Overview of Wi-Fi Security

What is left?

Philippe Teuwen

Security Engineer and Contributor to
Wi-Fi Alliance Easy Setup Task Group
N.V. Philips

October 14 & 15
Hack.lu 2005

Wireless security is something that most everyone wants, but which few actually use. Barriers to use include throughput loss in older 802.11b products, WEP's ability to be cracked, and difficulty in getting the darned thing working!

tom's networking

Outline

Outline

Dumb security

- MAC filtering
  - The most management effort for the least security
  - So easy to spoof, especially over wireless
  - Still largely used in HotSpots
- SSID hiding
  - Ok, SSID not displayed in the Beacons
  - But what about Probe Requests, Probe Responses and (re-)Association Requests??
- LEAP or EAP-FAST
  - Still around thanks to Cisco marketing
  - Incompatible with most clients and poorly secure

Dumb security

- MAC filtering
  - The most management effort for the least security
  - So easy to spoof, especially over wireless
  - Still largely used in HotSpots
- SSID hiding
  - Ok, SSID not displayed in the Beacons
  - But what about Probe Requests, Probe Responses and (re-)Association Requests??
- LEAP or EAP-FAST
  - Still around thanks to Cisco marketing
  - Incompatible with most clients and poorly secure

Dumb security

- MAC filtering
  - The most management effort for the least security
  - So easy to spoof, especially over wireless
  - Still largely used in HotSpots
- SSID hiding
  - Ok, SSID not displayed in the Beacons
  - But what about Probe Requests, Probe Responses and (re-)Association Requests??
- LEAP or EAP-FAST
  - Still around thanks to Cisco marketing
  - Incompatible with most clients and poorly secure

Dumb security

- MAC filtering
  - The most management effort for the least security
  - So easy to spoof, especially over wireless
  - Still largely used in HotSpots
- SSID hiding
  - Ok, SSID not displayed in the Beacons
  - But what about Probe Requests, Probe Responses and (re-)Association Requests??
- LEAP or EAP-FAST
  - Still around thanks to Cisco marketing
  - Incompatible with most clients and poorly secure

Dumb security

- Disable DHCP
  - Just waste of (your) time
- Antenna placement
  - Remember, the hacker will always have a bigger antenna than yours
- Shift to 802.11a or Bluetooth
  - 802.11a is just at PHY layer and Bluetooth has its own bunch of problems

Dumb security

- Disable DHCP
  - Just waste of (your) time
- Antenna placement
  - Remember, the hacker will always have a bigger antenna than yours
- Shift to 802.11a or Bluetooth
  - 802.11a is just at PHY layer and Bluetooth has its own bunch of problems

Dumb security

- Disable DHCP
  - Just waste of (your) time
- Antenna placement
  - Remember, the hacker will always have a bigger antenna than yours
- Shift to 802.11a or Bluetooth
  - 802.11a is just at PHY layer and Bluetooth has its own bunch of problems

Dumb security

- Disable DHCP
  - Just waste of (your) time
- Antenna placement
  - Remember, the hacker will always have a bigger antenna than yours
- Shift to 802.11a or Bluetooth
  - 802.11a is just at PHY layer and Bluetooth has its own bunch of problems

Outline

WEP is Dead

But do you know how much dead it is?
Any WEP based network with or without Dynamic WEP keys can now be cracked in minutes

Passive WEP cracking

- Since summer 2001:
  - **AirSnort**, implementing the Fluhrer-Mantin-Shamir (FMS) attack
  - Requires 5 to 10M of packets as only "weak" IVs are vulnerable
  - Manufacturers filter out these weak IVs
- State-of-the-art:
  - Augustus 8th, 2004: KoreK presents a new statistical cryptanalysis attack code (**chopper**)
  - No more "weak" packets, just need unique IVs, around 200.000 packets required
  - Now available in **aircrack** and **WepLab**
    - **aircrack** : better use fudge factor = 4
    - **WepLab** : better use –perc = 95%

Passive WEP cracking

- Since summer 2001:
  - **AirSnort**, implementing the Fluhrer-Mantin-Shamir (FMS) attack
  - Requires 5 to 10M of packets as only "weak" IVs are vulnerable
  - Manufacturers filter out these weak IVs
- State-of-the-art:
  - Augustus 8th, 2004: KoreK presents a new statistical cryptanalysis attack code (**chopper**)
  - No more "weak" packets, just need unique IVs, around 200.000 packets required
  - Now available in **aircrack** and **WepLab**
    - **aircrack** : better use fudge factor = 4
    - **WepLab** : better use –perc = 95%

Offline dictionary attacks

- **WepLab** and **WepAttack**, 2 ways:
  - use the most common MD5 hashing techniques to handle passphrases
  - or null terminated raw ASCII WEP keys
- **John the Ripper**
  - to feed these tools

Offline dictionary attacks

- **WepLab** and **WepAttack**, 2 ways:
  - use the most common MD5 hashing techniques to handle passphrases
  - or null terminated raw ASCII WEP keys
- **John the Ripper**
  - to feed these tools

Active attacks

- Replay attacks
  - Goal is to provoke traffic to help data collection
  - WEP: no replay protection, no need to decrypt, nature of packet easily guessable by its length
  - Most obvious: ARP Replay (look for length=68 and dest.addr=ff:ff:ff:ff:ff:ff), this is what **aireplay** does
- Known plaintext attacks
  - Goal is to send arbitrary packets
  - If you know (or guess) the plaintext of a packet, you know the XORed mask and you can forge your own encrypted packets (and you still don't know the WEP key!)
  - **WEPWedgie** by Anton Rager (2003)
- Single packet decryption
  - Using the AP as an oracle
  - **chopchop** by KoreK

Active attacks

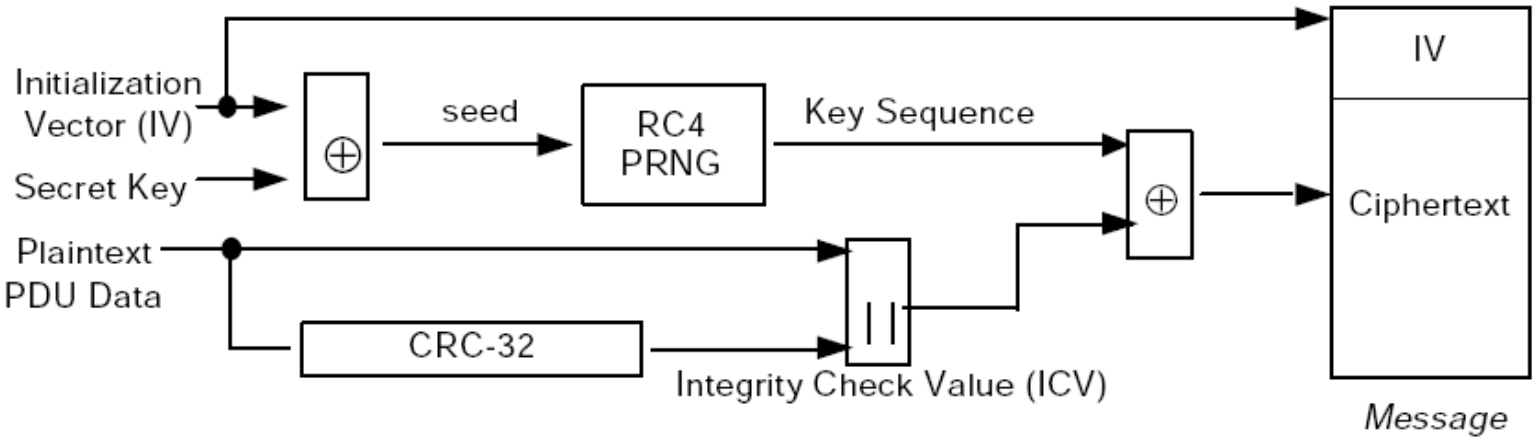
- Replay attacks
  - Goal is to provoke traffic to help data collection
  - WEP: no replay protection, no need to decrypt, nature of packet easily guessable by its length
  - Most obvious: ARP Replay (look for length=68 and dest.addr=ff:ff:ff:ff:ff:ff), this is what **aireplay** does
- Known plaintext attacks
  - Goal is to send arbitrary packets
  - If you know (or guess) the plaintext of a packet, you know the XORed mask and you can forge your own encrypted packets (and you still don't know the WEP key!)
  - **WEPWedgie** by Anton Rager (2003)
- Single packet decryption
  - Using the AP as an oracle
  - **chopchop** by KoreK

Active attacks

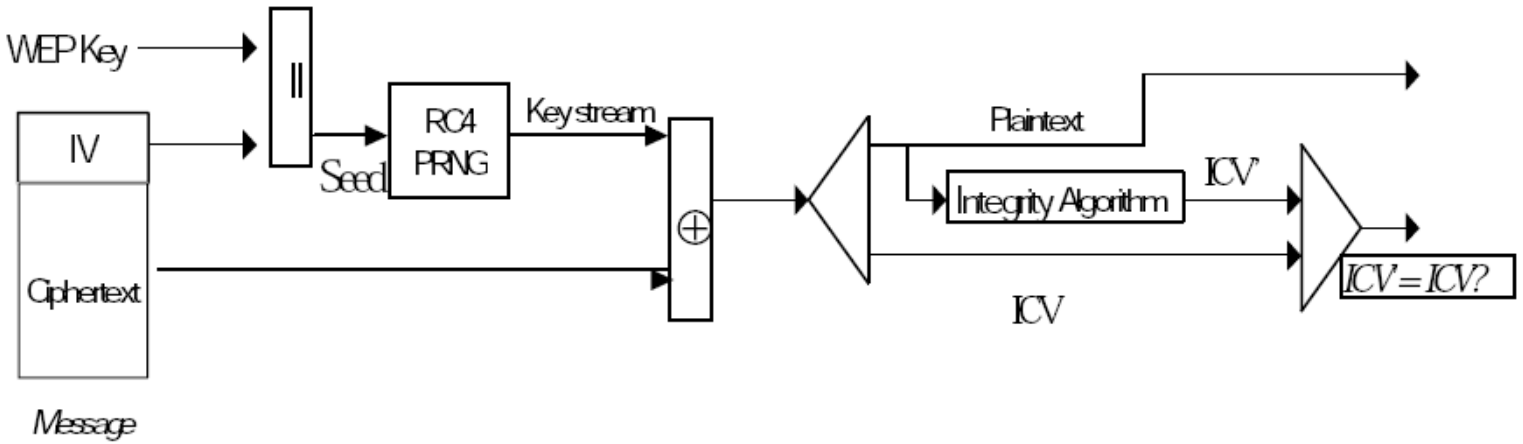
- Replay attacks
  - Goal is to provoke traffic to help data collection
  - WEP: no replay protection, no need to decrypt, nature of packet easily guessable by its length
  - Most obvious: ARP Replay (look for length=68 and dest.addr=ff:ff:ff:ff:ff:ff), this is what **aireplay** does
- Known plaintext attacks
  - Goal is to send arbitrary packets
  - If you know (or guess) the plaintext of a packet, you know the XORed mask and you can forge your own encrypted packets (and you still don't know the WEP key!)
  - **WEPWedgie** by Anton Rager (2003)
- Single packet decryption
  - Using the AP as an oracle
  - **chopchop** by KoreK

WEP Internals

Bundling:



Unbundling:



Outline

WPA TKIP

- Response of IEEE to WEP problem: 802.11i
  - But not ready in time!
- Intermediate response of Wi-Fi Alliance: WPA
  - Backward compatible subset of a draft (D3) of 802.11i
  - Allow firmware upgrades to WPA TKIP
  - Keys and IVs larger, dynamically changed every 10k
  - CRC replaced by a MAC (keyed-MIC) based on "Michael", including a frame counter
  - Replay attacks and alterations not possible anymore

WPA TKIP

- WPA still relies on the same RC4 algorithm than WEP
- Accelerated attack of $\mathcal{O}\left(2^{105}\right)$ vs. $\mathcal{O}\left(2^{128}\right)$ on TEK
- "Michael" subject to packet forgery attacks if IVs reused

$$m = Michael\left(M, k_{mic}\right) \Leftrightarrow k_{mic} = InvMichael\left(M, m\right)$$

- Risk of efficient DoS due to WPA "counter-attack" measures

Attacks will come...

Outline

AES-CCMP and WPA2
(IEEE 802.11i)

- Finally ratified by IEEE in June, 2004
- WPA2 certified products in September, 2004
- WPA2 mandatory by March 1^{st}, 2006
  - Extended EAP mandated for Enterprise Devices
- The current best Wi-Fi encryption available
  - Michael replaced by CCMP
  - RC4 replaced by AES

WPA2 with AES is eligible for FIPS 140-2 compliance

WEP/WPA/WPA2 mixed modes

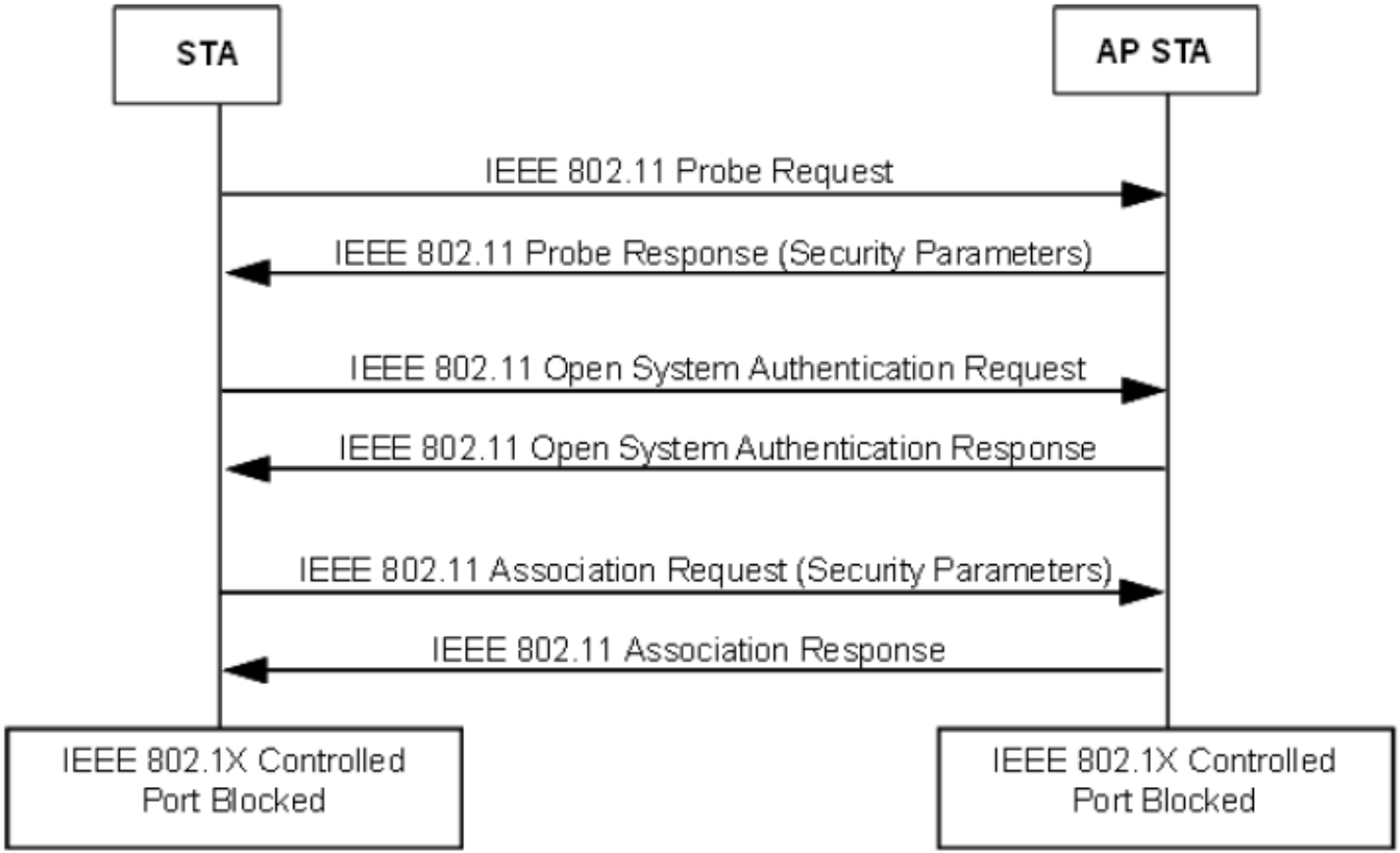
- RSN (Robust Security Network):
  - CCMP/TKIP-only networks
- TSN (Transient Security Network):
  - allows pre-RSN associations (WEP in group ciphers)
- WPA2 Wi-Fi certification:
  - RSN modes: WPA2-only and WPA/WPA2 mixed mode
- WPA/WPA2 mixed mode:
  - AP:
    - supports both WPA and WPA2 clients by using TKIP as group cipher suite and CCMP/TKIP as unicast cipher suite
  - STA:
    - WPA(TKIP) for unicast and WPA(TKIP) for multicast
    - WPA2(AES) for unicast and WPA(TKIP) for multicast

Are we safe?
(assuming that WPA2 is bullet-proof)

- Management frames are always in clear
- So are the SSID, src and dst MAC-addresses
- This is still possible to spoof mgmt frames (spoofed Disassociation or Deauthentication frames), see airjack and Scapy

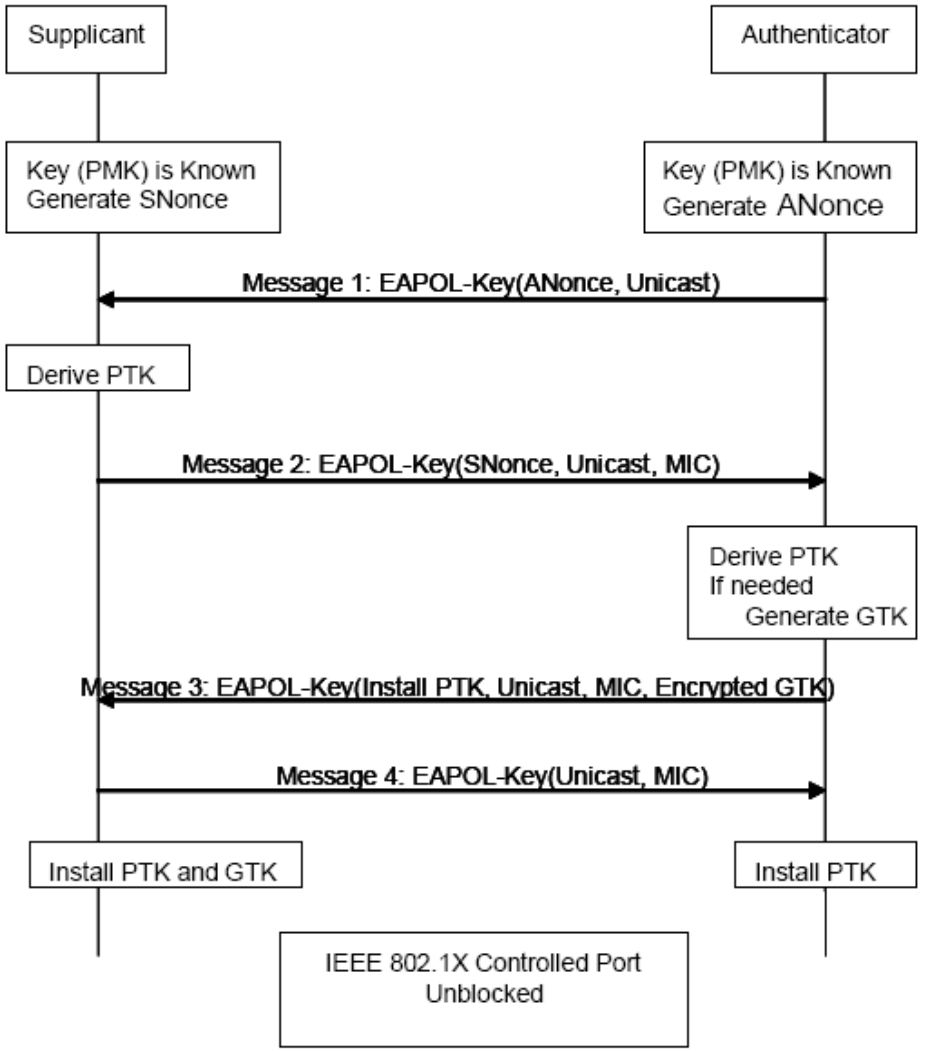
Outline

WPA(2) Authentication



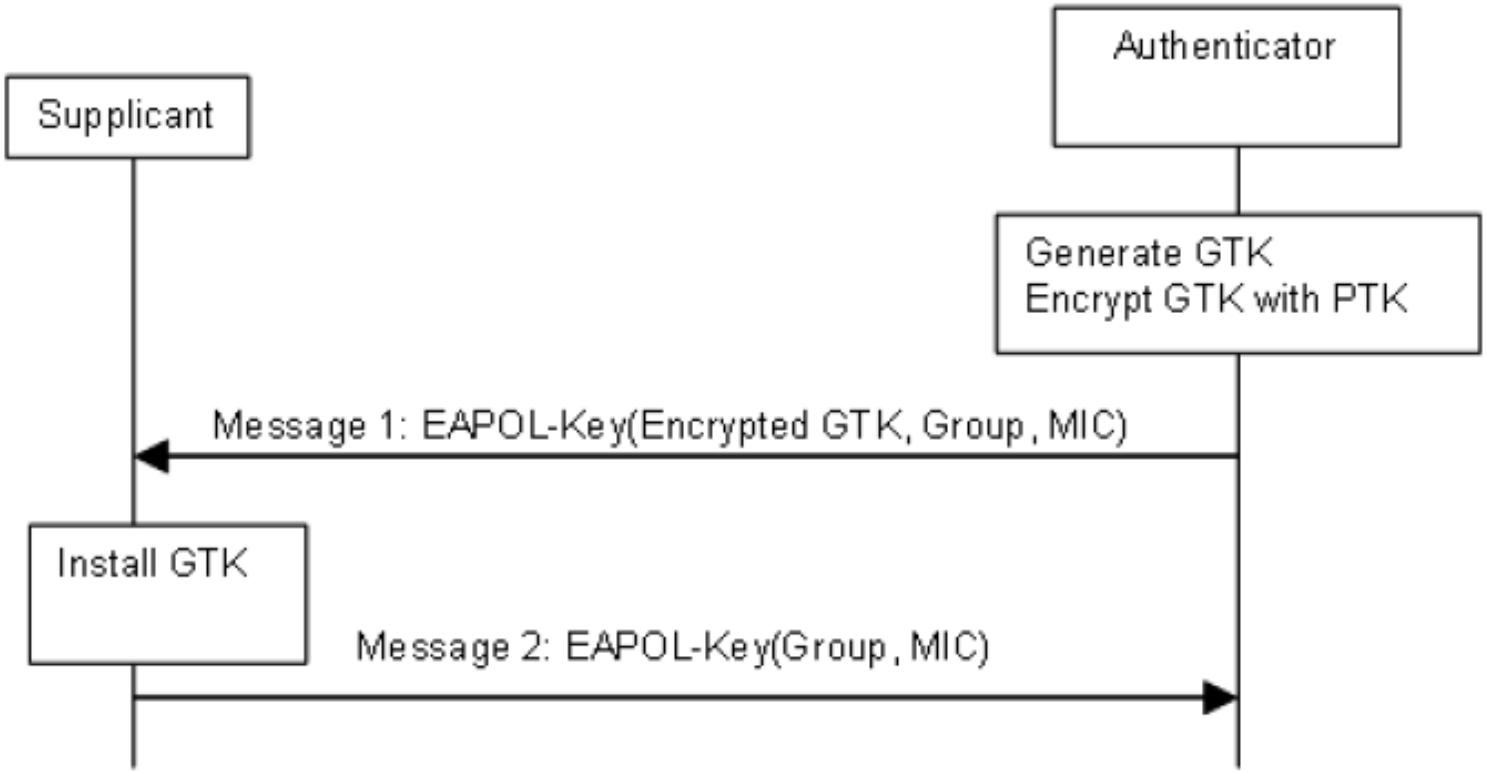
Then, optional limited communication (EAP) to share a PMK

WPA(2) 4-Way Handshake



For WPA, group keys are shared in a separate handshake

WPA(2) Subsequent 2-Way Handshakes
for group keys



WPA: 2-Way HS follows immediately 4-Way HS

Useful before a STA joins or after a STA leaves

WPA(2)
4-Way Handshake

1. AP→STA: EAPOL(..., ANonce)
2. STA→AP: EAPOL(..., SNonce,MIC,RSN IE)
3. AP→STA: EAPOL(..., ANonce,MIC,RSN IE)
4. STA→AP: EAPOL(..., MIC)

WPA(2)
Behind the scene

- Requires a Pair-wise Master Key, PMK

PTK derivation

$$\begin{aligned} \text{PTK} \leftarrow \text{PRF-X} \quad & (\text{PMK}, \ldots \\ & \text{"Pairwise key expansion"}, \ldots \\ & \min(\text{AA}, \text{SA}) \parallel \max(\text{AA}, \text{SA}) \parallel \ldots \\ & \min(\text{ANonce}, \text{SNonce}) \parallel \max(\text{ANonce}, \text{SNonce})) \end{aligned}$$

- PTK is split in several keys

$$\begin{aligned} \text{PTK} &\equiv \text{KCK}/\text{MK} \parallel \text{KEK} \parallel \text{TEK} \equiv \text{TK} \parallel \ldots \\ \text{MIC} &= \text{MIC}(\text{MK}, \text{EAPOL}) \end{aligned}$$

- Conclusion: All secrets are derived from PMK and public information
- WPA2: PMKID, key caching, pre-auth...

WPA(2)
Behind the scene

- Requires a Pair-wise Master Key, PMK

PTK derivation

$$\begin{aligned} \text{PTK} \leftarrow \text{PRF-X} \quad & (\text{PMK}, \ldots \\ & \text{"Pairwise key expansion"}, \ldots \\ & \min(\text{AA}, \text{SA}) \parallel \max(\text{AA}, \text{SA}) \parallel \ldots \\ & \min(\text{ANonce}, \text{SNonce}) \parallel \max(\text{ANonce}, \text{SNonce})) \end{aligned}$$

- PTK is split in several keys

$$\text{PTK} \equiv \text{KCK}/\text{MK} \parallel \text{KEK} \parallel \text{TEK} \equiv \text{TK} \parallel \ldots$$
$$\text{MIC} = \text{MIC}(\text{MK}, \text{EAPOL})$$

- Conclusion: All secrets are derived from PMK and public information
- WPA2: PMKID, key caching, pre-auth...

WPA(2)
Behind the scene

- Requires a Pair-wise Master Key, PMK

PTK derivation

$$\begin{aligned} \text{PTK} \leftarrow \text{PRF-X} \quad & (\text{PMK}, \ldots \\ & \text{"Pairwise key expansion"}, \ldots \\ & \min(\text{AA}, \text{SA}) \parallel \max(\text{AA}, \text{SA}) \parallel \ldots \\ & \min(\text{ANonce}, \text{SNonce}) \parallel \max(\text{ANonce}, \text{SNonce})) \end{aligned}$$

- PTK is split in several keys

$$\begin{aligned} \text{PTK} &\equiv \text{KCK}/\text{MK} \parallel \text{KEK} \parallel \text{TEK} \equiv \text{TK} \parallel \ldots \\ \text{MIC} &= \text{MIC}(\text{MK}, \text{EAPOL}) \end{aligned}$$

- Conclusion: All secrets are derived from PMK and public information
- WPA2: PMKID, key caching, pre-auth...

Outline

WPA-Personal
alias WPA-PSK

- For those who cannot afford a 802.1X server
- But TinyPEAP and hostapd could change this...
  - *Still relevant for non-PC devices, typically in Home Networks*
- One common passphrase (8..63) or PSK (256)
- PSK $= \mathrm{PBKDF2}(\mathrm{passphrase}, \mathrm{ssid}, \mathrm{ssidlength}, 4096, 256)$
- PMK $\equiv$ PSK!!
- Consequence:
  - *Any user of a WPA-PSK network can calculate PTKs of the other STAs and decrypt all the traffic,* not really nice for guest access
- Passphrases: dictionary attacks (Cowpatty)

$$\mathrm{passphrase} \Rightarrow \mathrm{PSK} \Rightarrow \mathrm{PMK} \Rightarrow \mathrm{PTK} \Rightarrow \mathrm{MK} \Rightarrow \mathrm{MIC}$$

WPA-Personal
alias WPA-PSK

- For those who cannot afford a 802.1X server
- But TinyPEAP and hostapd could change this...
  - *Still relevant for non-PC devices, typically in Home Networks*
- One common passphrase (8..63) or PSK (256)
- $\text{PSK} = \text{PBKDF2}(\text{passphrase}, \text{ssid}, \text{ssidlength}, 4096, 256)$
- $\text{PMK} \equiv \text{PSK}$!!
- Consequence:
  - *Any user of a WPA-PSK network can calculate PTKs of the other STAs and decrypt all the traffic,* not really nice for guest access
- Passphrases: dictionary attacks (Cowpatty)

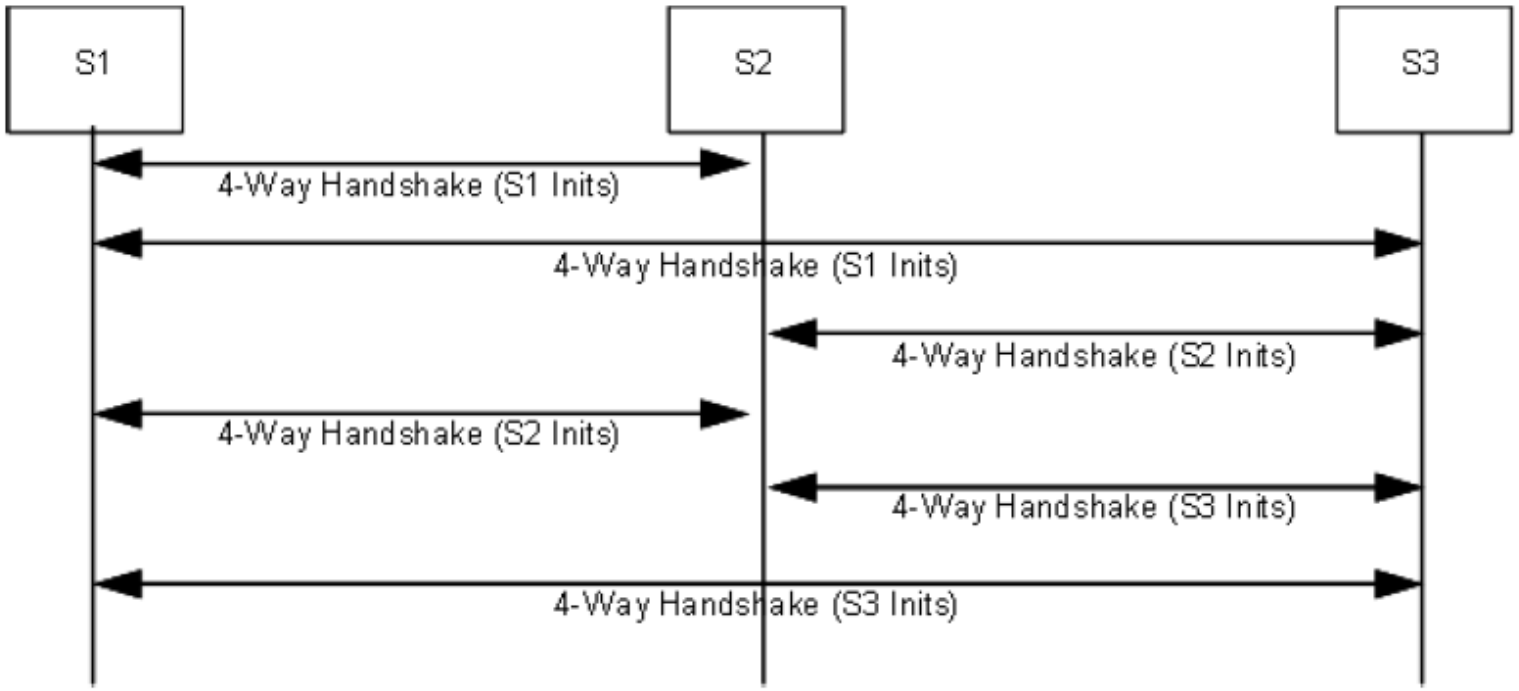
$\text{passphrase} \Rightarrow \text{PSK} \Rightarrow \text{PMK} \Rightarrow \text{PTK} \Rightarrow \text{MK} \Rightarrow \text{MIC}$

WPA-Personal
alias WPA-PSK

- For those who cannot afford a 802.1X server
- But TinyPEAP and hostapd could change this...
  - *Still relevant for non-PC devices, typically in Home Networks*
- One common passphrase (8..63) or PSK (256)
- $\text{PSK} = \text{PBKDF2}(\text{passphrase}, \text{ssid}, \text{ssidlength}, 4096, 256)$
- $\text{PMK} \equiv \text{PSK}$!!
- Consequence:
  - *Any user of a WPA-PSK network can calculate PTKs of the other STAs and decrypt all the traffic,* not really nice for guest access
- Passphrases: dictionary attacks (Cowpatty)

$$\text{passphrase} \Rightarrow \text{PSK} \Rightarrow \text{PMK} \Rightarrow \text{PTK} \Rightarrow \text{MK} \Rightarrow \text{MIC}$$

WPA(2) IBSS 4-Way Handshakes



N*(N-1) 4-Way handshakes for N STAs!
Twice more because each STA propagates its own GTK
Hardly imaginable with WPA-EAP...
Remember, this doesn't prevent any participant to sniff around ;-)

How to use WPA-PSK securely?

- Prefer strict WPA2-CCMP if possible
- No passphrase, only randomly-generated PSK
  - For strict Wi-Fi compliance, randomly-generated passphrase with enough entropy
    (8 Diceware words or 22 random chars for >100bits)
- If guest access foreseen, individual PSKs
  - (we'll see how later...)

How to use WPA-PSK securely?

PSK:

8BE25E7B5874DEE9779A4E5632BBD573B4B8D3404AE932F8E792BC3193B07153

Diceware:

cleftcamsynodlacyyrairilylowestgloat

Random:

JBXSYITPIUBTCPJORWIOXK

g27kXwrXcrYkxVYJ3

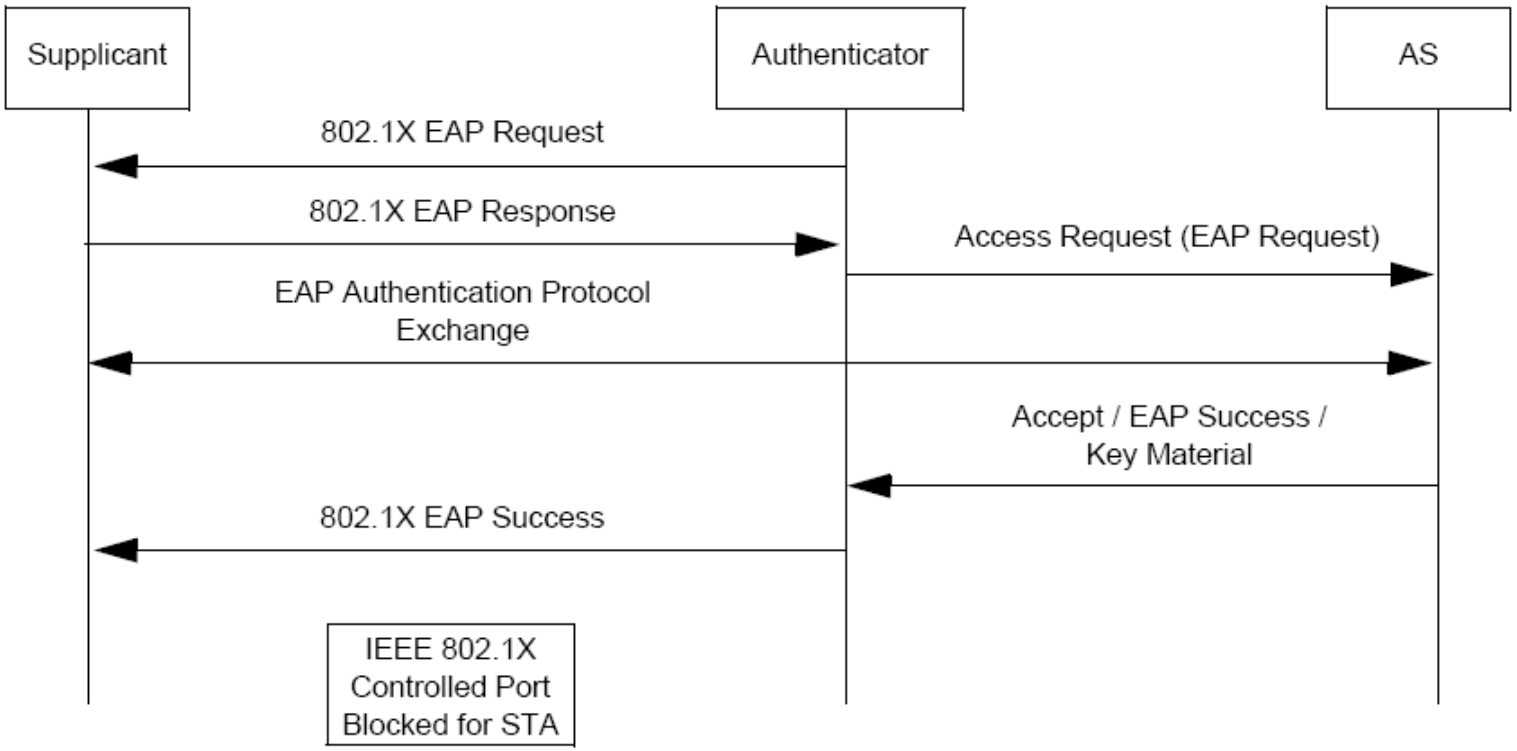
Wi-Fi security can be achieved in Home Networks but this will become true only if it is *easy* to do!

Outline

WPA-Enterprise
alias WPA-EAP, incl. 802.1X

- WPA-Enterprise certification is optional, only WPA-Personal is mandatory
- Now WPA-Enterprise certification with 4 more methods certified on top of EAP-TLS
  - EAP-TTLS/MSCHAPv2
  - PEAPv0/EAP-MSCHAPv2
  - PEAPv1/EAP-GTC
  - EAP-SIM
- PSK/EAP mixed mode is possible

WPA(2) EAP Authentication



EAP Methods

Many methods on top of the 5 Wi-Fi certified

- Good security with:
  - PEAP (Protected EAP) encapsulating MSCHAPv2
    - Server Side Digital Certificate and a Client Side Username/Password
  - TTLS (Tunneled Transport Layer Security) encapsulating MSCHAPv2
    - A little better as username not in clear text.
  - Compare it with Cisco's LEAP and its MSCHAPv2 session in clear ⇒offline dictionary attacks
  - Needs to implement a RADIUS Authentication Server. (but hostapd...)
- Very good security with:
  - EAP-TLS or PEAP-EAP-TLS with digital certificates stored on the clients
  - PEAP-EAP-TLS improves EAP-TLS as it goes further to encrypt client digital certificate information, but risk of incompatibility with some older supplicants

EAP Methods

Many methods on top of the 5 Wi-Fi certified

- Good security with:
  - PEAP (Protected EAP) encapsulating MSCHAPv2
    - Server Side Digital Certificate and a Client Side Username/Password
  - TTLS (Tunneled Transport Layer Security) encapsulating MSCHAPv2
    - A little better as username not in clear text.
  - Compare it with Cisco's LEAP and its MSCHAPv2 session in clear ⇒offline dictionary attacks
  - Needs to implement a RADIUS Authentication Server. (but hostapd...)
- Very good security with:
  - EAP-TLS or PEAP-EAP-TLS with digital certificates stored on the clients
  - PEAP-EAP-TLS improves EAP-TLS as it goes further to encrypt client digital certificate information, but risk of incompatibility with some older supplicants

Outline

Need for easy setup

- Wireless is not "plug and play"
  - Where to connect to?
  - Security bootstrap: distribution of the keys
- People expect setup of a Home Network and addition of devices to be easy, but till now...
  - High product return rates and support calls
  - For the others, up to 80% run without even WEP

Good security is technically feasible, but it has to be easy to install otherwise a majority won't use it.

Secure and easy setup

Numerous proprietary attempts, among others:

- Button-press
  - Broadcom Secure Easy Setup (SES)
  - Buffalo AirStation One-Touch Secure Setup (AOSS)
- LED-blinking + Passphrase
  - Atheros Jumpstart
- USB
  - Windows Connect Now (WCN)

Not obvious to be secure *and* easy to use while being non PC-centric, cost-effective, etc!

Secure and easy setup

Numerous proprietary attempts, among others:

- Button-press
  - Broadcom Secure Easy Setup (SES)
  - Buffalo AirStation One-Touch Secure Setup (AOSS)
- LED-blinking + Passphrase
  - Atheros Jumpstart
- USB
  - Windows Connect Now (WCN)

Not obvious to be secure *and* easy to use while being non PC-centric, cost-effective, etc!

Secure and easy setup

Numerous proprietary attempts, among others:

- Button-press
  - Broadcom Secure Easy Setup (SES)
  - Buffalo AirStation One-Touch Secure Setup (AOSS)
- LED-blinking + Passphrase
  - Atheros Jumpstart
- USB
  - Windows Connect Now (WCN)

Not obvious to be secure *and* easy to use while being non PC-centric, cost-effective, etc!

Secure and easy setup

Numerous proprietary attempts, among others:

- Button-press
  - Broadcom Secure Easy Setup (SES)
  - Buffalo AirStation One-Touch Secure Setup (AOSS)
- LED-blinking + Passphrase
  - Atheros Jumpstart
- USB
  - Windows Connect Now (WCN)

Not obvious to be secure *and* easy to use while being non PC-centric, cost-effective, etc!

Secure and easy setup

Easy setup is now a Wi-Fi priority
Dedicated task group in charge of specifying a solution
For the first time, Wi-Fi Alliance has to write a spec by itself

Outline

Multiple PSKs support

Remember the dictionary attack:

- Possible from the 2^{nd} message of the 4-Way Handshake
- This message is the first where one side proves the knowledge of PSK/ PMK (through MIC) to the other side
- This message is sent from the STA to the AP
- The AP is free to "crack" itself STA's PSK!

Multiple PSKs support

Scenario:

- STA wants to join AP
- 1^{st} message from AP: go on...
- 2^{nd} message from STA: includes MIC
- AP tries several PSKs from a "dictionary" of PSKs and checks the corresponding MIC
- If MIC is valid for one of those PSKs, then takes this PSK as STA's PMKand sends 3^{rd} message to STA

We now have a multiple-PSKs system completely transparent to the clients and Wi-Fi compliant!

Multiple PSKs implementations

- Each PSK can be linked to a specific STA (via its MAC-address) on the AP list.
  - From the start (but MAC has to be transferred)
  - After the first successful association
  - Use PMKID?
- HostAP
  - From version 0.3.0 (2004-12-05): added support for multiple WPA pre-shared keys (e.g., one for each client MAC address or keys shared by a group of clients)
  - Proof-of-concept patch available in the mailing list archives: added dynamic support (add/del) for mPSK
  - On a 90MHz Pentium: 1.430 ms to check 1000 PSKs
  - On a 1.4GHz Pentium: 600 ms to check 10.000 PSKs

Multiple PSKs implementations

- Each PSK can be linked to a specific STA (via its MAC-address) on the AP list.
  - From the start (but MAC has to be transferred)
  - After the first successful association
  - Use PMKID?
- HostAP
  - From version 0.3.0 (2004-12-05): added support for multiple WPA pre-shared keys (e.g., one for each client MAC address or keys shared by a group of clients)
  - Proof-of-concept patch available in the mailing list archives: added dynamic support (add/del) for mPSK
  - On a 90MHz Pentium: 1.430 ms to check 1000 PSKs
  - On a 1.4GHz Pentium: 600 ms to check 10.000 PSKs

Bibliography & Resources

- 802.11 Security Articles:
  http://www.wardrive.net/security/links
- 802.11 Security News:
  http://www.wifinetnews.com/archives/cat_security.html
  Occasionally http://blogs.zdnet.com/Ou/
- State-of-the-Art WEP cracking:
  http://securityfocus.com/infocus/1814
  http://securityfocus.com/infocus/1824
- Hacking Techniques in Wireless Networks:
  http://www.cs.wright.edu/~pmateti/InternetSecurity/Lectures/WirelessHacks/Mateti-WirelessHacks.htm
- Wireless LAN security guide:
  http://www.lanarchitect.net/Articles/Wireless/SecurityRating/
- Wikipedia (of course) with among others:
  http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access

The End

Thank you! Questions? EN/FR