Security in Mobile and Wireless Networks

APRICOT Tutorial
Perth Australia
27 February, 2006

Ray Hunt, Associate Professor
Dept. of Computer Science and Software Engineering
University of Canterbury, New Zealand

1

Security Issues in Wireless and Mobile IP Networks

- Section 1 - Wireless & Mobile IP Architecture, Standards, (Inter)operability, Developments
- Section 2 - Cryptographic Tools for Wireless Network Security
- Section 3 - Security Architectures and Protocols in Wireless LANs
- Section 4 - Security Architectures and Protocols in 3G Mobile Networks

2

Wireless & Mobile IP Architecture, Standards, (Inter)operability, Developments

(Section 1)

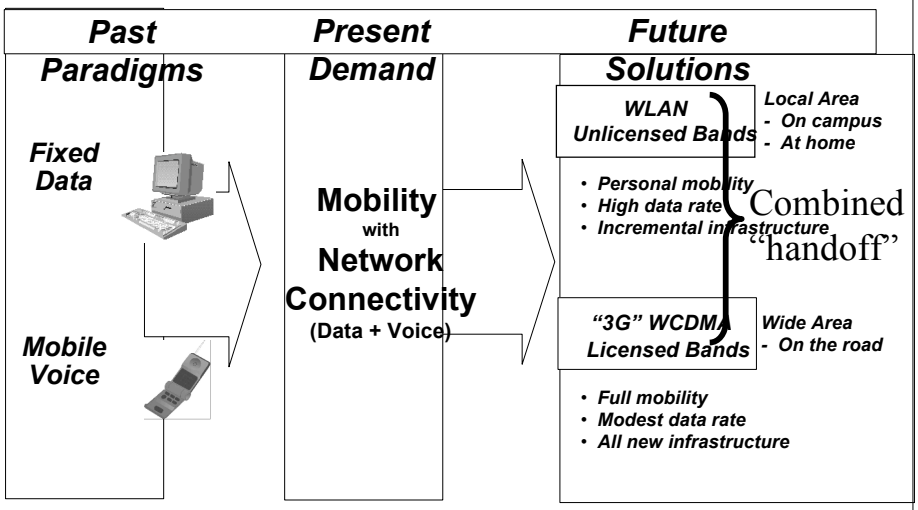
3

Outline

- Wireless LANs – Standards, Architecture
- IP roaming
- Wireless security and authentication
- QoS (Quality of Service)
- Integration of 3G and WLANs
- New Developments by IEEE - Broadband Wireless Access

4

Wireless IP Networking Revolution



5

Recent WLAN Activity ….

- IEEE and ETSI involved in standardisation
- WLAN standards are converging to achieve interoperability
- Integration of WLAN and 3G appearing
- Wireless IP momentum - rapid growth in requirements for mobile IP access
- WLAN offers good mobile solution for indoor IP access
- Major players investing in WLAN (CISCO, Intel, Ericsson, Nokia, others …)

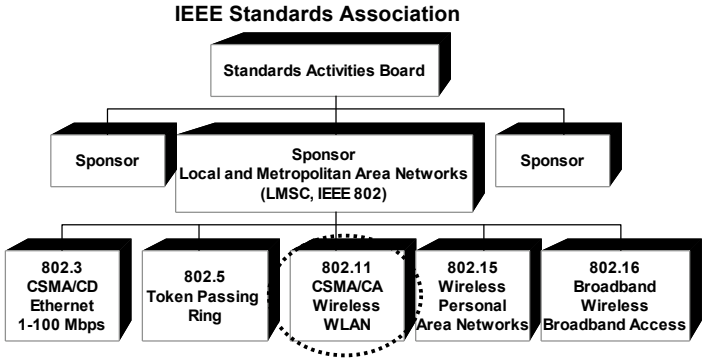
6

WLAN Architecture

Standards, MAC Layer, Frequency Spectrum, Speed/Distance

7

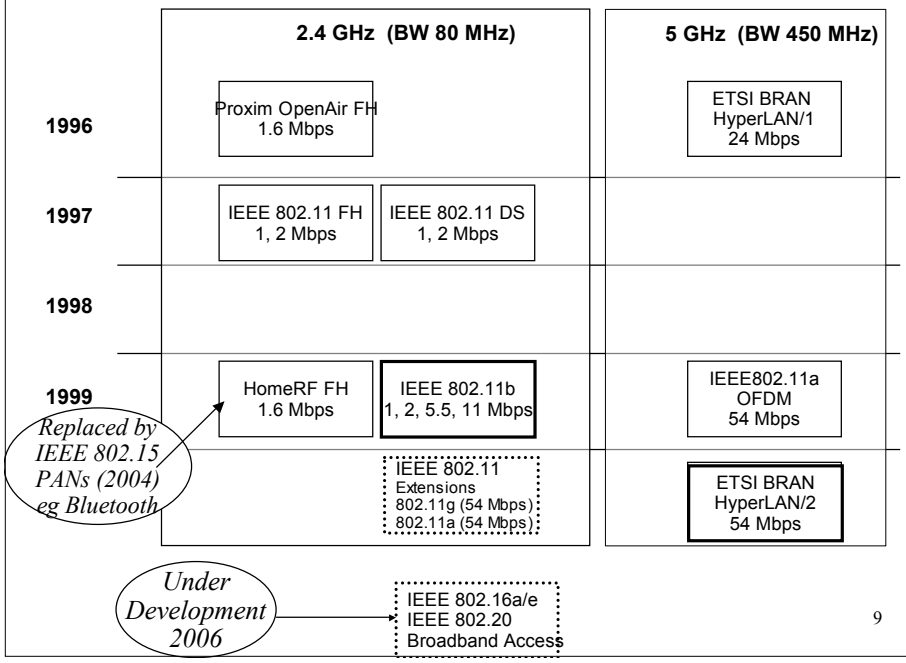
Standards Organisation in IEEE



- IEEE 802.11: ~650 Members, 250+ supporting companies
- www.ieee802.org/11

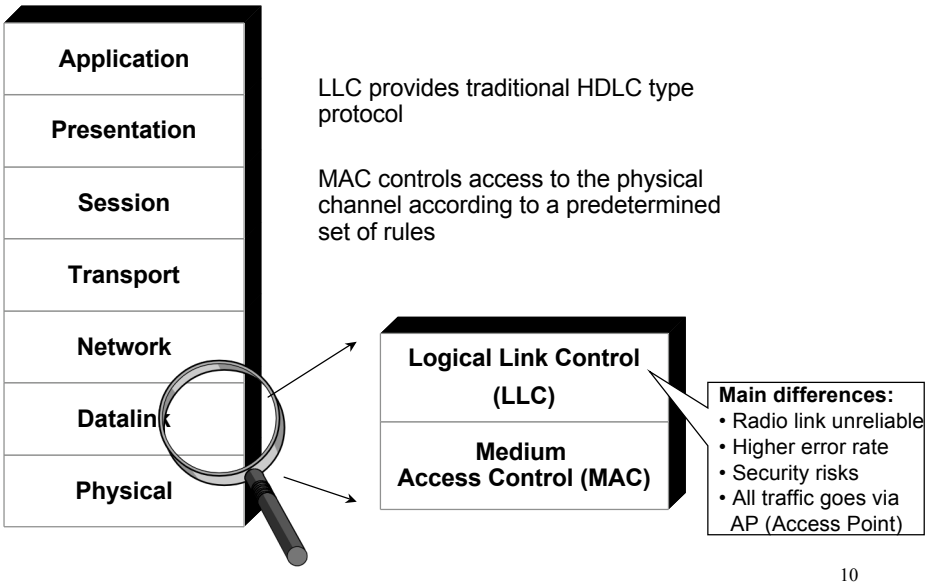
8

WLAN Standards Evolution



9

ISO Model Applied to WLANs



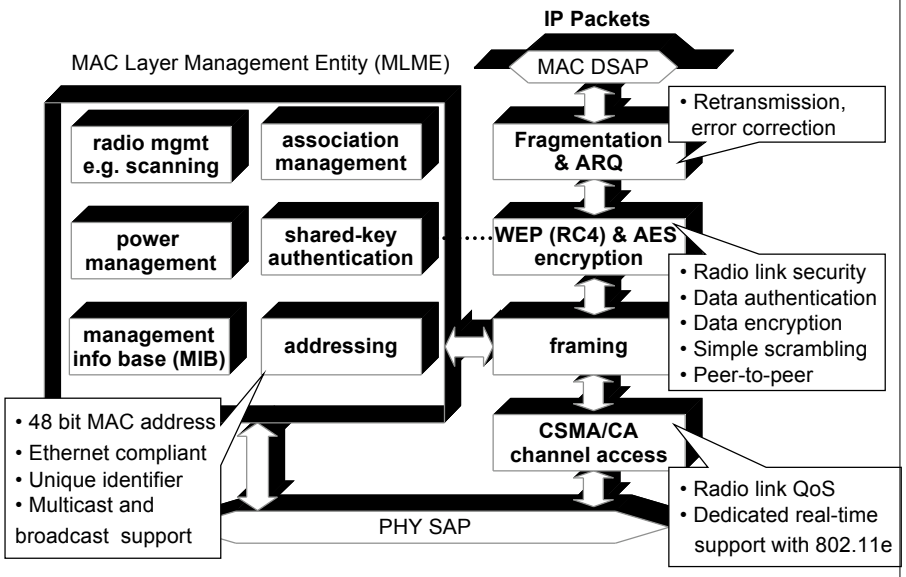
LLC provides traditional HDLC type protocol

MAC controls access to the physical channel according to a predetermined set of rules

Main differences:
- Radio link unreliable
- Higher error rate
- Security risks
- All traffic goes via AP (Access Point)

10

MAC Overview



11

Key Wireless LAN Technologies

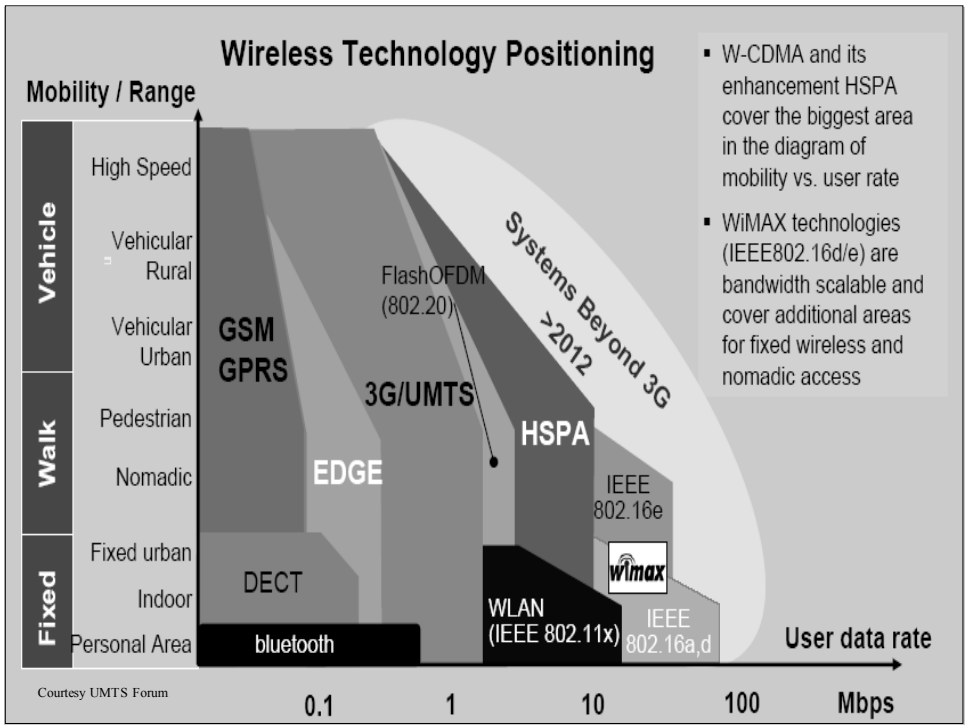
- Older technologies limited speed to 1-2 Mbps
- Significant developments by IEEE 802.11
- Variety of standards → speeds up to 54 Mbps
- IEEE 802.11a/b/g (11 & 54 Mbps) - popular
- To compete with traditional LANs, wireless must offer:
  - cost effect solutions
  - security
  - efficient power management

12

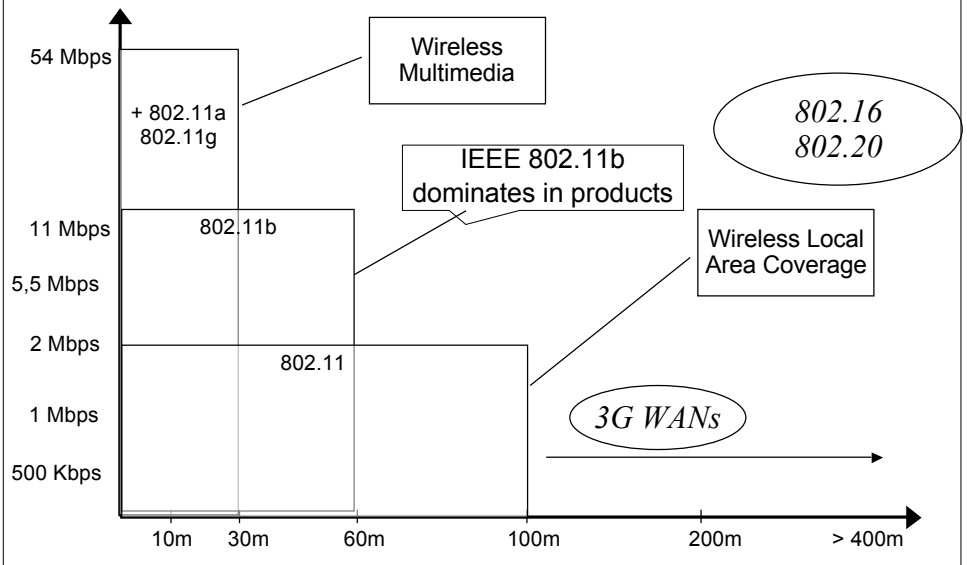
Key Wireless LAN Technologies

- IEEE 802.11b (11 Mbps) 2.4 GHz (Wi-Fi)
- IEEE 802.11a (54 Mbps) 5 GHz (Wi-Fi5)
- IEEE 802.11g (54 Mbps) 2.4 GHz
- IEEE 802.16 / 802.20 Broadband Wireless Access Standard (Wireless MANs)
- Bluetooth Wireless PAN (Personal Area Network) 2.4 GHz (= IEEE 802.15) www.bluetooth.com
- HomeRF (1.6 Mbps) 2.4 GHz www.homerf.org

13



WLANs: Speed/Distance Scenarios



15

IEEE 802.11 Standards contd ...

	802.11a	802.11b	802.11
Standard Approved	September 1999	September 1999	July 1997
Available Bandwidth	300MHz	83.5MHz	83.5MHz
Unlicensed Frequencies of Operation	5.15-5.35GHz, 5.725-5.825GHz	2.4-2.4835GHz	2.4-2.4835GHz
Number of Non-Overlapping Channels	4 (Indoor) 4 (Indoor/Outdoor) 4 (Indoor/Outdoor)	3 (Indoor/Outdoor)	3 (Indoor/Outdoor)
Data Rate per Channel	6, 9, 12, 18, 24, 36, 48, 54 Mbps	1, 2, 5.5, 11 Mbps	1, 2 Mbps
Modulation Type	OFDM	DSSS	FHSS, DSSS

ATM Speed

IEEE 802.11g

Ethernet Speed

16

“Actual” Realistic Speeds

Link Rate	11a 1500Byte throughput at: 0% PER	10% PER	50% PER
6 Mbps	5.4	4.8	2.5
24 Mbps	17.7	15.7	6.7
48 Mbps	28.7	25.3	9.5
[illegible]	[illegible]	[illegible]	9.9

MAC / PHY overhead

Higher rate & PER -> lower throughput

Link Rate	11b (long preamble) throughput: 0% PER	10% PER	50% PER
1 Mbps	0.9	0.8	0.4
2 Mbps	1.7	1.6	0.8
5.5 Mbps	4.0	3.6	1.6
11 Mbps	6.4	5.6	2.2

PER: Packet Error Rate

Courtesy of Atheros

17

IEEE 802.11a/b/g

- IEEE 802.11 Working Group provided extensions to 802.11b for data rates above 20 Mbps leading to IEEE 802.11g
- IEEE 802.11g offers 802.11a data rates in 2.4 GHz band and requires mandatory implementation of IEEE 802.11b modes
- This standard provides a path for development of multi-mode WLAN products

IEEE 802.11a → IEEE 802.11g ← IEEE 802.11b

18

Summary of Key Differences

Standard	Distance (m)	Speed (Mbps)	Power (mw)
IEEE802.11b	<100	11 (~6)	50-100
IEEE802.11g	<100	54 (~30)	50-100
IEEE802.11a	<50	55 (~30)	200
Bluetooth	10-100	1	1 (10m) 100 (100m)

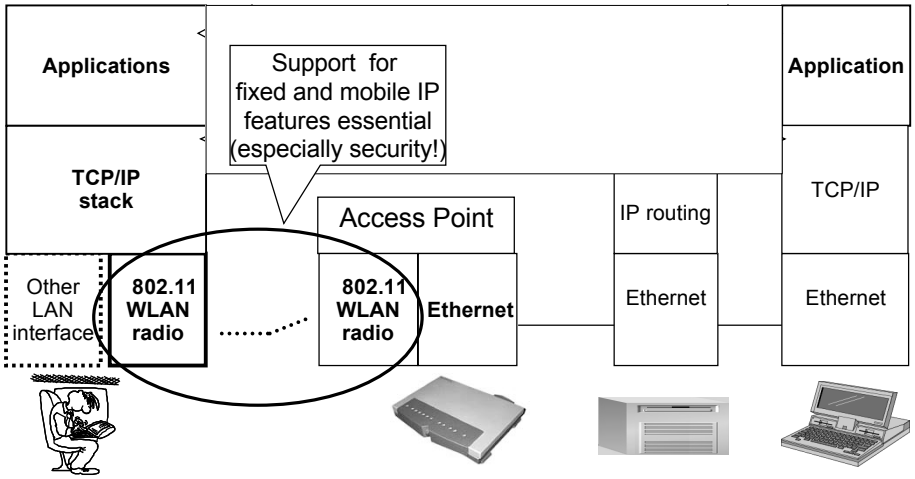
19

Additional Requirements …..

- IP Mobility between WLAN subnets and into 3G networks
- Authentication - local and remote
- Security across the airwaves, end-to-end, Wireless LAN, Wireless WAN (3G)
- Quality of Service - to support time dependant applications

20

WLAN - Plain Wireless Ethernet Extension for IP Mobility



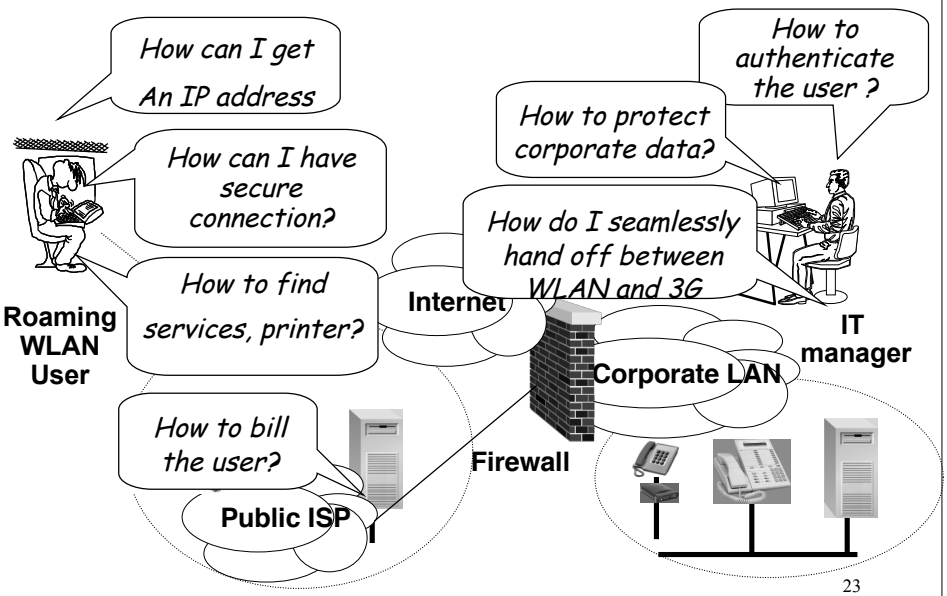
21

Design Challenges for IP Mobility

- Roaming IP devices with changing IP address, service location and ISP
- IP backbone and access networks have not been designed for mobile stations
- Wireless link is vulnerable to security attacks
- Wireless link subject to QoS (Quality of Service) deterioration

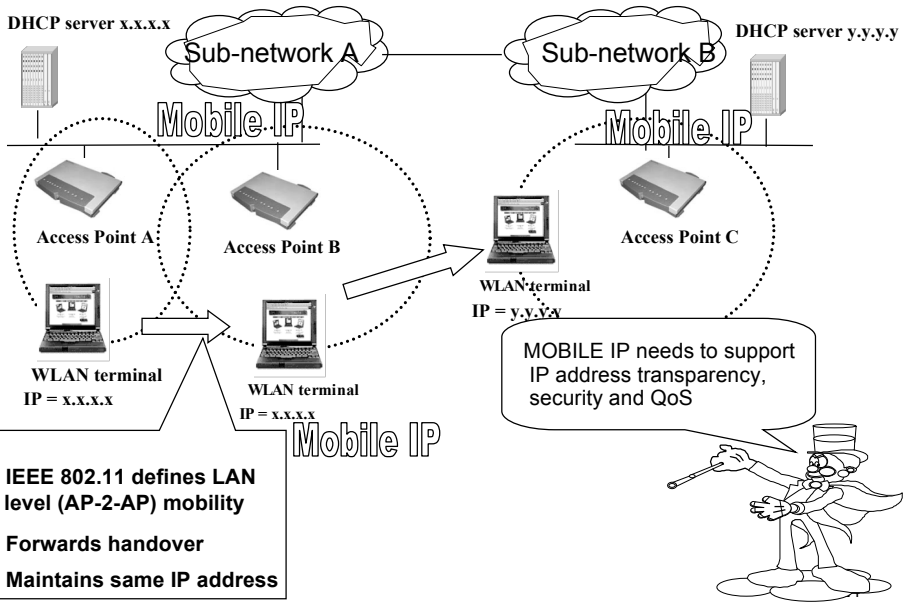
22

Challenges for IP Mobility



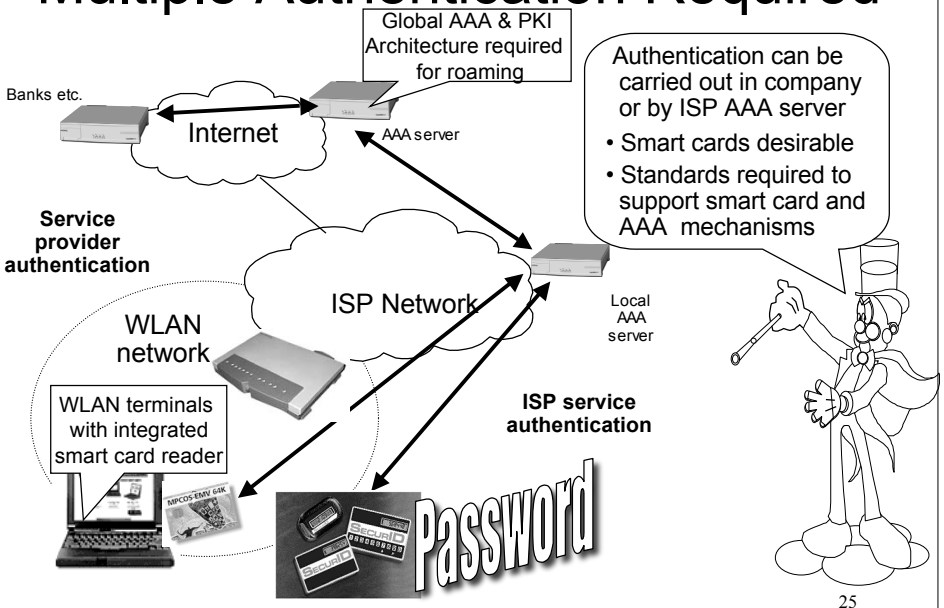
23

Essential WLAN Mobility Support



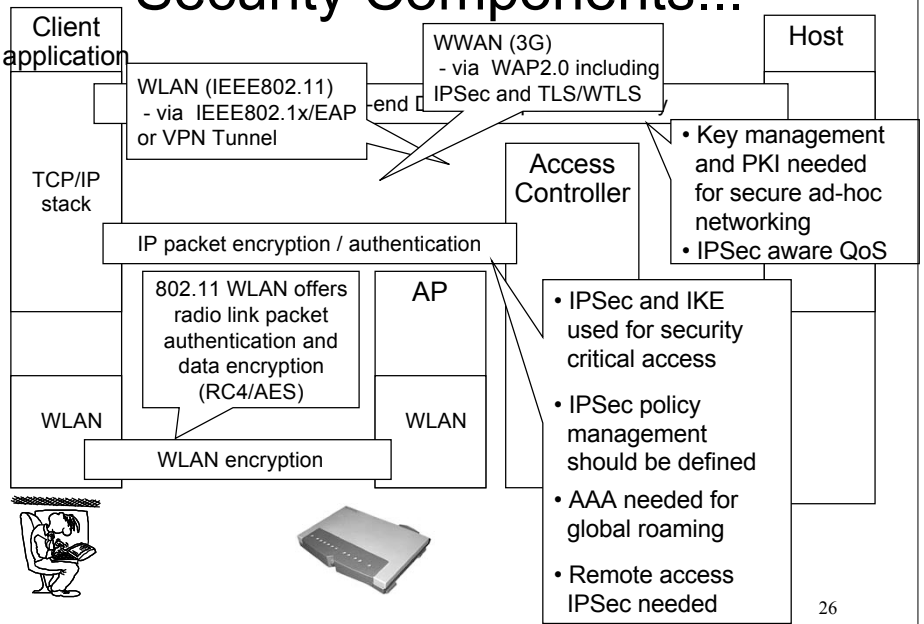
- **IEEE 802.11 defines LAN level (AP-2-AP) mobility**
- **Forwards handover**
- **Maintains same IP address**

Multiple Authentication Required



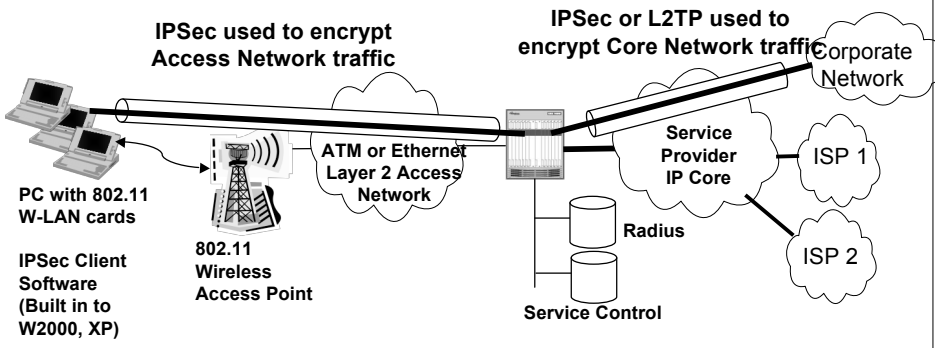
25

Security Components...



26

Hotspot Service with IPSec



- IPSec can be combined with Hotspot service to provide secure, encrypted traffic across access network
- This overcomes the security issues associated with WLAN networks

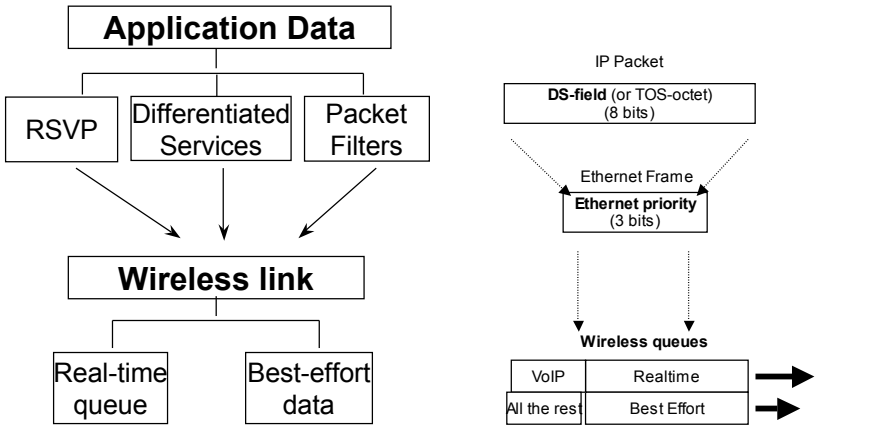
27

Quality of Service in WLANs

- Current WLAN devices mostly still operate with “best effort” data transmission - this has to change…..
- WLANs need to support voice over IP. Hence radio link QoS is essential
- Operators would like to apply traffic-based billing → QoS support needed

28

Mapping IP QoS into WLAN



WLAN QoS resembles 802.1p&Q approach:
- **Separate wireless link queues and priority scheduling**
- **IP packet filters and DiffServ bits define the queue**

Problems to Be Solved

- Terminal Mobility in the IP network
  - WLAN solves LAN level mobility but...
  - How to support mobility between IP sub-networks?

Mobile IP

- Security Issues
  - User authentication, encryption, billing etc
  - End-to-end data security and remote access

IPSec + IKE

- Configuration and Service discovery
  - How to know essential network parameters
  - How to locate services in a new network

CDP, SLP

- Wireless Quality of Service
  - How to map IP QoS classes into radio link
  - TCP behaviour is not optimal in wireless world

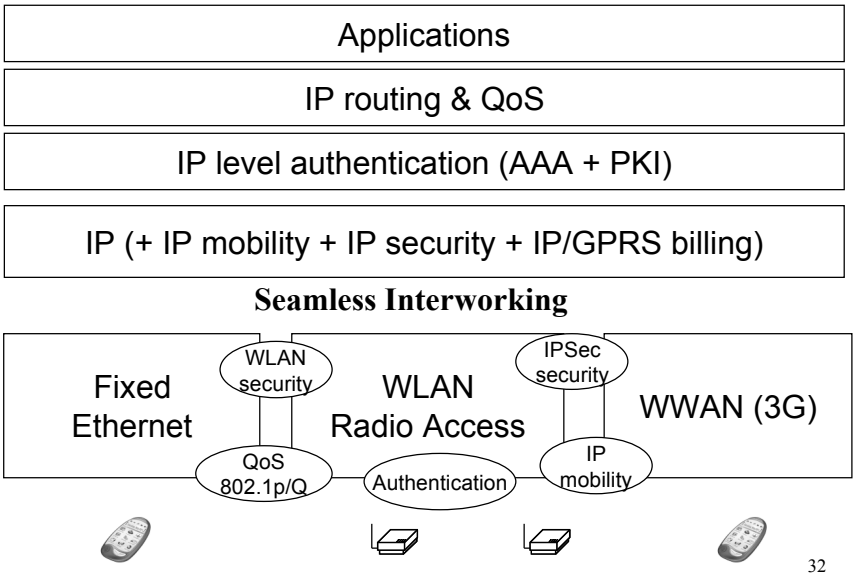
DiffServ, RSVP

30

The Desired Wireless Mobile IP Architecture Model

31

Layered View: IP Interworking



32

What is needed now is …

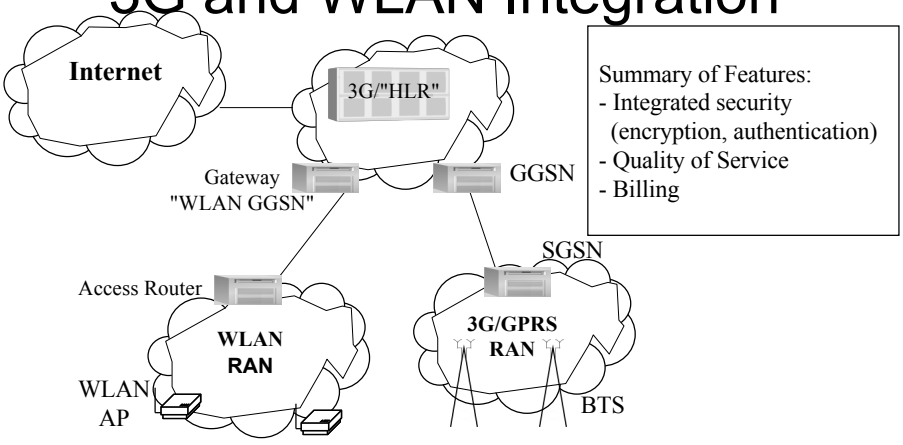
- 3G and WLAN Integration / Interworking
- 3G and WLAN Management

…. together with seamless:

IP roaming mobility
Security (authentication and encryption)
QoS
Billing etc

33

3G and WLAN Integration



Summary of Features:
- Integrated security (encryption, authentication)
- Quality of Service
- Billing


Multimode terminal with 3G user identity

SGSN - Serving GPRS Support Node
GGSN - Gateway GPRS Support Node
HLR - Home Location Register
RAN - Radio Area Network
BTS - Base Transceiver Station

34

WLAN Access Point Management

- Essential management features include:
  - Network Deployment Aid - Radio Frequency optimisation and site survey deployment aids
  - Rogue Access Point Detection - Wireless and wireline scanning mechanisms
  - Network Monitoring - Alerting, event capture, performance, reporting
  - Security Policy and Authentication Server - Kerberos, Active Directory, LDAP integration, etc
  - Policy Enforcement - Identifying misconfigured or insecure APs/devices, auditing network activity, penetration testing and detection

37

Other Standards and New Developments

IEEE 802.11e, .11f, .11h, .11i

http://standards/ieee.org/getieee802

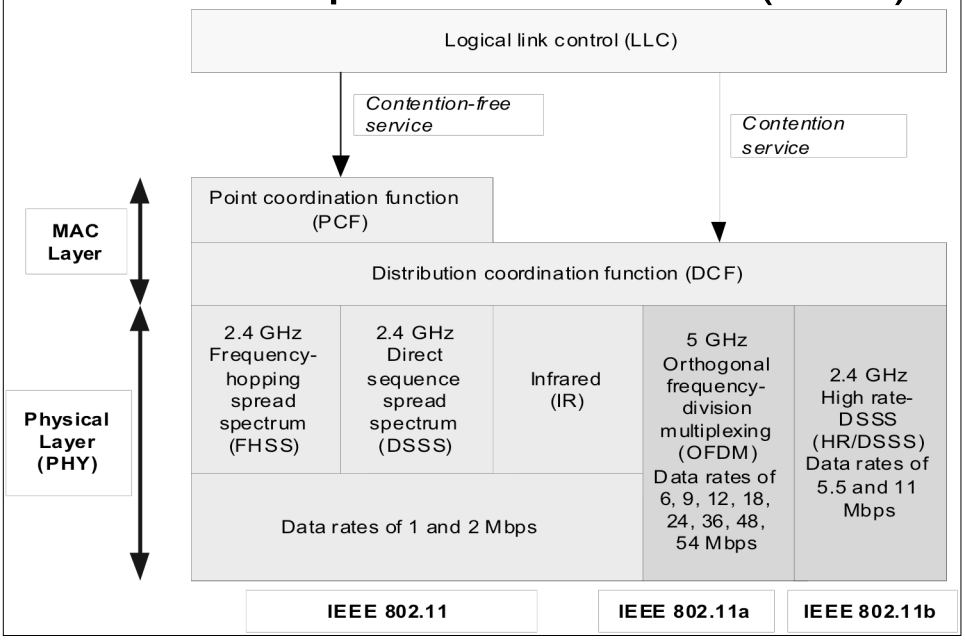
38

Task Group IEEE 802.11e (QoS)

- What is it?
  - Enhance 802.11 Medium Access Control (MAC) to improve and manage Quality of Service and provide classes of service
- Key Proposals:
  - EDCF - Referred to as “prioritised QoS.” Application assigns different priorities and allows them to contend for simultaneous channel access
  - HCF – Access Point creates a master schedule based on different traffic types. The AP then grants access to each station by individually polling each station. No contention (related to PCF).

39

Task Group IEEE 802.11e (QoS)



Task Group IEEE 802.11e (QoS)

- Quality of Service (QoS) Goals:
  - Data traffic:
    - Voice: ADPCM….20 msec
    - MPEG video – 3 Mbps, MPEG2, Firewire
    - TCP/IP Ethernet data streams at 10 Mbps
  - Quantify QoS Parameters
    - Jitter
    - Delay/Latency variations
    - Maximise throughput
  - Define traffic models for both Ad-hoc and Infrastructure
    - QoS support through handoff between BSS
    - 802.11a/g – 54 Mbps and 802.11b – 11 Mbps

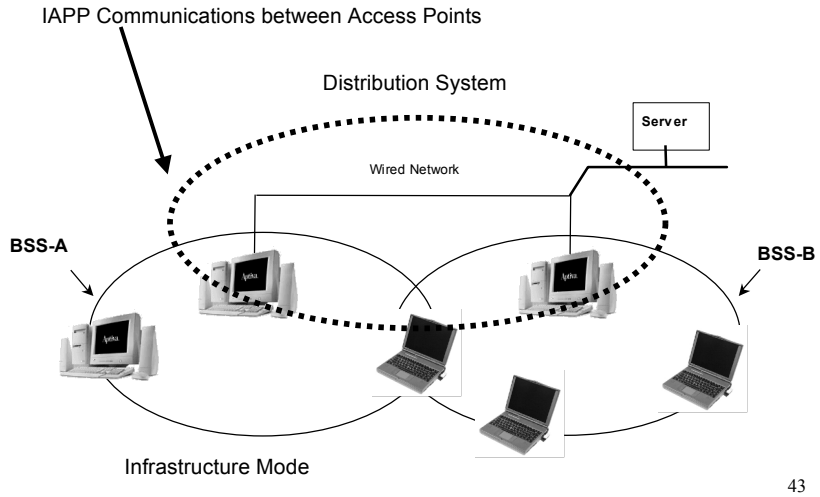
41

Task Group IEEE 802.11f (Inter-Access Point Protocol)

- What is it?
  - Develop recommended practices for an Inter-Access Point Protocol (IAPP) which provides capabilities to achieve multi-vendor Access Point interoperability across a Distribution System supporting IEEE 802.11
- Key Issues:
  - Interoperability
  - Security
  - Performance
- Next steps
  - Adopt draft and ratify standards

42

Task Group IEEE 802.11f (Inter-Access Point Protocol)



43

Task Group IEEE 802.11h DCS/TPC

- What is it?
  - Enhance 802.11 MAC and 802.11a PHY to provide Dynamic Channel Selection (DCS), and Transmit Power Control (TPC). Products achieve regulatory approval in respective country
- Key Proposals:
  - DCS (Dynamic Channel Selection)
    - To pass radar avoidance tests from the European Regulatory Committee (ERC)
    - New management packets for DFS request / responses
  - TPC (Transmit Power Control)
    - AP broadcasts a maximum “local” transmit power as a beacon element and probes response
    - Stations can independently choose a power level below

44

Task Group IEEE 802.11i (Advanced Security)

- What is it?
  - Enhance IEEE 802.11 MAC to improve security and authentication mechanisms. Also referred to as RSN (Robust Security Network). Ratified 2004
- Key Issues
  - Authentication
    - Recommend IEEE 802.1x and EAP as a 'framework'
    - Recommended practice for using Kerberos/RADIUS in this framework without mandating it
  - Encryption
    - AES with dynamic key exchange
    - Incorporates TKIP (Temporal Key Integrity Protocol)
    - Also referred to as WPA2 (WiFi Protected Access)
  - Available

45

Task Group IEEE 802.11i (Advanced Security)

- Implementation Issues
  - WPA was developed to address the poor key management issues associated with using WEP (incorporated TKIP). WPA still uses WEP
  - WPA2 (true 802.11i) uses AES encryption instead of WEP
  - This involves new hardware (APs and WNIC cards)
  - As of November 2004 this hardware is available but the true firmware to operate WPA2 available from mid 2005
  - This new hardware is backward compatible with WEP/WPA

46

IEEE 802.15 Standards Evolution

- IEEE 802.15.1
  - IEEE TG1 on PAN (Personal Area Networks) adopts Bluetooth as IEEE802.15.1
- IEEE 802.15.2
  - Changes to Bluetooth / 802.15.1, designed to mitigate interference with 802.11b/g networks
  - All use same 2.4GHz frequency band
  - Devices need 802.15.2 (or proprietary scheme) if they want to use both Bluetooth and 802.11b/g simultaneously

47

IEEE 802.15 Standards Evolution

- IEEE 802.15.3
  - Called UWB (Ultra Wide Band)
  - Speeds up to 55 Mbps (or possibly 100 Mbps)
  - Good for transferring large files, images
- IEEE 802.15.4
  - Called Zigbee (cheap wireless technology)
  - Speeds likely to be 10 Kbps and 115.2 Kbps
  - Low cost/low power home appliances

48

Proposed Applications for UWB (IEEE 802.15.3)

- Commercial:
  - High speed LANs/WANs (>20 Mbps)
  - Altimeter/Obstacle avoidance radars for commercial aviation
  - Precision Geolocation Systems
  - Industrial RF Monitoring Systems
  - Collision avoidance sensors
- Military:
  - Groundwave Communications
  - Intrusion Detection Radars
  - Unmanned Vehicles

49

IEEE 802.15 Project Activity

Project	Data Rate	Range	Configuration	Other Features
802.15.1 (Bluetooth)	1 Mbps	10M (class 3) 100M (class 1)	8 active device Piconet/ Scatternet	Authentication, Encryption, Voice
802.15.3 High Rate (UWB)	22, 33, 44, 55, 100 Mbps	10M	256 active device Piconet/ Scatternet	QoS, Fast Join Multi-Media
802.15.4 Low Rate (Zigbee)	10, 115.2 250 Kbps	10M nominal 1M-100M based on settings	Master/Slave (256 Devices or more) Peer to Peer	Battery Life: multi-month to infinite
802.15.SG3a Alternate 15.3 PHY	>100 Mbps	10M nominal	256 active device Piconet/ Scatternet	
802.15.2 Coexistence	Develop a Coexistence Model for 802.11 and 802.15.1/Bluetooth eg AFH (Adaptive Frequency Hopping) and BIAS (Bluetooth Interference Aware Scheduling)			

802.11 and Bluetooth

IEEE 802.16 Broadband Wireless Access Standard

- IEEE 802.16 - Wireless MANs or Wireless Digital Subscriber Loop (W-DSL or W-LL)
- IEEE 802.16a standard approved in 2003
- Air interface specification
- Licensed/licensed-exempt 2-11 GHz and 10-66 GHz bands
- Speeds up to 72 Mbps
- Designed for “first mile” and “last mile” access

51

Wireless Local Loop Access (W-DSL or W-LL or BWA or WiBRO)

- Broadband Implementation
  - Scalable
  - Central shared portal equipment
  - Initial investment – low cost of deployment
  - Individualised services
  - Designed for situations where fibre loop is impractical / expensive
  - Likely to be based upon new IEEE 802.16a standard

52

WiMAX

- Industry group promoting deployment of broadband wireless access networks via:
  - standards (IEEE 802.16a)
  - certifying interoperability of products and technology
- http://wimaxforum.org
- http://bbwexchange.com (Broadband Wireless Exchange)

53

Mobile Broadband Developments - IEEE 802.16e and 802.20

- Similarities and differences….
- Both specify new *mobile* air interfaces for wireless broadband services
- 802.16e: 2-6 GHz band 802.20: <3.5 GHz
- 802.16e builds on 802.16a (WiMax Forum)
- 802.16e due for completion 2006
- 802.20 starting from scratch
- 802.16e products likely earlier than 802.20

54

New Developments - IEEE 802.16e and 802.20

- 802.20 to operate at speeds < 250 kph (trains)
- 802.16e to operate at speeds <100 kph (cars)
- Boost real-time data in metropolitan areas to rival current DSL services based on 15 km cell
- 802.20 will have bigger footprint than 802.16e
- Single base station to support fixed and mobile broadband wireless access
- 802.20 - competes with 3G networks in certain areas

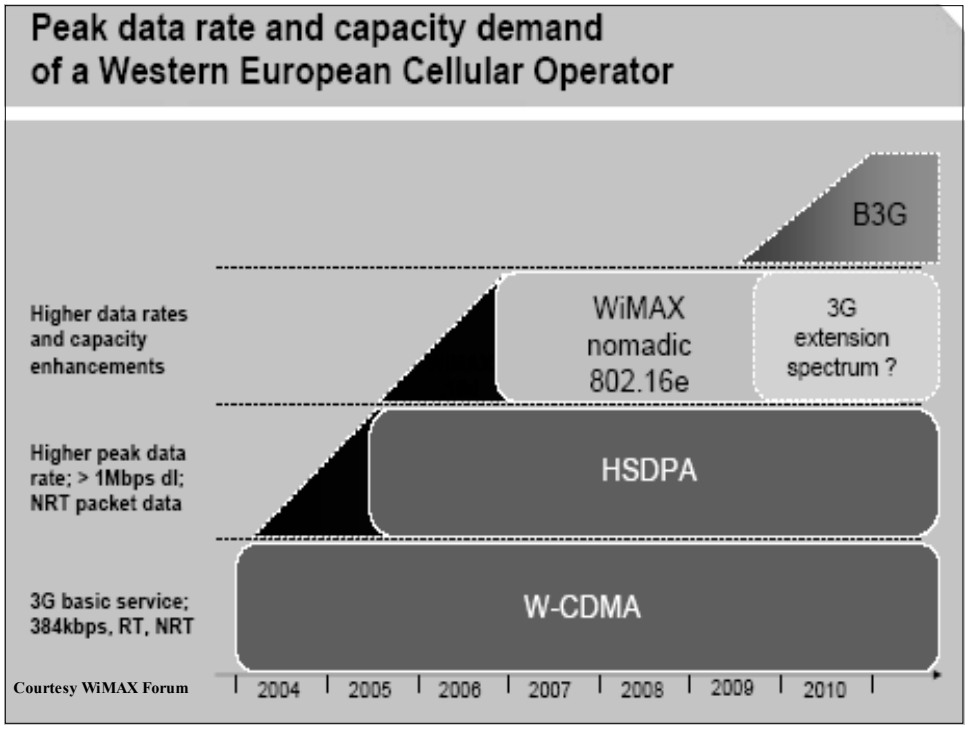
55

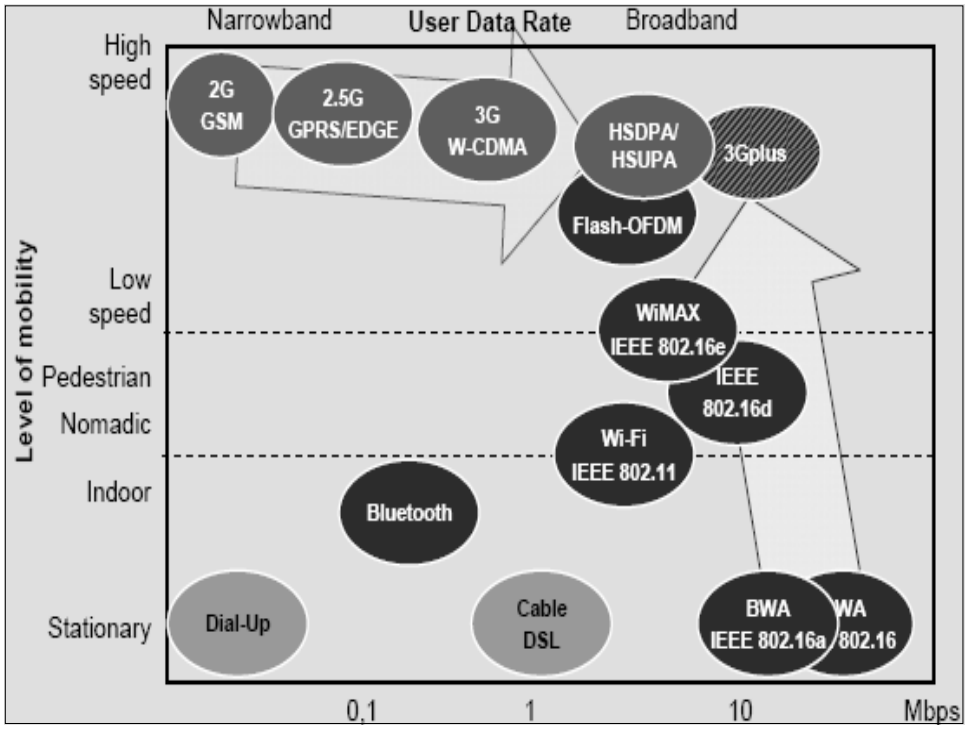
IEEE802.16/802.16e Standards

	802.16-2004	802.16e
IEEE Approval	June 2004 (formerly 802.16d)	Pending (est. Q4 2005)
Subscribers	Fixed / Portable	Fixed / Portable / Mobile
Channel Conditions	LOS, Near-LOS, Non-LOS	
Modulation	OFDM-256	S-OFDMA (128-2000)
Duplexing	TDD / FDD	
Sub-Carrier Modulation	BPSK, QPSK, 16QAM, 64QAM	
Channel Bandwidth	Scalable: 1.25 MHz - 20 MHz	
Data Rate (Peak)	75 Mbps @ 20 MHz 15 - 18 Mbps @ 5 MHz	15 Mbps @ 5 MHz
Cell Range	20+ km: rural 2 to 5 km: suburban, urban	1 - 3 km: indoor 2 - 5 km: outdoor

LOS: Line of Sight
OFDM(A): Orthogonal Frequency Division Multiplexing (Access)

56


Peak data rate and capacity demand
of a Western European Cellular Operator
B3G
Higher data rates
and capacity
enhancements
WiMAX
nomadic
802.16e
3G
extension
spectrum ?
Higher peak data
rate; > 1Mbps dl;
NRT packet data
HSDPA
3G basic service;
384kbps, RT, NRT
W-CDMA
Courtesy WiMAX Forum
2004
2005
2006
2007
2008
2009
2010


Narrowband
User Data Rate
Broadband
High
speed
Low
speed
Pedestrian
Nomadic
Indoor
Stationary
Level of mobility
2G
GSM
2.5G
GPRS/EDGE
3G
W-CDMA
HSDPA/
HSUPA
3Gplus
Flash-OFDM
WiMAX
IEEE 802.16e
IEEE
802.16d
Wi-Fi
IEEE 802.11
Bluetooth
Dial-Up
Cable
DSL
BWA
IEEE 802.16a
WA
802.16
0,1
1
10
Mbps

New Developments by IEEE

- IEEE802.11k
  - Standardisation of radio measurements across different manufacturers platforms
- IEEE802.11r
  - Task group focusing on reducing handoff latency when transitioning APs in an Extended Service Set. Critical for real-time and delay sensitive applications
- IEEE802.11s
  - Infrastructure mesh standards to allow APs from multiple manufactures to self-configure in multi-hop networks

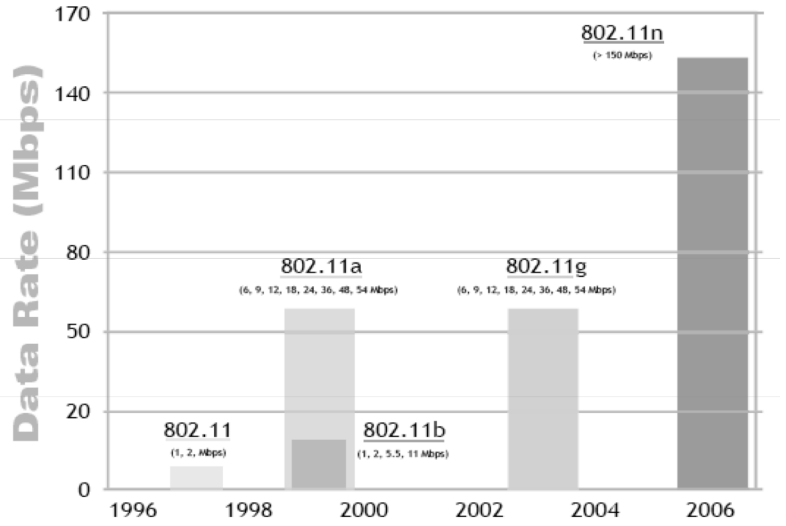
59

New Developments by IEEE

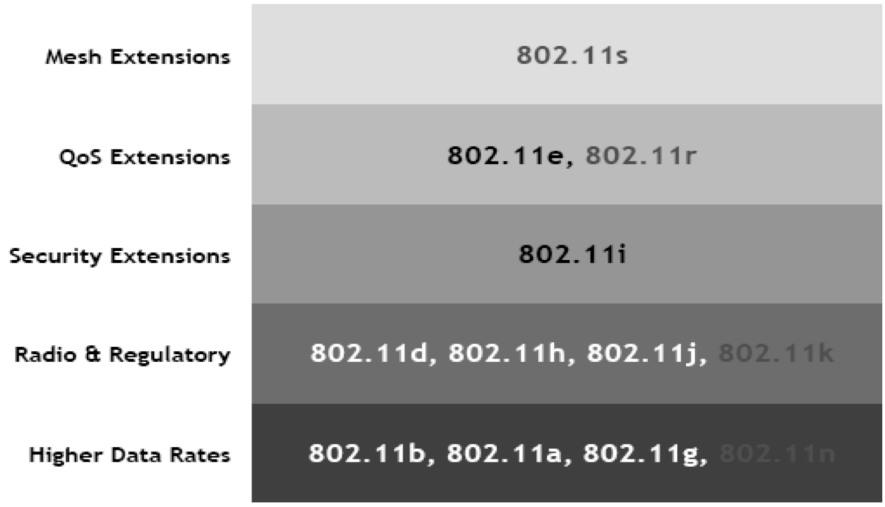
- IEEE802.11n
  - >150 Mbps across an 802.11 communications channel for data intensive applications and aggregation of traffic from multiple APs
- IEEE 802.17
  - Resilient Packet Ring Access Protocol for Local, Metropolitan and Wide Area Networks
  - Transfer rates scalable to gigabits/sec
  - Resilient architecture supporting QoS classes

60

New Developments by IEEE – emerging data rates



New Developments by IEEE



Items in red indicate standards not yet approved (2006)

Summary and Requirements

- IEEE wireless standards are becoming mature
- IEEE 802.11b/g leading standards in use today
- New requirements for
  - Authentication
  - IP mobility
  - Security
  - QoS (Quality of Service)
- IPv6 solves most of the listed obstacles with native mobility and security → should be adopted

63

Cryptographic Tools for Wireless Network Security

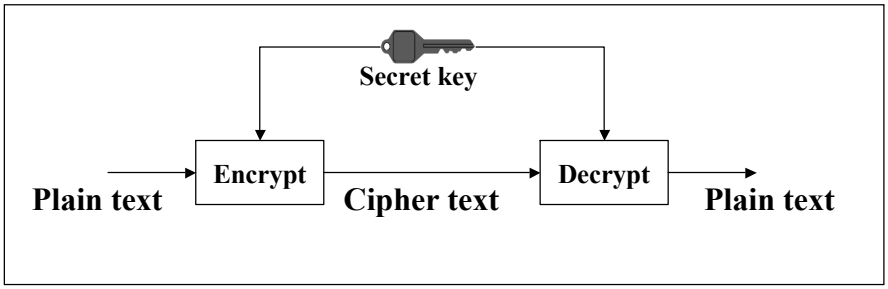
(Section 2)

Introduction to Cryptography

- Confidentiality – ensures that only the recipient sees message contents
- Integrity – receiver able to verify that message has not been modified in transit
- Authentication – enables receiver to ascertain message's origin
- Nonrepudiation – prevents sender from denying they sent message

Encryption issues

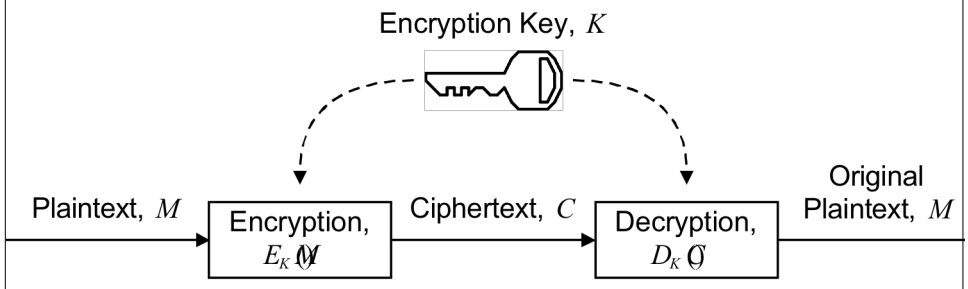
"Symmetric encryption" **...is also called...** **"Shared key encryption"**



The foundation for bulk encryption

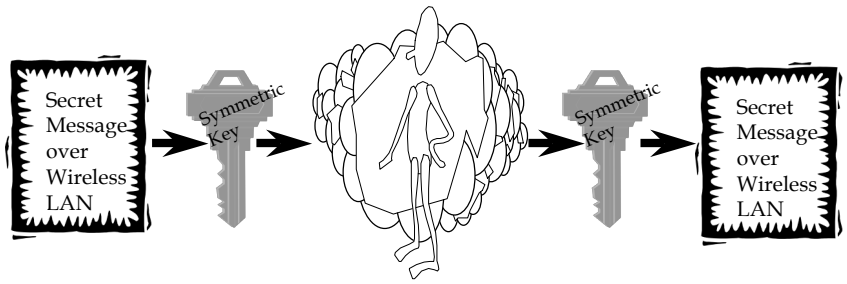
Secret-Key (Symmetric) Cryptography

- Sender and receiver share same key for encryption and decryption
- Distribution and storage of these keys presents major problems
- Key management for multiple participants is also a problem
- Problem insurmountable when end parties do not know each other and a secure channel does not exist



Symmetric Algorithm
Encryption and Decryption

Symmetric Key



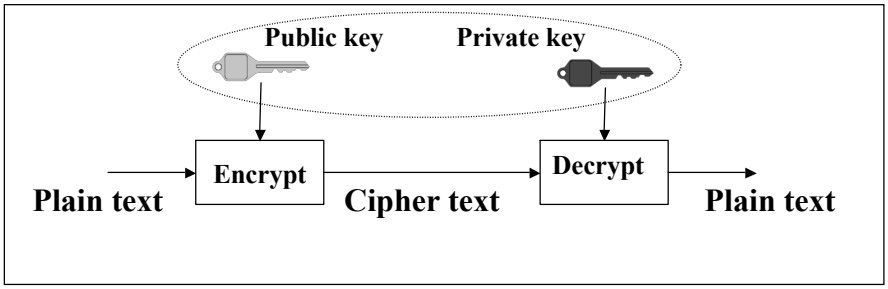
The same key is used to encrypt
and decrypt the data.
DES is one example, RC4 is another.

Symmetric Key

- *The Advantages*
  - Secure
  - Widely Used
  - The encrypted text is compact
  - Fast
- *The Disadvantages*
  - Complex Administration
  - Requires Secret Key Sharing
  - No non-repudiation
  - Subject to interception

Encryption issues

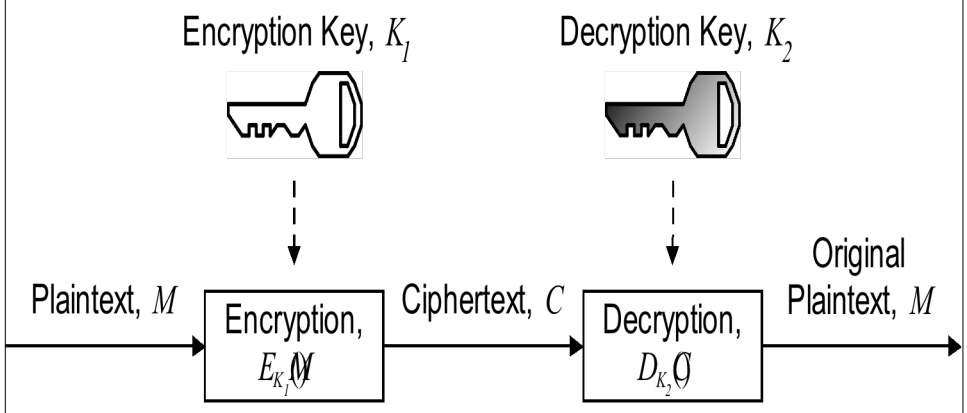
"Asymmetric encryption" ...is also called... "Public key encryption"



The foundation for the PKI

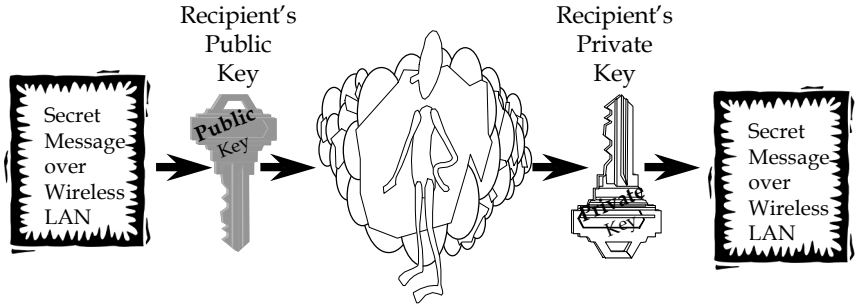
Public Key (Asymmetric) Cryptography

- Sender and receive have different keys (key pair) for encryption and decryption
- Key pairs mathematically dependant - message encrypted by one key can only be decrypted by other key
- Anybody can encrypt with public key but only receiver can decrypt with private key
- Common use of public key cryptography is to create a digital signature



Asymmetric Algorithm Encryption and Decryption

Public/Private Key

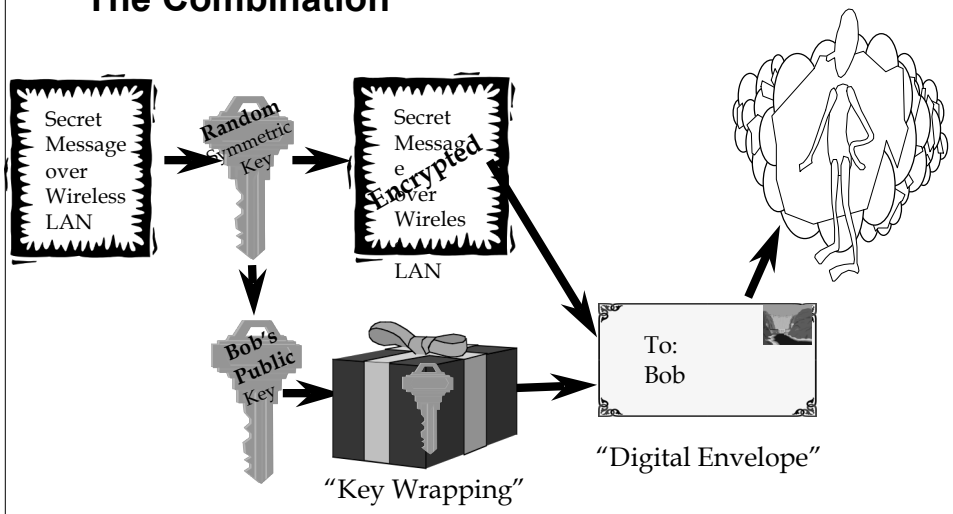


What is encrypted with one key,
can only be decrypted with the other key.
RSA is one example, Elliptic Curve is another.

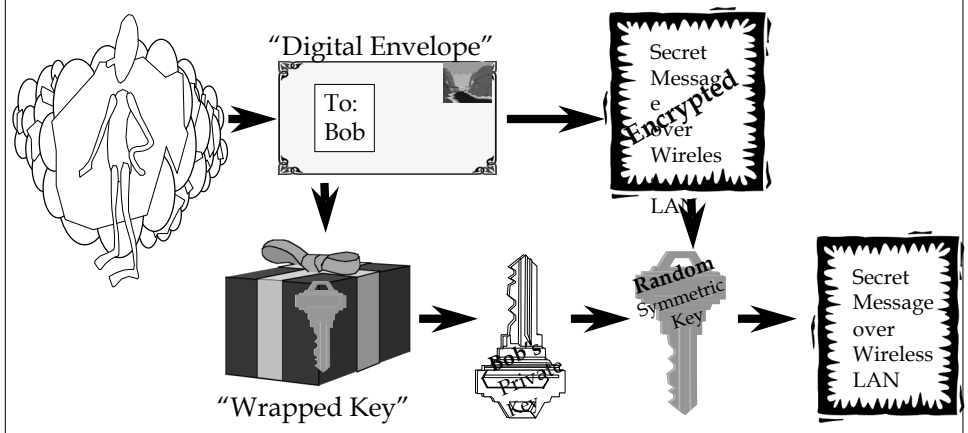
Public/Private Key

- *The Advantages*
  - Secure
  - No secret sharing
  - No prior relationship
  - Easier Administration
  - Supports non-repudiation
- *The Disadvantages*
  - Slower than symmetric key
  - Encrypted text is larger than with symmetric version

The Combination



The Combination



The Combination

- You get the best of both worlds
  - The benefits of Symmetric Key
    - Speed
    - Compact Encrypted Text
  - The benefits of Public Key
    - Simpler Key Management
    - Digital Signature
    - Non-Repudiation

Encryption examples

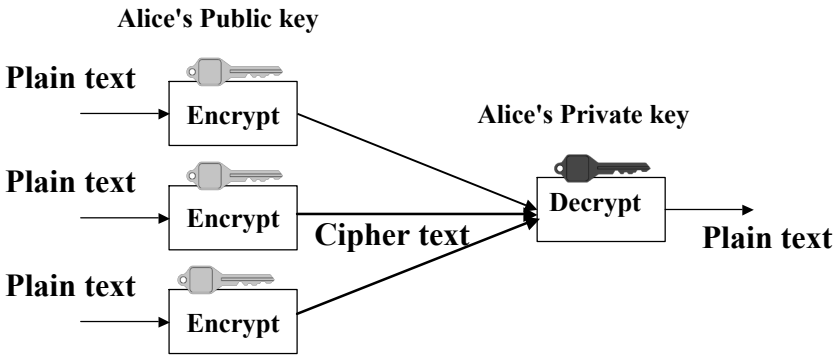
Some symmetric encryption algorithms

- **WEP (RC4)**
- **DES / 3DES**
- **RC2, RC4, RC5**
- **Blowfish**
- **IDEA**
- **CAST**
- **AES (Rijndael)**
- **...**

Some asymmetric encryption algorithms

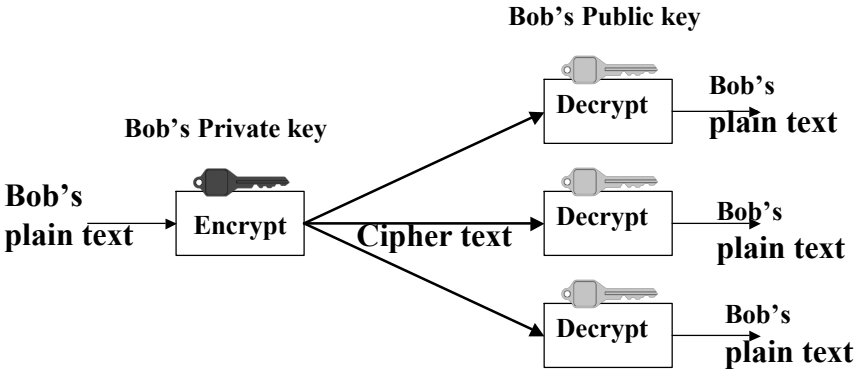
- **RSA**
- **Elliptic Curve Crypto (ECC)**
- **Diffie-Hellman/Elgamal**

Encryption



Many users may encrypt data that only the holder of the private key can decrypt

Authentication

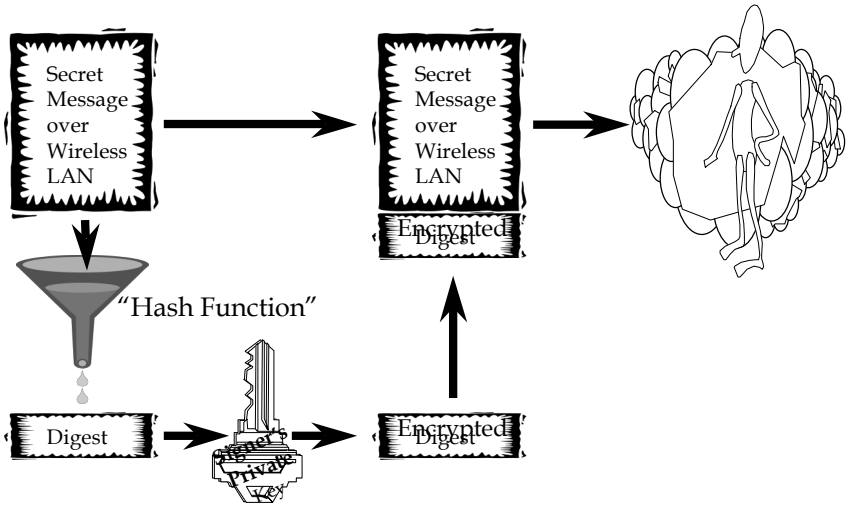


The private key can be used to "encrypt" data so others may authenticate its source

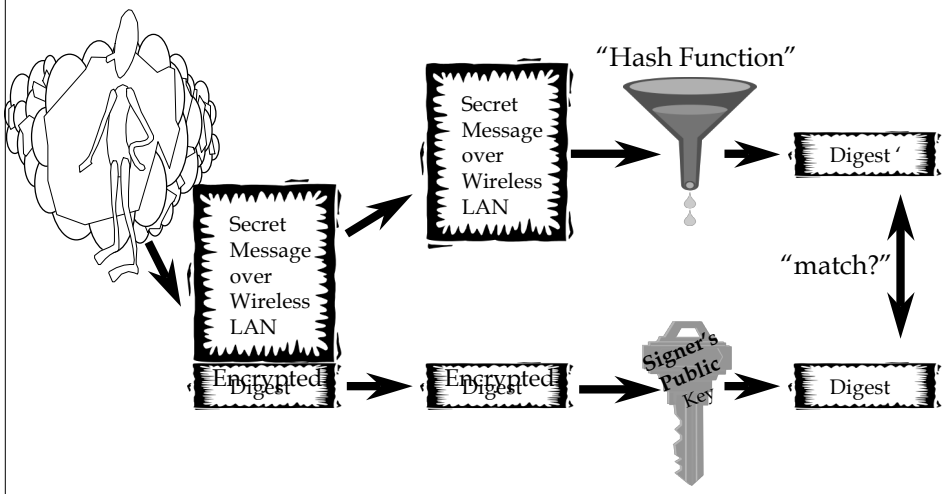
Supported security services

Strong authentication
Digital signatures
Encryption key distribution

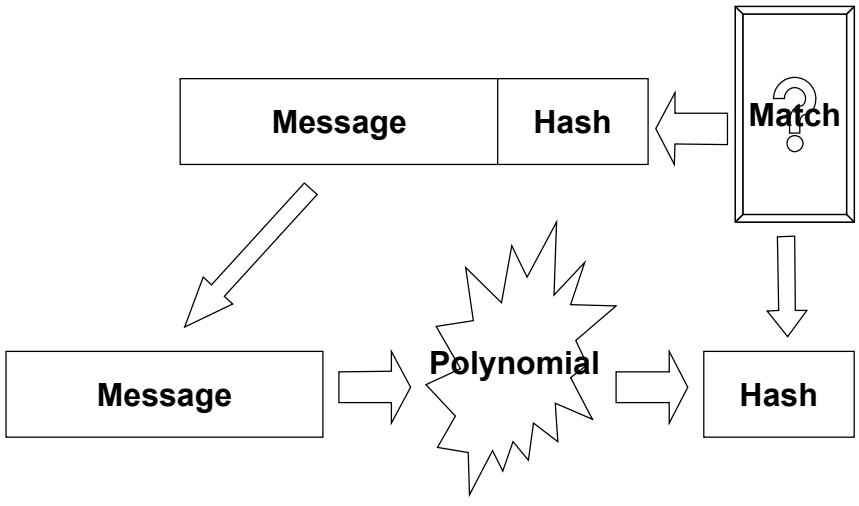
Digital Signatures for Strong Authentication



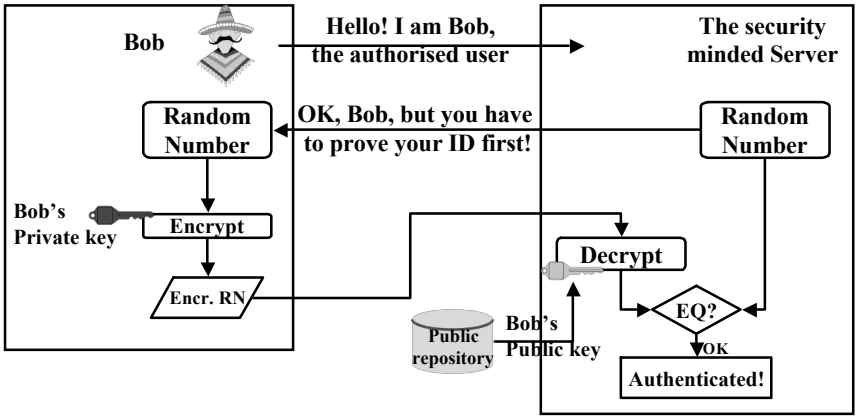
Digital Signatures for Strong Authentication



Creating the Hash for Strong Authentication

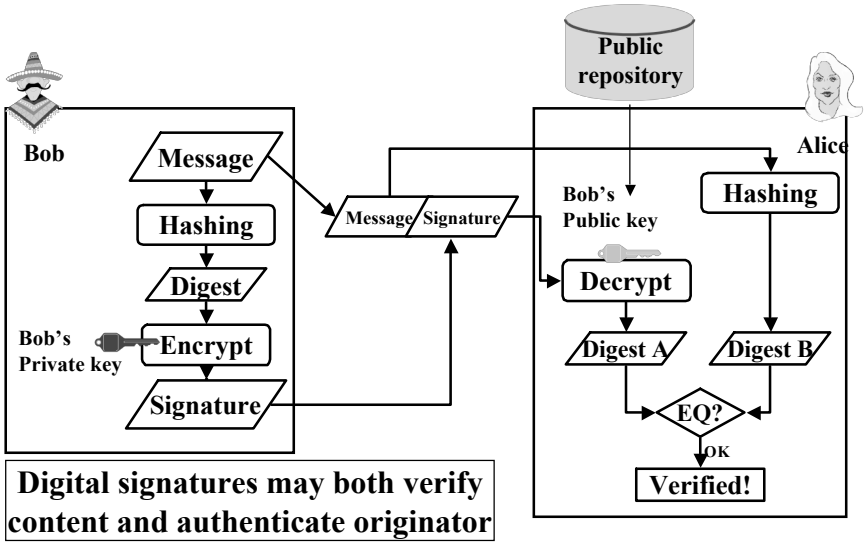


Strong Authentication



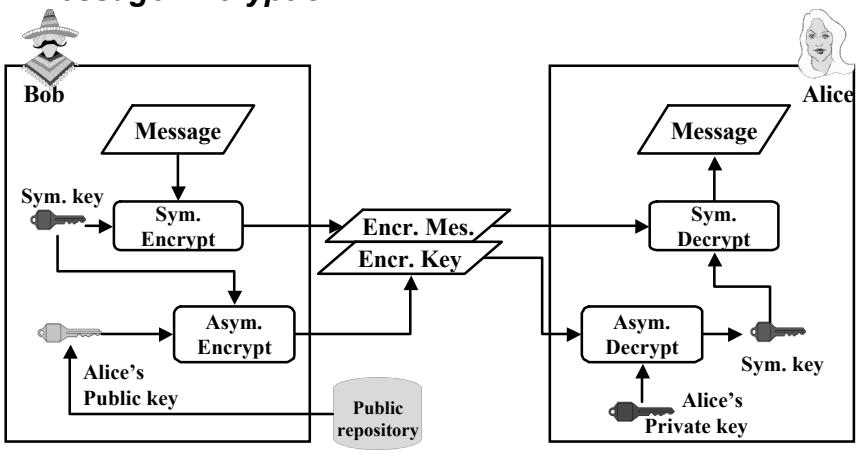
By digitally signing a random number we can authenticate the user

Digital Signatures



Digital signatures may both verify content and authenticate originator

Message Encryption



Public key encryption is only used for key distribution

Note! Bob's identity is not validated!

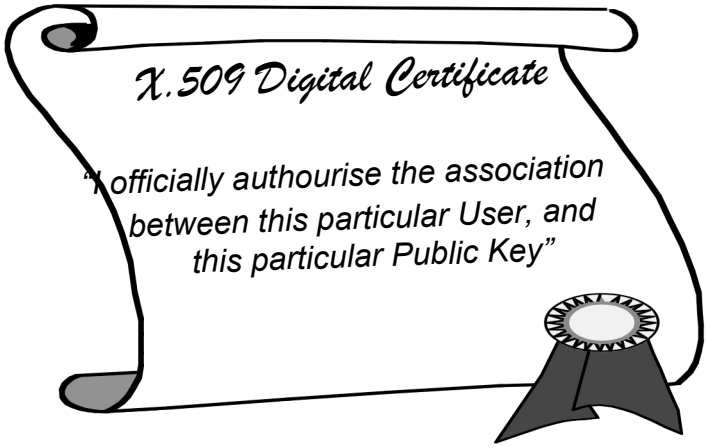
Certificates What is a "Certificate"?

All certification builds on trust:

You trust the Certification Authority (CA) that it does its job in a way that ensures that the information in the certificate is true and reliable and cannot be tampered with

We let a <u>trusted</u> Certificate Authority (CA) digitally sign an electronic document stating: This public key really belongs to this User/Entity!

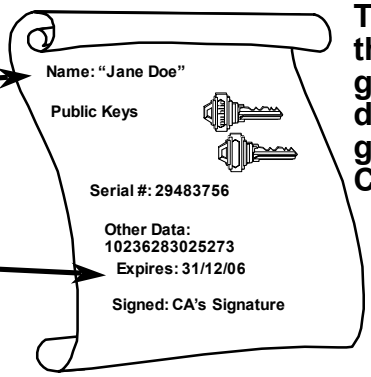
Certificates



How can you be sure that you get a real (and valid) public key?

Credential ties a name or identity to public keys

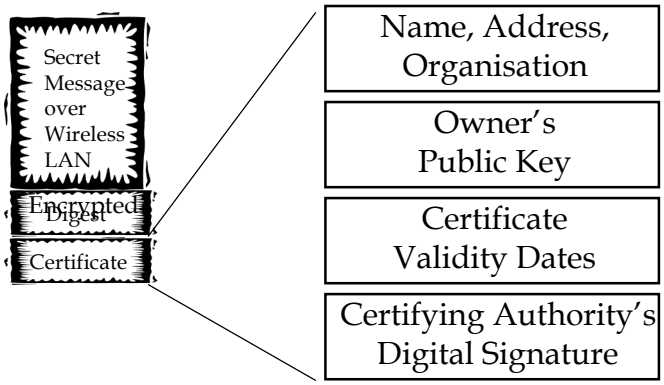
Credential expiration



The authenticity of the certificate is guaranteed by the digital signature generated using the CA's private key

Digital Certificate

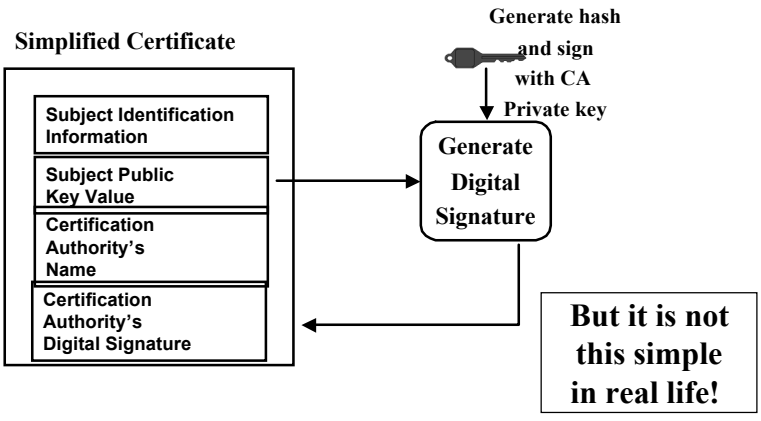
Digital Certificates



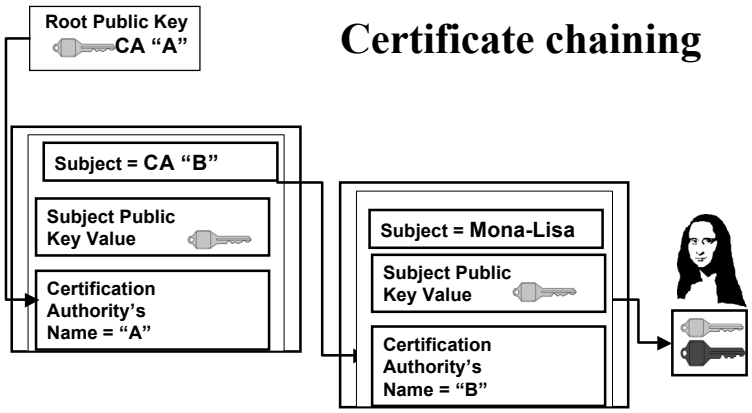
All you need is the CA's public key to verify the certificate and extract the owner's public key

Certificates

Certificate structure

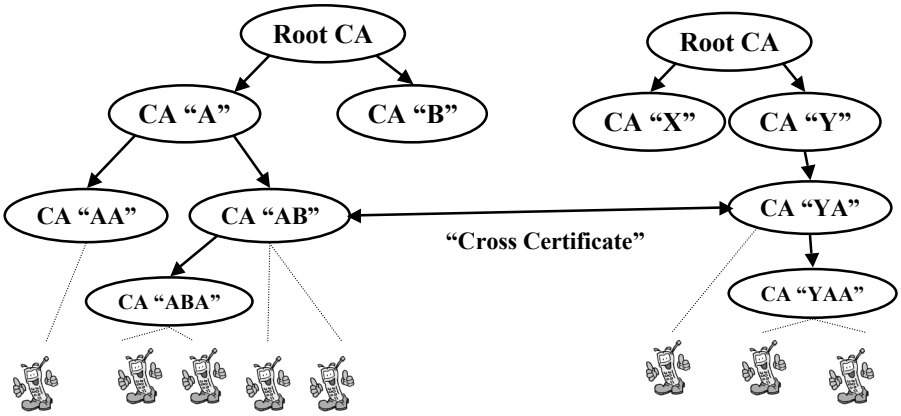


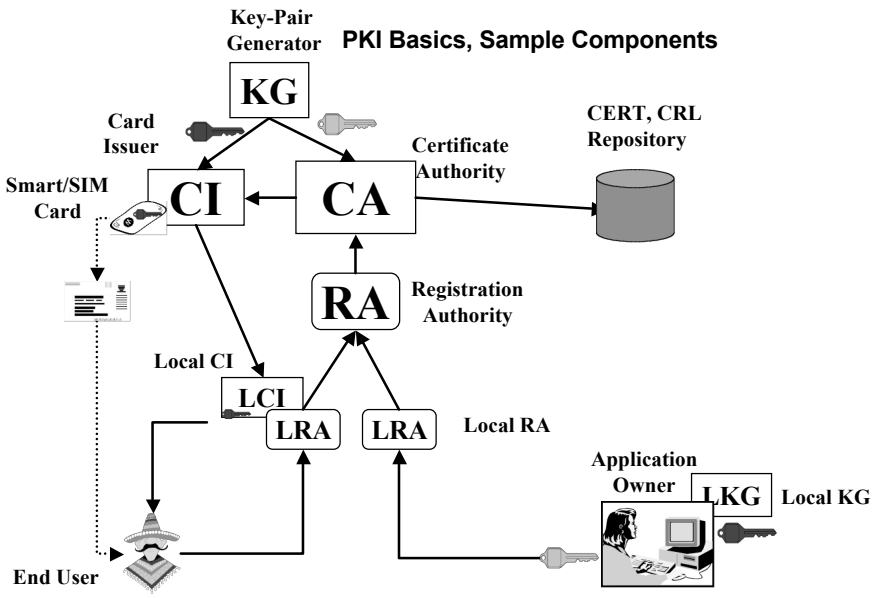
Certificate Chains



"Chains of Trust"

CA:s may be organised in hierarchies





Summary

Security Tools for Wireless Data Networking

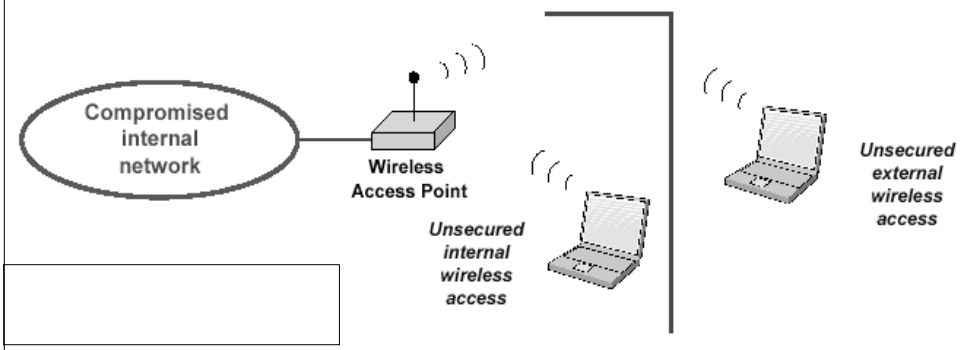
- Symmetric encryption
- Asymmetric (public/private key) encryption
- Digital Signatures
- Digital Certificates
- PKI - Public Key Infrastructure

Security Architectures and Protocols in Wireless LANs

(Section 3)

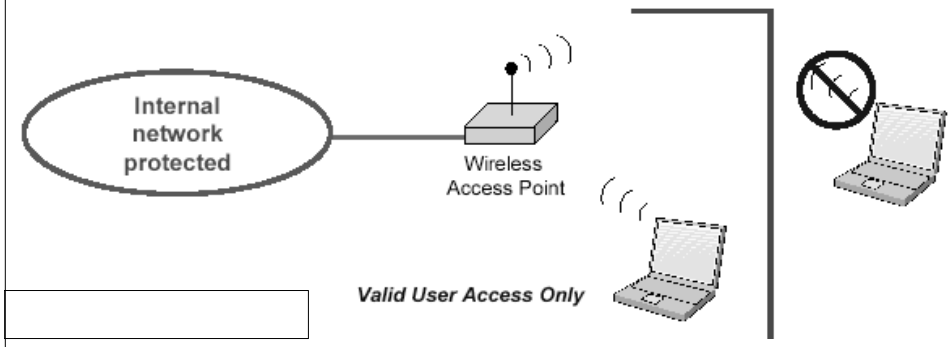
1

WLAN Security.. from this ...



2

WLAN Security .. to this ...



3

How Security Breaches Occur

- War (wide area roaming) Driving/War Chalking
  - Passing by in cars, pedestrians
  - Attack software available on Internet to assist
  - Access to an insecure WLAN network is potentially much easier than to a fixed network
- Without authentication and encryption, WLANs are extremely vulnerable
  - IDS must be monitored as with a fixed network

Anybody with shareware tools, WLAN card, antenna and GPS is capable of "war driving"

4

Wireless LAN
- Good Security Principles

5

WLAN - Good Security Principles

- Problems with bad WLAN architecture
  - Located behind firewall in trusted network
  - No authentication
  - Best to locate on DMZ with authentication
- Must consider security options:
  - Infrastructure design to enhance security?
  - Open access or MAC restricted?
  - Implement encryption/authentication or not?
- Problem with rogue WLAN
  - Can give access to trusted network as connection/installation as easy as connecting to a hub and without knowledge of administrator

6

WLAN - Good Security Principles

- Wireless LAN - out of the box
  - Enable WEP (RC4) (in spite of some issues)
  - Change default/identifiable SSID (Service Set Identifier) as network name not encrypted
  - Use products with dynamic key generation or security architectures which do the same
  - Do not use MAC address Authentication - tools are readily available to sniff a MAC address

7

WLAN - Good Security Principles

- Use MAC filters for lost or stolen cards
- VPNs and encryption tunnels to control access
- Lock down access point management interfaces
- Implement Layer 3 (or higher) functions:
  - IEEE 802.1x which supports EAP (Extensible Authentication Protocol)
  - AAA (Authentication, Authourisation and Accounting)
  - WEP dynamic session keys (WPA …)
  - PBNM (Policy Based Network Management)

8

Example of War Driving in Hong Kong*

- Background:
  - Dates: 7 July, 2002 and 5 Oct, 2003
- Equipment:
  - Notebook + Avaya Gold Wireless LAN card + Windows XP + NetStumbler
  - Notebook + Avaya Gold Wireless LAN card + Antenna + Windows 2000 + NetStumbler

*Ref: www.pisa.org/projects/wlan2003/wd2003.htm

War Driving Comparison - (July, 2002 and 5 Oct, 2003)

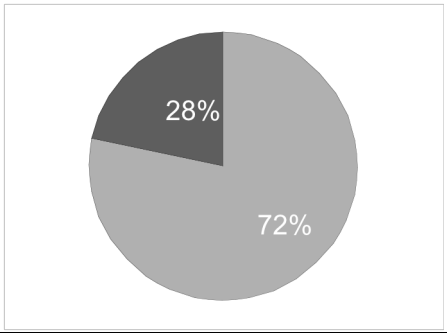
Date	7 July 2002	5 Oct 2003	5 Oct 2003
Weather	Occasional shower	Sunny	Sunny
Route	Kennedy Town – Causeway Bay		KennedyTown-Shau Kei Wan
No of APs	187	474	784
% WEP disabled	77%	69%	70%
% insecure SSID	51%	39%	43%

War Driving in Hong Kong

- Route:
  - Admiralty MTR Stations -> Pacific Place -> Tram (Admiralty to Kennedy Town) -> Tram (Kennedy Town to Causeway Bay)

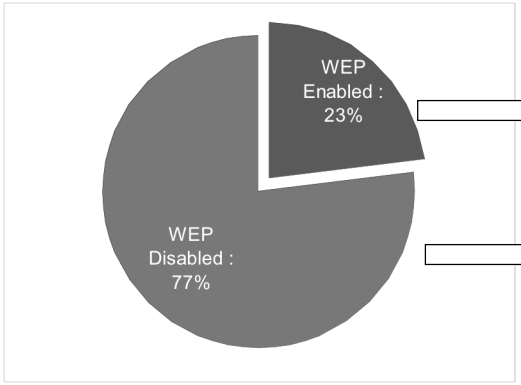
War Driving in Hong Kong

- Results
  - Number of Discovered Access Point with antenna: 187 (2002), up to 784 (2003)
  - Number of Discovered Access Point without antenna: 52 (subset of above)



War Driving in Hong Kong

- Result
  - WEP Usage: WEP Enable: 43 WEP Disable: 144 (2002)
  - WEP Usage: WEP Enable: 142 WEP Disable: 474 (2003)

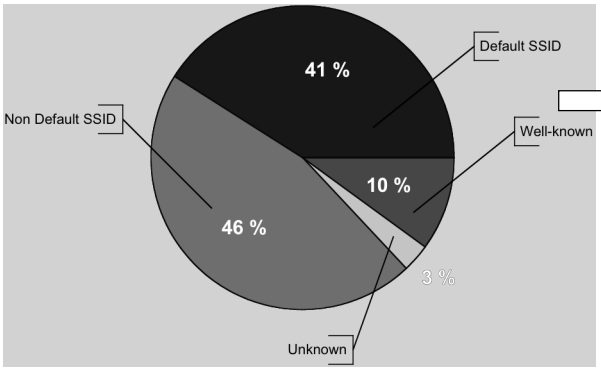


30% (2003)

70% (2003)

War Driving in Hong Kong

- Results (2002 and 2003)
  - SSID Usage: *Default SSID: 77 Use Non Default SSID: 87 Unknown: 5 Other: 18*



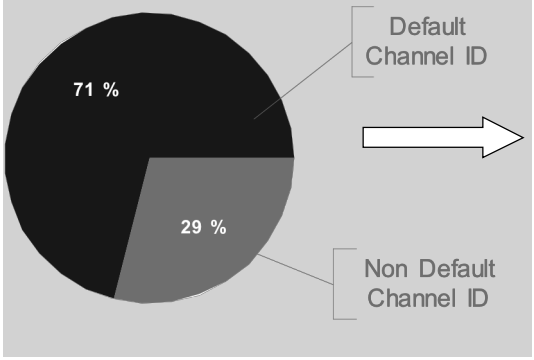
43% (2003)

Other means well known SSID, ie PCCW & i-cable
Some of the Default SSID list is referenced from http://wlana.net/acc_point.htm

War Driving in Hong Kong

- Result
  - Channel ID Setting Behaviour and Distribution:

Channel :	1	2	3	4	5	6	7	8	9	10	11
Number of APs :	78	1	13	4	1	18	9	2	6	14	37

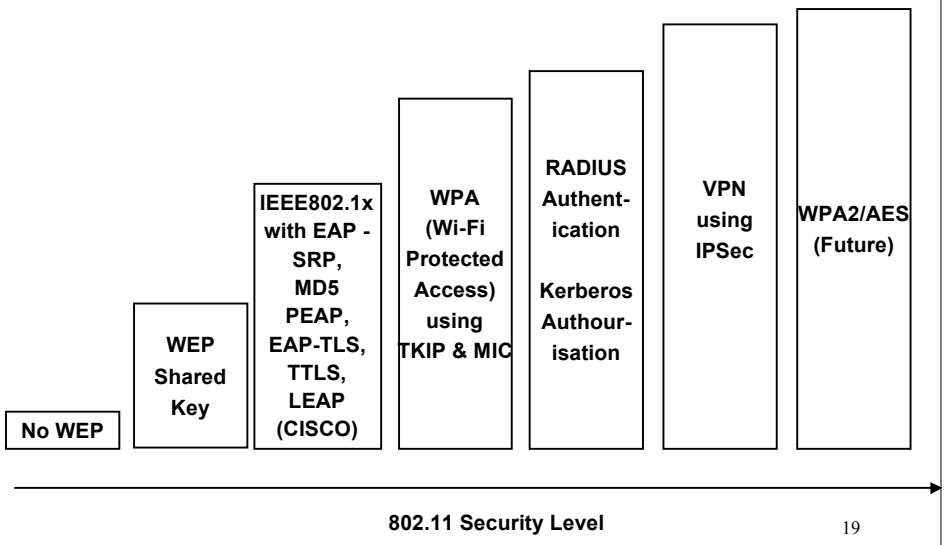


Most common channels still 1, 6 and 11 (2003)

Final Comments on the Hong Kong Experiment...

- The Hong Kong study demonstrated than there has been little improvement in the use of WEP and non-default SSID
- The range reached in these experiments was 10 km!! (Sau Mou Ping - Victoria Peak)
- In another test … direct drive from Melbourne airport to the city (September 2003) revealed *19* unprotected Wireless LAN networks
- Test in San Francisco revealed 140 WLANs from a central city point

WLAN - Security Options



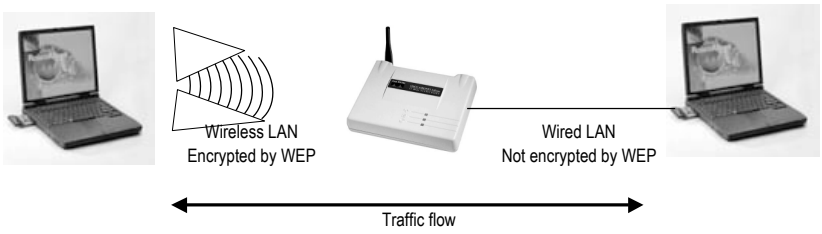
19

WEP
(Wired Equivalent Privacy)

20

WEP Security Features

- RC4 encryption
- Uses 40 or 104 bit shared key + 24 bit IV
- Encrypts payload while frame is *"in the air"*



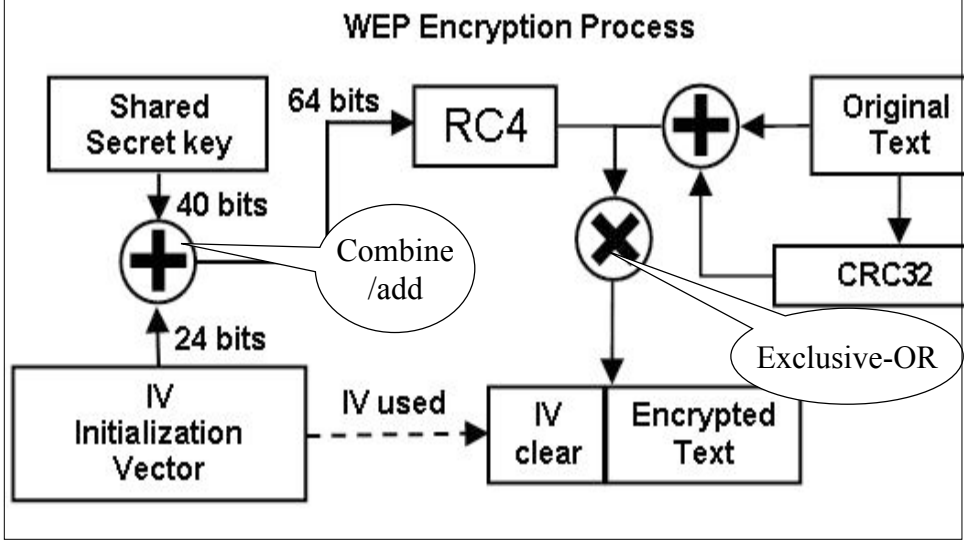
21

WEP Security Features

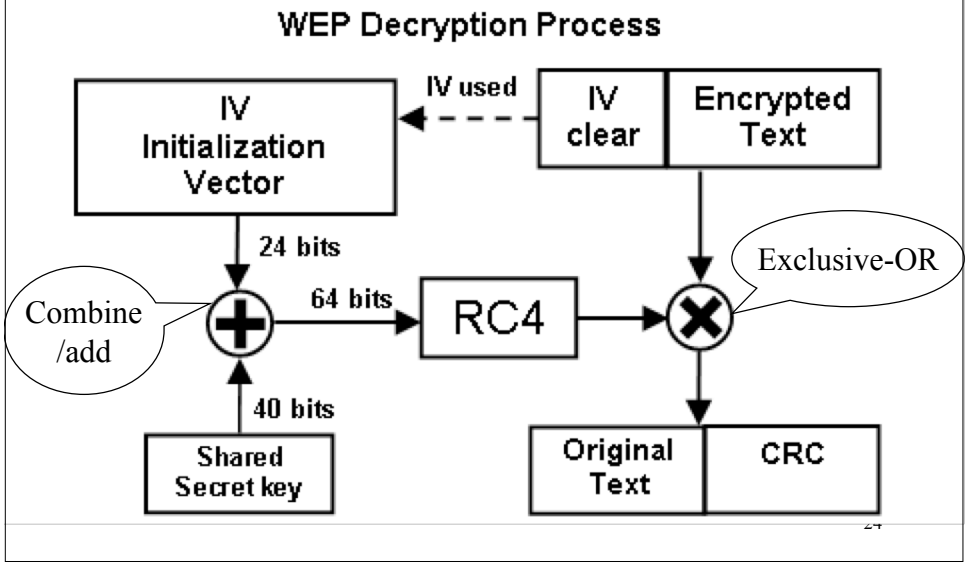
- WEP (Wired Equivalent Privacy)
- WEP has two main design goals:
  - Protection from eavesdropping
  - Prevent unauthourised access
- IEEE 802.11 defines mechanism for encrypting frames using WEP as follows...

22

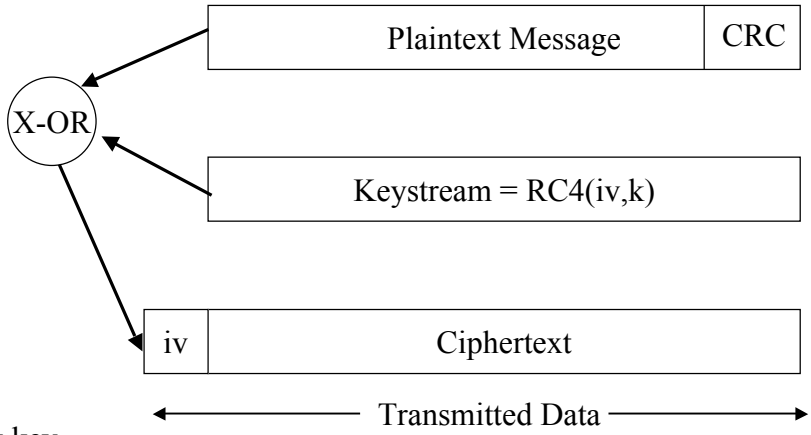
WEP Encryption / Decryption



WEP Encryption / Decryption



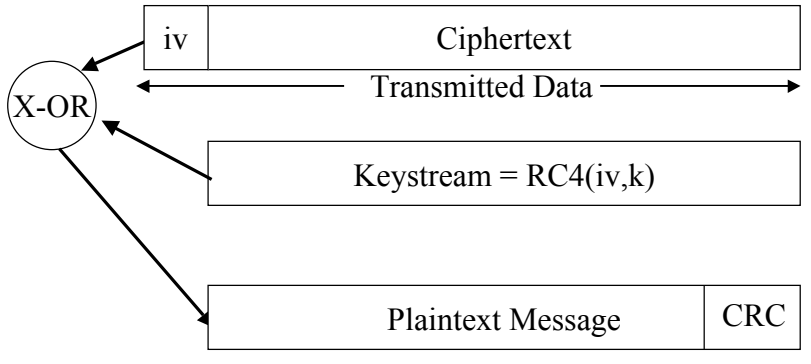
WEP Encryption



k = key
iv = Initialisation Vector
RC4 = Rivest Cipher 4 Stream Cipher

25

WEP Decryption



k = key
iv = Initialisation Vector
RC4 = Rivest Cipher 4 Stream Cipher

26

WEP Security Features

- Protocol for encryption and authentication
  - Operation based upon RC4 symmetric cipher with shared symmetric key
  - 40-bit key with a 24-bit IV (Initialisation Vector)
  - 104-bit keys (+24-bit IV) also possible
  - Integrity check using CRC-32
  - IV used to avoid encrypting two plaintexts with same key by augmenting shared RC4 key and thus produce different RC4 key for each packet

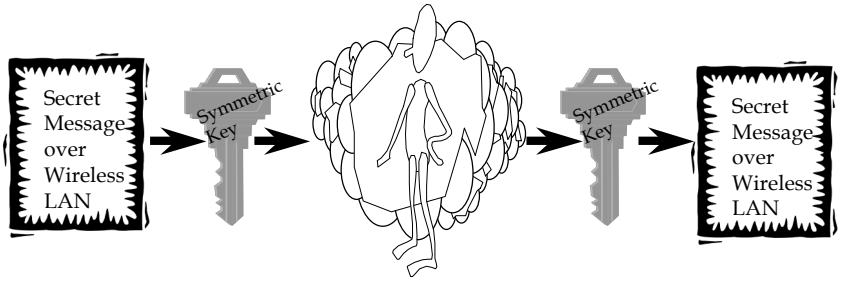
27

WEP Security Features

- WEP was never intended to be complete end-to-end solution
- Business policy will dictate if additional security mechanisms required such as:
  - access control, end-to-end encryption, password protection, authentication, VPNs, firewalls, etc
- WECA believe many reported attacks are difficult to carry out

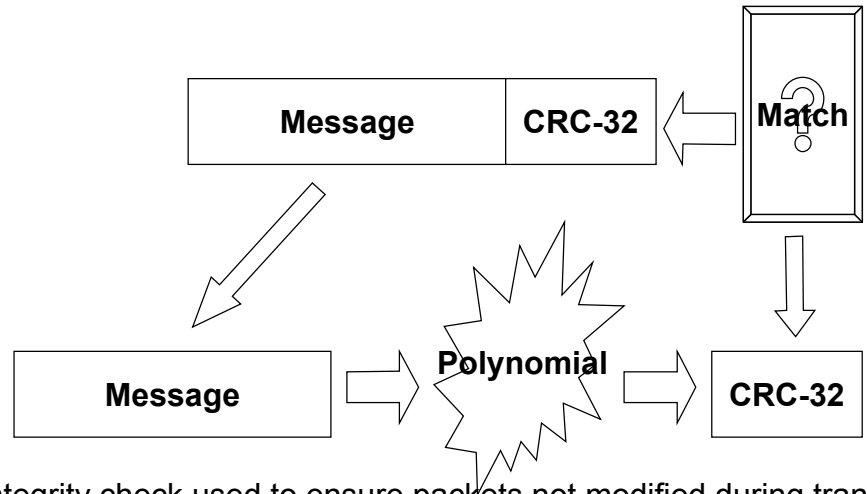
28

WEP Symmetric Key Operation



The same symmetric (RC4) key is used to encrypt and decrypt the data

WEP Integrity Check Using CRC-32



Integrity check used to ensure packets not modified during transit

WEP Security Weaknesses

- These attacks possible with inexpensive off-the-shelf equipment (opinion)
- These attacks apply to both 40-bit and 104-bit versions of WEP
- These also apply to any version of the IEEE 802.11 standards (802.11b in particular) that use WEP
- IEEE 802.11i recommend replacement of WEP by WPA and ultimately AES

32

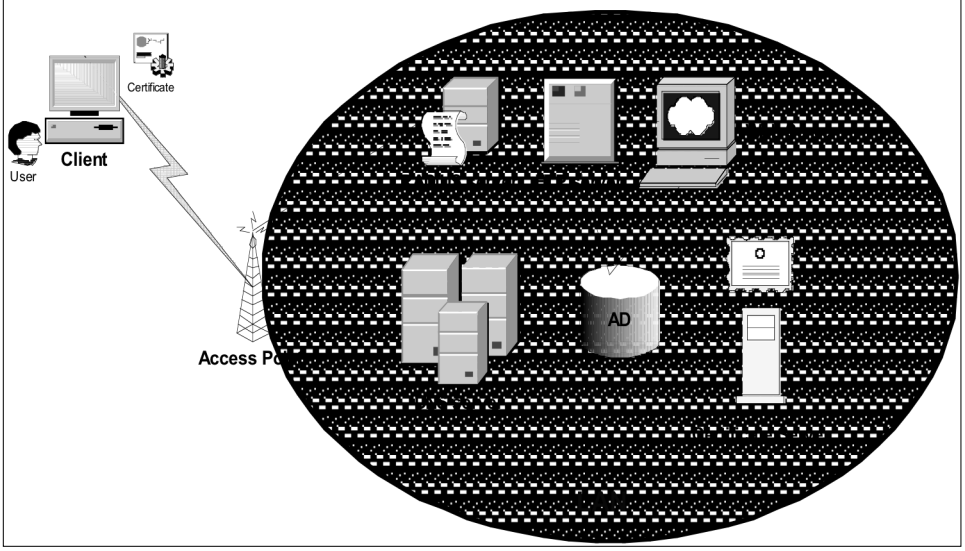
IEEE 802.1x

and

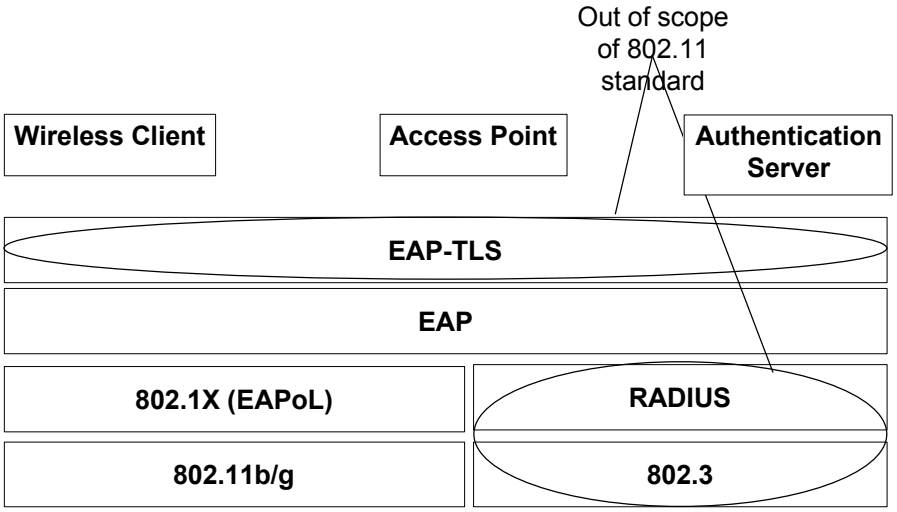
EAP
(Extensible Authentication Protocol)

36

IEEE802.1x Model Implementation



IEEE802.1x Model Implementation



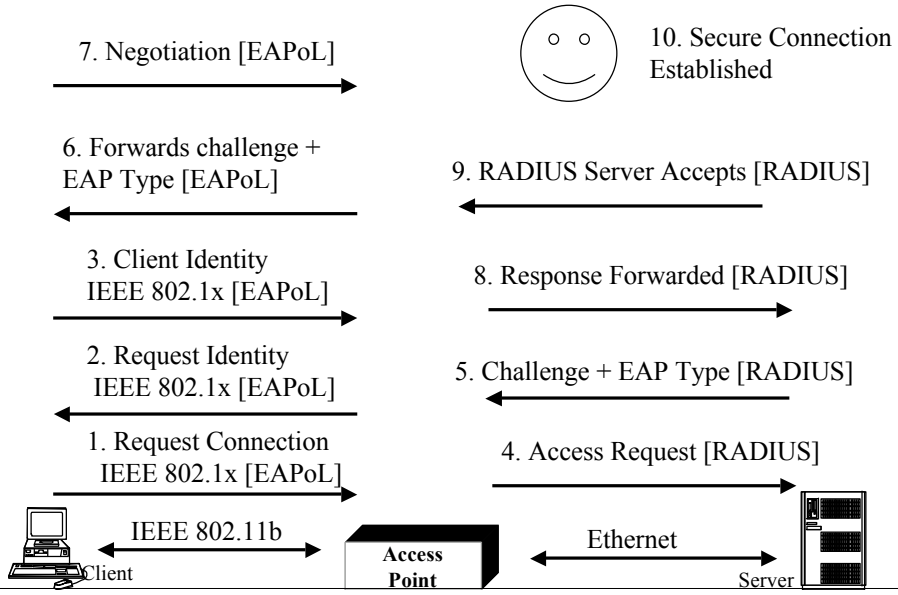
38

IEEE 802.1x Authentication

- IEEE 802.1x - implemented with different EAP types
  1. EAP-MD5 for Ethernet LANs (= Wireless CHAP)
  2. EAP-TLS for IEEE 802.11b WLANs but supplicant and authenticator must be able to handle digital certificates - hence PKI/CA infrastructure may be required
  3. EAP-SRP (Secure Remote Password) authentication
  4. CISCO - LEAP, FAST
  5. Microsoft - PEAP

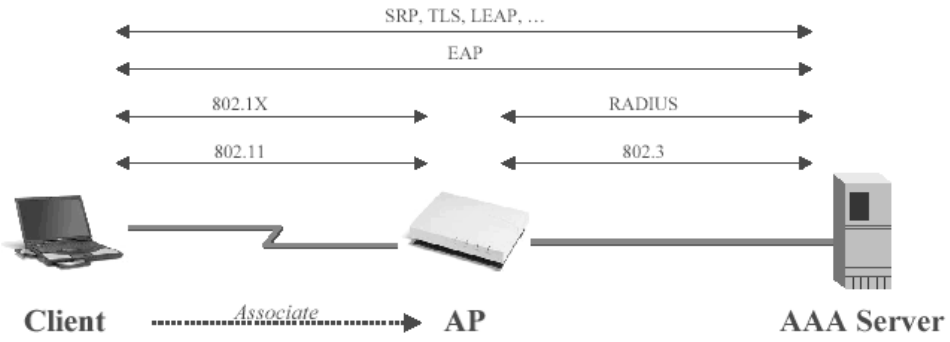
40

WLAN Security with 802.1X/EAP



WLAN Security with EAP

EAP (Extensible Authentication Protocol)



45

WLAN Security with EAP

- Extensible Authentication Protocol checklist:
  - Does it provide for secure exchange of user information during authentication?
  - Does it permit mutual authentication of the client and network thus preventing intrusion?
  - Does it require dynamic encryption keys for user and session?
  - Does it support generation of new keys at set intervals?
  - Is it easy to implement and manage, eg EAP-TLS requires client-side certificates?

46

EAP (Extensible Authentication Protocol) – RFC 2284 contd ...

- EAP is available with Windows 2000 & XP
- Common EAP authentication types include:
  1. EAP-SRP (Secure Remote Password) – offers a cryptographically strong “user” authentication mechanism suitable for negotiating secure connections and performing secure key exchange using a user-supplied password
  2. MD5 (Message Digest 5) - Wireless CHAP. Also released as PEAP - encrypts EAP transaction in tunnel (Windows XP)

48

EAP (Extensible Authentication Protocol) – RFC 2284 contd ...

3. LEAP (Lightweight EAP) and FAST (Flexible Authentication and Secure Tunneling) – CISCO vendor-specific authentication provides mutual authentication and dynamic WEP key generation
4. EAP-TLS (Transport Layer Security) offers full authentication consistent with PKI public/private keys, PKI and digital certificates.

RFC 2716 PPP EAP TLS Authentication Protocol

5. TTLS (Tunnelled Transport Layer Security) - requires server, but not client certificate

49

Some Authentication Options

- WEP

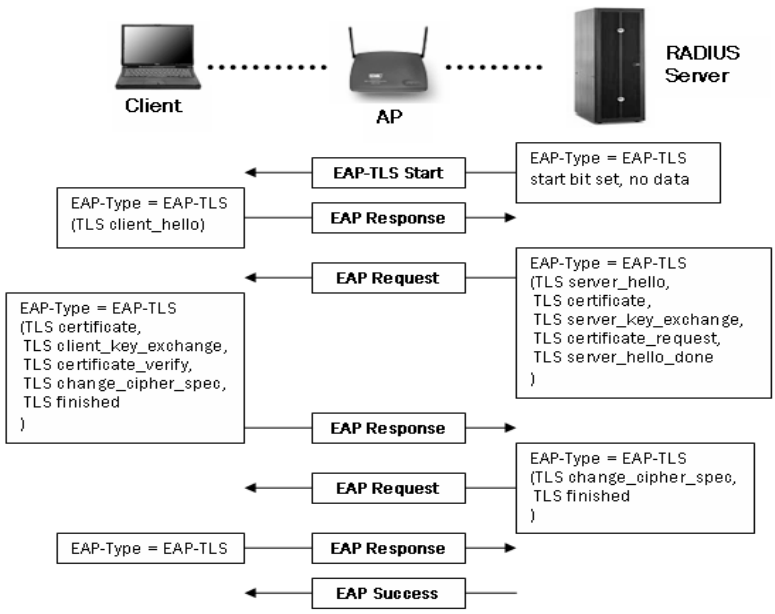
  Authenticates *node* (via MAC address only)
- EAP-MD5 / PEAP / LEAP (Wireless CHAP)

  Authenticates *user* (via encrypted password using challenge/response and key management)
- EAP-TLS

  Authenticates *node* and *user* (via digital certificates)

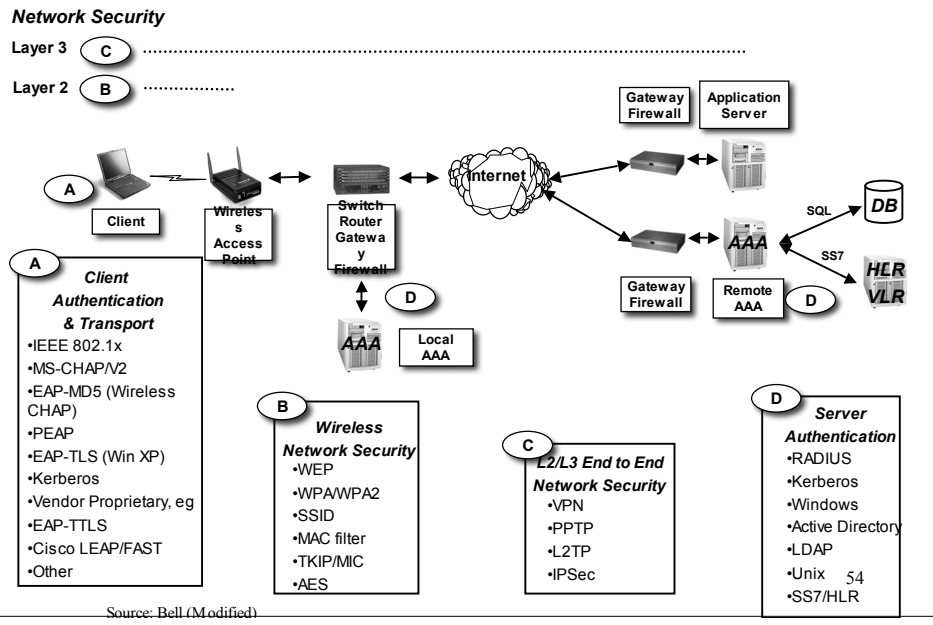
50

EAP-TLS Authentication



51

Security Infrastructure and Options



54

Source: Bell (Modified)

EAP TYPE	DYNAMIC RE-KEYING	MUTUAL AUTHENTI-CATION	USER ID & PASSWORD	ATTACK METHODS	COMMENTS
EAP-MD5	No	No	Yes	♦ Dictionary attack ♦ Man in the middle ♦ Session hijack	♦ Easy to implement ♦ Supported on many servers, but ♦ Insecure ♦ Requires cleartext databases
EAP-TLS	Yes	Yes	No	♦ Offers strong authentication security	♦ Requires client certificates ♦ Increases maintenance & token costs ♦ Two-factor authentication with smartcards
EAP-LEAP	Yes	Yes	Yes	♦ Dictionary attack	♦ Proprietary solution ♦ AP must have LEAP support

EAP-TTLS	Yes	Yes	No	♦ Offers strong authentication security	♦ Creation of secure TLS (SSL) tunnel ♦ Supports legacy authentication methods: PAP, CHAP, MS-CHAP, MS-CHAP V2 ♦ User identity is protected (encrypted)
EAP-PEAP	Yes	Yes	No	♦ Offers strong authentication security	♦ Similar to EAP-TTLS ♦ Creation of a secure TLS (SSL) tunnel ♦ User identity is protected (encrypted)

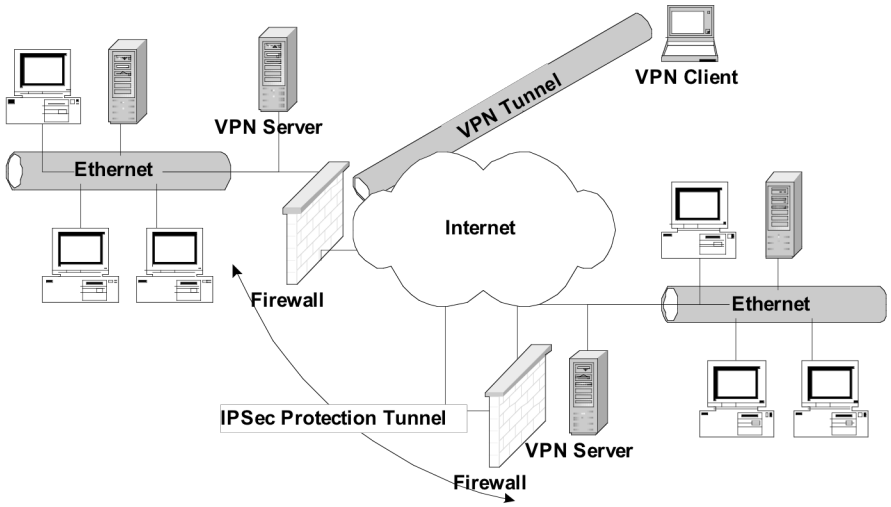
Source: Meetinghouse

56

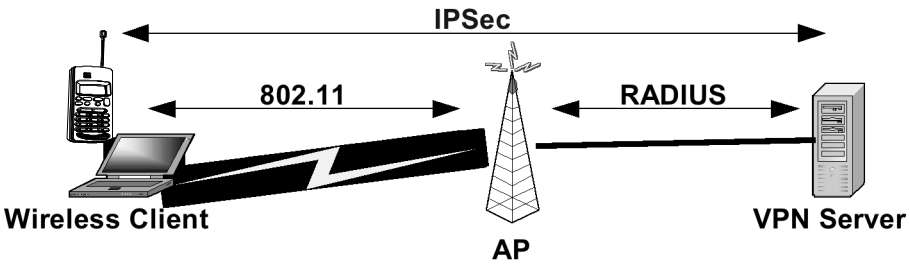
VPN Architecture in WLANs

57

Typical VPN Implementation



WLAN VPN Structure

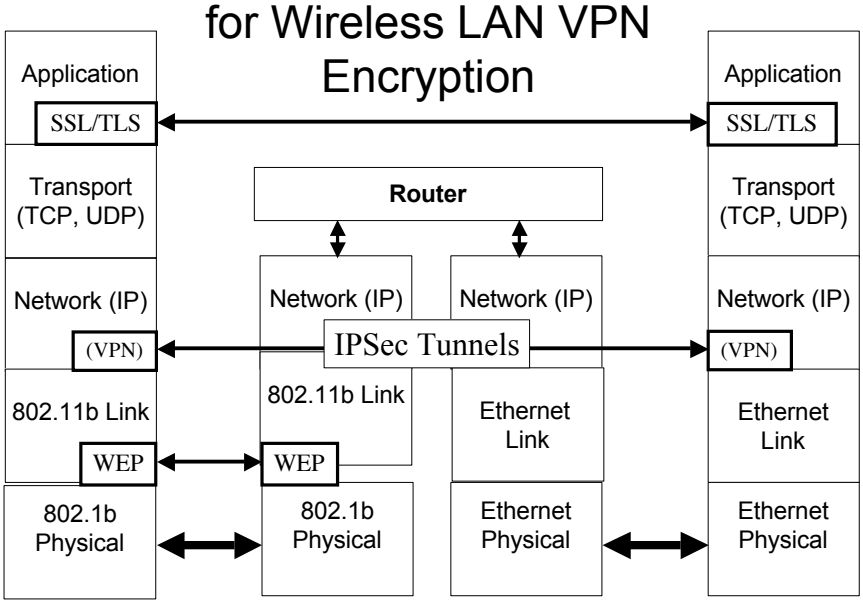


Firewalls and tunnels configured using:

IPSec, IKE, TLS, Digital Certificates

59

Secure Protocols for Wireless LAN VPN Encryption

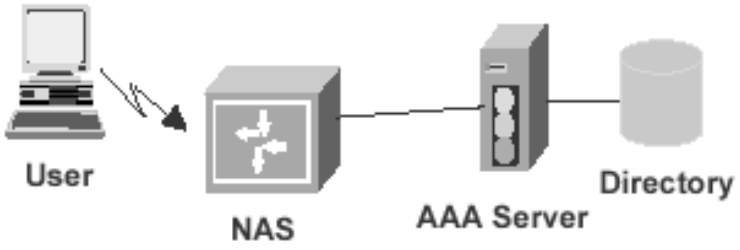


AAA (Authentication, Authourisation, Accounting)

62

AAA - Authentication Principles

- Authentication – Validating a User's Identity
  - Authentication protocols operate between user and AAA server:
    - PAP, CHAP, RADIUS, DIAMETER, IEEE 802.1x, EAP
  - Network Access Server (NAS) acts as relay device



65

AAA - Authourisation Principles

- Authourisation – What is user allowed to do?
  - Controls access to network services & applications
  - Access policy can be applied on a per user, group, global, or location basis
  - Attributes from an access request can be checked for existence or for specific values
  - Other attributes, eg time-of-day or number of active sessions with same username can also be checked
  - Outcome of policy decisions can be sent back to access device as *Access Reply* attributes

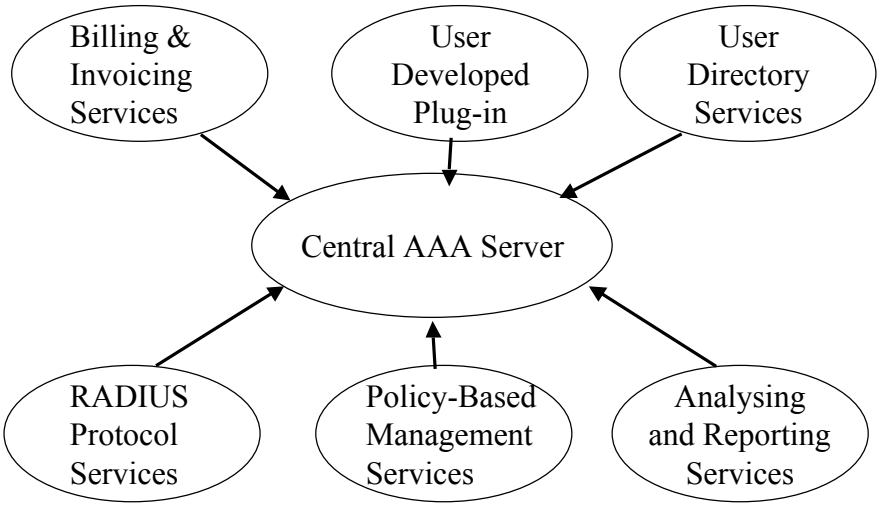
66

AAA - Accounting Principles

- Accounting – Collecting Usage Data
  - Data for each session is collected by access device and transmitted to AAA server
  - Usage data may include:
    - User Identities
    - Session Duration
    - Number of Packets, and Number of Bytes Transmitted
  - Accounting data may be used for:
    - Billing
    - Capacity Planning
    - Trend Analysis
    - Security Analysis
    - Auditing

67

AAA Server Architecture

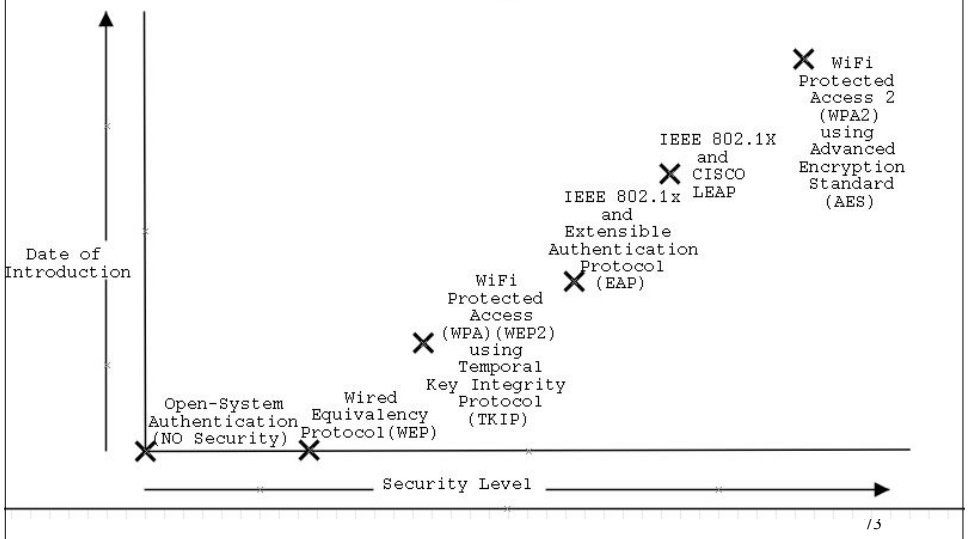


68

New Developments Beyond WEP - WPA, 802.11i, WPA2, AES, RSN

72

Improvements in Wireless Security



75

Recent Enhancements to WEP

- Temporary Key Integrity Protocol (TKIP) incorporated in intermediate standard (WPA) (2003) and in WPA2 (2005)
  - 128 bit encryption key + 40 bit Client MAC
  - 48 or 128 bit initialisation vector (IV)
  - Backward compatibility with WEP
  - Still uses RC4
  - Temporary Key changed every 10,000 packets

74

WPA (WiFi Protected Access)

- WPA (2003) was temporary fix pending release of WPA2 (IEEE 802.11i) in 2005
- Provides for dynamic key distribution and can be used across multiple vendor's equipment
- Good for legacy systems because firmware upgrade only required
- Step en route to IEEE 802.11i which has AES rather that RC4 encryption
- However AES requires more powerful processors (= H/W based encryption)

76

IEEE 802.11i & WPA Comparison

	802.11i	WPA
802.1X	Yes	Yes
Basic Service Set (BSS or infrastructure)	Yes	Yes
Independent BSS (IBSS or ad-hoc)	Yes	No
Pre-authentication (moving between APs)	Yes	No
Key Hierarchy	Yes	Yes
Key Management	Yes	Yes
Cipher & Authentication Negotiation	Yes	Yes
TKIP	Yes	Yes
AES-CCMP	Yes	No

80

WEP, WPA and WPA2

	WEP	WPA	WPA2 (802.11i)
Cipher	RC4	RC4	AES
Key Size	40 bits	128 bits encryption 64 bits authentication	128 bits
Key Life	24-bit IV	48/128-bit IV	48/128-bit IV
Packet Key	Concatenated	Mixing Function	Not Needed
Data Integrity	CRC-32	MIC	CCM
Header Integrity	None	MIC	CCM
Key Management	None	EAP-based	EAP-based

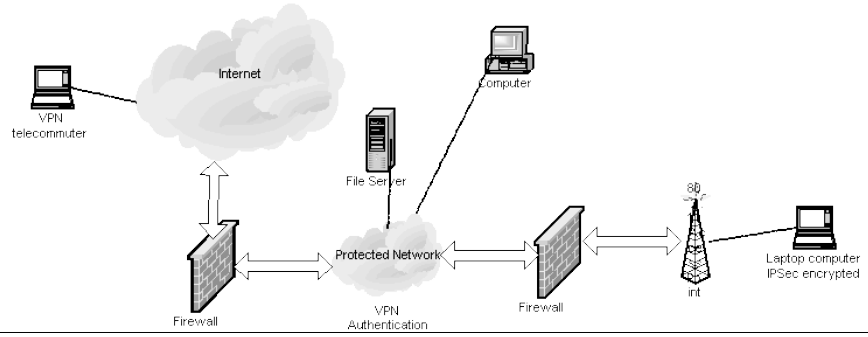
81

Conclusions - Good Security Principles Recommendation (1)

- Wireless LAN related Configuration
  - Enable WEP and/or AES encryption
  - Drop non-encrypted packets
  - Disable SSID (network name) broadcast
  - Change SSID to something unrelated to network
  - No SNMP access
  - Choose complex admin password
  - Enable firewall functionality
  - Use MAC (hardware) address to restrict access
  - Use MAC filtering to protect against primitive attackers
  - Non-default Access Point password
  - Change default Access Point Name
  - Use 802.1x

Conclusions - Good Security Principles Recommendation (2)

- Deployment Consideration
  - Separate and closed network
  - Treat Wireless LAN as external network
  - VPN and use strong encryption
  - No DHCP (use fixed private IP)



Conclusions - Good Security Principles Recommendation (3)

- Always (wired or wireless)
  - Install virus protection software plus automatic frequent pattern file update
  - Shared folders must impose password
- Management Issue
  - Carefully select physical location of AP, not near windows or front doors
  - Prohibit installation of AP without authorisation
  - Discover any new APs constantly (NetStumbler is free, Antenna is cheap)

Conclusion contd.

- Match new standards to four main components of a secure network:
  - Mutual authentication
    - EAP-based
  - Cryptographic integrity protection
    - MIC and CCM
  - Block cipher payload encryption
    - AES
  - Firewalls between wireless / wired components
  - *This implies using IEEE 802.11i (WPA2) from mid 2005 on …*

86

Wireless LAN Attacks and Protection Tools

(Section 3 contd….)

1

WLAN Attacks

- Passive Attack – unauthorised party gains access to a network and does not modify any resources on the network
- Active Attack – unauthorised party gains access to a network and modifies the resources on the network or disrupts the network services

2

Passive Attacks

- Traffic Analysis – most frequently used, helps attackers to gain basic network information before launching more damaging attacks
- Passive Eavesdropping – attacker monitors the WLAN traffic but does not modify. This also possibly includes cracking the encryption

3

Traffic Analysis

Three main forms of information are obtained:

- Existence
  - Detect AP (Access Point)
  - War driving
- Activity
- Protocol type and other useful information
  - Packet size
  - Packet type
  - Number of packets
  - Packet fragmentation info
  - …

4

War Driving

- People “drive” around in the city looking for active APs
- Easy to perform
- Equipment is cheap and easy to get:
  - Easily transported computer or handheld device
  - Wireless Network Interface Card (WNIC)
  - Software
  - Antennas (optional)
  - GPS (optional)

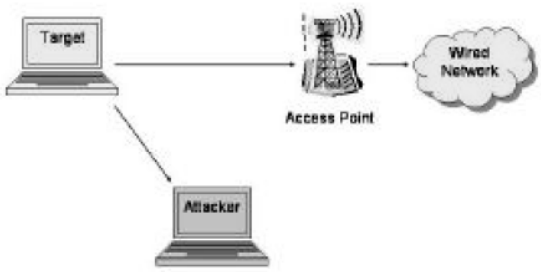
5

War Driving contd….

- APs periodically send out beacon frames, which can be detected and captured
- The most interesting fields to attackers:
  - Network SSID
  - MAC address of wireless device
  - WEP protocol status: enable or disable
  - Type of device: AP or peer
  - Signal strength and noise level
  - Longitude and latitude (for GPS)

6

Passive Eavesdropping



- Similar to traffic analysis
- Impossible to detect
- Can be prevented by employing layer 2/3 encryption as most information is in TCP header

7

Solutions to Passive Attacks

Unencrypted

802.11 Header	IP Header	TCP Header	E-mail Message

Layer 3: Network Layer Encrypted Tunnel

Frame Hr	IP Hr	IP Header	TCP Header	E-mail Message

Layer 2: Data Link Layer Encrypted Tunnel

802.11 Header	IP Header	TCP Header	E-mail Message

8

Active Attacks

1. Unauthorised Access
2. Rogue Access Points
3. Man-In-The-Middle (MITM)
4. Session Hijacking
5. Replay
6. Denial of Service

9

1. Unauthorised Access

- Different from all the other attacks
- Against the whole network instead of single user
- Key step for performing more damaging ARP-based MITM attack

10

Unauthorised Access contd.

- In some wireless security architectures, an attacker, who has already been granted access to wireless components, will be granted access to wired components
- In other security architectures, access to wired network is controlled by Access Control Lists (ACLs) / firewalls etc
- Attackers might still be able to spoof victim's MAC address and use it to login as a legitimate user

11

Unauthorised Access contd.

Treat the wireless network as something outside the security perimeter, but with special access to the inside of the network

A firewall should be used between the wireless and the wired network

Alternatively tunnel encrypted and authenticated wireless traffic through the firewall

12

2. Rogue Access Point

- Usually set up by employees for their own use
- Often with no security features enabled
- A single rogue AP can leave a back door open that can be easily exploited
- Some tools can detect APs based on detecting beacon frames

13

Solutions to Rogue Access Point

- Centralised detection – use central console attached to wired side of network for monitoring. If any authorised APs find a rogue AP, they alert network administrator
- TCP port scanning – examine packets sent to/from one particular port and it is possible to gather information about any APs and users active on this port

14

Solutions to Rogue Access Point

- Strong security policy and good education
- Sufficient level of security on destination servers and applications
- Detection of rogue APs by:
  - Physical detection with AirMagnet (www.airmagnet.com) and AirDefence (www.airdefence.com)
  - Centralised detection with AirWave and Aruba
  - IDS and monitor wireless traffic

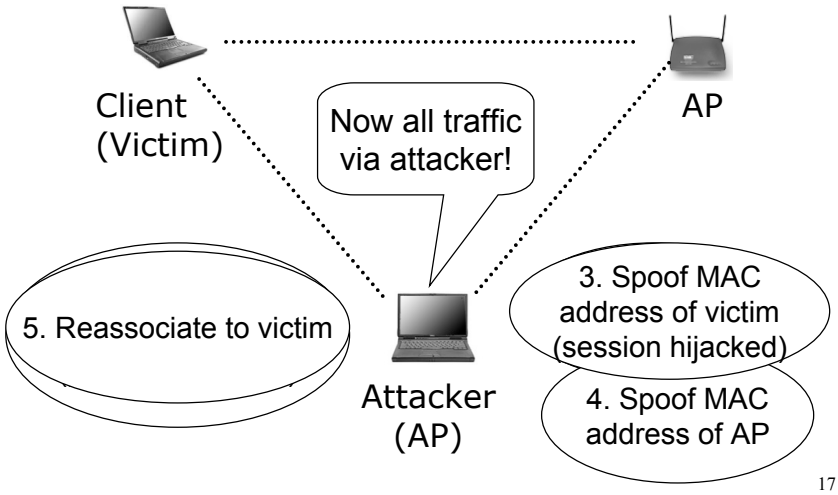
15

3. & 4. Man-In-The-Middle (MITM) Attack and Session Hijacking

- Cracking WEP with a small volume of traffic is still very difficult
- Large organisations should be using VPN or IPSec to protect from direct confidentiality attacks
- Therefore, MITM becomes popular and indirectly attacks data confidentiality

16

Operation of a MITM/Hijack Attack



17

Operation of a MITM/Hijack Attack

- Attacker spoofs MAC address of victim's AP
- Attacker constructs a disassociation frame and sends it to victim (pretending to be real AP)
- A session is now open from the previous user that the AP is unaware has ended
- Attacker now spoofs MAC address of the victim and hijacks their session
- On one wireless interface of attacker's machine: spoof MAC address of AP again

18

Operation of a MITM/Hijack Attack

- On another wireless interface of attacker's machine: re-associate victim's computer
- The victim's computer is now associated with the attacker's computer instead of the access point
- Route traffic between the two interfaces
- Now all network traffic is being passed through the attacker's computer, and can be sniffed

19

ARP Cache Poisoning

- ARP is too trusting and it provides no way to verify the responding device
- How does it work?
  - Attacker sends programmed malicious ARP reply and broadcasts it to target network (same subnet)
  - The faked ARP packet can change entries in OS's lookup table (ARP cache)
  - OS then redirects traffic through the designated (attacker's) host

20

ARP Cache Poisoning contd.

- Fortunately, ARP cache poisoning is trivial to detect
  - Only local attackers can use this attack. i.e. an attacker needs either physical access to network or control of machine on that LAN
  - Tools like ARPWatch can monitor ARP communication and alert unusual events

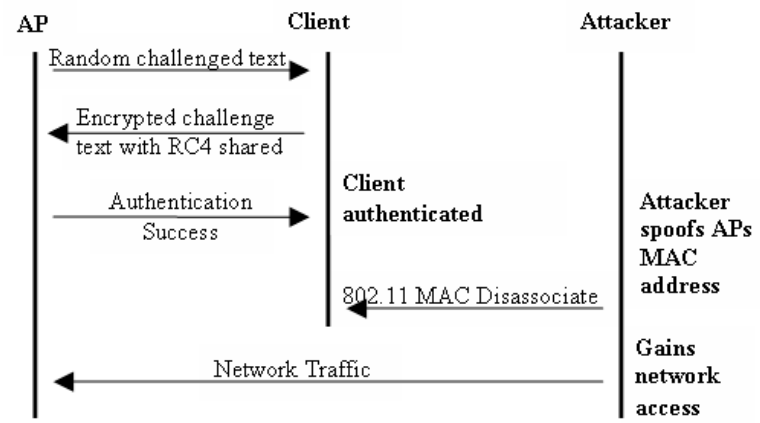
21

4. Session Hijacking

- Spoof the MAC of the AP
- Construct and send a disassociate frame to the victim
- Spoof the MAC of the victim
- Re-association is not needed, the AP is blind to this whole process

22

Session Hijacking contd.



23

Recommended Solutions for MITM and Session Hijacking

- Strong cryptographic protocol
- Mutual Authentication – both AP and client will need to prove their identities (e.g. EAP-TLS) before exchanging any sensitive data
- Per-frame authentication

24

5. Replay

- Similar to session hijacking and MITM
- Instead of real time attacking, replay occurs after the session ends
- An attacker captures the authentication packets of a session and replays them later
- Since the session was valid, the attacker may use the victim's authorisation and credentials

25

6. Denial of Service (DoS)

- DoS is one of the most popular attacking methods and wireless networks are particularly vulnerable to DoS attacks

- DoS attacks against layer 1 (physical) and layer 2 (data link) of WLAN cannot be defeated by any of the security technologies

26

Denial of Service (DoS) contd.

- An attacker can take down the entire WLAN by:
  - Generating enough noise
  - Attaching to an AP and generating a large amount of traffic
  - Injecting traffic into the radio network without attaching to an AP
- MITM, session hijacking and rogue APs can also end up creating a DoS attack

27

Wireless Tools for Monitoring and Detecting Attacks

28

Wireless Tools

- Most of the wireless tools can be classified into:
  - Monitoring Tools
    - Stumbling
    - Sniffing
  - Hacking Tools
    - WEP Cracking
    - ARP Poisoning
  - Intrusion Detection Tools

29

Stumbling Tools

- Identify the presence and the activity of wireless networks
- Look for beacon frames
- Broadcast client probes and wait for APs to respond

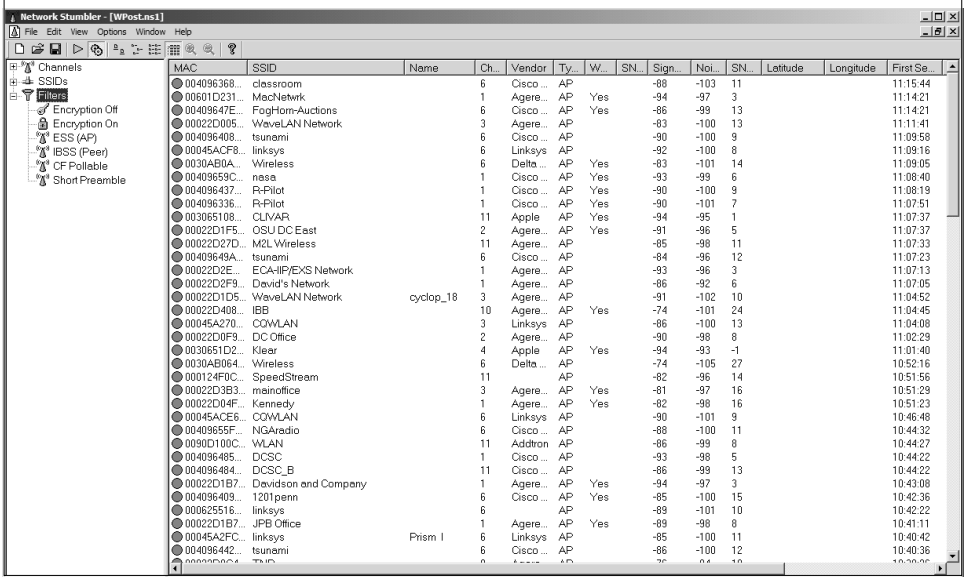
30

Stumbling Tools contd.

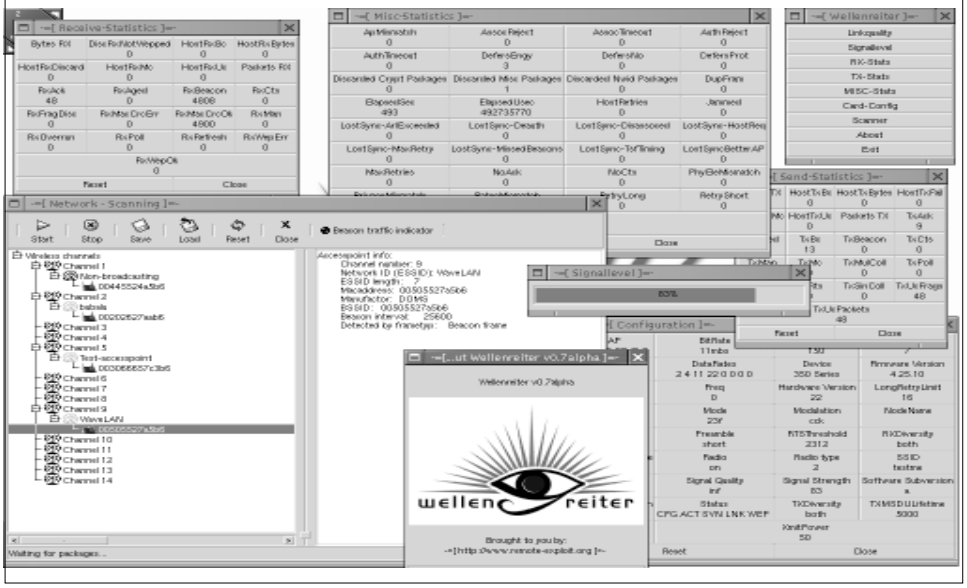
Name	Platform	Free/Open Source	Available from
Aerosol	Windows	Y/Y	http://www.sec33.com/sniph/aerosol.php
NetStumbler	Windows	Y/Y	http://www.netstumbler.com
MiniStumbler	Handheld	Y/Y	http://www.netstumbler.com
Wellenreiter	Linux	Y/Y	http://www.wellenreiter.net
Wellenreiter II	Handheld	Y/Y	http://www.vanille.de/projects/wellenreiter.html
MacStumbler	MacOS	N/Y	http://www.macstumbler.com
dStumbler	BSD	Y/Y	http://www.dachb0den.com/projects/dstumbler.html
Airfart	Linux	Y/Y	http://airfart.sourceforge.net
Wavestumbler	Linux	Y/Y	http://www.cqure.net/wp/?page_id=14
AP Scanner	MacOS	Y/N	http://www.macupdate.com/info.php/id/5726
iStumber	MacOS	Y/Y	http://istumbler.net
gWireless	Linux	Y/Y	http://gwifiapplet.sourceforge.net

31

NetStumbler



Wellenreiter



Sniffing Tools

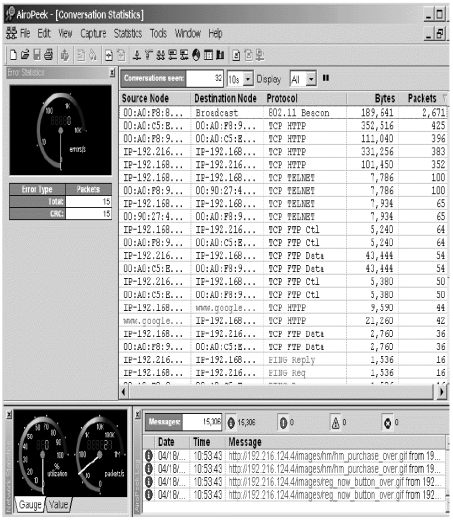
- Capture wireless traffic
- View data passed through air waves

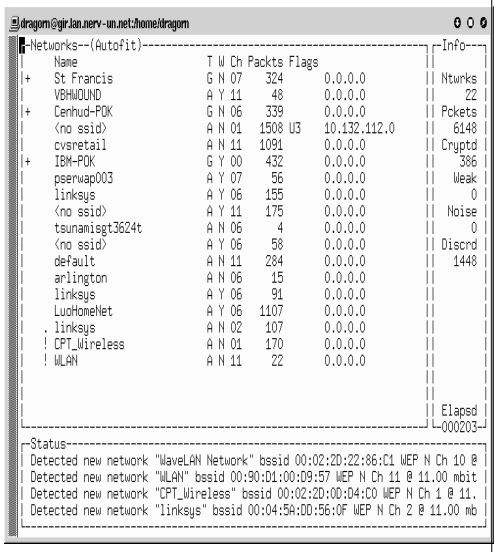
Sniffing Tools contd.

Name	Platform	Free/Open Source	Available from
Ethereal	All	Y/Y	http://www.ethereal.com
Kismet	Linux	Y/Y	http://www.kismetwireless.net
KisMAC	MacOS	Y/Y	http://kismac.binaervarianz.de
Packetyzer	Windows	Y/Y	http://www.networkchemistry.com/products/packetyzer.php
Prism2dump	BSD	Y/Y	http://www.dachb0den.com/projects/prism2dump.html
BSD-Airtools	BSD	Y/Y	http://www.dachb0den.com/projects/bsd-airtools.html
AirTraf	Linux	Y/Y	http://airtraf.sourceforge.net
Airscanner	Handheld	Y/N	http://www.snapfiles.com/get/pocketpc/airscanner.html
APsniff	Winodws	Y/N	http://www.monolith81.de/mirrors/index.php?path=apsniff

35

AiroPeek Kismit

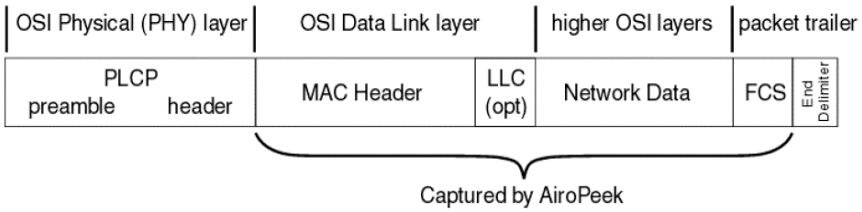




36

AiroPeek contd.

802.11 packet structure



37

Hacking Tools

Type	Name	Free/Open Source	Available from
MITM & Hijacking	Ettercap	Y/Y	http://ettercap.sourceforge.net
	dSniff	Y/Y	http://monkey.org/~dugsong/dsniff
	Hotspotter	Y/Y	http://www.remote-exploit.org/index.php/Hotspotter_main
Rogue AP	Airsnarf	Y/Y	http://airsnarf.shmoo.com
	FakeAP	Y/Y	http://www.blackalchemy.to/project/fakeap
Traffic Injection can be used for: DoS/DDoS Spoofing Hijacking	File2air	Y/Y	http://www.wi-foo.com/soft/attack/file2air-0.1.tar.bz2
	AirJack	Y/Y	http://sourceforge.net/projects/airjack
	Void11	Y/Y	http://www.wlsec.net/void11
	Omerta	Y/Y	http://www.securityfocus.com/archive/89/326248
	Dissassociate	Y/Y	http://www.hunz.org/other/disassociate.c
	Wifitag	Y/Y	http://sid.rstack.org/index.php/Wifitap_EN
	Airpwn	Y/Y	http:///sourceforge.net/projects/airpwn

38

Hacking Tools contd.

Type	Name	Free/Open Source	Available from
Cracking	WEPCrack	Y/Y	http://wepcrack.sourceforge.net
	AirSnort	Y/Y	http://airsnort.shmoo.com
	WepAttack	Y/Y	http://wepattack.sourceforge.net
	Asleap	Y/Y	http://asleap.sourceforge.net
	WEPWedgie	Y/Y	http://sourceforge.net/projects/wepwedgie
	anwrap(Leap crack)	Y/Y	http://www.securiteam.com/tools/6O00P2060I.html
	coWPAatty	Y/Y	http://www.remote-exploit.org
	Aircrack	Y/Y	http://www.remote-exploit.org
	Weplab	Y/Y	http://sourceforge.net/projects/weplab
	THC-LEAPcracker	Y/Y	http://www.thc.org
	Chopchop	Y/Y	http://www.netstumbler.org/showthread.php?t=12489

39

AirSnort

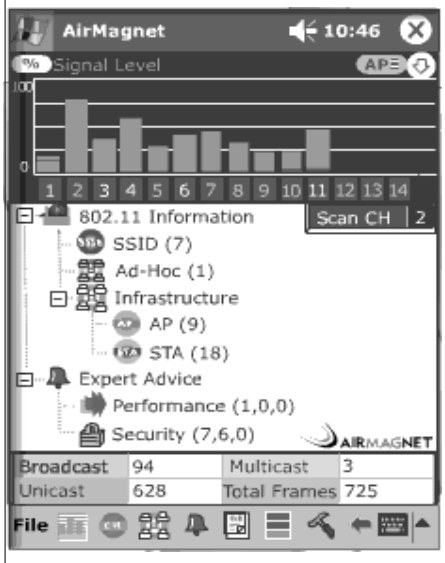
40

Handheld Tools

Name	Platform	Available from:
AirMagnet	Pocket PC	http://www.airmagnet.com
Waverunner	Linux kernel iPaq	http://www.flukenetworks.com/us/LAN/Handheld+Testers/WaveRunner/Overview.html
Kismet	Linux Sharp Zaurus	http://www.kismetwireless.net

41

AirMagnet Waverunner



42

All-Purpose Tools

Name	Platform	Free/Open Source	Available from
AirMagnet	All	N/N	http://www.airmagnet.com
AiroPeek NX	Windows	N/N	http://www.wildpackets.com/products/airopeek_nx
AiroPeek SE	Windows	N/N	http://www.wildpackets.com/products/airopeek
AirWave	Linux	N/N	http://www.airwave.com
LinkFerret Network Monitor and Protocol Analyzer	Windows	N/N	http://www.linkferret.ws
YellowJacket	Handheld	N/N	http://www.bvsystems.com/Products/WLAN/WLAN.htm
OptiView Series II Integrated Network Analyzer	Handheld	N/N	http://www.flukenetworks.com/us/LAN/Handheld+Testers/OptiView/Overview.htm
Javvin Network Packet Analyzer	Windows	N/N	http://www.javvin.com/packet.html
TamoSoft CommView for Wi-Fi	Windows	N/N	http://www.tamos.com/products/commwifi
Network Instruments Observer	Windows	N/N	http://www.networkinstruments.com/products/observer_wireless.html

43

Management Tools & IDS (Intrusion Detection Tools)

- Wireless Intrusion Detection Systems:
  - AirDefense (www.airdefense.net/products/intrusion_detection.shtm)
  - AirIDS (www.zone-h.com/en/download/category=18)
- Access Point:
  - FakeAP - effectively an AP honeypot (www.blackalchemy.to/project/fakeap)

44

Management Tools & IDS contd.

Name	Platform	Free/Open Source	Available from
WIDZ	Linux	Y/Y	http://www.loud-fat-bloke.co.uk/tools.html
AirDefense Products	Windows	N/N	www.airdefense.net/products/airdefense_ids.shtm
Highwall Products	Windows	N/N	http://www.highwalltech.com
Newbury Products	Windows	N/N	http://www.newburynetworks.com
Red-M Products	Windows	N/N	http://www.red-m.com/products-and-services

45

Summary of Attacks

- Three key components of information related to network security:
  - Confidentiality (C)
    - Privacy of information
  - Integrity (I)
    - Information is unmodified
    - Know identity (i.e. authentication)
    - Know action (i.e. non-repudiation)
  - Availability (A)
    - When and where needed

46

Summary of Attacks contd.

CIA Type	Attack Methods	*Weaknesses*
C	Traffic Analysis	• Networks announce themselves to the public • 802.11 frame headers are sent in clear • WEP is vulnerable to cracking tools • Lack of authentication mechanism • Lack of physical security and protection • Authorised users or attackers set up unauthorised APs with default setting
	Passive Eavesdropping	
	Rogue AP	
I	Unauthorised Access	• No firewall between Wireless LAN and Wired LAN • MAC addresses are sent in clear and lack of MAC address authentication mechanism • Lack of per-frame or per-session authentication mechanisms • Some wireless devices default associate APs with stronger signals • ARP is too trusting
	MITM	
	Session Hijacking	
	Replay	
A	DoS	• Relatively low bit rates of WLAN, easily overwhelmed • Easy access to the physical layer

47

Summary of Attacks contd.

CIA Type	Attack Methods	*Countermeasures*
C	Traffic Analysis	Layer 2 and Layer 3 encryption
	Passive Eavesdropping	Strong cryptography, TLS, SSH, IPSec
	Rogue AP	Centralised monitoring, port scanning, firewall
I	Unauthorised Access	Firewall
	MITM	Mutual authentication, strong encryption
	Session Hijacking	Mutual authentication, strong encryption, TLS, per-frame authentication
	Replay	Strong authentication, timestamp
A	DoS	No effective methods

48

Summary of Attacks contd.

- To mitigate risks from these attacks, security architecture must have four components:
  - Mutual authentication
    - MITM
    - Session hijacking
    - Replay
  - Block cipher encryption of payload
    - Eavesdropping
    - Traffic analysis
    - Session hijacking

49

Summary of Attacks contd.

- Strong cryptographic integrity protection
  - Eavesdropping
  - Session hijacking
  - Replay
- Firewall between wireless / wired network
  - Unauthorised access
  - Rogue AP
  - ARP Cache Poisoning

50

Wireless Vulnerabilities Addressed by Security Certification Testing Criteria (www.icsalabs.com - August 2003)

Threat	Unauthorised Access	Denial of Service
• Jamming		✓
• DoS		✓
• Rogue APs	✓	✓
• Replay Attacks	✓	✓
• Tampering	✓	
• Spoofing	✓	
• Eavesdropping	✓	
• Man-in-the-middle	✓	
• Forgeries	✓	
• Dictionary Attacks	✓	

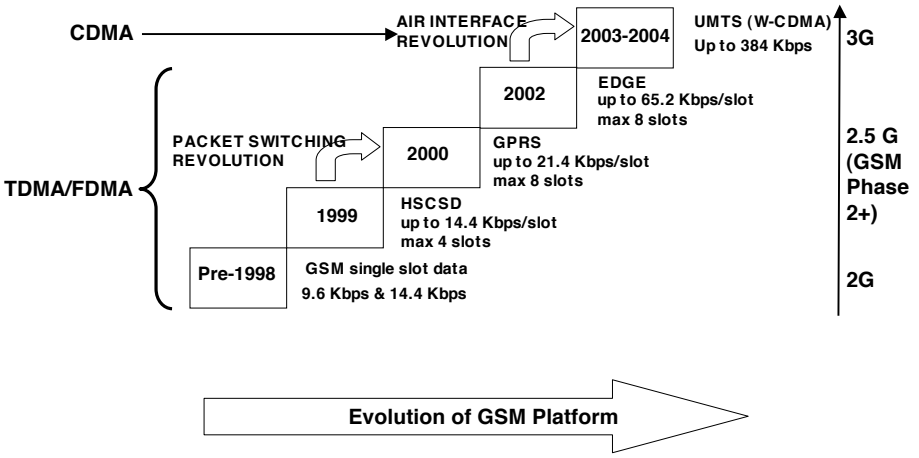
51

Security Architectures and Protocols in 3G Mobile Networks

(Section 4)

1

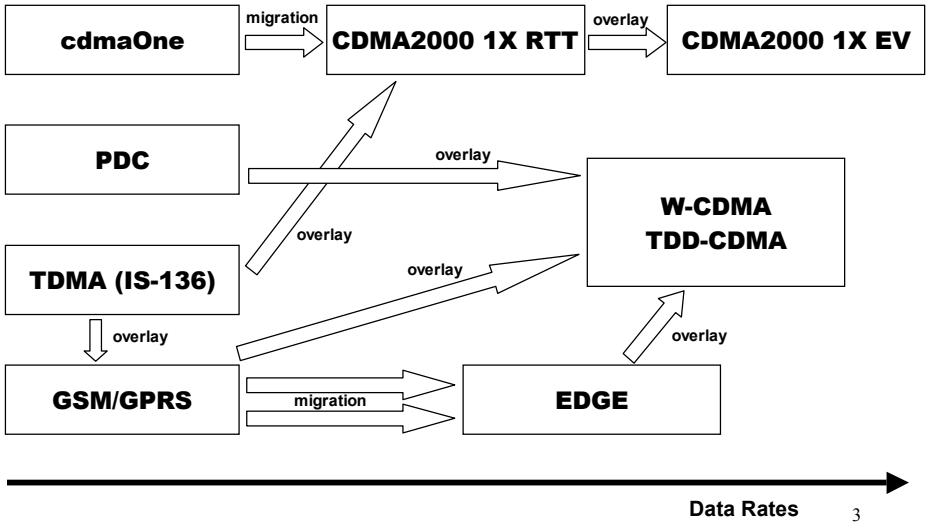
GSM Evolution Towards UMTS*



*** Universal Mobile Telecommunications System**

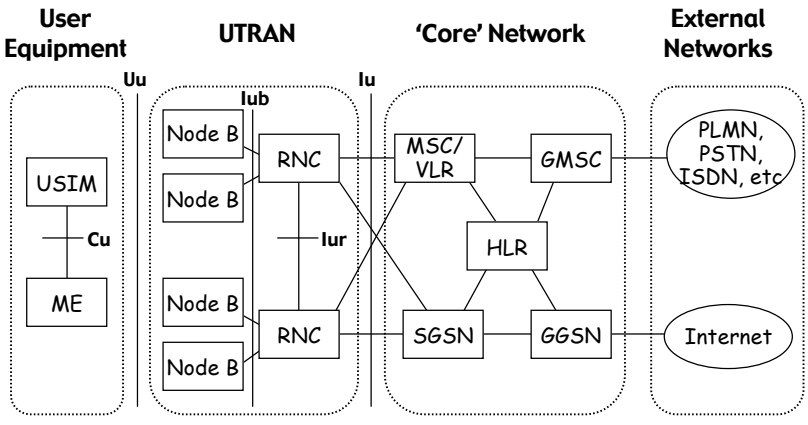
2

Migrations and Overlays



3

UMTS Architecture



USIM - UMTS Subscriber Identity Module
ME - Mobile Equipment
RNC - Radio Network Controller
Node B = Base Station

5

UMTS Security Features

- *Main* GSM security elements:
- Subscriber authentication
- Subscriber identity confidentially
- SIM to be removable from terminal hardware
- Radio interface encryption
- *Additional* UMTS security features:
- ……..

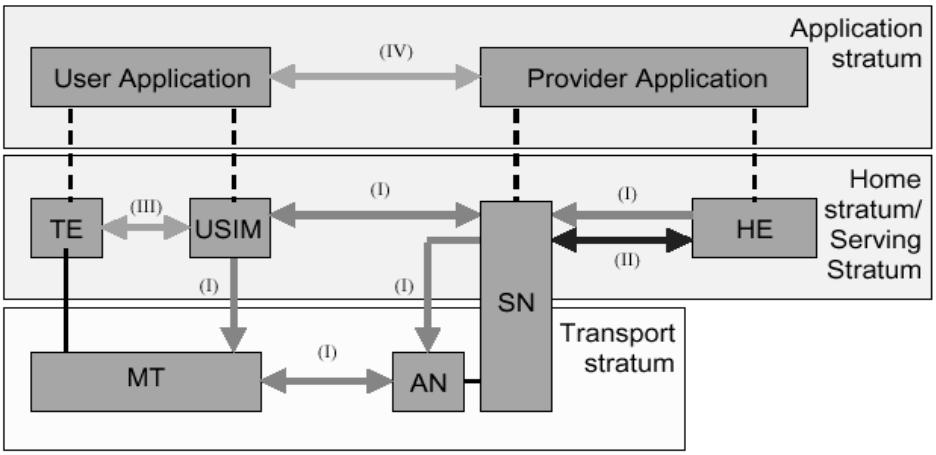
7

UMTS Security Features

- *Main* GSM security elements:
- ……..
- *Additional* UMTS security features:
- Security against using false base-stations with mutual authentication
- Encryption extended from air interface only to include Node-B (Base Station) to RNC connection
- Data in network will be protected in storage and while transmitting ciphering keys and authentication data
- Mechanism for upgrading security features

8

UMTS Security Architecture



AN: Access Network
HE: Home Equipment
MT: Mobile Terminal
SN: Serving Network
TE: Terminal Equipment
USIM: User Service Identity Module

UMTS Security Features - Terms

- TE - terminal equipment
- USIM - UMTS subscriber identity module
- MT - mobile terminal
- AN - access network
- SN - serving network
- HE - home equipment / environment
- UE - Wireless UMTS terminal
- Note:
  - TE + MT + USIM = UE

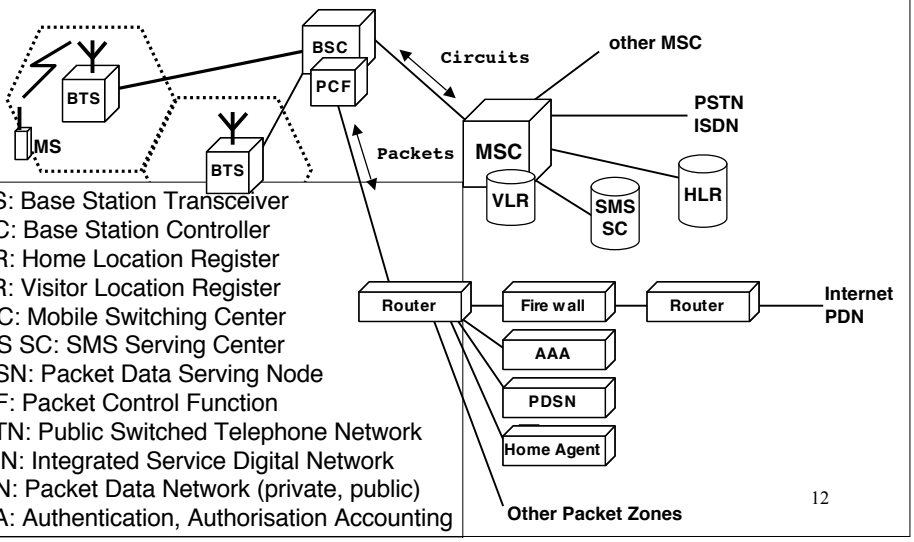
10

UMTS Security Features

- UMTS specifies (3GPP TS 33.102):
  - Network access security (I)
  - Network domain security (II)
  - User domain security (III)
  - Application domain security (IV)
  - Visibility and configurability of security (V)
- UMTS focuses on architecture and *not* on cryptographic algorithms, but for airlink encryption specifies [see note] ...
  - KASUMI 64-bit Feistel block cipher, 128-bit key

11

cdma2000 System Architecture



BTS: Base Station Transceiver
BSC: Base Station Controller
HLR: Home Location Register
VLR: Visitor Location Register
MSC: Mobile Switching Center
SMS SC: SMS Serving Center
PDSN: Packet Data Serving Node
PCF: Packet Control Function
PSTN: Public Switched Telephone Network
ISDN: Integrated Service Digital Network
PDN: Packet Data Network (private, public)
AAA: Authentication, Authorisation Accounting

12

Throughput in CDMA and UMTS ….

- Variety of bearer services:
  - cdmaOne → 115.2 Kbps
  - CDMA2000 → 1x 144 →307 Kbps, 3x 2 Mbps
  - CDMA2000 1xEV-DO (Data Only) → 2.4 Mbps*
  - CDMA2000 1xEV-DV (Data/Voice)→ 2.4 Mbps
  - W-CDMA (UMTS) → 384 Kbps
- CDMA2000 1x at 144 Kbps implies "best-effort" delivery without QoS / Security architectures (= 2.5G)
- CMDA2000 1x/3x at 307 Kbps and 2.4 Mbps implies QoS and Security functionality (= 3G)

1xEV-DO and UMTS Roadmaps

Courtesy UMTS Forum	1xEV-DO Rev. 0	1xEV-DO Rev. A	NxEV-DO Rev. B	UMTS R99	UMTS HSDPA R5	UMTS HSDPA/ HSUPA R6
Carrier Size (MHz)	1.25	1.25	5 (ex.)	5	5	5
Peak Forward Data Rate (Mbps)	2.4	3.1	14.4	.384	3.6	14.4
Typical Forward Data Rate (Mbps)	.4-.5	.5-.6	1.8 (est.)	.064-.3	.4-.7	.5-.7
Peak Reverse Data Rate (Mbps)	.144	1.8	5.4	.064	.384	1.5
Typical Reverse Data Rate (Mbps)	.06-.08	.3-.5	1.5 (est.)	.03-.04	.06-.08	.2-.4
Forward Capacity (Mbps/Sector)	.8	1.0	3.0	.5	2.1 (est.)	2.5 (est.)
Reverse Capacity (Mbps/Sector)	.4	.8	2.4	.4	.5 (est.)	.6 (est.)
Forward Spectral Efficiency (est.)	0.64	0.8	.8	0.102	0.42	0.5
Reverse Spectral Efficiency (est.)	0.32	0.64	.64	0.08	0.1	0.12
Estimated Commercial Deployment	2002	2H2006	2008 (est.)	2005	2H2006?	2008?

Security Architectures in 3G - WAP 2.0, IPSec/VPN

27

Security Architectures in 3G

- WAP2.0
  - Web based applications including browsing, imaging, multimedia messaging, telephony services etc
  - Involves use of TLS, Digital Certificates, PKI, crypto libraries, etc
- IPSec and VPN
  - Firewalls and tunneling - consistent with secure architectures in fixed networks
  - Many handheld devices do not yet support IPSec

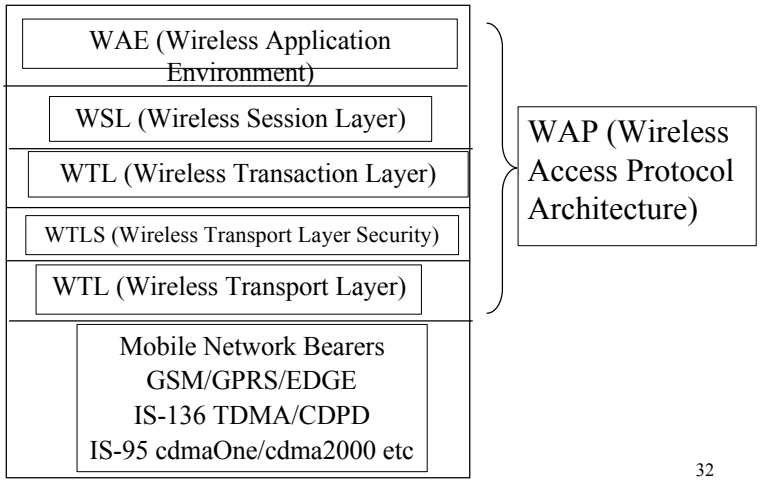
28

WAP 2.0 Architecture

- WAP 2.0 has to be able to support the "legacy WAP 1.x stack as well as low-bandwidth IP bearers
  - References:
    - www.wapforum.org/what/whitepapers.htm
    - www.wapforum.org/what/technical.htm

31

WAP Overview of Architecture

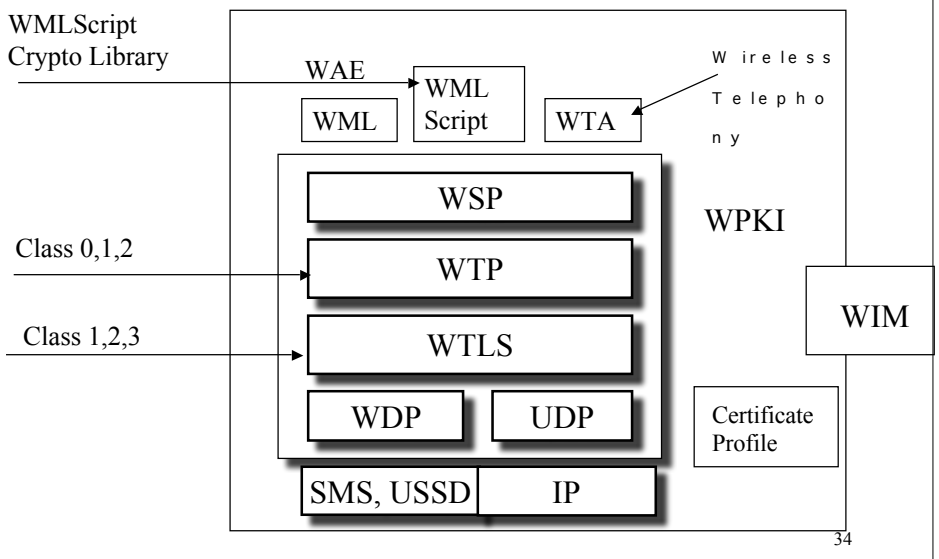


32

- **WAE**: Wireless Application Environment - includes micro-browser, WML (Wireless Markup Language), WMLScript (client-side scripting language), telephony services, formats for commonly used data such as images
- **WSP**: Wireless Session Protocol, providing HTTP 1.1 functionality, session state management, and reliable / unreliable data push / pull
- **WTP**: Wireless Transaction Protocol: transaction layer providing transport services (one way / two way)
- **WTLS**: Wireless Transport Layer Security: security layer, confidentiality, integrity, authentication, + some protection against denial-of-service attacks
- **WDP**: (= UDP/IP) Wireless Datagram Protocol: connectionless transport layer

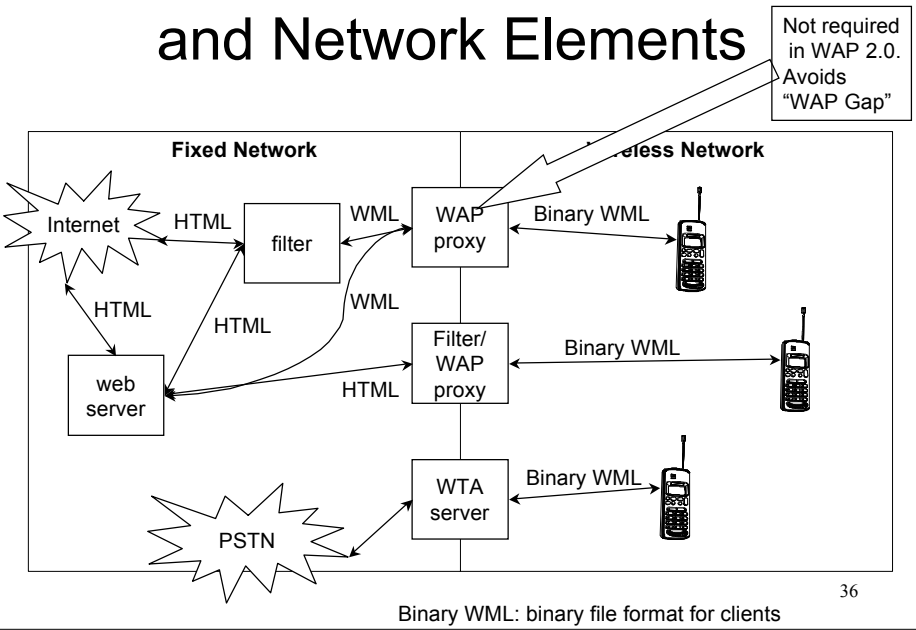
33

WAP - Overview of Architecture



34

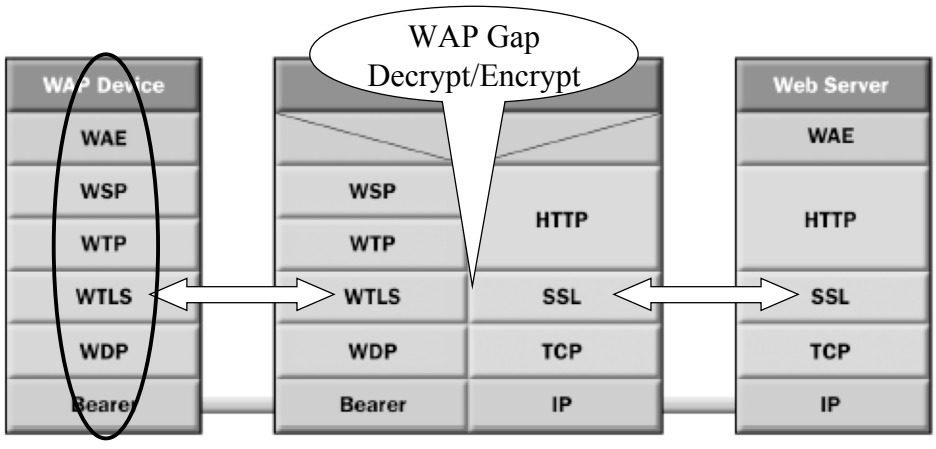
WAP - Different Scenarios and Network Elements



36

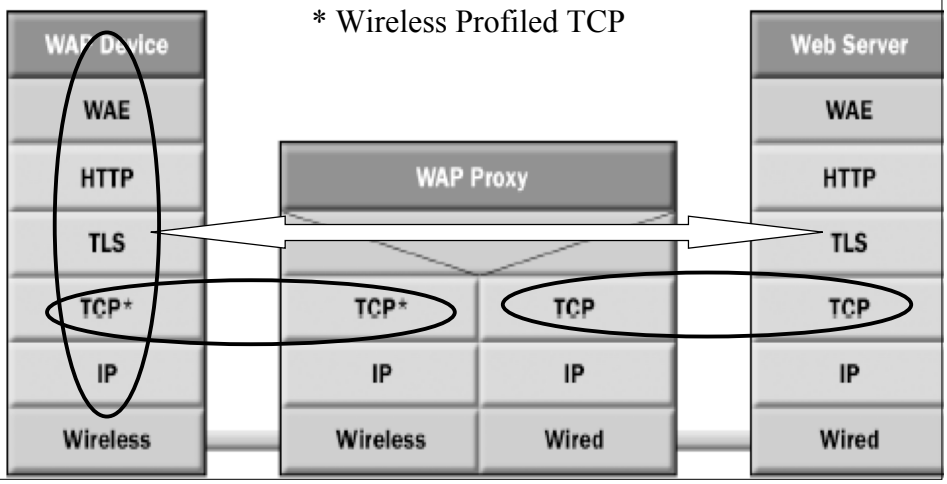
Binary WML: binary file format for clients

WAP 1.x Gateway



37

WAP 2.0 - Proxy with Profiled TCP and HTTP



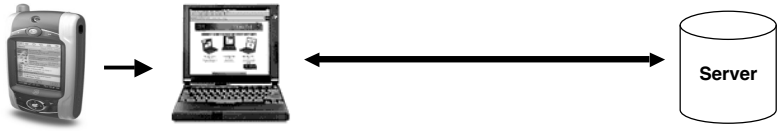
Security Issues in Wireless Networks

- Adding separate security infrastructure to support WAP is expensive
- Better to deploy single security system for both *fixed* web and *wireless* web applications
- Integration of WAP and web security can be achieved by using protocols already designed for fixed networks
- WTLS (Wireless Transport Layer Security) is virtually identical to SSL/TLS

39

Security Issues in Wireless Networks

- Server may not care what device (laptop, phone) is on end of secure tunnel
- Difficult to do all crypto functions expected by server on phone, then phone may connect to laptop where full security functionality can be provided (IPSec, DES, AES, MD5, SHA-1 etc)



40

Wireless Transport Layer Security (WTLS)

- Goals
  - Integrity - no change to data in transit
  - Privacy - not possible to snoop
  - Authentication - via digital signature
  - Protection against some DOS attacks
- WTLS
  - Released in WAP 1.0, used in WAP 2.0
  - Based on TLS 1.0 (formerly SSLv3) RFC 2246
  - Adapted for low-bandwidth communication channels

41

Wireless Transport Layer Security (WTLS)

- A few differences between TLS 1.0 and WTLS:
  - adapted for high-latency and low-bandwidth wireless environment
  - accommodates unreliable link
  - reduces client code size and processor requirements
  - reduces number of round trips for high latency networks

43

Wireless Transport Layer Security (WTLS)

- Provides security facilities for encryption, strong authentication, integrity, key management using:
  - Data encryption: RC4, DES or Triple DES
  - Key exchange and authentication: RSA, Diffie-Hellman, Elliptic Curve Crypto (ECC)
  - Message integrity: SHA-1, MD5
- Compliant with regulations on use of crypto algorithms + key lengths in different countries

45

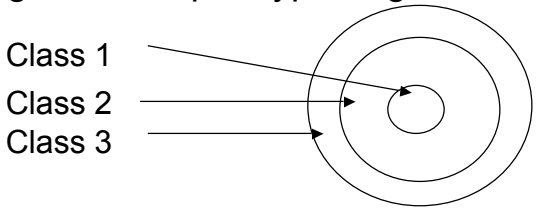
Wireless Transport Layer Security (WTLS)

- WTLS has 4 classes:
- *Class 1* provides:
  - privacy - using encryption
  - integrity - using authentication codes (MACs)
  - no client or server authentication
- *Class 2* provides:
  - PKI based handshake with *server* authentication - using server certificate and private key
    - eg Blackberry Mobile Device

46

Wireless Transport Layer Security (WTLS)

- *Class 3* provides:
  - client authentication - using *client* certificate and private key
- *Class 4* provides:
  - client authentication with digital signatures using WMLScript Crypto.SignText

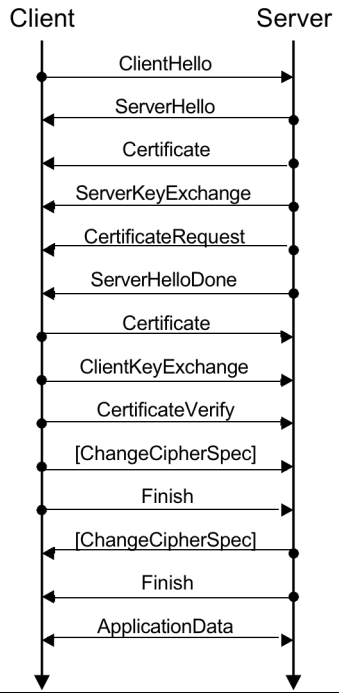


47

WMLScrypt (WMLScript Crypto)

- API allowing access to security functions in WMLScript Crypto Library:
  - key-pair generation
  - digital signature generation
  - PKI keys and certificates
- Current use is to sign text and confirm using WMLScript Crypto.SignText function
- Example: Blackberry Mobile Device
- Reference:
  - WAP Forum: *WMLScript Crypto Library*, 2001, www.wapforum.org

48

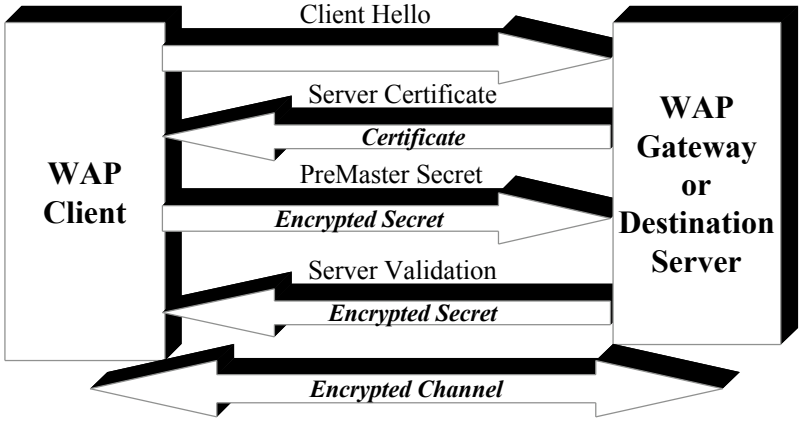


WTLS Handshake Session-Establishment Sequence

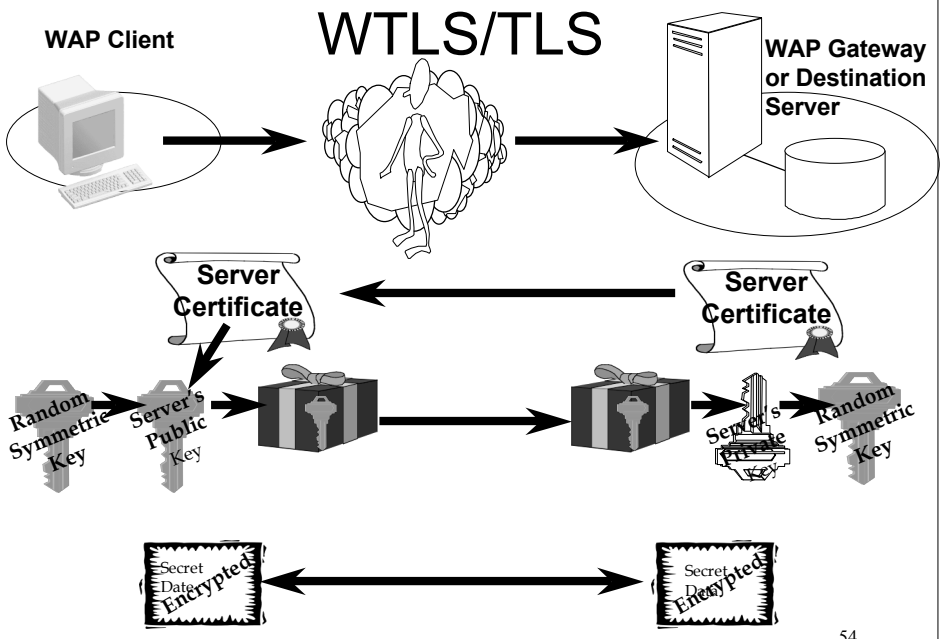
52

WTLS/TLS Protocol Interactions

Server Side Authentication

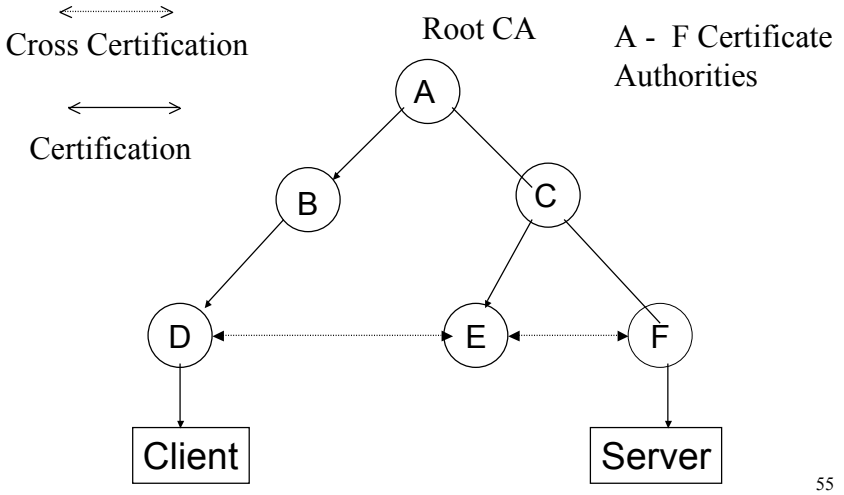


53



54

Path of Trust and Certificate Path Validation



55

IPSec and VPN Architecture

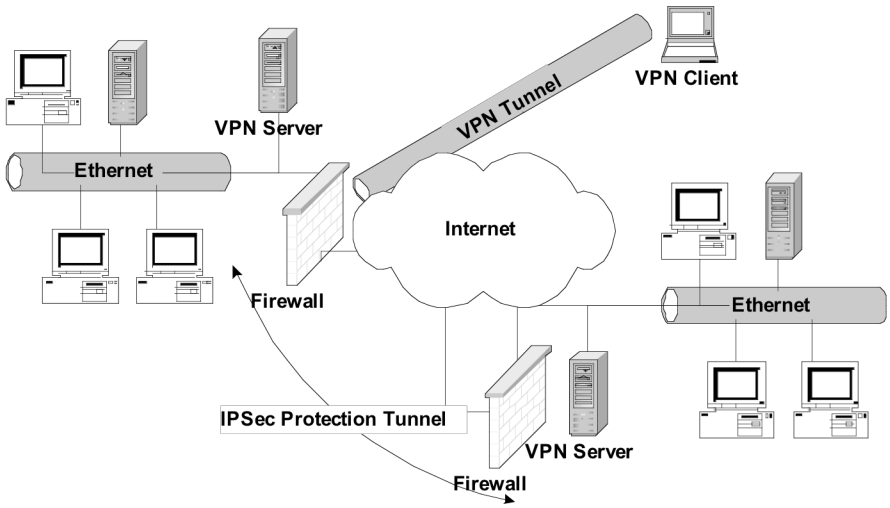
57

IPSec and VPN Architecture in 3G

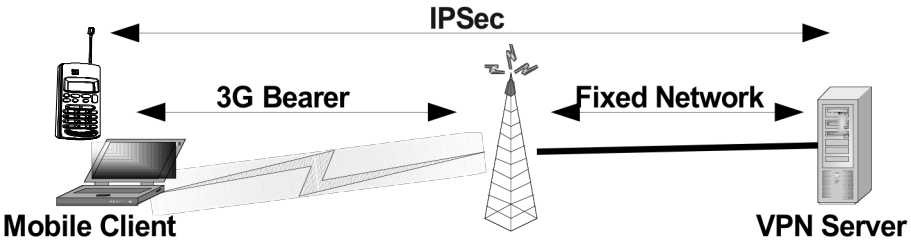
- Essentially consistent with fixed networks
- VPN tunnels created with IPSec
- SSH (Secure Shell)
- Need for Wireless Profiled TCP
- Need for powerful chip sets in order to carry out all crypto in small mobile devices

58

Typical VPN Implementation



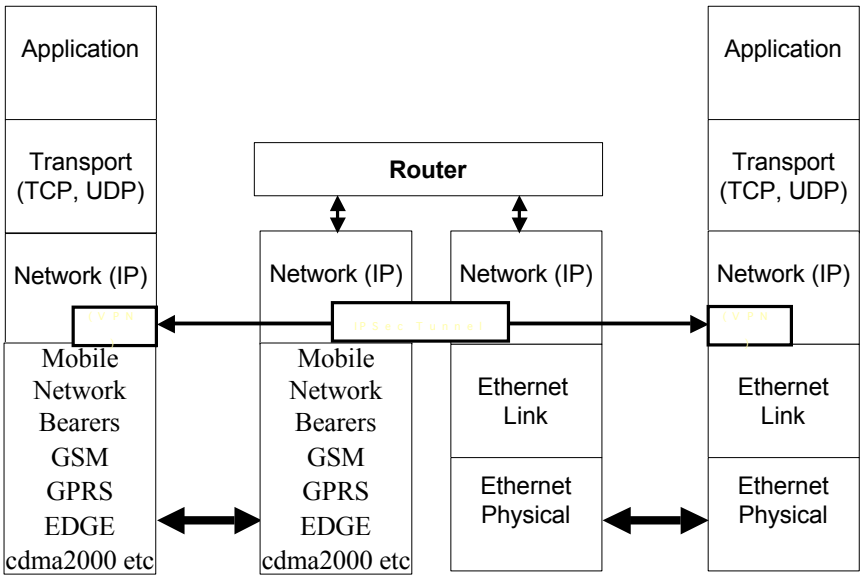
IPSec and VPN Architecture in 3G



Tunnels configured using IPSec and IKE

60

IPSec and VPN Architecture in 3G



Blackberry VPN Wireless Architecture

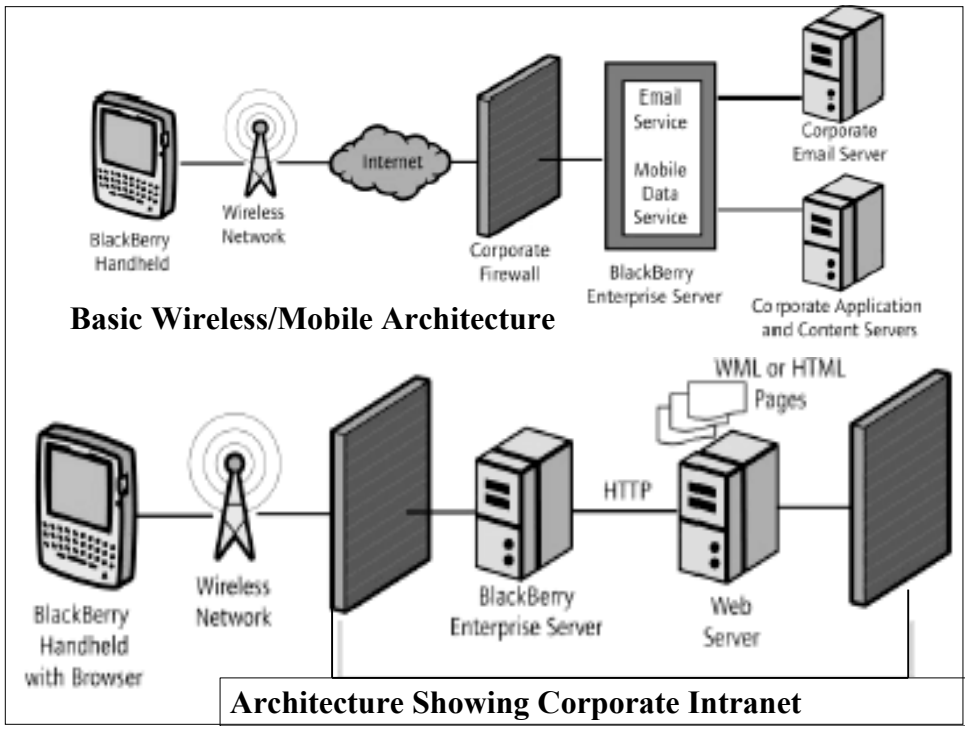
- Proprietary solution using many wireless / mobile technologies already described
- “Always connected” + “push” solution
- Graphical browser for e-mail and mobile applications to Blackberry’s enterprise server
- Operates over GPRS and CDMA networks
- Utilises Motorola’s iDEN (Integrated Digital Enhanced Network) and J2ME system development kits

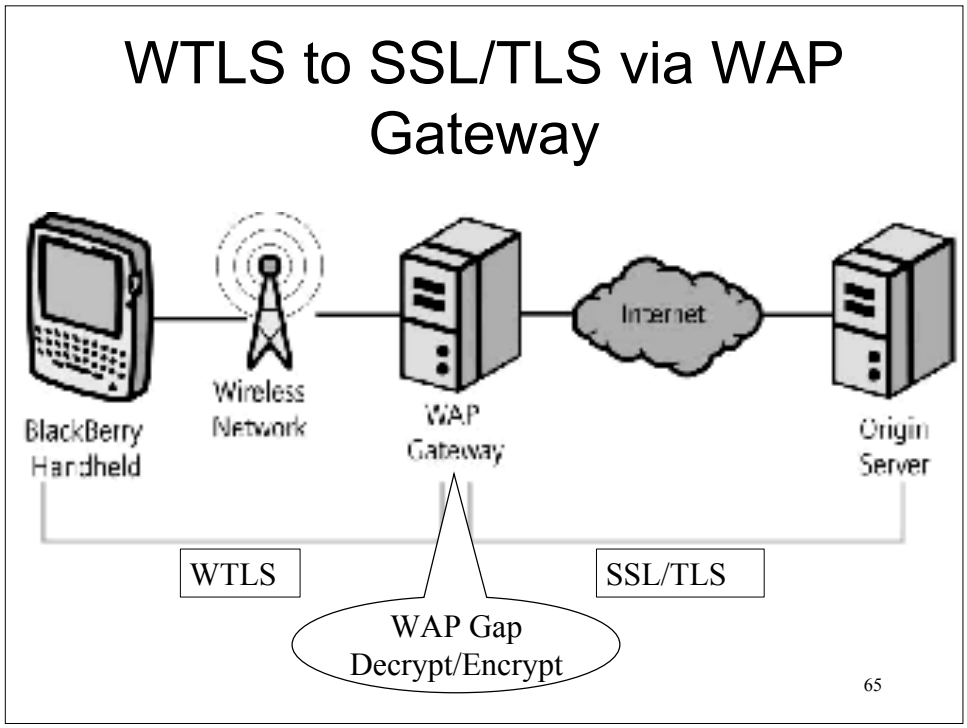
62

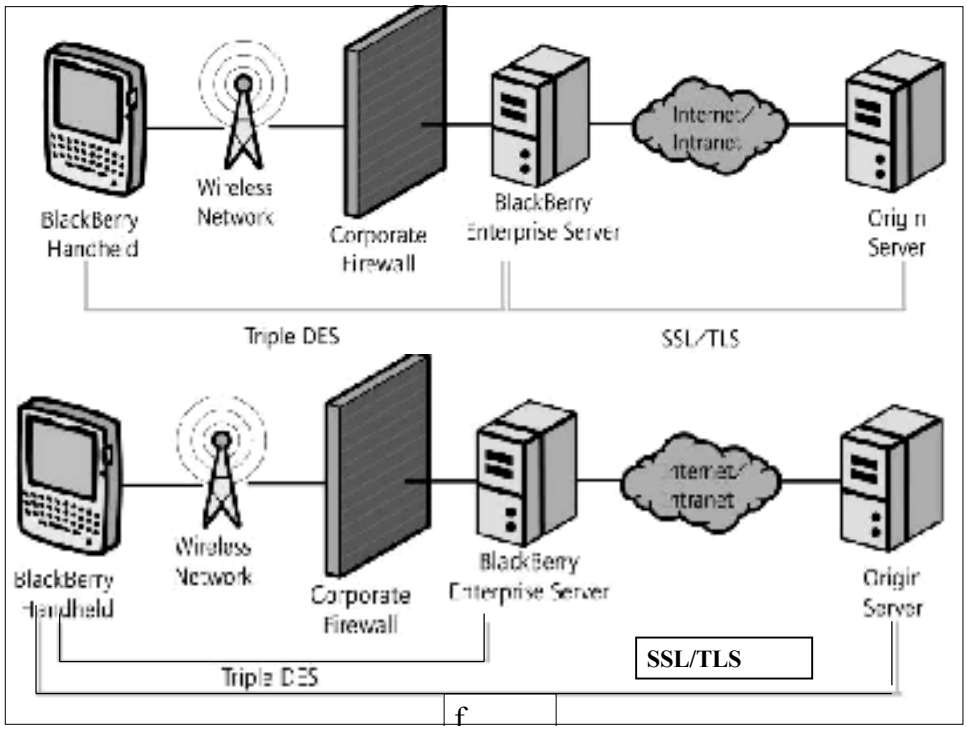
Blackberry VPN Wireless Architecture

- Supports standard TCP/IP and HTTP interfaces
- Blackberry mobile cannot be used to access Internet - can only interact with:
  - Blackberry server
  - WAP Gateway
- Crypto - 3DES and/or SSL/TLS
- Can suffer from “WAP Gap” (3DES←→SSL/TLS)
- Supports WTLS Class 2 (server certificate only)
- Uses WMLScript Crypto.SignText function, ie client authentication with digital signature

63


Email Service
Mobile Data Service
Corporate Email Server
Internet
BlackBerry Handheld
Wireless Network
Corporate Firewall
BlackBerry Enterprise Server
Corporate Application and Content Servers
Basic Wireless/Mobile Architecture
WML or HTML Pages
HTTP
BlackBerry Handheld with Browser
Wireless Network
BlackBerry Enterprise Server
Web Server
Architecture Showing Corporate Intranet


WTLS to SSL/TLS via WAP Gateway
BlackBerry Handheld
Wireless Network
WAP Gateway
Internet
Origin Server
WTLS
SSL/TLS
WAP Gap
Decrypt/Encrypt
65



Technical Additions for Secure WAN Wireless/Mobile Operation

- Wireless Profiled TCP (WP-TCP)
- SSH - Secure Shell
- Specialised crypto processors

67

WP-TCP - Wireless Profiled TCP

- TCP connection-orientated services optimised for wireless networks and interoperates with standard TCP
- WP-TCP supports:
  - Large window size
  - Round trip time (delay) measurement
  - Large initial window RFC 2414
  - MTU (Maximum Transmission Unit) discovery and size

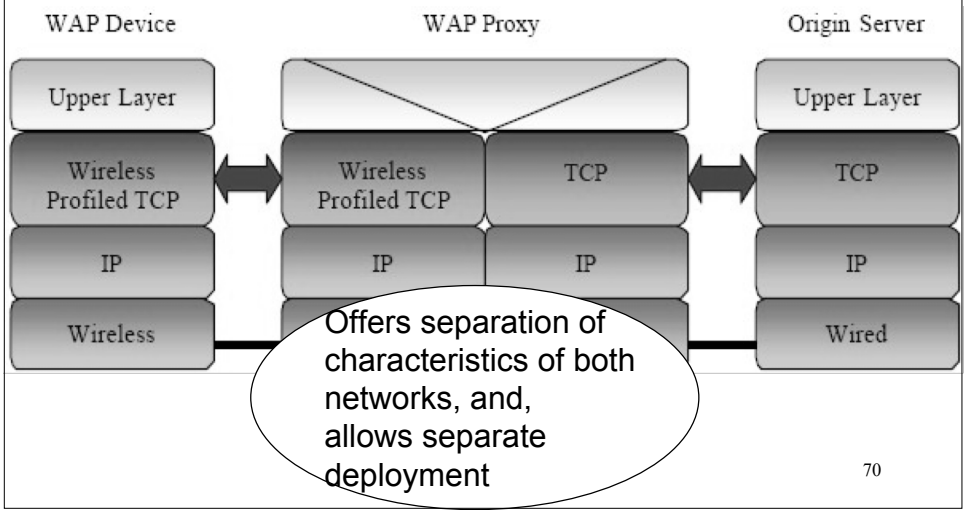
68

WP-TCP - Wireless Profiled TCP

- WP-TCP supports contd:
  - SACK (Selective Acknowledgement) RFC 2018
  - TCP Slow-Start RFC 2001
  - Congestion Avoidance (RED) RFC 2581
  - Fast Retransmission
  - Fast Recovery
- References:
  - WAP Forum: *Wireless Profiled TCP*, 2001, www.wmlclub.com/docs/ especwap2.0 /WAP-225-TCP-20010331-a.pdf
  - RFC 2757 Long Thin Networks

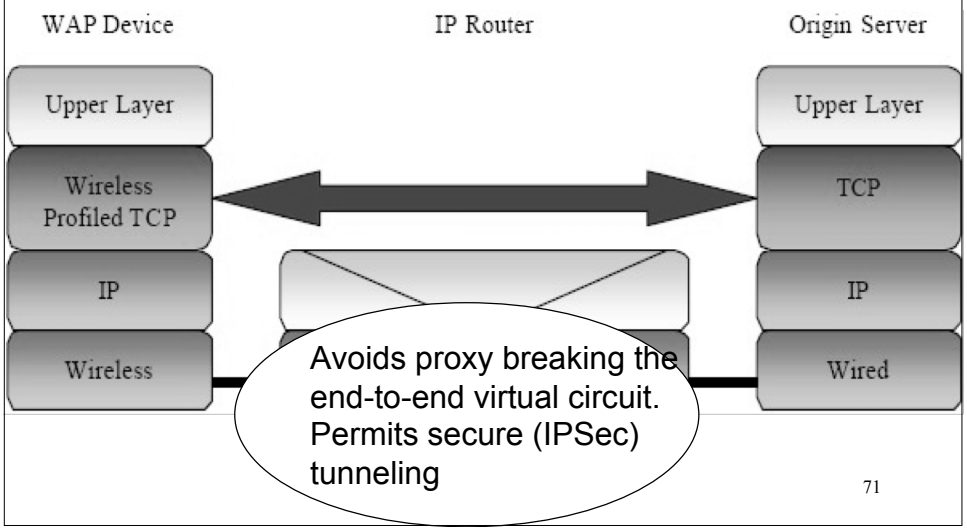
69

Split (Proxy) WP-TCP Mode



70

End-to-End WP-TCP Mode



71

SSH (Secure Shell)

- SSH can be used in mobile systems to provide strong cryptographic authentication for administration and monitoring functions in mobile devices
- SSH Secure Shell 3.2 (www.ssh.com)
  - SSH Secure Tool Toolkit
  - SSH IPSec Toolkit
  - SSH Certificate/TLS Toolkit
  - Sonera provides mobile PKI solution

72

SSH (Secure Shell)

- SSH functions include:
  - All transmitted data is encrypted
  - Provides security for Telnet, FTP ... connections
  - Secure tunnelling of any TPC/IP ports
  - Supports IPv4 and IPv6
  - Public key based user authentication
  - Public key based host authentication verifies that connection is established to correct server preventing man-in-the-middle attacks

73

Security Processors for 3G

- Important that crypto be carried out in dedicated processor if throughput is an important factor - eg Motorola's MPC190 Security Processors
  - IPSec + Internet Key Exchange (IKE)
  - Secure Sockets Layer (SSLv3)
  - Transport Layer Security (TLS 1.0)
  - Wireless Transport Layer Security (WTLS/TLS)

74

Summary - 3G Security

- Considerable development in progress:
  - underlying bearer services, UMTS, cdma2000
- Security solutions carried over from fixed networks include:
  - IPSec, VPN etc
- WAP2 (TLS/WTLS) provides security for web-based mobile applications
- Significant work yet to be carried out to fully implement UMTS security architecture

77