PV222
Security Architectures

Lecture 3

Wireless LAN Security

Lecture Overview

- Introduction to wireless networking technologies
- Radio Frequency IDentification (RFID)
- IEEE 802.11 Standards
- Security of IEEE 802.11 Wireless LANs
- Securing Wireless LANs
- Recent Developments

Objectives of Lecture

- Study the security issues arising in wireless networks, in particular, those conforming to the IEEE 802.11 family of standards.
- Understand countermeasures available to reduce threats in wireless LANs.
- Discuss the continuing development of IEEE security standards for wireless LANs.

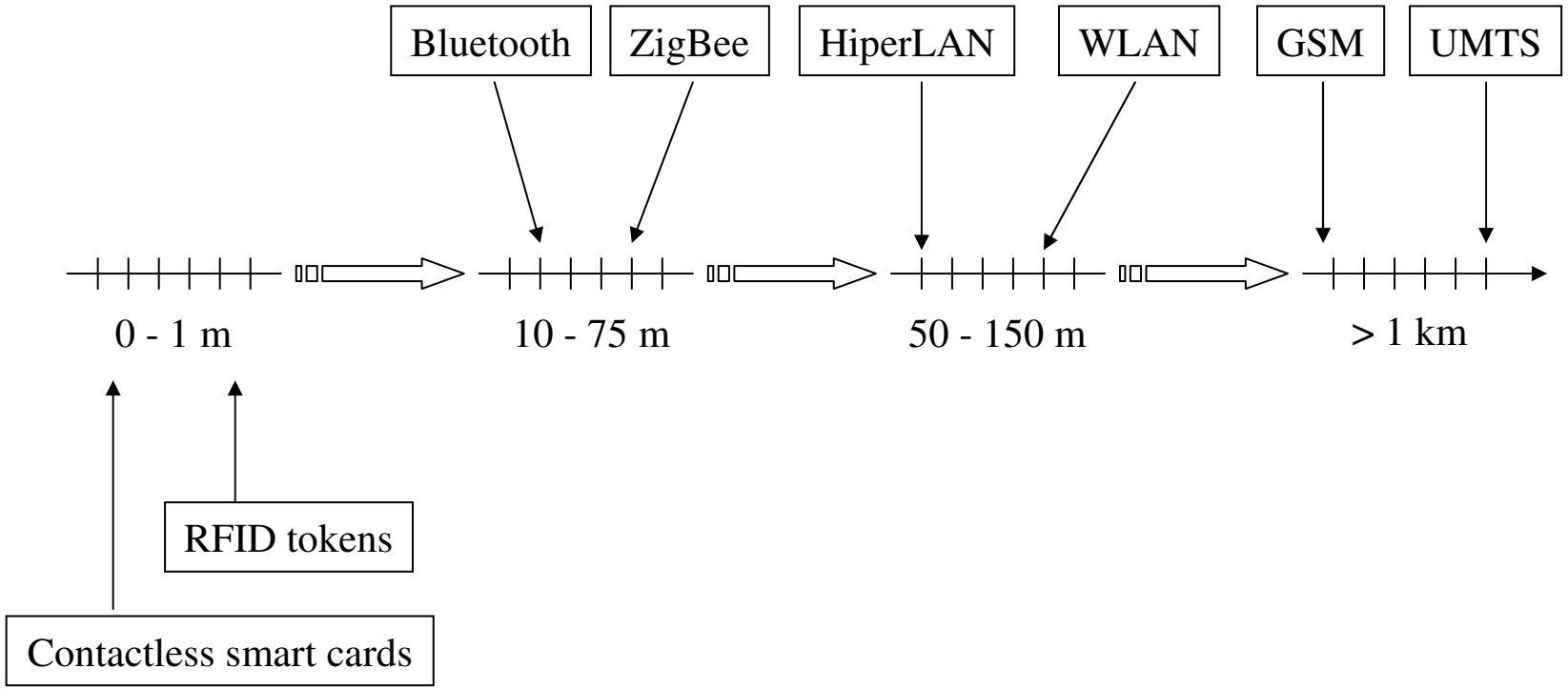
Introduction to wireless networking technologies

- Wired technologies
  - Use cables
- Wireless technologies
  - Use radio transmission as the means for transmitting data
  - Allows mobility
  - Receive and transmit information using electromagnetic (EM) waves, ranging from the radio frequency (RF) band up and above the infrared (IR) band.

Types of Wireless Networks

- WWAN (Wireless Wide Area Networks)
  - e.g. GSM, UMTS
- WLAN (Wireless Local Area Networks)
  - e.g. 802.11, HiperLAN, HomeRF
- WPAN (Wireless Personal Area Networks)
  - e.g. Bluetooth, ZigBee, Infrared

Initiatives and Techniques



Threats and Vulnerabilities of Wireless Systems

- ISO 7498-2 Fundamental Threats
  - Information leakage
  - Integrity violation
  - Denial of service
  - Illegitimate use

Threats and Vulnerabilities of Wireless Systems

- ISO 7498-2 Primary enabling threats
  - Masquerade
  - Bypassing controls
  - Authorisation violation
  - Trojan horse
  - Trapdoor

Radio Frequency IDentification (RFID)

- Automatic Identification and Data Capture (AIDC) technology.
- Small data-carrying tokens (*tags*).
  - Integrated circuit (*chip*).
  - Read from and write to tags using readers.
- Fixed or mobile scanners (*readers*).
- Readers and tags communicate using low power radio frequency (RF) signals.
- Data captured from tags is transferred between distributed readers and a host environment using wired or wireless communications.

RFID Tags and Readers

- *Active* tags contain a radio transceiver and a power source.
- *Passive* tags respond to the reader.
  - Optionally contain a battery (*semi-passive*).
- Tags typically offer very limited functionality.
  - Often read-only with around 128 bits of storage.
  - Some tags are read/write.

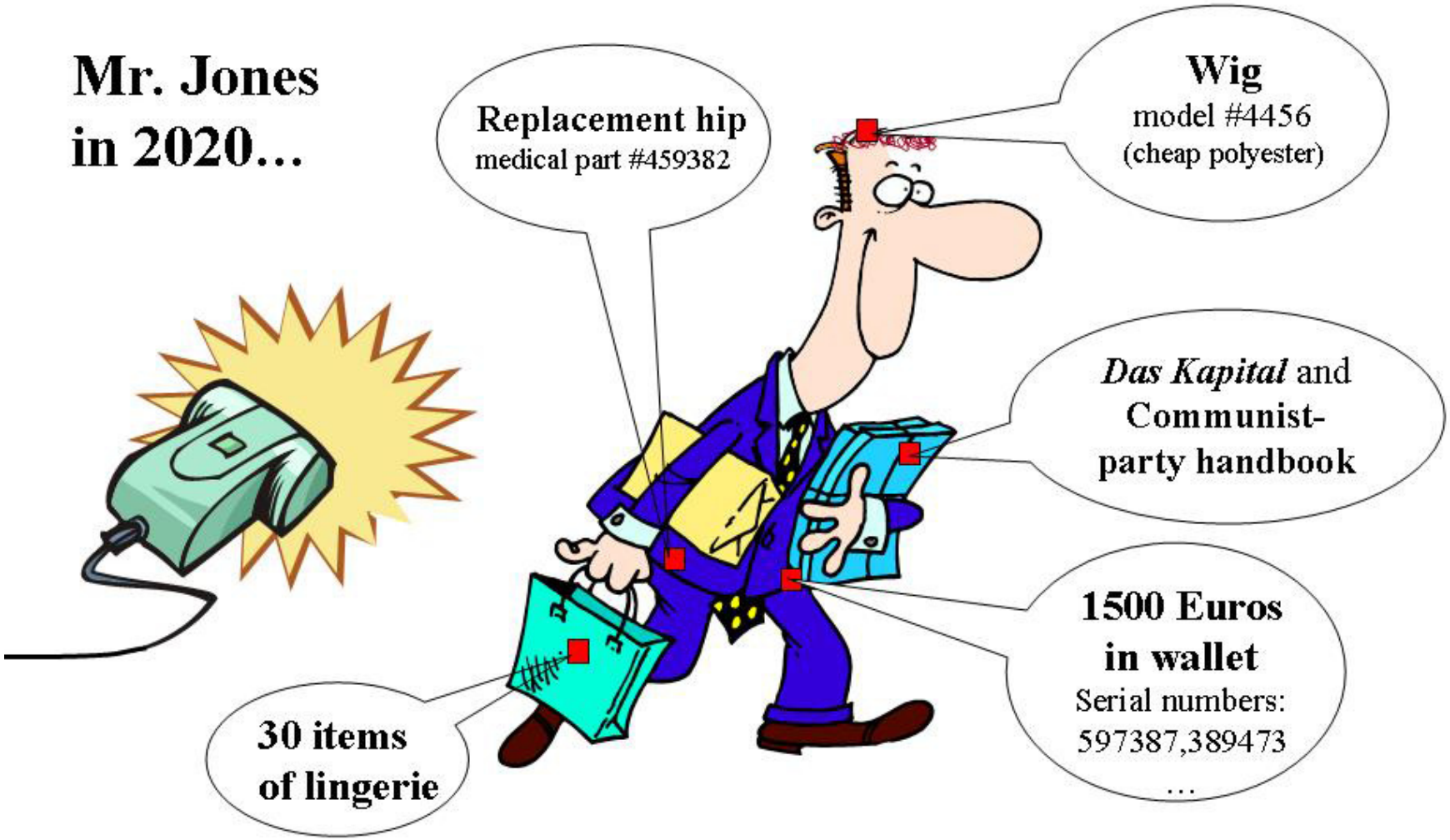
RFID Tags

- The main advantage of RFID tags are:
  - Cost and size
    - e.g. the Hitachi *mu-chip* is 0.4mm^2 and costs \$0.20.
- The main disadvantage of RFID tags are:
  - Limited computation power and range.
  - Fractured standardisation efforts across the industry and internationally.
- Many applications manage to balance these conflicts!
  - Applications will typically have low security requirements.

RFID Security

- Traditionally, little-to-no security (due to the constrained nature of the RFID tag).
- Security solutions mainly password-based or symmetric key-based (all tags and readers share the same symmetric key).
- Public key solutions are coming.

RFID Security (2)



New Applications

- "… Marks & Spencer … began replacing bar codes with an RFID system in its $4.4 billion fresh-food business. The company is putting radio tags on all of the 3.5 million plastic containers it uses to tote food from suppliers to stores. Before, suppliers had to print bar-coded labels for each of the 7 million bins M&S handles every week. Now, each time one of M&S's 340 suppliers pack one of these bins, the system encodes shipment data – including product codes, quantities, and expiration dates – onto RFID tags embedded in the carton. About 50 plastic containers can be read at once, slashing the average time required to scan each one by 83%, to five seconds from 29. Thanks to increased handling efficiencies, less spoiled food, and fewer lost shipments, M&S expects to recoup its $3 million smart tag investment in three years.
- (`http://www.businessweek.com/magazine/content/02_27/b3790093.htm`)

IEEE 802.11 Standards

- IEEE 802 is a dominant collection of networking standards developed by IEEE.
  - E.g. IEEE 802.3 specifies the physical and data link layer properties of Ethernet.
- IEEE 802.11 is a family of standards for wireless LANs.
  - Baseline IEEE Std 802.11-1997 was approved in June 1997
  - Current standard is IEEE Std 802.11-1999
  - Supplemented by amendment documents (in the sequence a,b,d,g,h,i, j, and e) and one corrigendum document
  - IEEE Std 802.11-1999 was reaffirmed by the 802.11 working group in 2003 without changes

802.11b

- 802.11b ratified in 1999 adding 5.5 Mbps and 11 Mbps.
- DSSS as physical layer.
  - 11 channels (3 non-overlapping)
- Dynamic rate shifting.
  - Transparent to higher layers
  - Ideally 11 Mbps.
  - Shifts down through 5.5 Mbps, 2 Mbps to 1 Mbps.
    - Higher ranges.
    - Interference.
  - Shifts back up when possible.
- Maximum specified range 100 metres
- Average throughput of 4Mbps

802.11a

- 802.11a ratified in 2001
  - Supports up to 54Mbps in 5 Ghz range.
  - Higher frequency limits the range
  - Regulated frequency reduces interference from other devices
  - 12 non-overlapping channels
  - Usable range of 30 metres
  - Average throughput of 30 Mbps
  - Not backwards compatible with 802.11b

802.11g

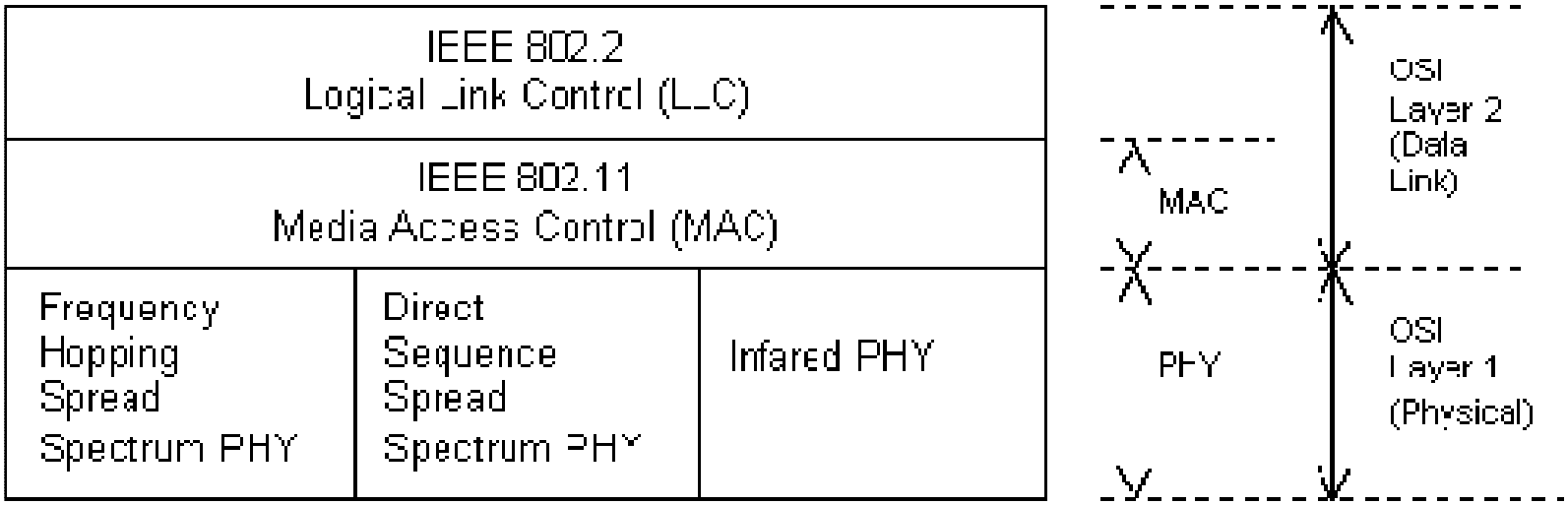
- 802.11g ratified in 2002
  - Supports up to 54Mbps in 2.4Ghz range.
  - Backwards compatible with 802.11b
  - 3 non-overlapping channels
  - Range similar to 802.11b
  - Average throughput of 30 Mbps
- 802.11n aiming for final approval in April 2008
  - Aiming for typical 200Mbps and maximum of 540Mbps (theoretical!)
  - Range of 50m (indoor)
  - Products already appearing, based on draft standard
  - Standards process has been bumpy

Wireless LANs

- IEEE Std 802.11-1997 provided wireless LAN at 1 Mbps & 2 Mbps.
- WECA (Wireless Ethernet Compatibility Alliance) promoted Interoperability.
  - Now Wi-Fi Alliance
- 802.11 provides protocols at Layer 1 & Layer 2 of OSI model.
  - Physical layer
  - Data link layer

IEEE 802.11 mapped to OSI Model

- 802.11 focuses on layer 1 and layer 2 of OSI model:
  - Physical layer
  - Data link layer



802.11 Physical Layer

- Originally three alternative physical layers
  - Two incompatible spread-spectrum methods in 2.4Ghz Industrial-Scientific-Medical (ISM) band
    - Frequency Hopping Spread Spectrum (FHSS)
      - 75 channels
    - Direct Sequence Spread Spectrum (DSSS)
      - 14 channels (11 channels in US)
  - One diffuse infrared layer
- 802.11 speed
  - 1 Mbps or 2 Mbps.

802.11 Data Link Layer

- Layer 2 split into:
  - Logical Link Control (LLC) layer.
  - Media Access Control (MAC) layer.
- LLC - same 48-bit MAC addresses as 802.3.
- MAC layer - CSMA/CD not possible.
  - Can't listen for collision while transmitting.
- CSMA/CA – Collision Avoidance.
  - Sender waits for clear air, waits random time, then sends data.
  - Receiver sends explicit ACK when data arrives intact.
  - Also handles interference.
  - But adds overhead.
- 802.11 always slower than equivalent 802.3.

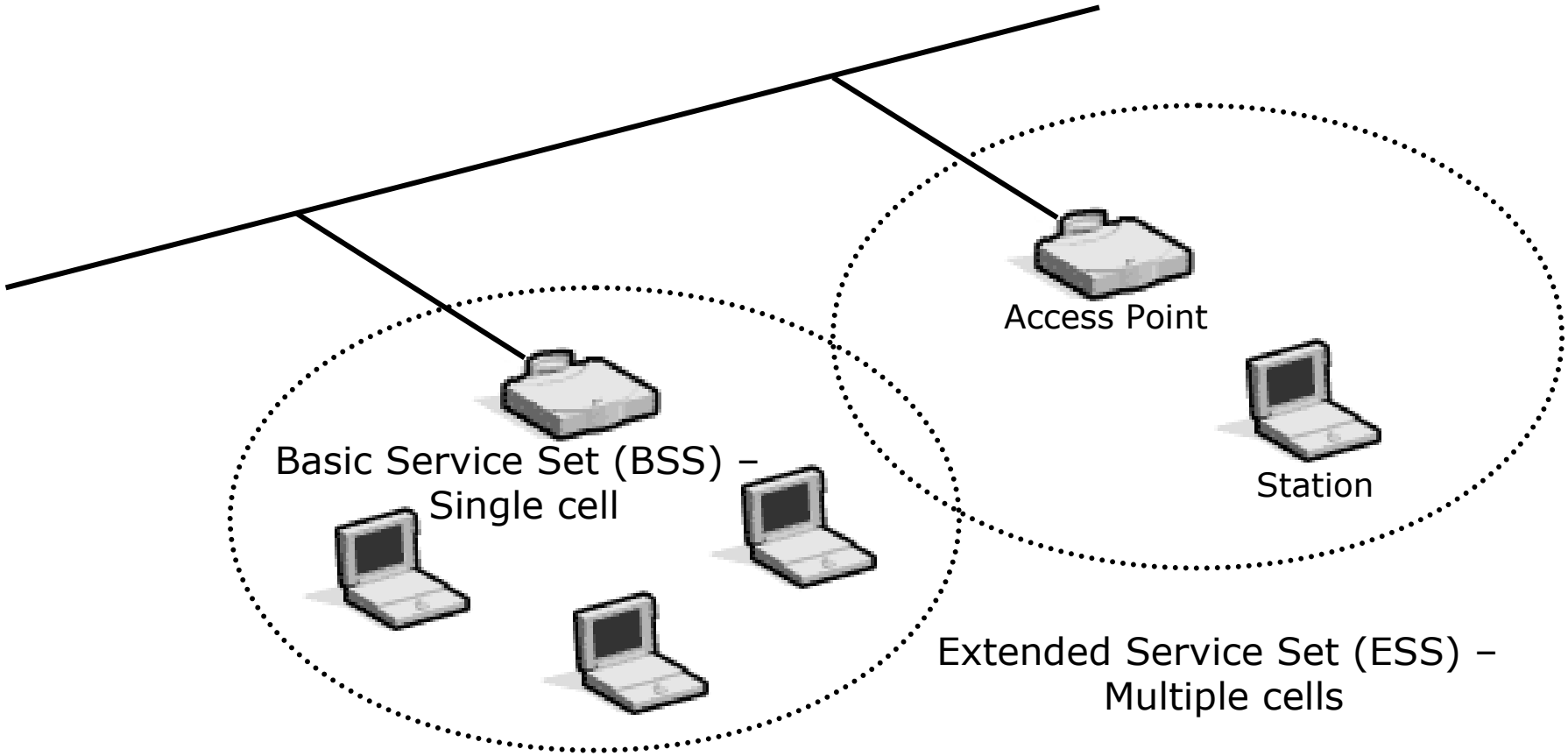
802.11 Components

- Two pieces of equipment defined:
  - Wireless station
    - A desktop or laptop PC or PDA with a wireless NIC.
  - Access point
    - A bridge between wireless and wired networks
    - Composed of
      - Radio
      - Wired network interface (usually 802.3)
      - Bridging software
    - Aggregates access for multiple wireless stations to wired network.

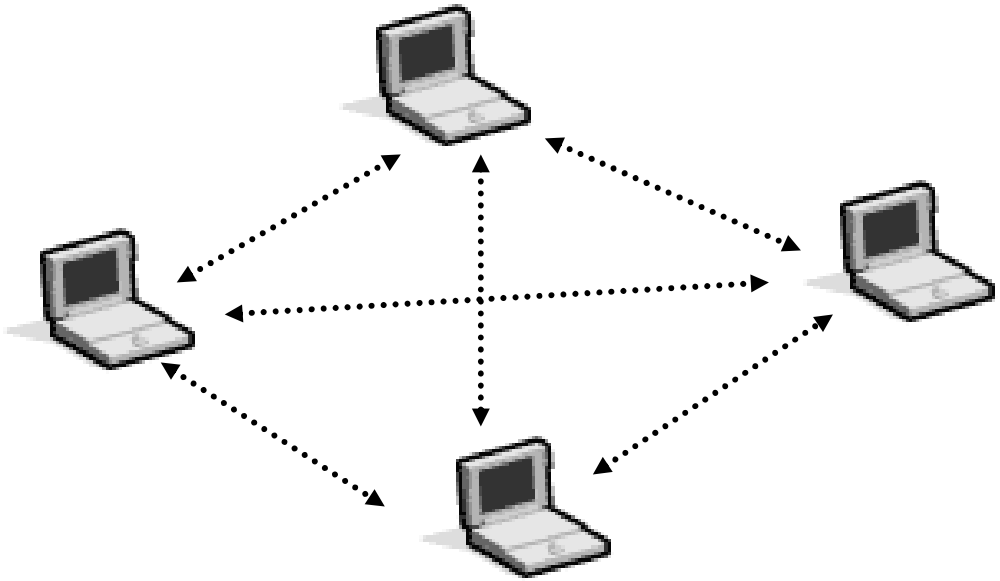
802.11 modes

- Infrastructure mode
  - Basic Service Set
    - One access point
  - Extended Service Set
    - Two or more BSSs forming a single subnet.
  - Corporate WLANs operate in this mode.
- Ad-hoc mode
  - Also called peer-to-peer.
  - Independent Basic Service Set
  - Set of 802.11 wireless stations that communicate directly without an access point.
    - Useful for quick & easy wireless networks.

Infrastructure mode

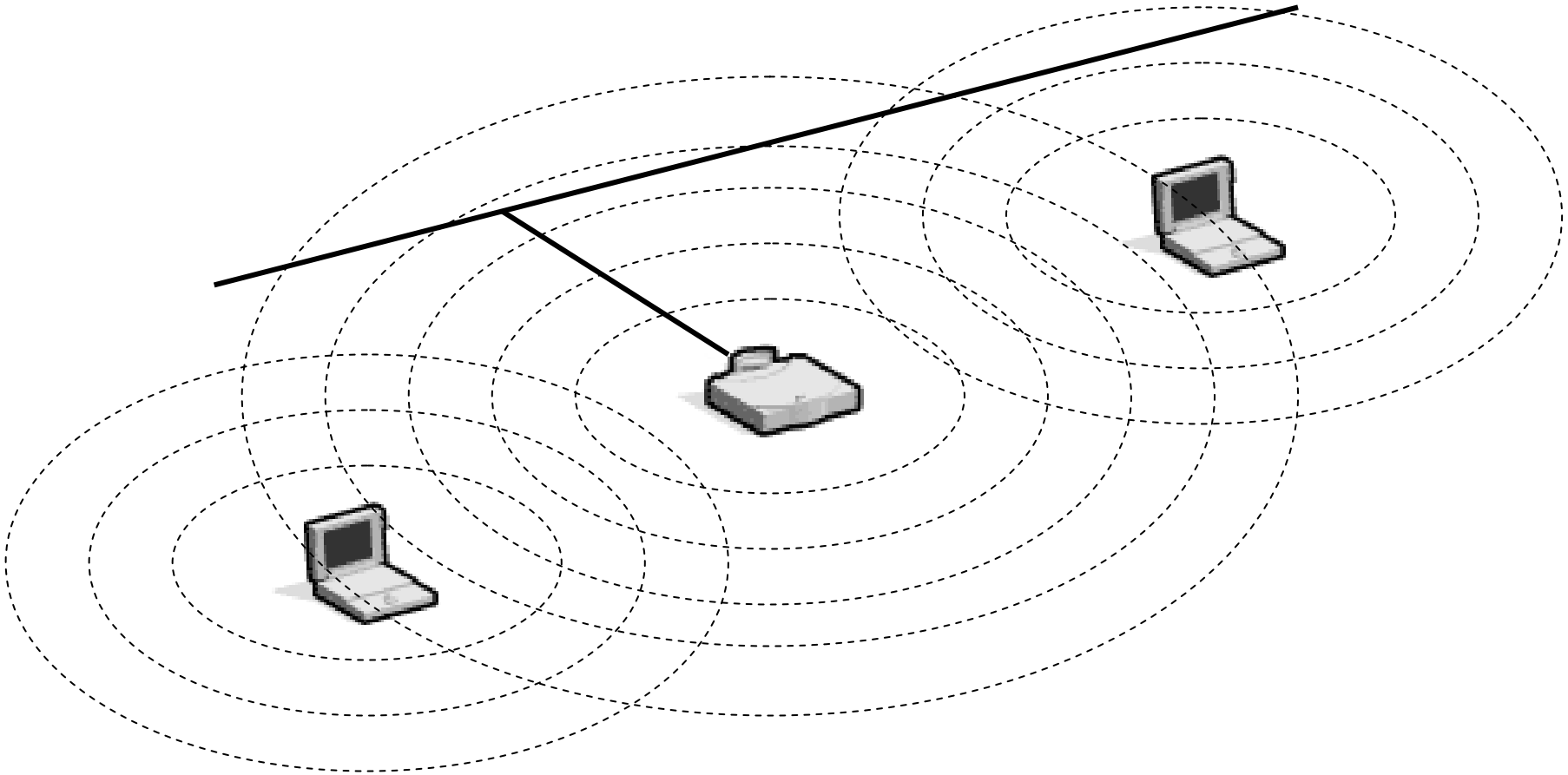


Ad-hoc mode



Independent Basic Service Set (IBSS)

Hidden nodes



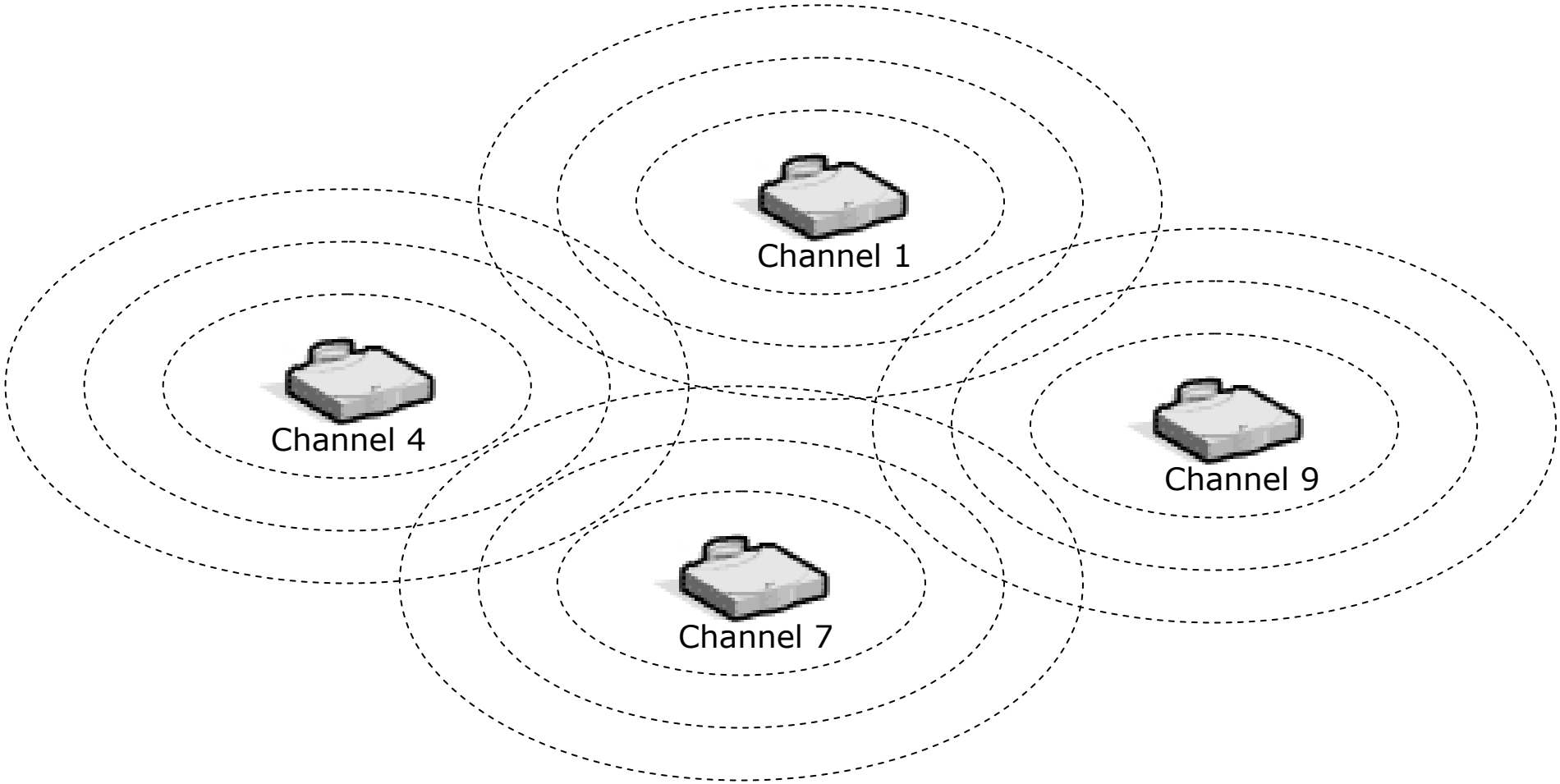
RTS / CTS

- To handle hidden nodes
- Sending station sends
  - “Request to Send”
- Access point responds with
  - “Clear to Send”
  - All other stations hear this and delay any transmissions.
- Only used for larger pieces of data.
  - When retransmission may waste significant time.

Joining a BSS

- When 802.11 client enters range of one or more APs
  - APs send beacons.
  - AP beacon can include SSID.
  - AP chosen on signal strength and observed error rates.
  - After AP accepts client.
    - Client tunes to AP channel.
- Periodically, all channels surveyed.
  - To check for stronger or more reliable APs.
  - If found, may reassociate with new AP.

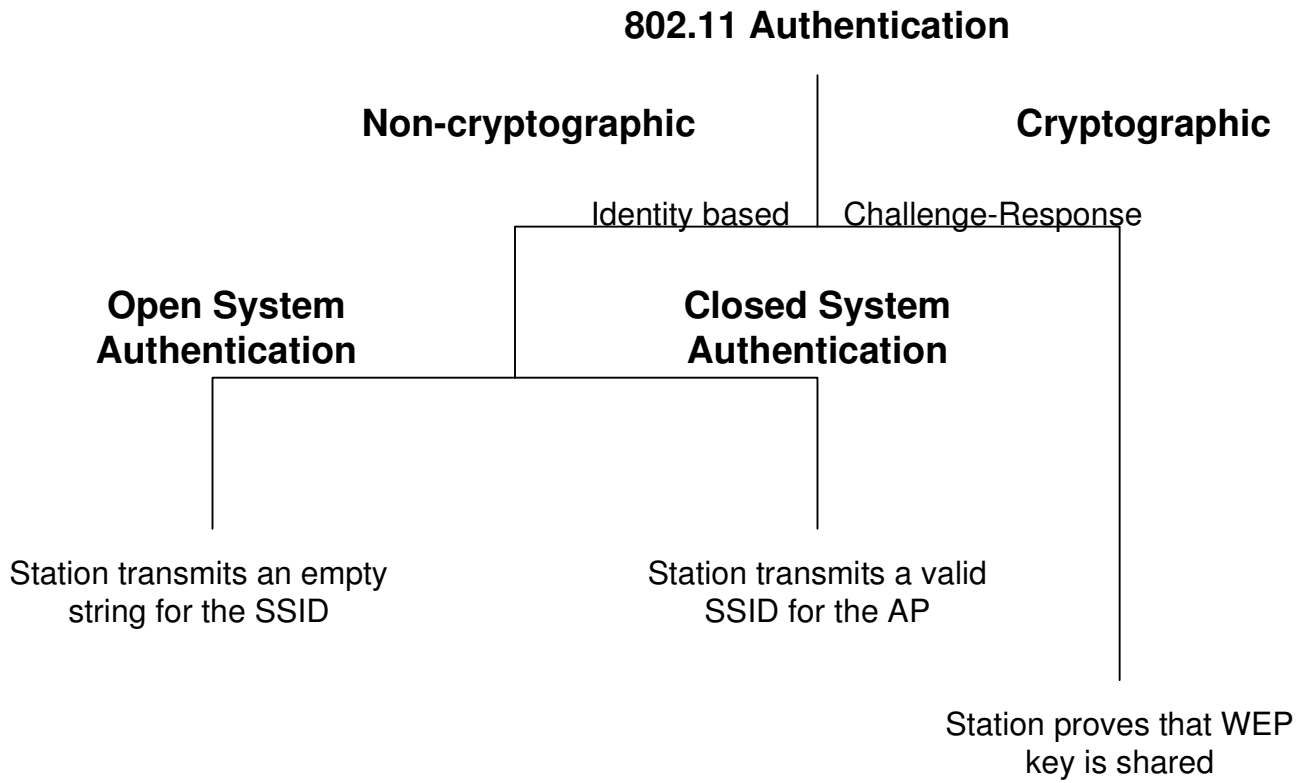
Access Point Roaming



Roaming and Channels

- Reassociation with APs
  - Moving out of range.
  - High error rates.
  - High network traffic.
    - Allows load balancing.
- Each AP has a channel.
  - Multiple partially overlapping channels.
  - Certain channels have no overlap.
    - Best for multicell coverage.

Security of IEEE 802.11 Wireless LANs



Non-Cryptographic

- *Open system (NULL) authentication* – a station is allowed to join a network if it transmits an empty SSID (Service Set Identifier).
- *Closed system authentication* – a station is allowed to join a network if it transmits a valid SSID for the AP
- Both highly vulnerable to attack

SSID hiding

- AP can choose not to transmit SSID in its beacons.
- Can still attack APs that don't transmit SSID:
  - Send deauthenticate frames to client
  - SSID then captured when client sends reauthenticate frames containing SSID
  - Implemented in essid_jack tool
- Open System Authentication only provides **trivial** level of security.

MAC ACLs

- Access points may have Access Control Lists (ACLs).
- ACL is list of allowed MAC addresses.
  - E.g. Allow access to:
    - 00:01:42:0E:12:1F
    - 00:01:42:F1:72:AE
    - 00:01:42:4F:E2:01
- But MAC addresses are sniffable and spoofable.
- Hence MAC ACLs of limited value.
  - Will not prevent determined attacker.

Cryptographic

Two security services provided:

- Encryption
  - Wired Equivalence Privacy (WEP)
- Authentication
  - Shared Key Authentication

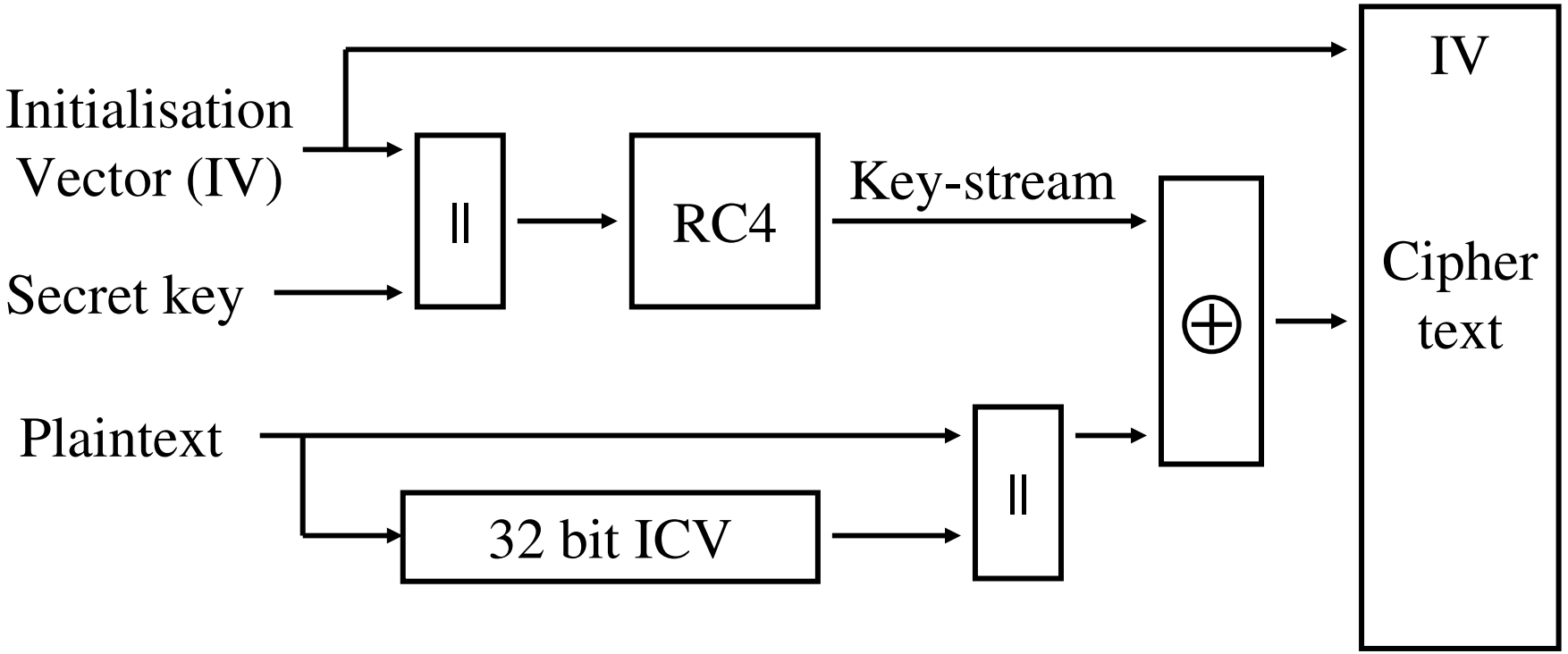
WEP Stream Cipher

- WEP uses RC4 stream cipher
  - Proprietary to RSA Security Inc.
  - Designed in 1987 by Ron Rivest.
  - Trade secret until leak in 1994.
- RC4 can use key sizes from 1 bit to 2048 bits.
- RC4 algorithm generates a stream of pseudo-random bits.

WEP – Sending

- Compute Integrity Check Vector (ICV).
  - Provides (weak form of) integrity.
  - 32 bit Cyclic Redundancy Check.
  - Appended to message to create plaintext.
- Plaintext encrypted using RC4 stream cipher.
  - RC4 initialised with
    - 40-bit secret key
    - 24 bit initialisation vector (IV)
  - RC4 generates key-stream as function of these 64 bits.
  - Key-stream XORed with plaintext to generate ciphertext.
- Ciphertext is transmitted along with IV.

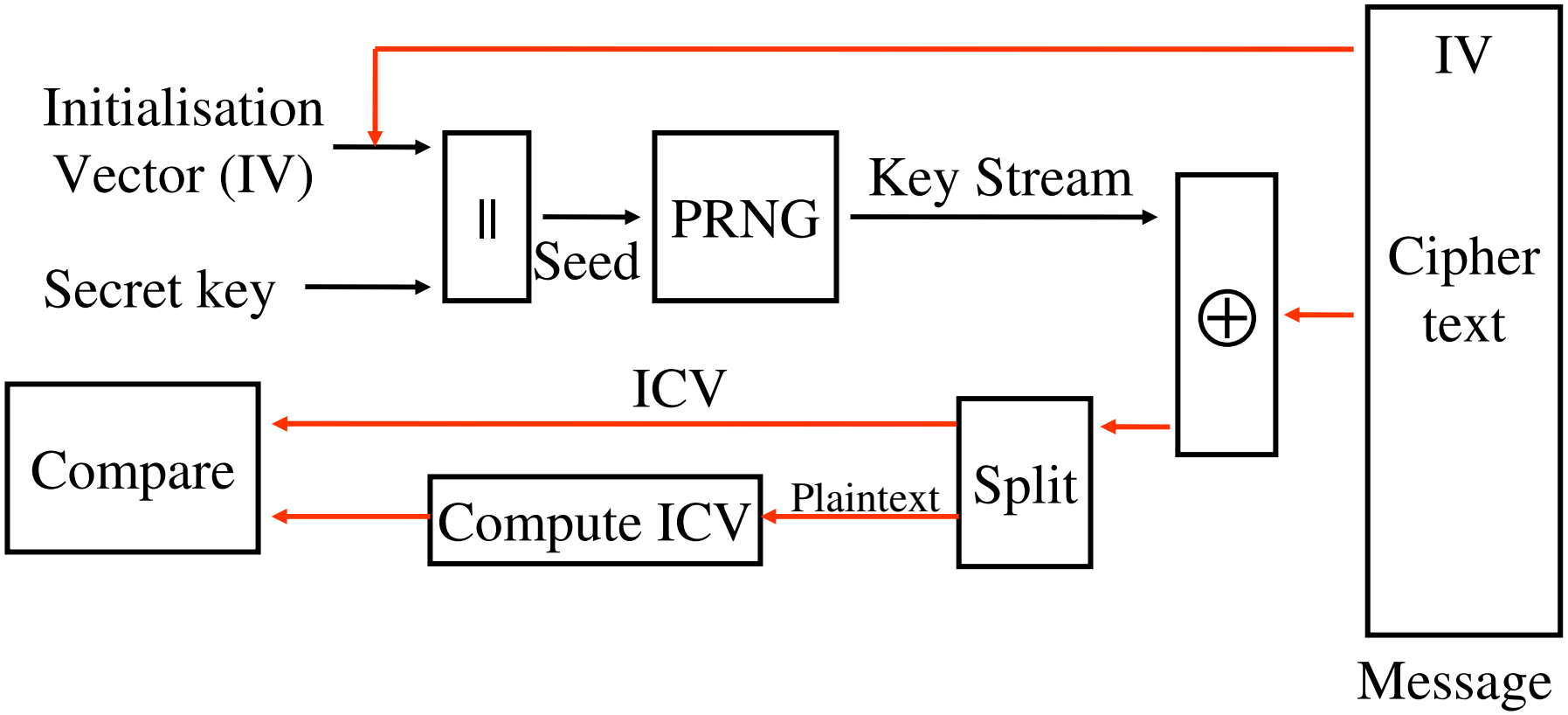
WEP Encryption



WEP – Receiving

- Ciphertext is received.
- Ciphertext decrypted using RC4 stream cipher.
  - RC4 initialised with
    - 40-bit secret key
    - 24 bit initialisation vector (IV)
  - RC4 generates key-stream as function of these 64 bits.
  - Key-stream XORed with ciphertext to recover plaintext.
- Check ICV
  - Separate ICV from message.
  - Compute ICV for message.
  - Compare with received ICV.

WEP - Receiving



Shared Key Authentication

- Station requests association with AP
- AP sends challenge to station.
- Station encrypts challenge using WEP to produce response.
  - Uses RC4, 40 bit shared secret key & 24 bit IV selected by station.
- Response received by AP, decrypted by AP and result compared to initial challenge.
- Challenge-response protocol.

WEP Safeguards

- Shared secret key required for:
  - Associating with an access point.
  - Sending data.
  - Receiving data.
- Messages are encrypted.
  - Confidentiality.
- Messages have checksum.
  - Integrity.
- But management traffic still broadcast in clear containing SSID.
- And other critical vulnerabilities….

Insecurity of Shared Key Authentication

- Rogue station records run of authentication protocol.
- Uses known plaintext (challenge) to compute portion of key-stream for the (known) IV.
- Rogue station can now respond to *any* future authentication challenge from AP.
  - Rogue receives fresh challenge.
  - Same IV (and secret key) leads to same key-stream from RC4 algorithm!
  - Wireless station gets to choose IV in protocol.
  - Hence rogue can force use of old keystream portion to encrypt.
- A stream cipher is a very poor choice as an encryption primitive in an authentication protocol.
  - Even worse if the IV choice is left to party being authenticated.

Initialisation Vector

- IV should be different for every message transmitted.
- But 802.11 standard doesn't specify how IV is calculated.
- Wireless cards use several methods
  - Some use a simple ascending counter for each message.
  - Some switch between alternate ascending and descending counters.
  - Some use a pseudo-random IV generator.

Passive WEP attack

- If 24 bit IV is an ascending counter,
- If Access Point transmits at 11 Mbps,
- All IVs are exhausted in roughly 5 hours.
- Passive attack:
  - Attacker collects all traffic.
  - Attacker will eventually collect two messages encrypted with same key and same IV.
  - Statistical attacks may then reveal plaintext:

    XOR of ciphertexts = XOR of plaintexts.
  - Very hard to extract plaintexts in reality.
  - Much better attacks are available against WEP…

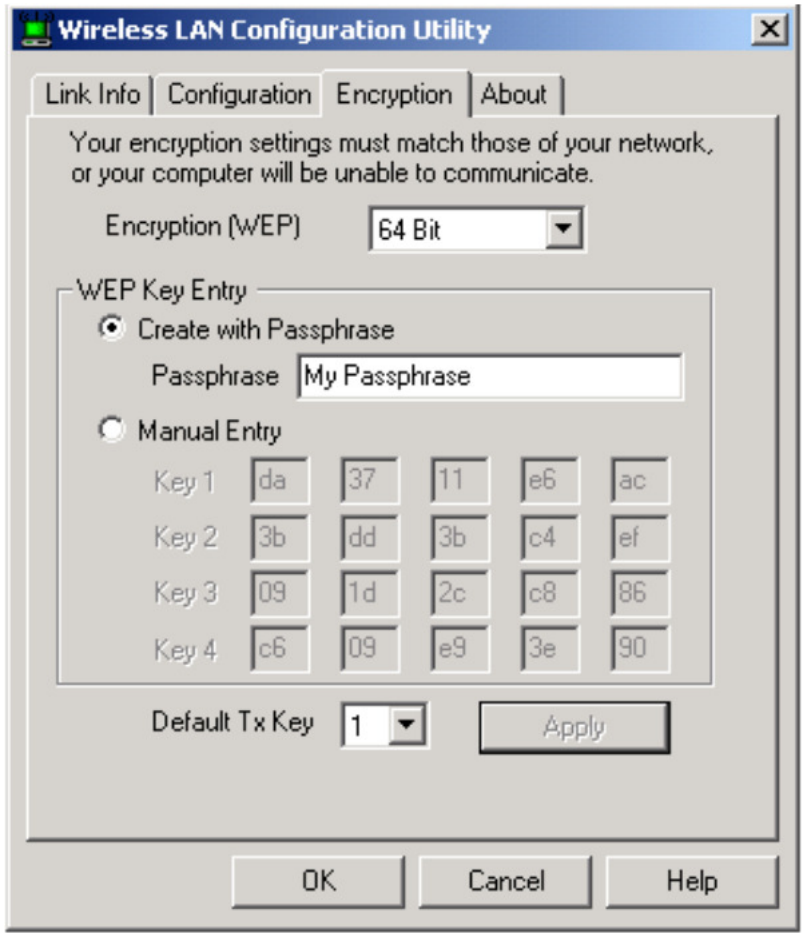
Active WEP attacks

- If attacker knows plaintext/ciphertext pair and IV:
  - Corresponding key-stream is then known.
  - Attacker can create correctly encrypted messages by repeating IV.
  - Access Point is deceived into accepting messages.
  - And short key-streams are obtained for free by observing authentication protocol!
- Bit-flipping:
  - Flip a bit in ciphertext.
  - Either changes 0 to 1 or 1 to 0 in plaintext.
  - Corresponding bit difference in CRC-32 can be computed.
    - Because bits of CRC-32 are linear functions of the message bits.
    - Not a robust integrity protection mechanism.
  - So can “repair” ICV after bit-flipping.

Limited WEP keys

- Some vendors allow limited WEP keys
  - User types in a pass-phrase.
  - WEP key is generated from pass-phrase.
  - Pass-phrases creates as few as 21 bits of entropy in 40 bit key.
    - Reduces key strength to 21 bits; 2^{21} = 2,097,152.
    - 21 bit key can be brute forced in minutes.
  - www.lava.net/~newsham/wlan/WEP_password_cracker.ppt

Creating limited WEP keys



Brute force key attack

- Capture ciphertext.
  - IV is included in message.
- Search all 2^{40} possible secret keys.
  - 1,099,511,627,776 keys.
  - A few tens of days on a modern laptop.
- Select key that decrypts ciphertext to a meaningful plaintext.
  - WLAN logical link control layer frames have well-defined format.
  - E.g. first two bytes are always AA, AA (hex).
  - Automated recognition of correct key is possible.

128 bit WEP

- Vendors have extended WEP to 128 bit keys.
  - 104 bit secret key.
  - 24 bit IV.
- Brute force takes 10^19 years for 104-bit key.
- Effectively safeguards against brute force attacks.

The FMS attack

Paper from Fluhrer, Mantin, Shamir, 2001.

- http://www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf
- Detailed analysis of several features of RC4 key scheduling algorithm.
- Main result of interest to us:
  - If the RC4 key is composed from a known IV and a unknown secret part,
  - And if the attacker knows the first byte of key-stream for enough different IVs,
  - Then the *whole* RC4 key can be determined in a statistical attack.
  - Attack only makes use of some of the IVs – "weak" IVs.

The FMS attack (2)

- In WEP, RC4 key material is composed by combining known IV with 40/104-bit secret key.
- And initial byte of key-stream is known because of fixed 802.11 frame format.
- So the FMS method is applicable to RC4 as used in WEP.
- The FMS attack is practical for 40 bit and 128 bit keys.
  - Complexity of attack grows only linearly with key size rather than exponentially.
- The attack is passive.
  - Non-intrusive.
  - No warning that it is being conducted.

Wepcrack

- First tool to demonstrate FMS attack using IV weakness.
  - Open source, Anton Rager.
- Three components
  - Weaker IV generator.
  - Search sniffer output for weaker IVs & record 1st byte.
  - Cracker to combine weaker IVs and selected 1st bytes.
- Cumbersome.

Airsnort

- Automated tool for mounting FMS attack
  - Cypher42, Minnesota, USA.
  - Does it all!
  - Sniffs
  - Searches for weaker IVs
  - Records encrypted data
  - Until key is derived.
- 100 Mb to 1 Gb of transmitted data.
- 3 to 4 hours on a very busy WLAN.

Countermeasures to FMS attack

- FMS attack uses a particular class of IVs.
  - Most IV values are not useful in the FMS analysis.
  - Many manufacturers avoided the “weak” IVs after 2002.
  - Therefore Airsnort and others may not work on recent hardware.
- However David Hulton (aka h1kari) conducted an extended analysis:
  - Identified class of IVs that lead to leak of RC4 key into *second* byte of key-stream.
  - Second byte of SNAP header is often also 0xAA
  - So attack still works on recent hardware that reject weak IVs for FMS attack.
  - And is faster on older hardware
  - Implemented in dwepcrack, weplab, aircrack
  - http://www.dachb0den.com/projects/bsd-airtools/wepexp.txt

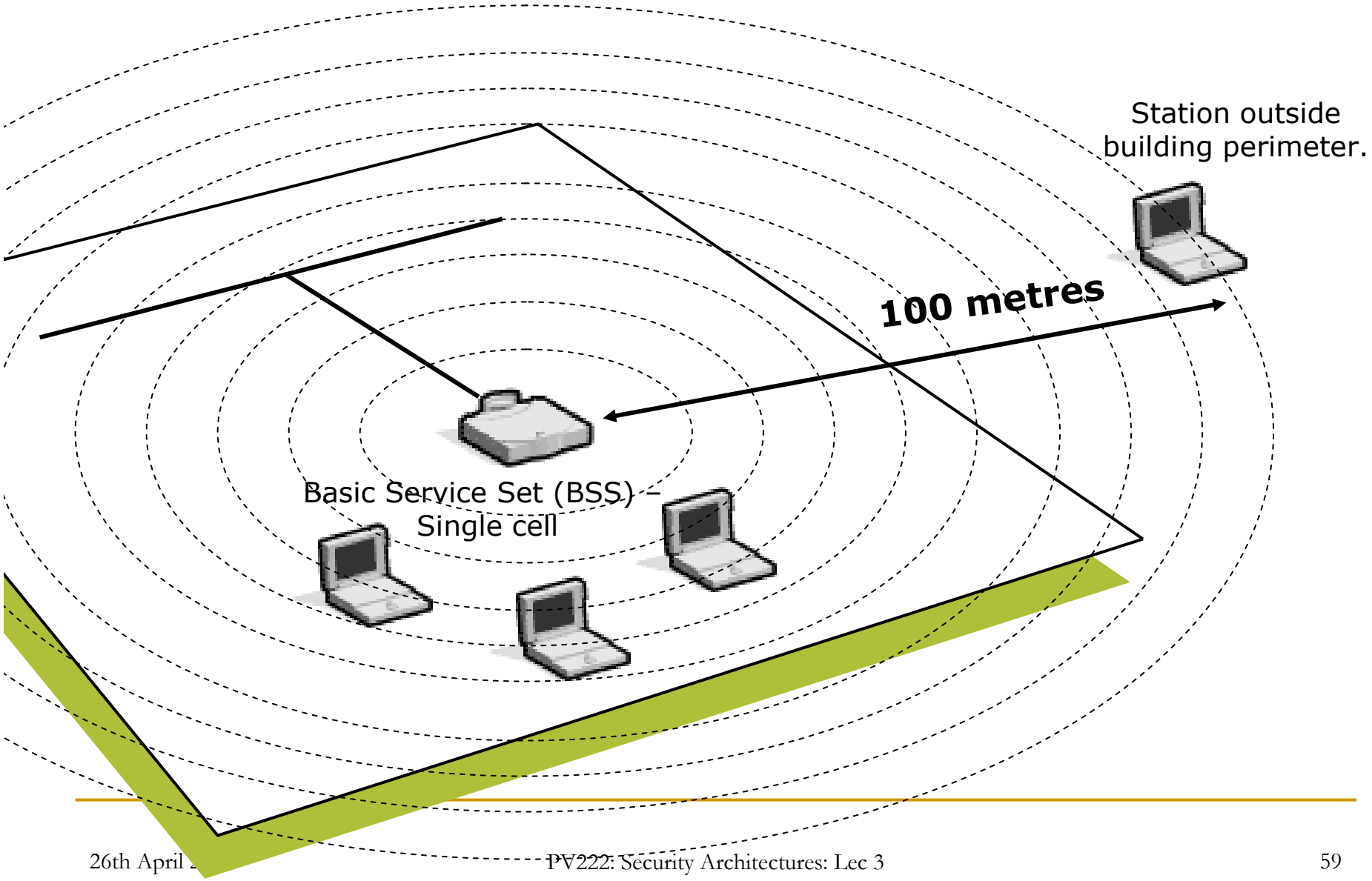
Generating WEP traffic

- Not capturing enough traffic for FMS attack?
  - Capture encrypted ARP request packets
  - Anecdotally lengths of 68, 118 and 368 bytes appear appropriate
  - Replay encrypted ARP packets to generate encrypted ARP replies
  - These replies provide more traffic, potentially with IVs indicating weak keys
  - Aireplay implements this.
- In summary:
  - The WEP authentication protocol is trivially breakable.
  - The WEP encryption method is severely weakened by FMS and other attacks.

Interception

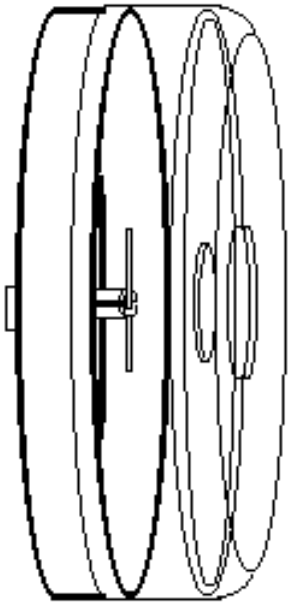
- Wireless LAN uses radio signal.
- Not limited to physical building.
- Signal is weakened by:
  - Walls
  - Floors
  - Interference
- Directional antenna allows interception over longer distances.
  - Record is 124 miles for an unamplified 802.11b signal (4 metre dish)

Interception Range



Directional Antenna

- Directional antenna provides focused reception.
- DIY plans available.
  - Aluminium cake tin
  - Chinese cooking sieve



  - http://www.saunalahti.fi/~elepal/antennie.html
  - http://www.usbwifi.orcon.net.nz/

WarDriving

- Software
  - Netstumbler
  - And many more
- Laptop
- 802.11a,b,g PC card
- Optional:
  - Global Positioning System
- Logging of MAC address, network name, SSID, manufacturer, channel, signal strength, noise (GPS - location).

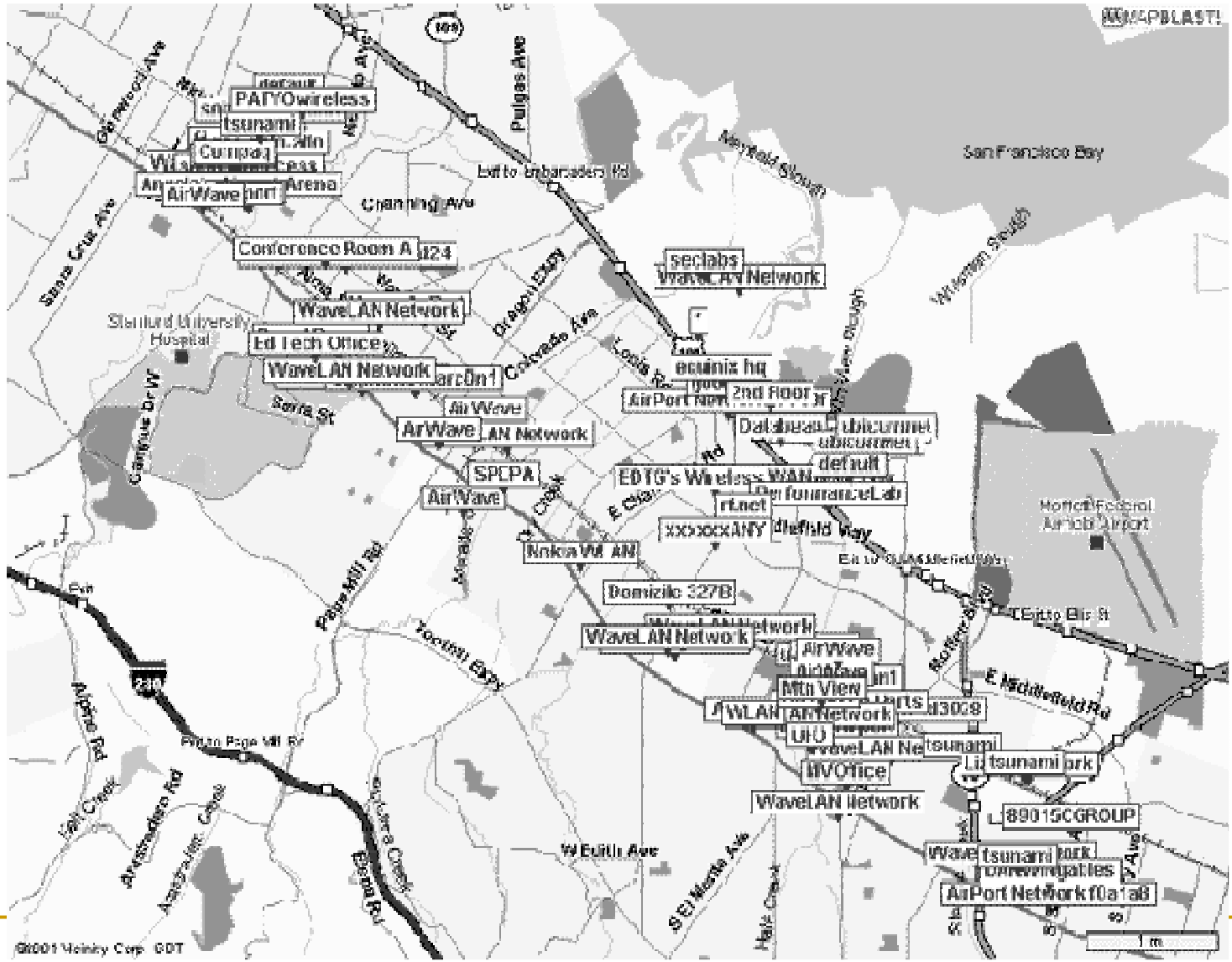
WarDriving results

- San Francisco, 2001
  - Maximum 55 miles per hour.
  - 1500 Access Points
  - 60% in default configuration.
  - Most connected to internal backbones.
  - 85% use Open System Authentication.
- Commercial directional antenna
  - 25 mile range from hilltops.

- Peter Shipley - http://www.dis.org/filez/openlans.pdf

WarDriving map

Source: www.dis.org/wl/maps/



Worldwide War Drive 2004

- Fourth and last worldwide war drive
  - www.worldwidewardrive.org
- 228,537 Access points
- 82,755 (35%) with default SSID
- 140,890 (60%) with Open System Authentication
- 62,859 (27%) with both, probably default configuration

War Driving prosecutions

- June 2004, North Carolina, Lowes DIY store
  - Salcedo convicted for stealing credit card numbers via unprotected WLAN
  - Botbyl convicted for checking email & web browsing via unprotected WLAN
- June 2004, Connecticut, Myron Tereshchuk guilty of drive-by extortion via unprotected WLANs
  - “make the check payable to M.Tereshchuk”
- July 2005, London, Gregory Straszkiewicz guilty of dishonestly obtaining a communications service
  - Warwalking in Ealing, £500 fine and 12 month suspended sentence under Communications Act (2003).

Further issues

- Access Point configuration
  - Mixtures of SNMP, web, serial, telnet.
    - Default community strings, default passwords.
- Evil Twin Access Points
  - Stronger signal, capture user authentication.
- Renegade Access Points
  - Unauthorised wireless LANs.

Securing wireless LANs

- Security Policy & Architecture Design
- Treat as untrusted LAN
- Discover unauthorised use
- Access point audits
- Station protection
- Access point location
- Antenna design

Security Policy & Architecture

- Define use of wireless network
  - What is allowed
  - What is not allowed
- Holistic architecture and implementation
  - Consider all threats.
  - Design entire architecture
    - To minimise risk.

Wireless as untrusted LAN

- Treat wireless as untrusted.
  - Similar to Internet.
- Firewall between WLAN and Backbone.
- Extra authentication required.
- Intrusion Detection
  - at WLAN / Backbone junction.
- Vulnerability assessments

Discover unauthorised use

- Search for unauthorised access points, ad-hoc networks or clients.
- Port scanning
  - For unknown SNMP agents.
  - For unknown web or telnet interfaces.
- Warwalking!
  - Sniff 802.11 packets
  - Identify IP addresses
  - Detect signal strength
  - But may sniff your neighbours…
- Wireless Intrusion Detection
  - AirMagnet, AirDefense, Trapeze, Aruba,…

Access point audits

- Review security of access points.
- Are passwords and community strings secure?
- Use Firewalls & router ACLs
  - Limit use of access point administration interfaces.
- Standard access point config:
  - SSID
  - WEP keys
  - Community string & password policy

Station protection

- Personal firewalls
  - Protect the station from attackers.
- VPN from station into Intranet
  - End-to-end encryption into the trusted network.
  - But consider roaming issues.
- Host intrusion detection
  - Provide early warning of intrusions onto a station.
- Configuration scanning
  - Check that stations are securely configured.

Location of Access Points

- Ideally locate access points
  - In centre of buildings.
- Try to avoid access points
  - By windows
  - On external walls
  - Line of sight to outside
- Use directional antenna to “point” radio signal.

Wireless IDS/IPS

- Sensors deployed in WLAN
- Monitoring to detect
  - Unauthorised clients by MAC address
    - Accidental
    - Malicious
  - Ad-hoc mode networks
  - Unauthorised access points
  - Policy violations
- Possible to identify approximate locations

Recent Developments

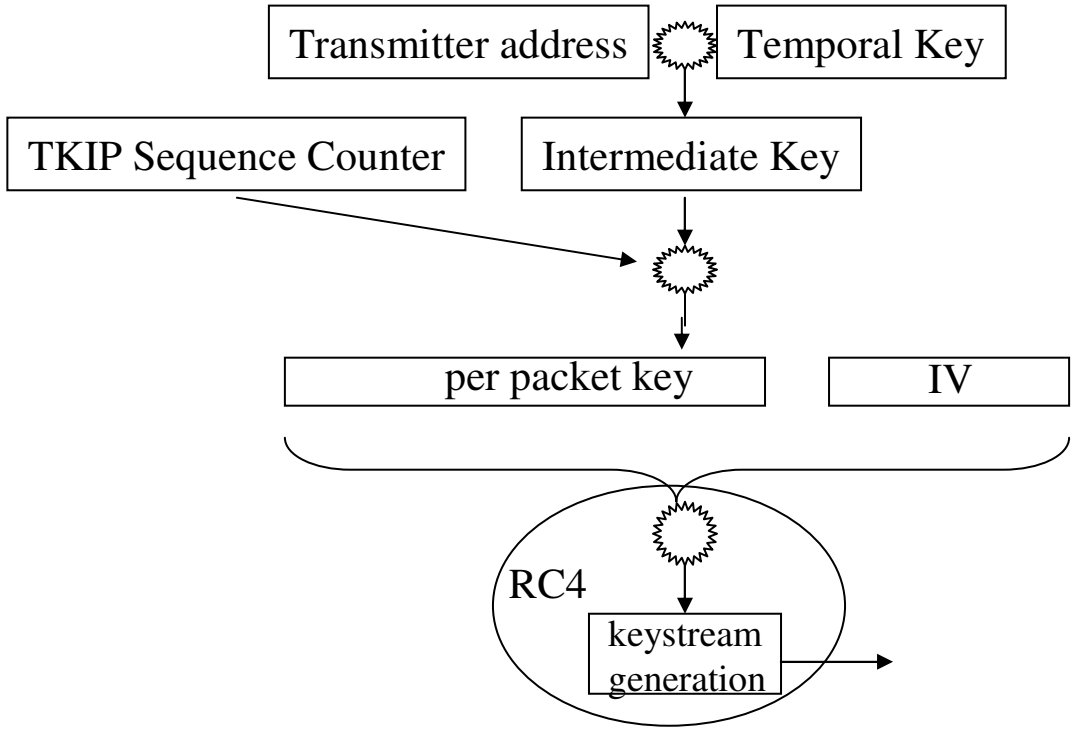
- Wi-Fi Protected Access (WPA)
  - Works with 802.11b, a and g
- An intermediate solution to address WEP's problems
- Existing hardware can still be used; firmware upgrade needed.
- WPA introduces Temporal Key Integrity Protocol (TKIP):
  - RC4 session-based dynamic encryption keys
  - Per-packet key derivation
  - Unicast and broadcast key management
- WPA uses 48 bit IV which is hashed with 128 bit secret to create RC4 key.
- WPA uses special-purpose 8 byte message integrity code (MIC) called "Michael" to replace WEP's CRC.

TKIP Overview

- A intermediate solution is provided by the Temporal Key Integrity Protocol (TKIP)
  - Designed as a wrapper around WEP
    - Fully compatible with WEP
    - Deployed as a software upgrade to existing infrastructure
  - Attempts to mitigate the most glaring problems
    - This process became a very significant engineering effort
    - Existing hardware and software in the field raises compatibility issues
    - Accepted (and sound) cryptographic techniques cannot be directly used since performance demands are so high
      - The load generated by normal WLAN traffic often consumes around 90% of processor resources

TKIP

- TKIP enhances the way RC4 is used



Practical WPA attacks

- Dictionary attack on pre-shared key mode
  - Attack first proposed by Robert Moskowitz
  - Works if pre-shared key has low entropy (e.g. derived from pass-phrase)
  - Implemented in CoWPAtty (Joshua Wright)
- Denial of service attack
  - If WPA equipment sees two packets with invalid MICs in 1 second
    - All clients are disassociated
    - All activity stopped for one minute
    - Two malicious packets a minute enough to stop a wireless network

WPA and 802.1x

- 802.1x user-level authentication
- 802.1x is a general purpose network access control mechanism
- WPA has two modes
  - Pre-shared mode, using pre-shared keys.
  - Enterprise mode, uses Extensible Authentication Protocol (EAP) with a RADIUS server making the authentication decision
  - EAP is a transport for authentication, not authentication itself
  - EAP allows arbitrary authentication methods
  - For example, Windows supports
    - EAP-TLS requiring client and server certificates
    - PEAP-MS-CHAPv2

802.11i (WPA2)

- IEEE 802.11i published in 2004.
  - Draft versions available much before this.
- Supersedes WPA's interim solution to WEP issues.
- Does require new hardware.
- Main features:
  - Pre-shared mode and 802.1X for key management, as in WPA
    - Pre-shared mode has same dictionary attack issue as WPA.
  - Use of 128-bit AES-CCMP (AES Counter Mode with Cipher Block Chaining Message Authentication Code) for confidentiality and integrity.
  - Use of 4-way handshake protocol for distributing AES-CCMP keys.
  - Negotiation of algorithms and parameters.
- Lots more info at www.drizzle.com/~aboba/IEEE/

Conclusions