Wireless Security

Privacy in Wireless Communications Data Retention

- Arguments for
  - Necessary to combat terrorism
  - Data retention assists the police to find criminals after the attacks have taken place
  - Important contribution to investigation of Madrid and London bombings
- Arguments against
  - Invasion of privacy and disproportionate response to terrorist threat
  - Easy for terrorists to avoid having communications recorded: P2P technologies, anonymous proxies
  - High cost of data retention hardware and software
  - May be abused to track activities of non-terrorist groups
  - Excessive retention periods

Privacy in Wireless Communications Data Retention II

- Ireland
  - Data retention law passed in February 2005
  - Three years data retention at all phone companies that provide fixed line and mobile services
  - The stored data includes traffic data (time and duration of calls) and location data (Cell ID)
- Europe
  - EU Parliament passed a data retention directive in Dec 2005
  - Specifies data retention from 6 to 24 months
  - Type of data to be retained includes phone call location data, SMS and internet use (email, web, VoIP)
  - Limited to investigation of “serious criminal offences”
  - It doesn’t require storage of content, only logs

Privacy in Wireless Communications Data Retention III

- Issues with data retention implications
  - Some Internet protocols (P2P, VoIP) are difficult to track without watching the contents of every packet
  - Tunneling and VPNs make impossible to look at content
- Circumvention
  - VPN: encryption of all data and mixing of communications of all employees
  - Anonymising proxies: provide anonymous web access
  - Webmail: use of HTTPS and non-EU providers prevents tracking of email
  - P2P Communications:
  - Privacy enhancing tools: network overlays (Tor, Freenet), email encryption

Security in Ad Hoc Wireless Networks

Threats

- Availability
  - Sleep Deprivation Torture: power consumption more dangerous than computational or network resource use, impossible recovery after attack
- Jamming
  - Spread Spectrum, Frequency Hopping
- Confidentiality
  - Easy passive eavesdropping
  - Can’t rely on computationally expensive crypto
    - Use of symmetric key cryptography

Threats II

- Authorisation
  - Network resources: vulnerable to bandwidth stealing, shouldn't route unauthorised packets
  - Transient states: unfeasible static authorisation policy, transient associations
- Authentication
  - Can't rely on central server or public key cryptography
  - Need to be adaptive to transient authorisation policy
  - Quick renewals of symmetric keys

Routing Attacks

- Routing based on cooperation among nodes
  - Assumption of trust relationship makes routing an attack target
  - Attacks aim to distort routing info, causing network partitioning, high traffic load or energy consumption
- Internal attacks
  - From nodes on the network
  - Important on networks operating in hostile environments (battlefields)
  - Difficult to detect if information changes due to topology change or node being compromised
- External attacks
  - From nodes not on the network

Secure Routing

- Cryptographic
  - Authenticated Routing for Ad Hoc Networks (ARAN)
    - Uses PKC, nodes sign messages with private key, receivers verify authenticity and prevent external routing attacks
    - Doesn't protect against internal attacks
  - Security-aware Ad Hoc Routing (SAR)
    - Uses SKC, each node is assigned a trust level and all nodes at each trust level share an encryption key
    - Initiating node specifies minimum trust level, ensuring lower trust level nodes can't tamper with in-transit routing messages

Secure Routing II

- Non-cryptographic
  - Watchdogs and pathraters
    - Each node acts as watchdog by verifying that the node it forwarded a message to routes it correctly
    - Each node acts also as a pathrater by using information from the watchdog to select the most robust routing links/nodes
    - Prevents internal routing attacks that aim to modify routing paths but it doesn't prevent against internal routing attacks which aim to partition the network, compromised watchdogs can report false information

Key Establishment and Authentication

- Public Key Infrastructure (PKI) enables key establishment and authentication
  - Requires a Certification Authority (CA)
- There is no centralised and always accessible CA in ad hoc networks
  - Need a virtual distributed CA, implemented with threshold cryptography
- Threshold cryptography
  - Divide the secret in N partial secrets
  - Any M < N parts put together can be used to retrieve the secret, but not with less than M parts

Virtual Certification Authority

- Threshold cryptography can be used to distribute the CA private key among multiple nodes
- Each node only needs to have a part of the key
- Any node A that wants to obtain another node B's public key can broadcast a request for the certificate for B, which will be replied with partial certificates by the server nodes forming the virtual CA, and the certificates will be combined to form a complete certificate for B
- Secure because it only requires a subset of the virtual CA nodes to be non-compromised to obtain a valid certificate
- Issues
  - Requires collaborative nodes - have to respond with to partial certificate request anytime
  - Need initial bootstrap phase in which secret parts are given to nodes

Confidentiality and Integrity

- Once two nodes have authenticated each other and established keys, encryption and integrity algorithms can be used to secure the communication
- Requires algorithms suitable for the environment (processing power, battery) in which the network is expected to operate
- Most use a stream cipher and an integrity algorithm algorithm that aren't too computationally intensive

Security in 802.11 Networks

Issues in Wireless LAN deployments

- Uncontrolled and shared medium
  - No physical network boundaries
    - Equivalent to Ethernet port in parking lot
  - "Accidental association"
  - Broadcast monitoring
- Configuration
  - Default SSIDs
  - Only use VPN for authenticated users
  - Ad hoc networks between users
  - SNMP community password
  - Default passwords in administration interface

Issues in Wireless LAN deployments II

- Performance and Management
  - Lack of monitoring
  - Insufficient performance
- Security Standards
  - Encryption: WEP, WPA, WPA2/802.11i
  - MAC Address filtering
- Interaction with fixed networks
  - Trusted access to fixed network bypassing firewall
- Client side security risk
  - SSID and WEP keys in Windows registry
  - File sharing and network services

Attacks Against Wireless LANs

- War-driving
  - Off-hours traffic
- Man in the Middle Attacks / AP Clone (Evil Twin) Intercept Traffic
  - Rogue APs pretending to be the legitimate APs
  - AP clones collect authentication info to impersonate user
- Denial of Service Attacks / Jamming
  - Frequency noise to stop communication
  - Insertion of bogus packets, flooding the network
  - Sending of dissociate commands from rogue APs

Attacks Against Wireless LANs II

- MAC Address Spoofing / Session hijacking / Identity Theft
  - MAC spoofing for DoS, access control bypassing and false service advertisement
  - MAC spoofing allows to impersonate a different user to hijack SSH or SSL session
- Interception and Unauthorised Monitoring of Traffic / eavesdropping
  - Industrial or political/military espionage
  - Used for session hijacking, AP cloning, etc
- Client to Client Attacks (bypassing the APs)
  - No need to access AP to attack client machines with high-level protocol or application attacks
- Encryption Attacks (WEP)

WEP

- The 802.11 security architecture and protocol is Wired Equivalent Privacy (WEP)
- WEP provides authentication, confidentiality and data integrity in 802.11 networks
- Aim of WEP is to provide the same level of security as is available in Ethernet networks, a "wireless ethernet”
- WEP fails to achieve the goal of making the 802.11 physical medium (air), as secure as the Ethernet cable

Key Establishment

- Simple key establishment protocol, there is none
- Problems caused by lack of key establishment protocol
  - Manual configuration of keys into APs
  - Manual intervention leads to manual errors
  - People can't be expected to use a "strong" key, the opposite is true, humans will tend to choose easy to remember, weak keys
  - Clients can't be assigned unique keys, they share a global key with the AP, impossible to identify the clients securely
  - Most deployments use the same key across the extended set of APs, to simplify roaming but making the key more susceptible to compromise

Anonymity

- Anonymity important in GSM, because IMSI is used for call routing and it identifies a subscriber uniquely
- In 802.11 networks the IP address fulfills the role of the IMSI in GSM
- Difficult to determine the identity of the subscriber from the IP address
  - IP addresses can be dynamically assigned (DHCP)
  - Use of Network Address Translation (NAT), allows sharing of IP addresses, so several hosts can access the Internet with just a single IP address

Authentication

- One of the main uses of authentication is to provide access control
- In wired LANs, there is some kind of built-in physical access control, as anyone who wants to connect has to obtain physical access to the network, this doesn't exist in wireless LANs
- Network joining is more complex in WLANs, both the client and the network need to authenticate each other before the connection can be allowed

Authentication II

- WEP authentication process
  - 802.11 APs broadcast beacons containing the Service Set Identifier (SSID)
  - Clients send probes to AP requesting permission to connect, gets list of networks that it can join, chooses one and the authentication process begins, with two choices possible
    - Open System Authentication (OSA): no authentication
    - Shared Key Authentication (SKA): AP verifies that the client is in possession of a shared secret key using challenge-response messages and the WEP encryption algorithm

Authentication III

- What's wrong with WEP authentication?
  - OSA irrelevant from an authentication point of view
  - SKA uses the same shared key for all clients allowed to join the network
  - SKA authentication only verifies that the client belongs to a group that knows the secret key, not the exact identity of the subscriber
  - The secret key is frequently shared between several APs
  - Difficult to remove access to a given client, need to change and redistribute the shared key
  - No mechanism for the client to authenticate the AP

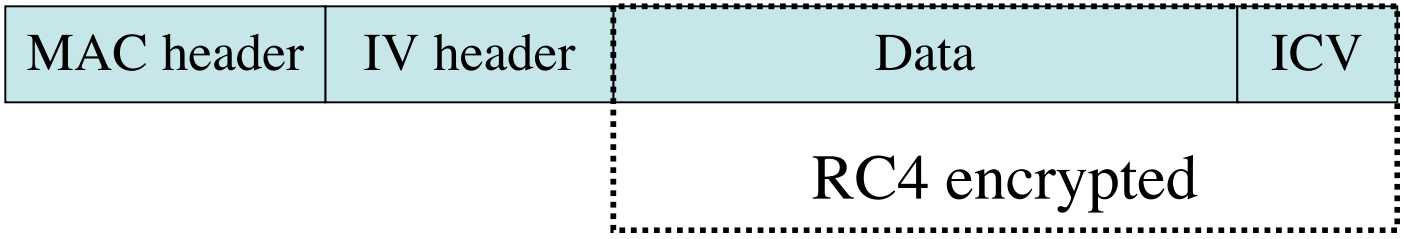
Confidentiality

- Packets are encrypted to provide confidentiality
- What's wrong with WEP encryption?
  - It uses a synchronous stream cipher (RC4)
    - Bad choice for wireless lossy mediums
  - It has to use a unique key for each packet
    - Derived trivially by concatenation of a random 3-byte value (IV) with the master key
    - IV is transmitted in clear text with the packet, leading to generation of weak RC4 keys
    - RC4 requires to never repeat the key, the way it's used in WEP makes it possible to get repeats every few hours
    - The 802.11 standard doesn't even enforce that the IV has to change at all, only recommends "frequent" change

Data Integrity

- 802.11 uses an Integrity Check Value (ICV) value field in the packet to check the integrity of the payload data
- It uses the CRC-32 algorithm
  - Adds Integrity Check Value (ICV) to data
  - Not cryptographically strong
  - Not computed over the 802.11 header, allowing redirection attacks

802.11 frame format



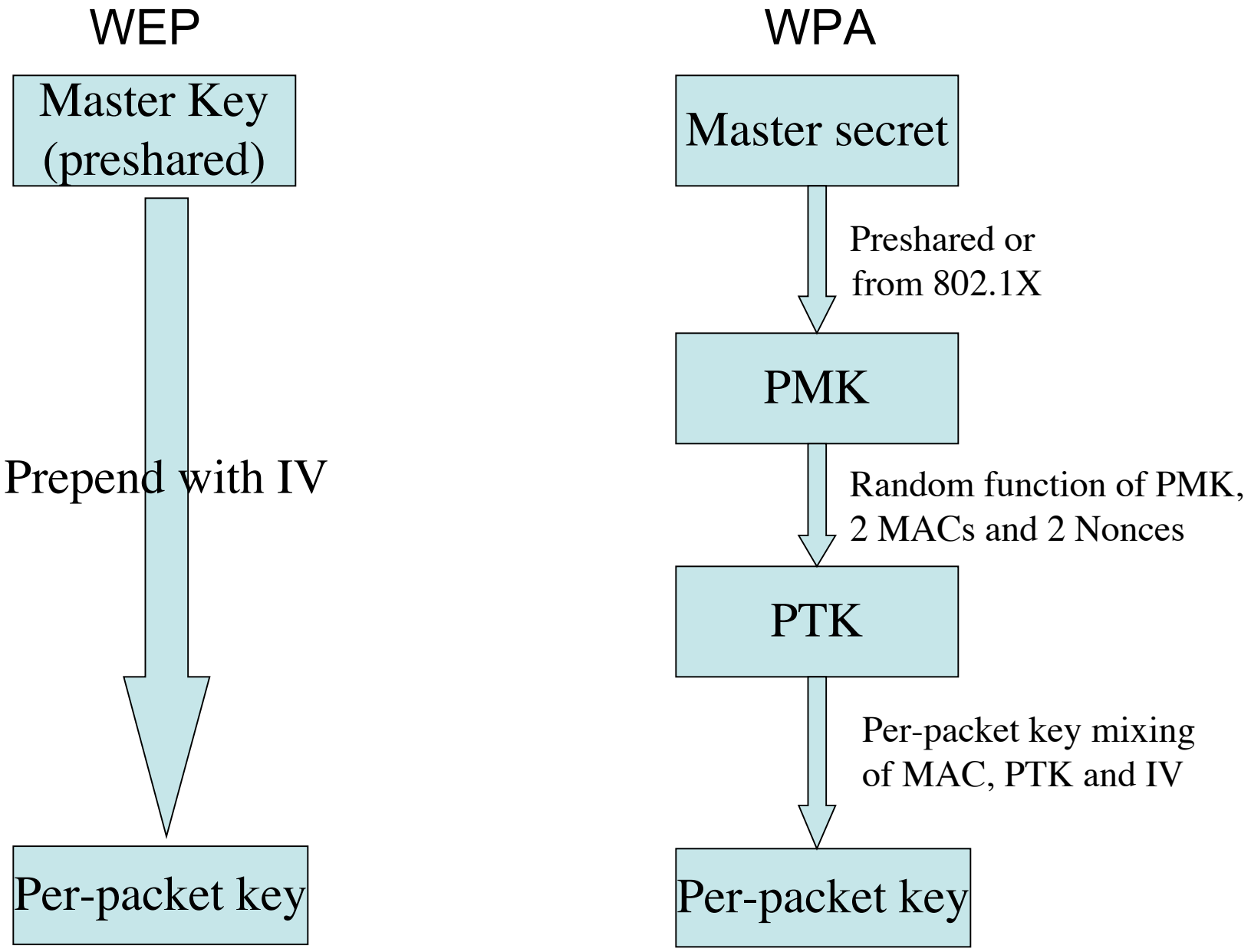
Loopholes in WEP

- No key establishment protocol over insecure medium
- Use of a synchronous stream cipher over a medium where it's difficult to ensure synchronisation
- Per-packet RC4 key created concatenating the master key with the IV, exposes the master key to attacks
- The master key occupies 40 of the 64 bit key, leaving a very limited key-space
- Change of the IV key is optional, reuse probable
- The CRC-32 used for message integrity is linear
- It doesn't protect the 802.11 header's integrity
- No protection against replay attacks
- No support for clients to authenticate the network

Wi-Fi Protected Access (WPA)

- Created by the Wi-Fi Alliance to fix WEP problems while operating within the constraints of the existing 802.11 equipment
- It uses the Temporal Key Integrity Protocol (TKIP) standard
- A subset of 802.11i (WPA2), uses TKIP for confidentiality and MICHAEL for integrity
- 802.11i / WPA2 uses AES for both
- Uses the 802.11i key management and authentication architecture (802.1X) or the WEP-style preshared key for home deployment

Key Hierarchy



How does WPA Fix WEP Issues?

WEP	WPA
No key establishment	802.1X for authentication and key establishment
Synchronous cipher	Same as WEP
Exposure of master key in per-packet RC4 key	Use of PTK in key hierarchy and key mixing instead of concatenation
Master key-space limited to 40 bits	Increase of IV size to 56 bits and per-session PTKs increase effective key-space
Optional variation of IV key	Explicit IV initialisation and change rules
CRC-32 is cryptographically poor	Use MICHAEL instead of CRC-32
No header integrity protection	Header included in ICV computation
No protection against replay attacks	Uses IV as sequence number
No support for clients to authenticate network	802.1X allows authentication

802.11i / WPA2

- Security proposal from the 802.11i group, called Robust Security Network (RSN) or 802.11i security solution
- Called WPA2 by the Wi-Fi Alliance
- Almost like WPA, but uses the AES block cipher in stream mode for confidentiality
- Extends AES with CCMP (Counter-Mode CBC-MAC Protocol) to guarantee message integrity together with confidentiality

Comparison of WPA2 with WPA

WPA	WPA2
802.1X for authentication and key establishment	Same as WPA
Synchronous cipher	Replaces a stream cipher (RC4) with a strong block cipher (AES)
Use of PTK in key hierarchy and key mixing instead of concatenation	Same as WPA
IV size of 56 bits and per-session PTKs increase effective key-space	Same as WPA
Explicit IV initialisation and change rules	Same as WPA
Use MICHAEL instead of CRC-32	Stronger integrity protection with AES-based CCMP
Header included in ICV computation	Same as WPA
Uses IV as sequence number	Same as WPA
802.1X allows authentication	Same as WPA