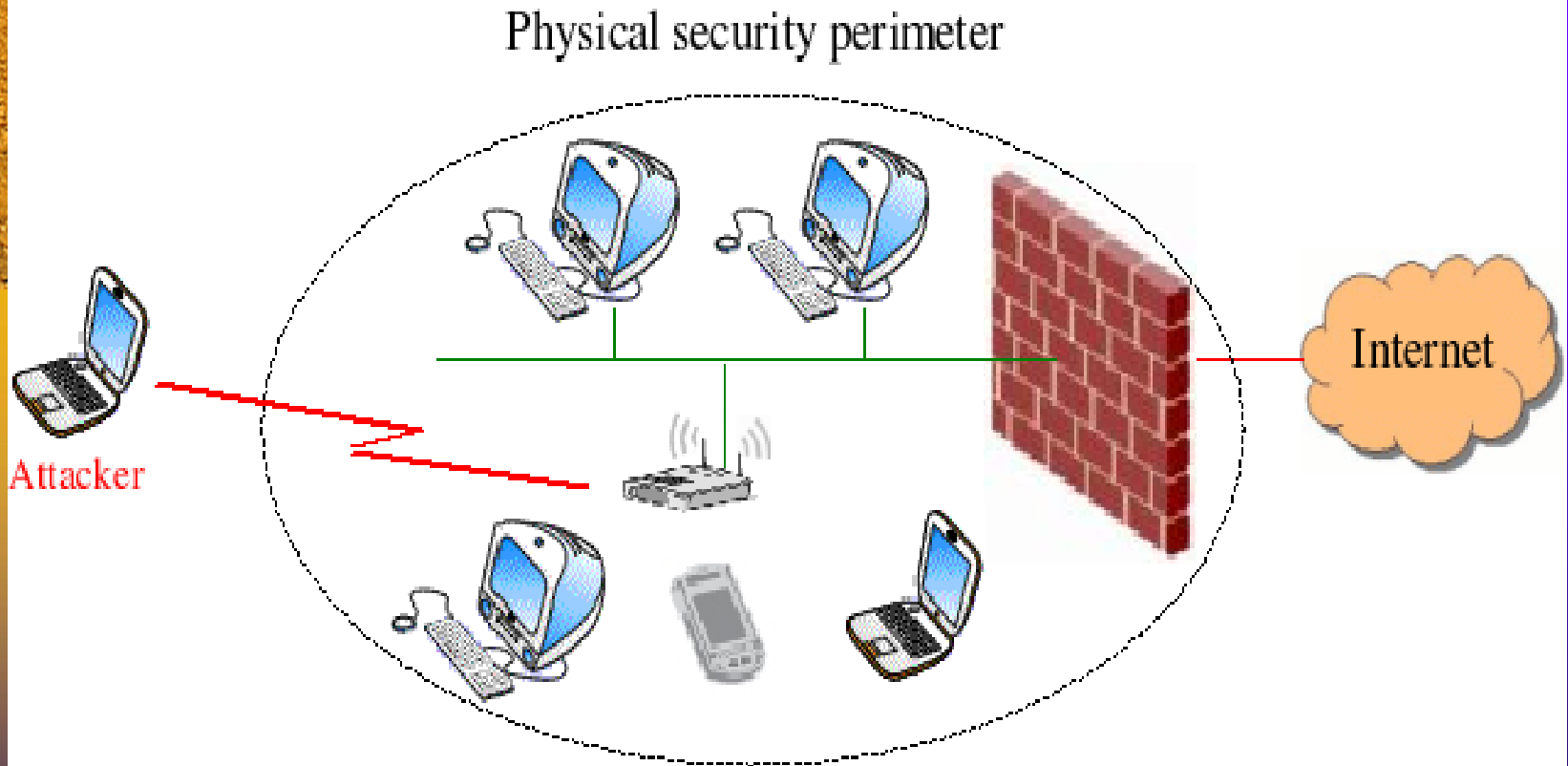
- ◆ Wireless Personal Area Networks (WPAN)
- ◆ 802.15.1 – adapted from Bluetooth specification
- ◆ 2.4 GHz band ~ 1 Mbps
- ◆ Low power, short range
- ◆ Frequency-Hopping Spread Spectrum



Security Issues in Wireless

- ◆ There are many security threats associated with wireless/mobile devices. These include:
 - All of the vulnerabilities associated with wired networks!
 - Unauthorized access
 - Interception of information (it is a transmitter after all!)
 - Denial of Services

The Wired Internet





Security Issues in Wireless

- Impersonation attacks
- Tracking of an individual's movements
- Theft of devices and access to information
- Theft of data (without detection)
- Modification of data (without detection)
- Introduction of viruses



Types of Attacks

- ◆ There are two general forms of attack – passive and active
- ◆ A passive attacker simply monitors the channel in an effort to recover information
- ◆ An Active attacker not only listens, but may actively try to subvert the system



Passive Attacks

- ◆ Eavesdropping – in this case the attacker simply listens and tries to interpret the data being exchanged – if the data is in-the-clear, they succeed
- ◆ Traffic Analysis – the attacker gains information by determining how much activity there is, where access points are located, and what protocols are being used (and what possible weaknesses there are)



Active Attacks

- ◆ There are several flavours of active attacks. These include:
 - Unauthorized system access
 - Man-in-the- Middle attacks
 - Message modification attacks
 - Session Hijacking
 - Replay



Unauthorized Access

- ◆ The attacker tries to gain access to the network to obtain files or free usage (war driving)
- ◆ Once inside the attacker may do more harmful attacks



Man-in-the Middle

- ◆ This is a real-time attack
- ◆ Many protocols do not enforce mutual authentication (such as Diffie Hellman)
- ◆ The attacker places him/herself between the two communicating parties and regulates all communications – this can be accomplished with *rogue* base stations or access points
- ◆ Address Resolution Protocol (ARP) attacks are very dangerous



Message Modification

- ◆ The attacker may attempt to modify messages in the system
- ◆ They may also try to delay messages in order to cause the system/users to change their behaviour



Session Hijacking

- ◆ Here the attacker attempts to take control of an authorized and authenticated session
- ◆ In a wireless system, the attacker can collect information about the session (enough to appear as the authorized user) then block the authorized wireless device from the system



Replay

- ◆ The attacker records traffic from legitimate sessions then replays them into the network at a later date
- ◆ This may allow the attacker to gain access by convincing the network that they are a valid user



Attacking 802.11



Modes of Operation

- ◆ 802.11 allows two modes of operation
 - Ad hoc or Independent Basic Service Set (IBSS)
 - Infrastructure or Basic Service Set (BSS)



Independent Basic Service Set

- ◆ Applications such as Windows Sharing, peer-to-peer networks, etc.
- ◆ No central control
- ◆ Authentication is optional
- ◆ Attacker may have access to all services and data on a particular machine



Wired Equivalent Privacy (WEP)

- ◆ Part of IEEE 802.11 standard
- ◆ There are several methods employed to provide security
 - Service Set Identifiers (SSID)
 - Media Access Control Access List
 - A Shared RC4 key for Authentication



WEP

- ◆ Service Set Identifier can be used as a shared secret and access point will not respond to probe
- ◆ But, it is transmitted in the clear
- ◆ Attacker sends a forged disassociate message then waits for target to begin automatic reassociation



Breaking the WEP Shared Key Protocol

- ◆ Keystream is XOR'd with data – predictable changes can be made to data/CRC (as we shall see in a second...)



Attacking WEP

- ◆ Minimum keys are 40 bits (shared by all stations on the WLAN) and a 24 bit Initialization Vector (IV) intended to randomize
- ◆ With multiple users – 50% probability that two packets use the same IV after only 5000 packets



Attacking WEP

- ◆ At 11 Mbps, all possible IV's can be exhausted in about 5 hours on a busy access point
- ◆ This results in repeated use of the same key stream (which is very insecure)
- ◆ (even better, some wireless cards always start at the same IV and increment for each new packet!



Attacking WEP

- ◆ 32 bit CRC is also subject to attack
- ◆ Only 2^{16} or 64K tries are required to have a high probability of a message being accepted (Birthday Paradox)



MAC

- ◆ Access points can be set to only allow access to WLAN by certain MAC addresses
 - Not scaleable to large systems
 - No protection from inside attacks
 - Outside attacks are possible



Transport Layer Security - TLS

- ◆ Effort by IETF to produce Internet standard version of SSL
- ◆ Very similar to SSL v3 except:
 - Uses HMAC
 - Pseudorandom function generation
 - Some cipher suite options
 - Padding methods



Wireless TLS (WTLS)

- ◆ Extension of TLS to wireless environment
- ◆ There are three modes operation:
 - Class 1 – anonymous authentication
 - Class 2 – server authentication
 - Class 3 – authentication of both server and client (this is the most secure)



WTLS Security Concerns

- ◆ Some modifications of TLS to WTLS have caused some security problems
 - Predictable IV's which lead to a chosen-plaintext attack
 - WTLS supports a 40-bit XOR- MAC – bits in message can be changed and MAC corrected to prevent detection
 - 35-bit DES encryption
 - PKCS#1 attack – attacking the padding bits



WTLS Security Concerns

- Unauthenticated alert messages – some alerts are sent in the clear – alerts take up a sequence number “slot” - attacker can replace an encrypted datagram with an alert
- Using exportable keys – IV of each message can be determined from “Hello” message and sequence number
- Probable plaintext attacks – ciphers are small enough that brute-force attacks to recover the key can be performed



IEEE 802.1x

- ◆ Originally developed as a protocol for port-based authentication of wired networks
- ◆ Extended to wireless
- ◆ It provides
 - User-based authentication
 - Access control
 - Key Transport
- ◆ Relies on Extensible Authentication Protocol (EAP) for authentication



Extensible Authentication Protocol

- ◆ EAP originally designed for Point-to-Point protocols
- ◆ Defines three entities
 - Client
 - Access controller (AC)
 - Authentication Server (AS)



EAP

- ◆ Usually, AS is a Remote Authentication Dial-In User Service (RADIUS) coupled to the wired network
- ◆ Access Point usually is also the AC
- ◆ In the wireless environment, access point must allow traffic to pass to the AS prior to authentication
- ◆ System is subject to hijacking because of this



EAP

- ◆ In EAP, only the client is authenticated – this allows the attacker to spoof access points
- ◆ RADIUS relies on a shared secret key with the Authenticator – this can lead to problems with key distribution and interception in larger WLANs



Extensible Authentication Protocol – Transport Layer Security

- ◆ EAP-TLS is one mode of EAP – it makes use of TLS as the authentication mechanism
- ◆ Supports mutual authentication based on certificates (prevents man-in-the-middle attacks) and dynamic keying and requires a PKI (at a price!)
- ◆ Identity exchange is done in the clear which allows traffic analysis attacks



Tunneled Transport Layer Security

- ◆ TTLS was developed to avoid the requirement for a PKI
- ◆ Two stage protocol
 - Establish a TLS tunnel and authenticate the server to the client (one certificate)
 - Clients credentials (Attribute Value Pairs – AVPs similar to RADIUS) are sent to the server for verification using encrypted tunnel (thus, no digital signature required)



Protected Extensible Authentication Protocol

- ◆ PEAP is very similar to TTLS
- ◆ Similar two stage method just uses an authentication protocol defined in EAP
- ◆ Backed by Microsoft so...



IEEE 802.11i

- ◆ 802.11i is the security standard for wireless networks – ratified June 2004 and replaces WEP
- ◆ “Fixes” holes in WEP
- ◆ Enforces mutual authentication and the use of a “fresh” session key
- ◆ Uses stronger encryption (AES)



IEEE 802.11i

- ◆ Defines 3 protocols for protected data transfer:
 - CCMP
 - WRAP
 - TKIP (for legacy systems)



Counter Mode with Cipher Block Chaining Message Authentication Code Protocol

- ◆ CCMP uses Counter Mode Encryption with CBC-MAC Data Origin Authentication
 - Based on AES
 - Powerful method to combine encryption and authentication techniques in one algorithm



Wireless Robust Authentication Protocol

- ◆ WRAP - Original 11i protocol but was replaced due to IPR problems
- ◆ Based on Offset Codebook Mode of AES



Temporal Key Integrity Protocol

- ◆ TKIP – designed as a wrapper around EAP
- ◆ Enhances WEP by adding a per-packet key mixing function to public initialization vectors (IVs)
- ◆ Also adds a re-keying mechanism to provide fresh encryption and integrity keys
- ◆ More resistant to attacks involving key reuse
- ◆ Prevents some known-ciphertext attacks




WiFi Protected Access WPA – Temporal Key Integrity Protocol (TKIP)

- ◆ Well, manufactures got tired of waiting for 802.11i
- ◆ Introduced by Wi-Fi Alliance in 2002
- ◆ It is a subset of 802.11i



Backbone 3G Architectures and Security



Global System for Mobile Communications (GSM)

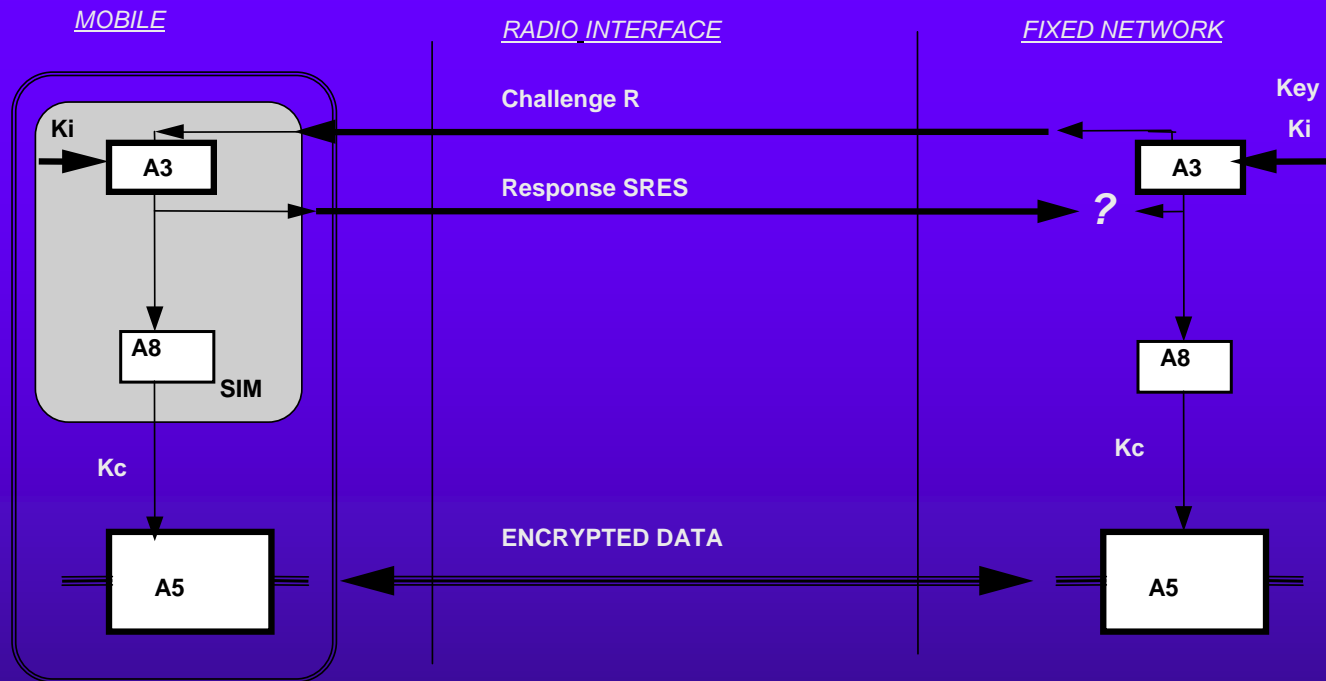
- ◆ Started as a European standard but has spread across the world
- ◆ Designed to ensure correct billing and prevent fraudulent use
- ◆ Provide privacy for customer traffic



GSM Security

- ◆ Security is based on Subscriber Identity Module (SIM) that must be present in the handset.
- ◆ SIM cards implement a number of cryptographic algorithms:
 - A3 – an authentication algorithm
 - A5 – a stream cipher
 - A8 – a key agreement algorithm

GSM Security



Source: GSM Security and Encryption, C. Brookson



GSM Algorithms

- ◆ The design of A3 and A8 is not in the GSM specification
- ◆ An example – *COMP128* – is used by many operators
 - COMP128 was cryptanalyzed allowing the recovery of shared master keys – thus allowing cloning of devices



GSM Algorithms

- ◆ There are two versions of the A5 algorithm
 - A5/1 – domestic (strong) version
 - A5/2 – export (weak version)
- ◆ A5 algorithms is part of the GSM spec. but never made public
- ◆ A5/2 was reverse engineered and quickly cryptanalyzed – there is an instant cipher-text only attack on A5/2



GSM Algorithms

- ◆ There have been several attacks on A5/1 – most recently by Barkan et.al., who exploit weaknesses in the protocol (Man-in-the-middle attack)
- ◆ A5/3 has recently been introduced to address some of the problems



General Packet Radio Service (GPRS)

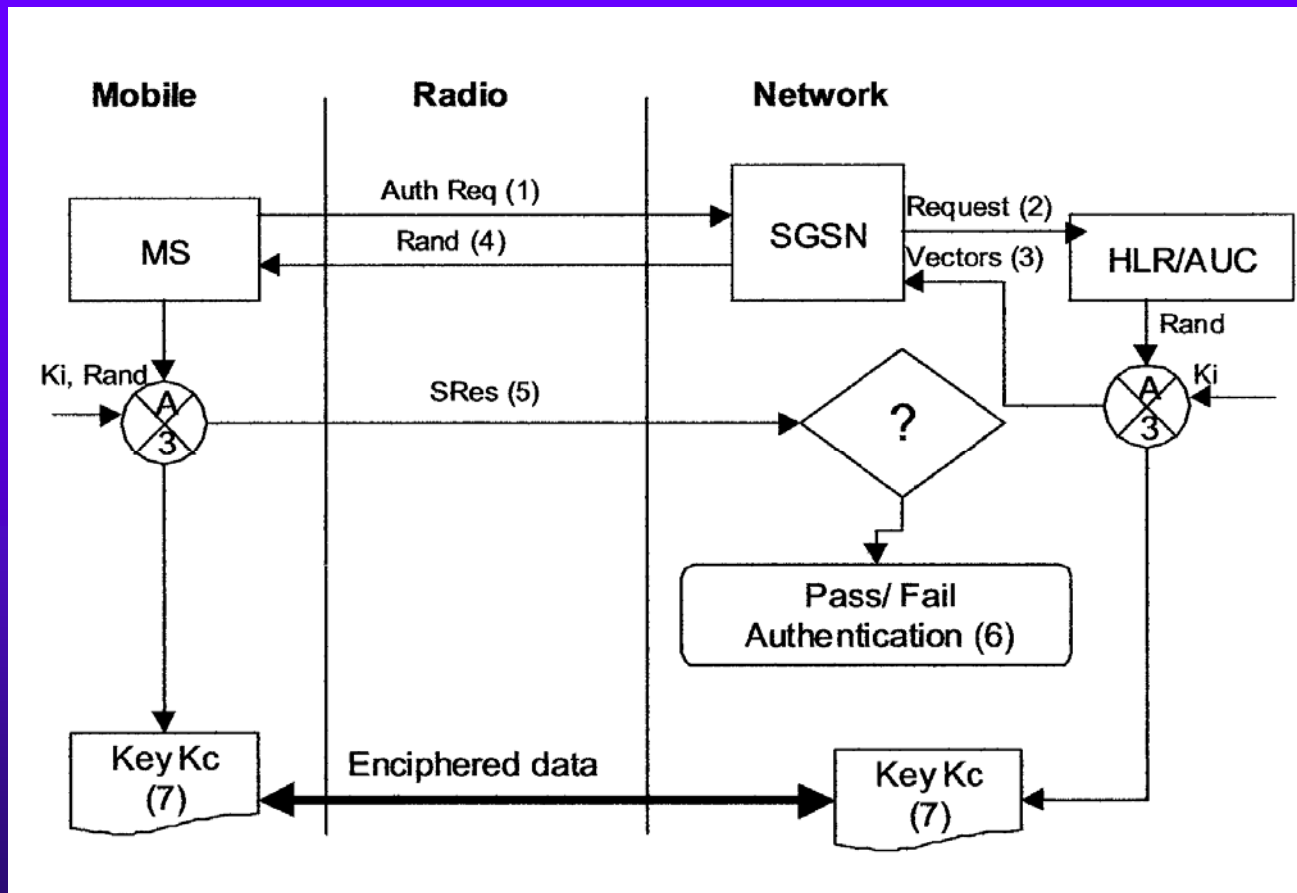
- ◆ GSM service billing is based on connect time – wasteful for data which may be intermittent and bursty
- ◆ GPRS introduced as a packet service providing end-to-end IP connectivity
- ◆ Security very similar to GSM



GPRS Security

- ◆ Components
 - Mobile Station (MS)
 - GPRS Serving Node (SGSN)
- ◆ Use same A3/A8 algorithms of GSM but the randomization function is slightly different
- ◆ Three GPRS Encryption Algorithms (GEA1, GEA2 and GEA3 which is A5/3)

GPRS Security



Source: GPRS Security, C. Brookson



Enhanced Data Rate for GSM Evolution (EDGE)

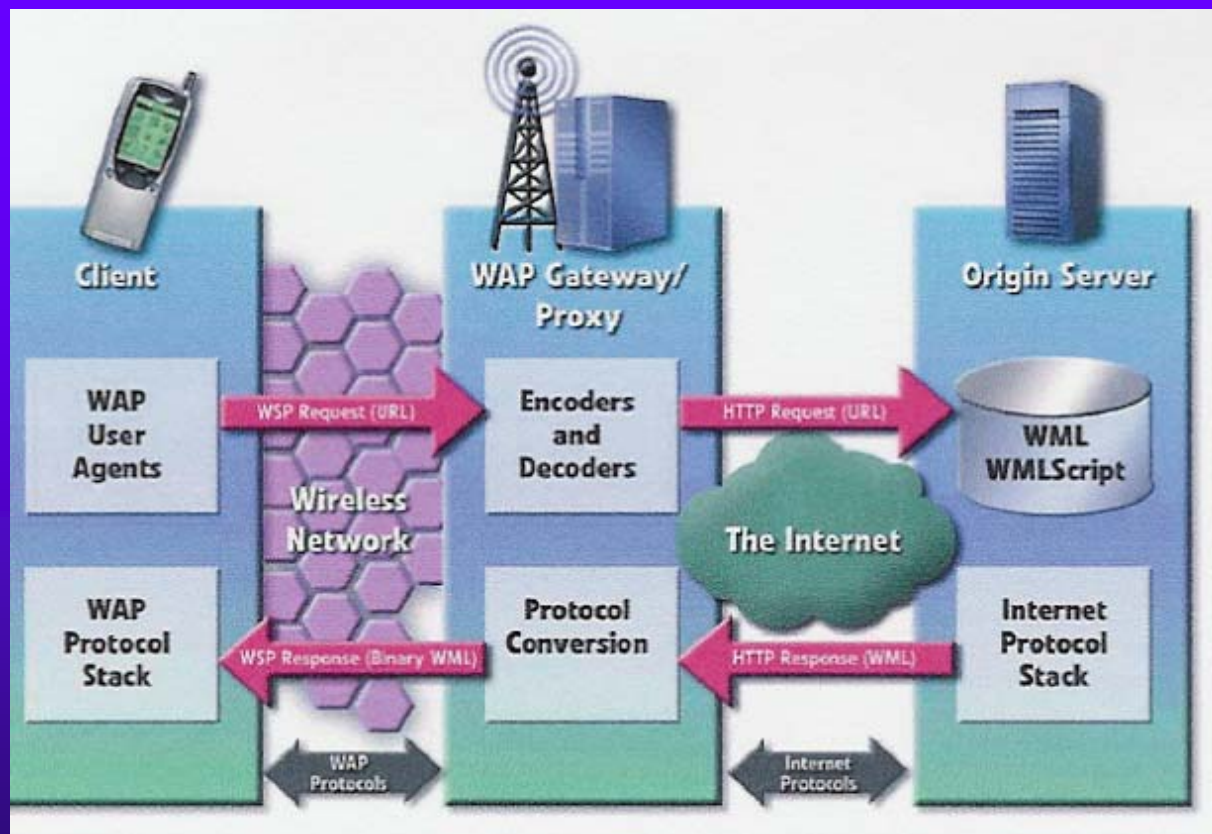
- ◆ Two types of service
 - Packet Switching – Enhanced GPRS
 - Circuit Switching – Enhanced Circuit Switched Data (ECSD)
- ◆ Higher bandwidth available (up to 384Kbps)



Wireless Application Protocol (WAP)

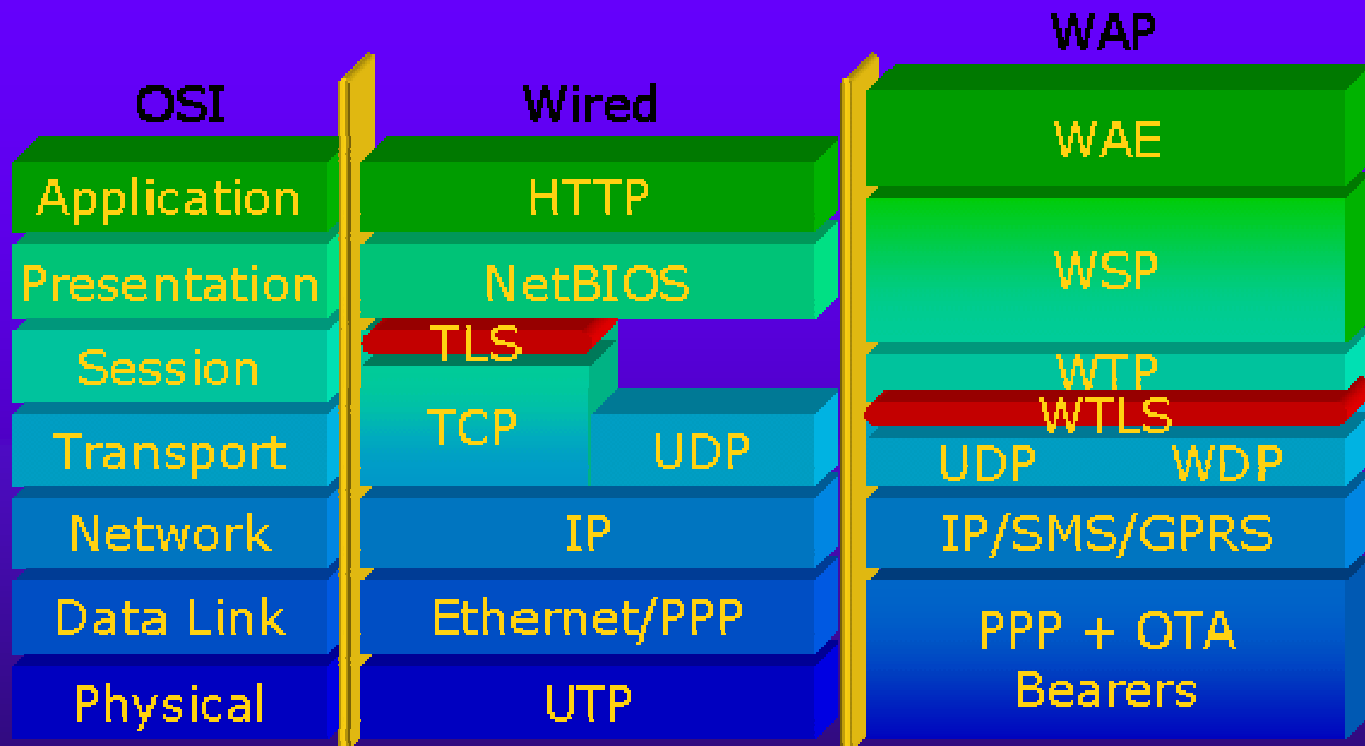
- ◆ WAP defines a set of protocols at the transport, session and application layers to enable advanced mobile services
- ◆ Security was not a primary consideration in the initial architecture (WAP 1.0)
- ◆ WAP was inherited from the Internet

WAP



Source: CERTICOM Corp.

WAP Stack Mapping



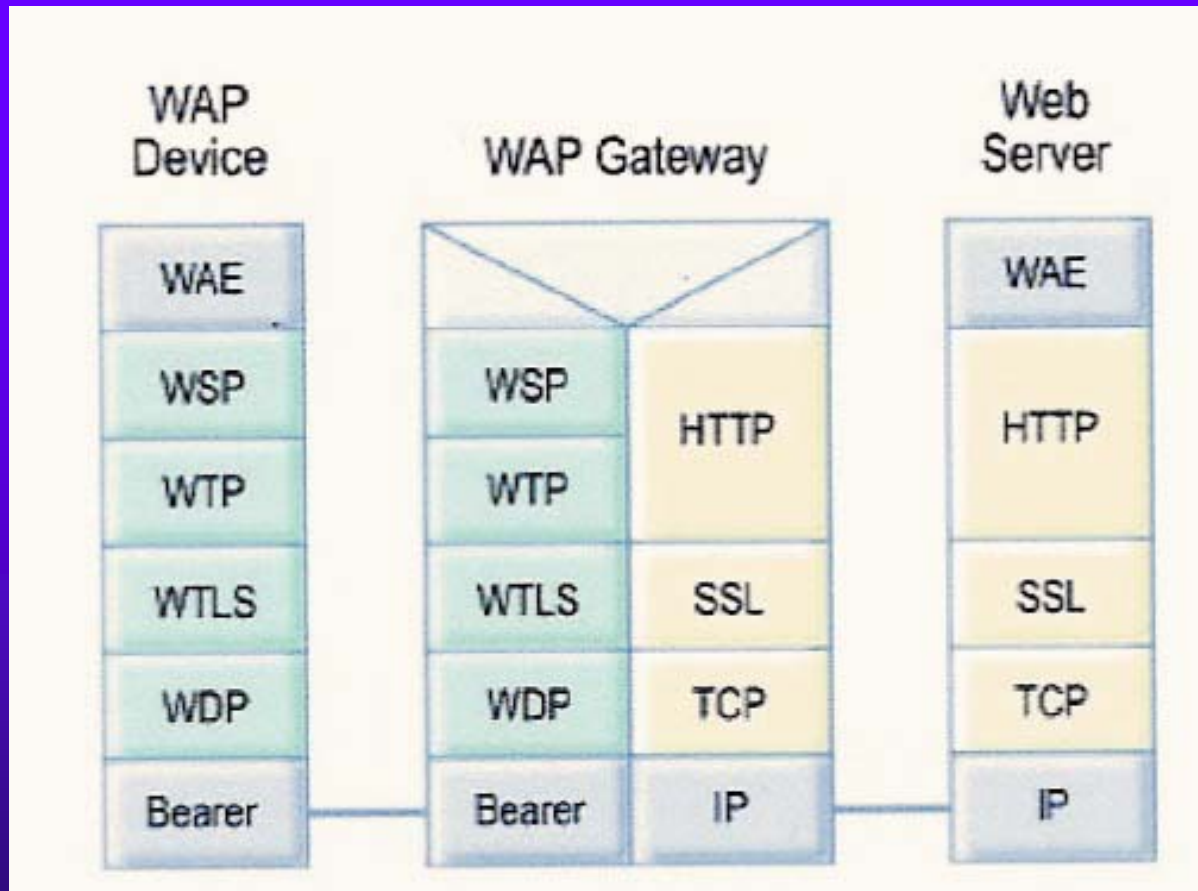
Source: WAP Security, R. Howell



WAP 1.x Security

- ◆ Security in WAP 1.x is in the WTLS protocol
- ◆ WAP Gateway translates WAP protocol to HTTP
- ◆ In reality, there are two connections
- ◆ System security relies on security of Gateway

WAP 1.x



Source: Wireless Application Protocol Forum Ltd.

Workshop on Security in Electronic
Commerce



WAP 2.0 Security

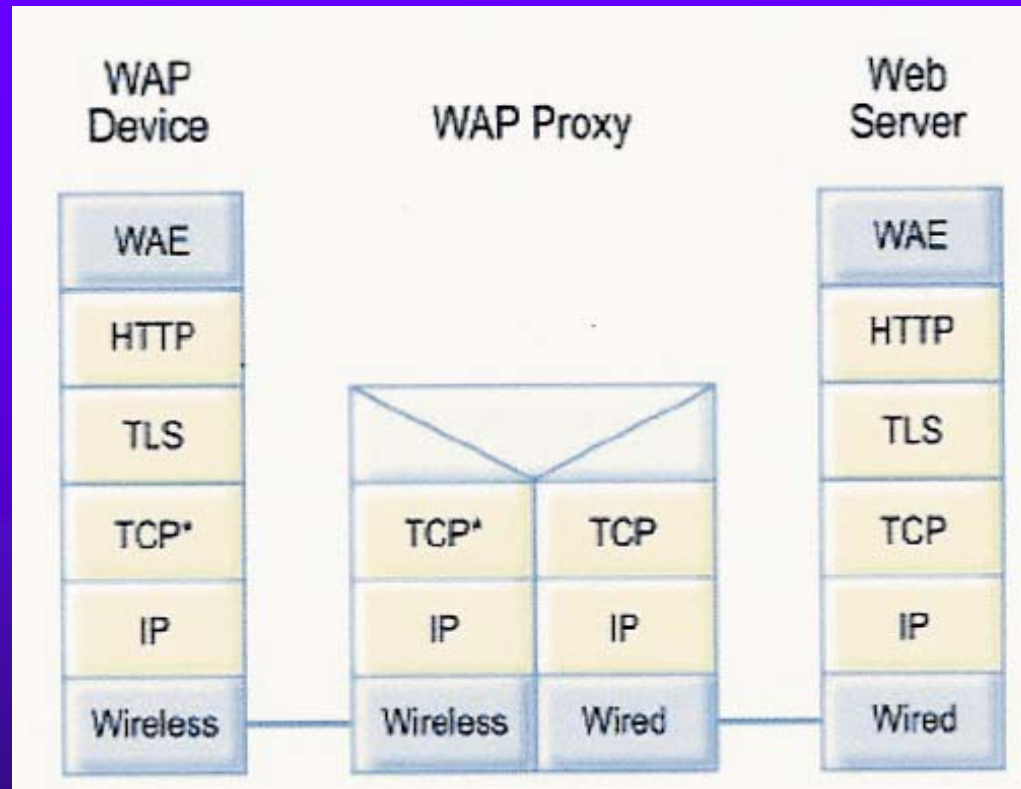
- ◆ There is a need for true end-to-end security
- ◆ WAP 2.0 uses a number of new protocols to provide such connections
 - TLS (which supports WPKI)
 - Wireless Profiled HTTP (WP-HTTP)
 - Wireless Profile TCP (WP-TCP)



Wireless Profiled TCP

- ◆ WP-TCP provides a connection-oriented service optimized for wireless
 - Larger window sizes
 - Selective acks
- ◆ Designed to allow for fading channels, long delay, packet re-ordering, etc.
- ◆ Fully interoperable with TCP

WAP 2.0 Architecture



Source: Wireless Application Protocol Forum Ltd.

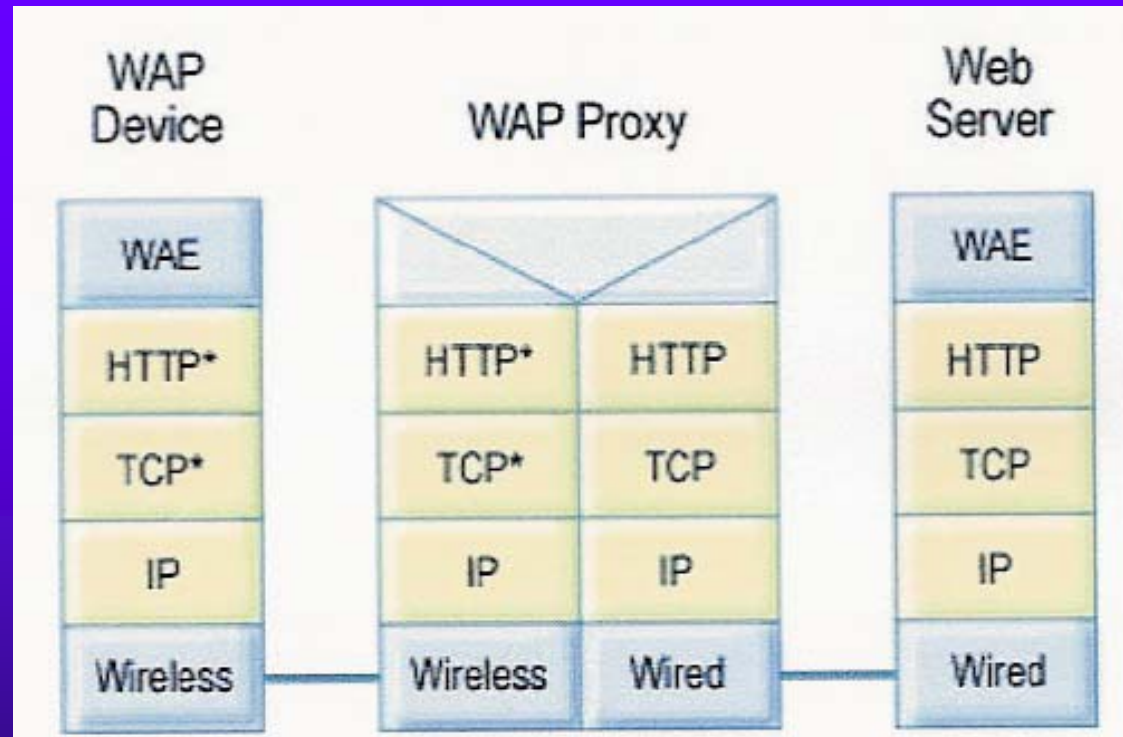
Workshop on Security in Electronic
Commerce



Wireless Profiled HTTP

- ◆ WP-HTTP is interoperable with HTTP 1.1 and again is optimized for the wireless environment
- ◆ It supports the establishment of an end-to-end tunnel

WAP 2.0



Source: Wireless Application Protocol Forum Ltd.



WAP 2.0 Security

- ◆ In addition to end-to-end protocols, WAP 2.0 employs WAP Identity Modules (WIM) – tamper-resistant devices that reside in the WAP enabled device
- ◆ Also, WML Script Crypto API (WMLSCrypt) was developed as an application programming interface that allows access to basic security functions in the WML Script Crypto Library (WMLSCLib)



Future Directions



True Wireless Security

- ◆ Most of the security problems encountered in networks are a result of resource problems in wireless, handheld devices
 - Battery power
 - Processing power
 - Bandwidth
- ◆ (Very similar to the state of desktops 15 – 20 years ago!)



True Wireless Security

◆ What is needed

- Design with security as the primary requirement (not a patch)
- Multiple levels of encryption/authentication
 - Physical
 - IP/TCP
 - Application
- Deployment of full PKI
- Convergence of crypto algorithms



Will it be possible?

- ◆ Battery technology is getting better (but at a much slower rate than processors/memory)
- ◆ Wireless devices have much more powerful processors
- ◆ Bandwidth is increasing
- ◆ We know a lot more about formal security design methods



Questions?