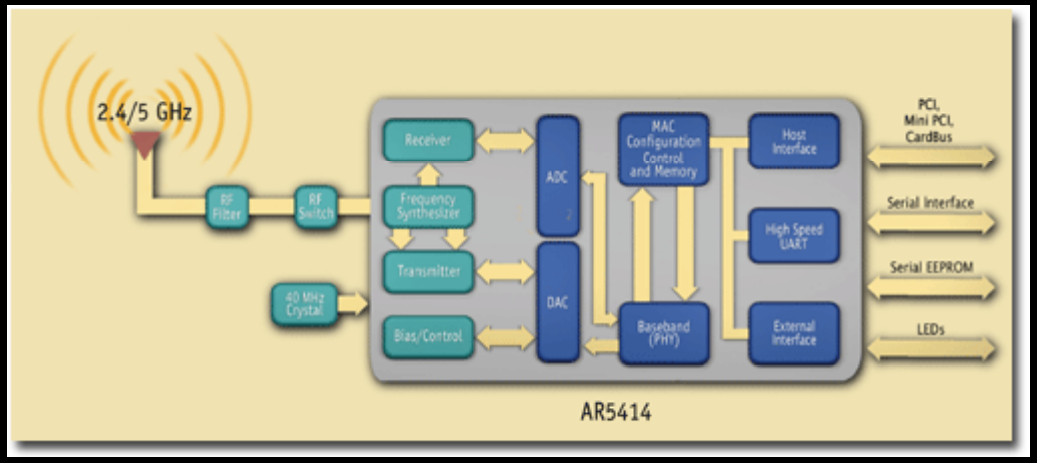
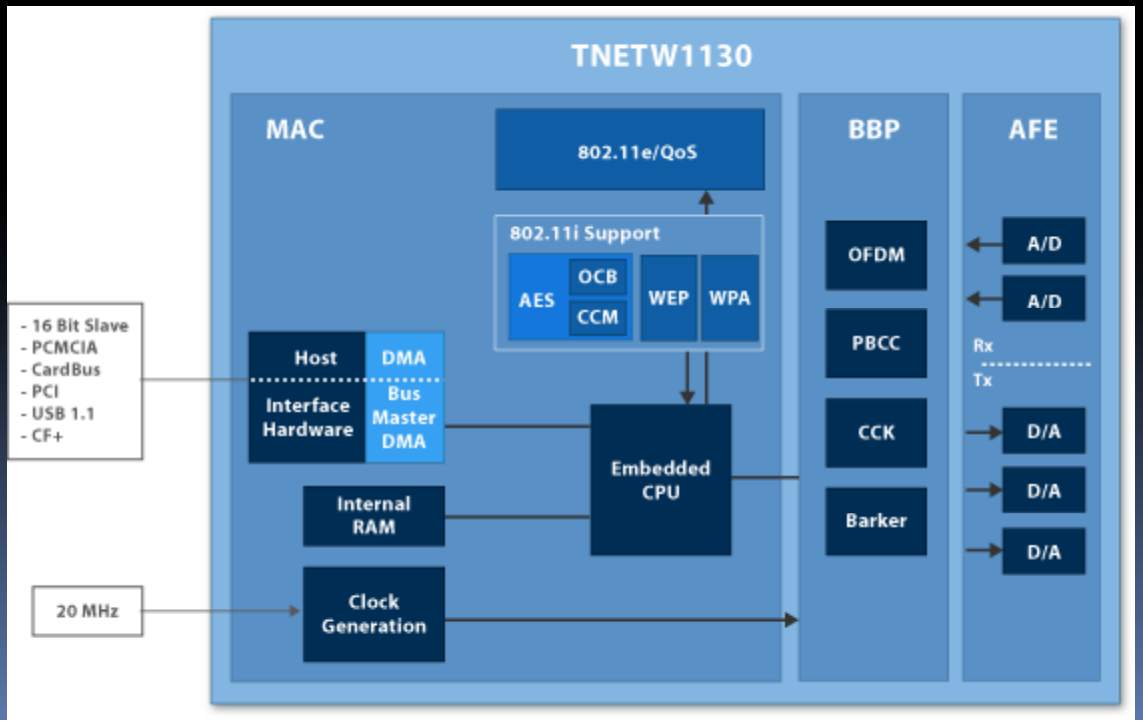
Rick Ellinger
Wireless Communications Alliance
www.wca.org
skype: flipchip

ETHERNET – INTERNET WIRELESS AND STANDARDS IEEE, ISA, IEC, ISO, IET

Embedded Wireless Security





WAPI (WLAN Authentication and Privacy Infrastructure)

- Chinese National Standard for Wireless LAN (GB 15629.11-2003).
- On top of WiFi or a conflict?
- WAPI Central Authentication Service Unit (ASU)
  - known to wireless user & access point
  - (US utility patent on this for banking)
- WAPI standard requires the use of a symmetric encryption algorithm[1], SMS4, which was declassified in January 2006. The standard and its cryptographic implementation remain unpublished.

Wireless (802.11) Embedded Security

- WEP ***W****ired* ***E****quivalent* ***P****rivacy*, security protocol ,wireless local area networks defined in the 802.11b standard.
  - WEP encrypts data over radio waves.
  - WEP two layers OSI model - data link, physical layers; no end-to-end security.
- SIP ***S****ession* ***I****nitiation* ***P****rotocol*, application-layer control protocol; a signaling protocol for Internet Telephony.
- SIP features audio/videoconferencing,
- interactive gaming,
- call forwarding over IP networks,
- …enables service providers to integrate basic IP telephony services with Web, e-mail, and chat services, mobility

802.11i

- **IEEE 802.11i**, also known as **WPA2**, is an amendment to the 802.11 standard specifying security mechanisms for wireless networks (see Wi-Fi).
- Ratified on 24 June 2004, supersedes, Wired Equivalent Privacy (WEP).
- Wi-Fi Protected Access (WPA) introduced by Wi-Fi Alliance as intermediate solution to WEP insecurities. WPA implemented a subset of 802.11i. The Wi-Fi Alliance refers to their approved, interoperable implementation of the full 802.11i as **WPA2**. 802.11i makes use of the Advanced Encryption Standard (AES) block cipher; WEP and WPA use the RC4 stream cipher.

802.11i architecture components

- The 802.11i architecture contains the following components:
- 802.1X for authentication
- RSN for keeping track of associations,
- AES-based CCMP to provide confidentiality, integrity and origin authentication.
- Four-way handshake

Secrets in a Standards Process?

- WAPI symmetric encryption algorithm, SMS4, declassified in January 2006.
- The standard, cryptographic implementation remain unpublished
- Standards process: participants duplicate implementation.

Convergence - Conflict

Telecoms

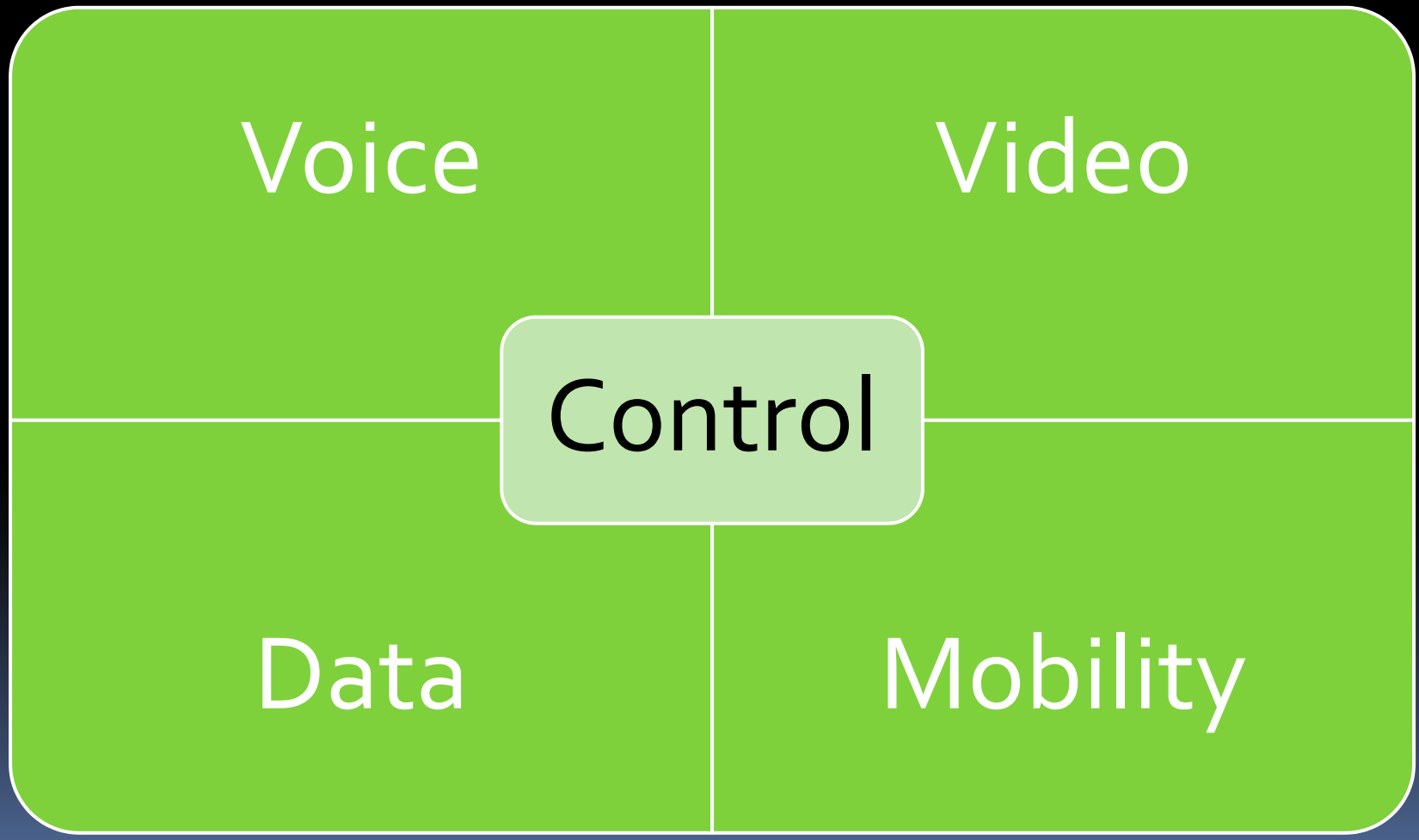
- Cell phones:
  - Add WiFi
  - Big data storage
  - Video streaming
- Subscribe to service

LAN Networking

- PDA adds cell module
- Laptop has 802.11 a, b, e, g and adds G3 (EVDO and Edge…)
- Access 'flat rate' Internet

Access Control – Subscribers?
Content control – accessibility, monitoring, pricing?

Basis for Arguments



A Regulation or a Standard?

- 2003, China announced a policy: wireless devices sold in China include WAPI support.
  - To play, partner with 1 of 11 Chinese companies
- US State Dept objected - China postponed policy

Timeline for discussion and dispute

- SC6 Orlando plenary Nov 2004
- Geneva May 2005
- Beijing August 2005
- SC6 September 2005
- ISC/IEC leadership discussions on path
- IEEE had variety of complaints on harmonization

IEC/ISO Parallel Fast Track balloting

- 802.11
MAR06 - ☺
- JUN06 – Ballot Resolution confirmed
- Pub. JUL06 STD802.11i

- WAPI
- MAR06 - ☹
- China news agency claims appeals in April, May
- China may insist TBT status for policy-> WTO

Economics: VAT on chips

- U.S. chipmakers: "value-added tax (VAT) on semiconductors discriminates against companies that do not partly or wholly manufacture chips in China."
- Chips imported into China – 17 percent VAT.
- Chips made in China – 3 percent VAT.
- China pushing own 3G cellular networks.
- Wi-Fi chip and gear makers -confusion
  - about the Chinese security standard
  - product development impact.
  - Intel : stop selling Centrino chip packages for notebooks
  - Broadcom: similar position by Wi-Fi chipmaker.

Voter's Comments

- "The outcome came as no surprise, given the popularity of the 802.11 technology."
- "Moreover, the Chinese hamstrung their candidate, formally known as the WLAN Authentication and Privacy Infrastructure, by declining to reveal the underlying encryption algorithms."
- ISO members also expressed concerns about WAPI's incompatibility with the well-established 802.11 protocol and noted that WAPI's development process was relatively closed.

Chinese apparent goals

- Control Access
- Provide Signal intercept and interpretation
- Assure user ID of all transfers
- Preclude foreign monitoring

What's Next?

- WAPI Industrial Union - China
  - 22 members
  - Lenova
  - Huawei
  - Founder Electronics (Beijing)
  - 4 China telecom operators
  - …

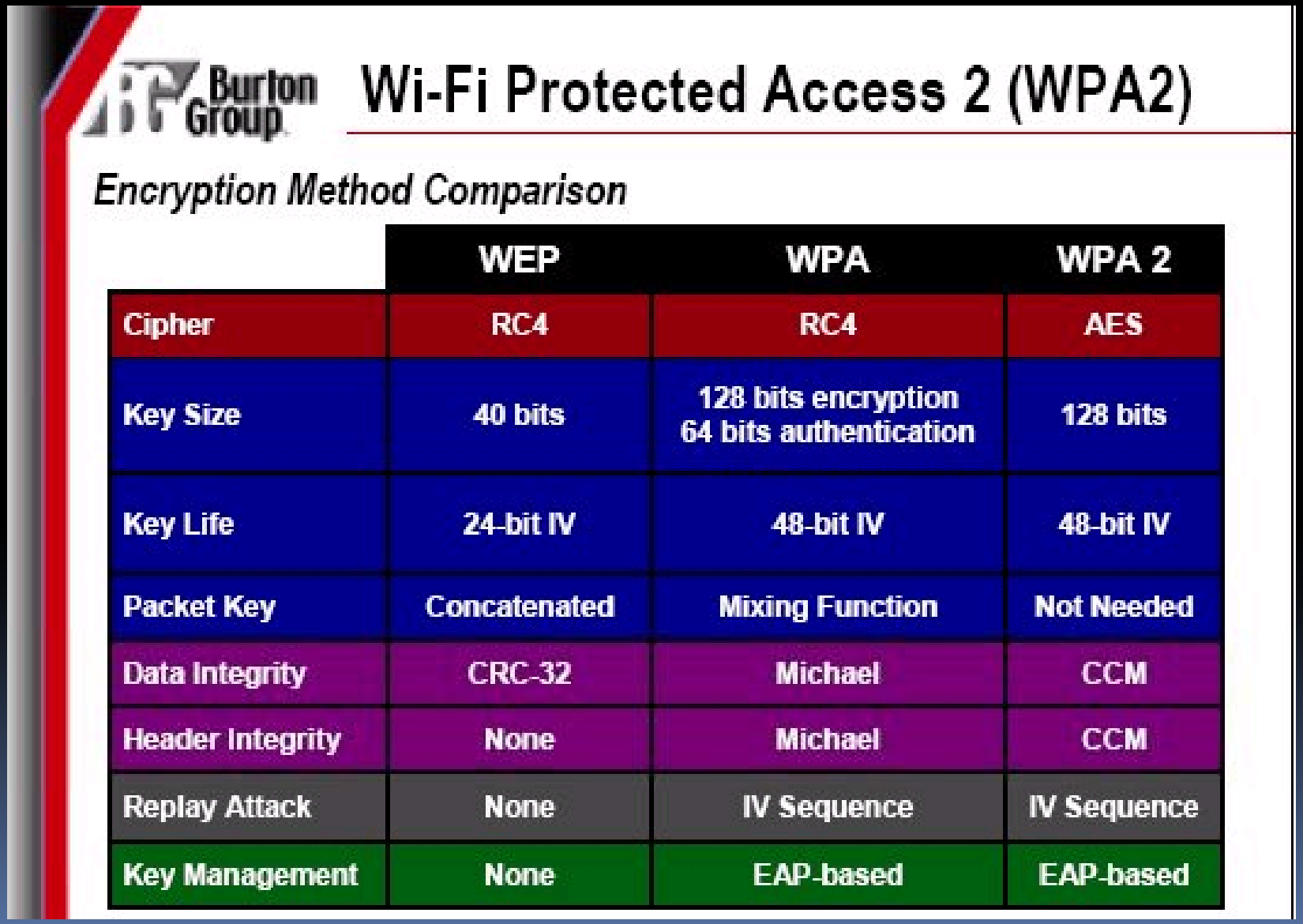
Myth Breaking

- The Internet is NOT free -
  - BIG stake holders
- The Network is no longer net-neutral,
  - in US or China

Questions?

- Rick Ellinger
- ellinger@sbcglobal.net
- www.wca.org

802.11i



	WEP	WPA	WPA 2
Cipher	RC4	RC4	AES
Key Size	40 bits	128 bits encryption 64 bits authentication	128 bits
Key Life	24-bit IV	48-bit IV	48-bit IV
Packet Key	Concatenated	Mixing Function	Not Needed
Data Integrity	CRC-32	Michael	CCM
Header Integrity	None	Michael	CCM
Replay Attack	None	IV Sequence	IV Sequence
Key Management	None	EAP-based	EAP-based

802.11 IEEE Standards and task groups within IEEE 802.11 working group:

- IEEE 802.11 - The original 1 Mbit/s and 2 Mbit/s, 2.4 GHz RF and IR standard (1999)
- IEEE 802.11a - 54 Mbit/s, 5 GHz standard (1999, shipping products in 2001)
- IEEE 802.11b - Enhancements to 802.11 to support 5.5 and 11 Mbit/s (1999)
- IEEE 802.11c - Bridge operation procedures; included in the IEEE 802.1D standard (2001)
- IEEE 802.11d - International (country-to-country) roaming extensions (2001)
- IEEE 802.11e - Enhancements: QoS, including packet bursting (2005)
- IEEE 802.11f - Inter-Access Point Protocol (2003) Withdrawn February 2006
- IEEE 802.11g - 54 Mbit/s, 2.4 GHz standard (backwards compatible with b) (2003)
- IEEE 802.11h - Spectrum Managed 802.11a (5 GHz) for European compatibility (2004)
- IEEE 802.11i - Enhanced security (2004)
- IEEE 802.11j - Extensions for Japan (2004)
-
- IEEE 802.11k - Radio resource measurement enhancements (proposed - 2007?)
- IEEE 802.11l - (reserved and will not be used)
- IEEE 802.11m - Maintenance of the standard; odds and ends. (ongoing)
- IEEE 802.11n - Higher throughput improvements (pre-draft - 2007?)
- IEEE 802.11o - (reserved and will not be used)
- IEEE 802.11p - WAVE - Wireless Access for the Vehicular Environment (such as ambulances and passenger cars) (working - 2008?)
- IEEE 802.11q - (reserved and will not be used, can be confused with 802.1Q VLAN trunking)
- IEEE 802.11r - Fast roaming (unapproved)
- IEEE 802.11s - ESS Mesh Networking (working - 2008?)
- IEEE 802.11T - Wireless Performance Prediction (WPP) - test methods and metrics Recommendation (working - 2008?)
- IEEE 802.11u - Interworking with non-802 networks (for example, cellular) (proposal evaluation - ?)
- IEEE 802.11v - Wireless network management (early proposal stages - ?)
- IEEE 802.11w - Protected Management Frames (early proposal stages - 2008?)
- IEEE 802.11x - (reserved and will not be used)
- IEEE 802.11y - 3650-3700 Operation in the U.S. (early proposal stages - ?)

Western goals, RIAA
U.S.-China Joint Commission on Commerce and Trade. (APR2004)

- China: “new copyright policies curtailing rampant piracy” (RIAA).
- China will ..reduce piracy on CDs: criminal charges against accused pirates; and bring China's laws into line with international copyright treaties.
- RIAA called on China to open trade barriers and streamline censorship

WAPI Detail

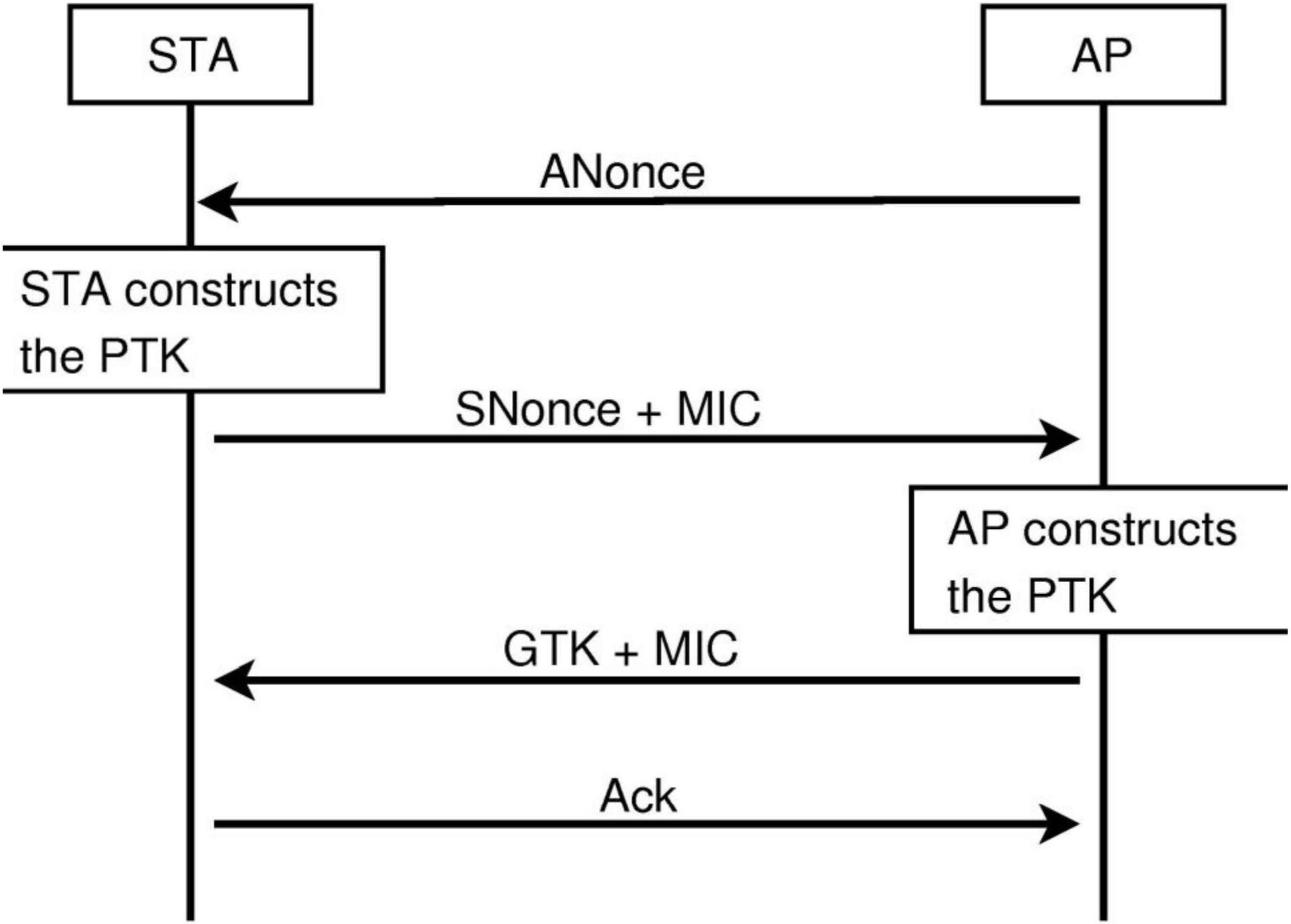
- **SMS4** proprietary block cipher , Chinese National Standard, forWireless LAN WAPI (Wired Authentication and Privacy Infrastructure).
- SMS4 proposed cipher in IEEE 802.11i standard, but rejected by ISO.
  - opposition to WAPI fast-track proposal by the IEEE.
- SMS4 is patented by Beijing Data Security Technology Co. Ltd. (BDST), meaning that it is proprietary, as opposed to free or open source. According to an article on The Register, any Wi-Fi equipment makers that want to support WAPI must work with one of eleven designated implementors of WAPI.
- One thing that sets the WAPI proposal apart from other WLAN security standards is the use of central key servers.
- The SMS4 algorithm was declassified in January, 2006. A few details of the SMS4 cipher are:
- It has a block size of 128 bits.
- Uses an 8-bit S-box
- The key size is 128 bits.
- The only operations used are XOR, circular shifts and S-Box applications
- Performs 32 rounds to process one block.
- Each round updates a quarter (32 bits) of the internal state.
- A non-linear key schedule is used to produce the round keys.
- Decryption is using the same keys as encryption, but in reversed order.

Some declassified Secrets

- The SMS4 algorithm declassified in January, 2006.
- A few details of the SMS4 cipher:
  - block size of 128 bits.
  - 8-bit S-box
  - Key size is 128 bits.
  - only operations: XOR, circular shifts, S-Box applications
  - Performs 32 rounds for one block.
  - Each round updates a quarter (32 bits) of the internal state.
  - Non-linear key produces the round keys.
  - Decryption uses the same keys as encryption, but in reversed order.
- *These details do NOT provide ability to operate the algorithm*.

Encryption key distribution
The Four-Way Handshake

- Authentication : access point (AP) authenticate itself to the client station (STA), and keys to encrypt the traffic need to be derived.
- The earlier EAP exchange provided shared secret key PMK (Pairwise Master Key).
- Key is designed to last the entire session and should be exposed as little as possible. Therefore the four-way handshake is used to establish another key called the PTK (Pairwise Transient Key). The PTK is generated by concatenating the following attributes: PMK, AP nonce (ANonce), STA nonce (SNonce), AP MAC address and STA MAC address. The product is then put through a cryptographic hash function.
- The handshake also yields the GTK (Group Temporal Key), used to decrypt multicast and broadcast traffic. The actual messages exchanged during the handshake are depicted in the figure and explained below:
- The AP sends a nonce-value to the STA (ANonce). The client now has all the attributes to construct the PTK.
- The STA sends its own nonce-value (SNonce) to the AP together with a MIC.
- The AP sends the GTK and a sequence number together with another MIC. The sequence number is the sequence number that will be used in the next multicast or broadcast frame, so that the receiving STA can perform basic replay detection.
- The STA sends a confirmation to the AP.
- As soon as the PTK is obtained it is divided into three separate keys:
- EAPOL-Key Confirmation Key (KCK) - The key used to compute the MIC for EAPOL-Key packets.
- EAPOL-Key Encryption Key (KEK) - The key used to encrypt the EAPOL-Key packets.
- Temporal Key (TK) - The key used to encrypt the actual wireless traffic.
- s

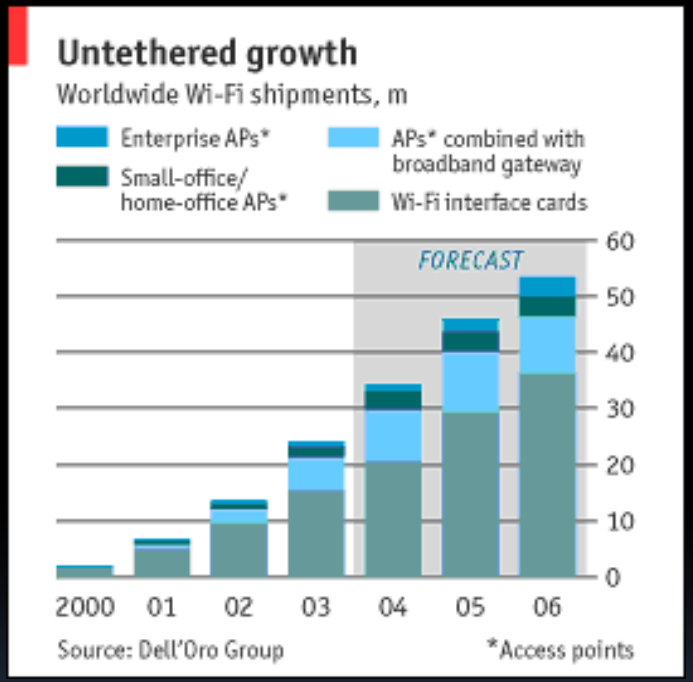

STA
AP
ANonce
STA constructs
the PTK
SNonce + MIC
AP constructs
the PTK
GTK + MIC
Ack

Keys

- The four-way handshake is used to establish another key called the PTK (Pairwise Transient Key). The PTK is generated by concatenating the following attributes: PMK, AP nonce (ANonce), STA nonce (SNonce), AP MAC address and STA MAC address. The product is then put through a cryptographic hash function.
- The handshake also yields the GTK (Group Temporal Key), used to decrypt multicast and broadcast traffic. The actual messages exchanged during the handshake are depicted in the figure and explained below:
- The AP sends a nonce-value to the STA (ANonce). The client now has all the attributes to construct the PTK.
- The STA sends its own nonce-value (SNonce) to the AP together with a MIC.
- The AP sends the GTK and a sequence number together with another MIC. The sequence number is the sequence number that will be used in the next multicast or broadcast frame, so that the receiving STA can perform basic replay detection.
- The STA sends a confirmation to the AP.
- As soon as the PTK is obtained it is divided into three separate keys:
- EAPOL-Key Confirmation Key (KCK) - The key used to compute the MIC for EAPOL-Key packets.
- EAPOL-Key Encryption Key (KEK) - The key used to encrypt the EAPOL-Key packets.
- Temporal Key (TK) - The key used to encrypt the actual wireless traffic.

Wireless Access Points

South Korea's telecommunications provider KT doubled the number of its hotspots to 18,000 by the end of 2004. This gave the company the world's largest commercial Wi-Fi network. KT will have more commercial hotspots than all of North America and slightly less than Europe. With entire city blocks as hotspots, South Korea may be the most advanced wireless market on the planet.



Wireless LAN Throughput by IEEE Standard

IEEE WLAN Standard	Over-the-Air (OTA) Estimates	Media Access Control Layer, Service Access Point (MAC SAP) Estimates
802.11b	11 Mbps	5 Mbps
802.11g	54 Mbps	25 Mbps (when .11b is not present)
802.11a	54 Mbps	25 Mbps
802.11n	200+ Mbps	100 Mbps

History, IEEE Wireless LANs

- IEEE 802.11 - The original 1 Mbit/s and 2 Mbit/s, 2.4 GHz RF and IR standard (1999)
- IEEE 802.11a - 54 Mbit/s, 5 GHz standard (1999, shipping products in 2001)
- IEEE 802.11b - Enhancements to 802.11 to support 5.5 and 11 Mbit/s (1999)
- IEEE 802.11c - Bridge operation procedures; included in the IEEE 802.1D standard (2001)
- IEEE 802.11d - International (country-to-country) roaming extensions (2001)
- IEEE 802.11e - Enhancements: QoS, including packet bursting (2005)
- IEEE 802.11F - Inter-Access Point Protocol (2003)
- IEEE 802.11g - 54 Mbit/s, 2.4 GHz standard (backwards compatible with b) (2003)
- IEEE 802.11h - Spectrum Managed 802.11a (5 GHz) for European compatibility (2004)
- IEEE 802.11i - Enhanced security (2004)
- IEEE 802.11j - Extensions for Japan (2004)
- IEEE 802.11k - Radio resource measurement enhancements
- IEEE 802.11m - Maintenance of the standard; odds and ends.
- IEEE 802.11n - Higher throughput improvements
- IEEE 802.11p - WAVE - Wireless Access for the Vehicular Environment (such as ambulances and passenger cars)
- IEEE 802.11r - Fast roaming
- IEEE 802.11s - ESS Mesh Networking
- IEEE 802.11T - Wireless Performance Prediction (WPP) - test methods and metrics
- IEEE 802.11u - Interworking with non-802 networks (e.g., cellular)
- IEEE 802.11v - Wireless network management
- IEEE 802.11w - Protected Management Frames