802.11 Security

Inaccessible star?

Cédric Blancher & Philippe Teuwen

Research engineer at EADS
NXP Contributor to Wi-Fi Alliance Simple Config Task Groups

October 19
Hack.lu 2006

sid@rstack.org
phil@teuwen.org

Wi-Fi securities and attacks
Dumb security
WEP
WPA
WPA2
Are we safe?
WPA(2) Auth
Overview
WPA-PSK
WPA-EAP
Going further
WPS
mPSKs
Bibliography

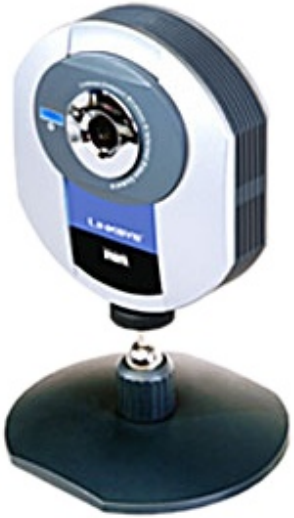
Wireless security is something that most everyone wants, but which few actually use. Barriers to use include throughput loss in older 802.11b products, WEP's ability to be cracked, and difficulty in getting the darned thing working!

tom's networking

Scope: Home Networks, I mean...

sid@rstack.org
phil@teuwen.org

Wi-Fi securities and attacks
Dumb security
WEP
WPA
WPA2
Are we safe?
WPA(2) Auth
Overview
WPA-PSK
WPA-EAP
Going further
WPS
mPSKs
Bibliography



Wi-fi is everywhere

Outline

1. Wi-Fi securities and attacks
   - Dumb security
   - WEP (Wired Equivalent Privacy)
   - WPA (Wi-Fi Protected Access)
   - WPA2
   - Are we safe?
2. WPA(2) Authentication mechanisms
   - Overview
   - WPA-PSK (Pre-Shared Key)
   - WPA-EAP (Extensible Authentication Protocol)
3. Going further for Home Networks
   - WPS
   - mPSKs
4. Bibliography & Resources

sid@rstack.org
phil@teuwen.org

Wi-Fi securities and attacks
Dumb security
WEP
WPA
WPA2
Are we safe?
WPA(2) Auth
Overview
WPA-PSK
WPA-EAP
Going further
WPS
mPSKs
Bibliography

Outline

1. Wi-Fi securities and attacks
   - Dumb security
   - WEP (Wired Equivalent Privacy)
   - WPA (Wi-Fi Protected Access)
   - WPA2
   - Are we safe?
2. WPA(2) Authentication mechanisms
   - Overview
   - WPA-PSK (Pre-Shared Key)
   - WPA-EAP (Extensible Authentication Protocol)
3. Going further for Home Networks
   - WPS
   - mPSKs
4. Bibliography & Resources

sid@rstack.org
phil@teuwen.org

Wi-Fi securities and attacks
Dumb security
WEP
WPA
WPA2
Are we safe?
WPA(2) Auth
Overview
WPA-PSK
WPA-EAP
Going further
WPS
mPSKs
Bibliography

Dumb security: wasting YOUR time

- 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??
- Disable DHCP
  - Observing little traffic is enough to guess all LAN parameters
- Antenna placement
  - Remember, the hacker will always have a bigger one than yours (and for cheaper)

sid@rstack.org
phil@teuwen.org

Wi-Fi securities and attacks
Dumb security
WEP
WPA
WPA2
Are we safe?
WPA(2) Auth
Overview
WPA-PSK
WPA-EAP
Going further
WPS
mPSKs
Bibliography

Dumb security: wasting YOUR time

- 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??
- Disable DHCP
  - Observing little traffic is enough to guess all LAN parameters
- Antenna placement
  - Remember, the hacker will always have a bigger one than yours (and for cheaper)

sid@rstack.org
phil@teuwen.org

Wi-Fi securities and attacks
Dumb security
WEP
WPA
WPA2
Are we safe?
WPA(2) Auth
Overview
WPA-PSK
WPA-EAP
Going further
WPS
mPSKs
Bibliography

Dumb security: wasting YOUR time

- 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??
- Disable DHCP
  - Observing little traffic is enough to guess all LAN parameters
- Antenna placement
  - Remember, the hacker will always have a bigger one than yours (and for cheaper)

sid@rstack.org
phil@teuwen.org

Wi-Fi securities and attacks
Dumb security
WEP
WPA
WPA2
Are we safe?
WPA(2) Auth
Overview
WPA-PSK
WPA-EAP
Going further
WPS
mPSKs
Bibliography

Dumb security: wasting YOUR time

- 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??
- Disable DHCP
  - Observing little traffic is enough to guess all LAN parameters
- Antenna placement
  - Remember, the hacker will always have a bigger one than yours (and for cheaper)

sid@rstack.org
phil@teuwen.org

Wi-Fi securities and attacks
Dumb security
WEP
WPA
WPA2
Are we safe?
WPA(2) Auth
Overview
WPA-PSK
WPA-EAP
Going further
WPS
mPSKs
Bibliography

Dumb security: wasting YOUR time

- 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??
- Disable DHCP
  - Observing little traffic is enough to guess all LAN parameters
- Antenna placement
  - Remember, the hacker will always have a bigger one than yours (and for cheaper)

sid@rstack.org
phil@teuwen.org

Wi-Fi securities and attacks
Dumb security
WEP
WPA
WPA2
Are we safe?
WPA(2) Auth
Overview
WPA-PSK
WPA-EAP
Going further
WPS
mPSKs
Bibliography

Outline

1. Wi-Fi securities and attacks
   - Dumb security
   - WEP (Wired Equivalent Privacy)
   - WPA (Wi-Fi Protected Access)
   - WPA2
   - Are we safe?
2. WPA(2) Authentication mechanisms
   - Overview
   - WPA-PSK (Pre-Shared Key)
   - WPA-EAP (Extensible Authentication Protocol)
3. Going further for Home Networks
   - WPS
   - mPSKs
4. Bibliography & Resources

sid@rstack.org
phil@teuwen.org

Wi-Fi securities and attacks
Dumb security
WEP
WPA
WPA2
Are we safe?
WPA(2) Auth
Overview
WPA-PSK
WPA-EAP
Going further
WPS
mPSKs
Bibliography

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%

sid@rstack.org
phil@teuwen.org

Wi-Fi securities and attacks
Dumb security
WEP
WPA
WPA2
Are we safe?
WPA(2) Auth
Overview
WPA-PSK
WPA-EAP
Going further
WPS
mPSKs
Bibliography

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%

sid@rstack.org
phil@teuwen.org

Wi-Fi securities and attacks
Dumb security
WEP
WPA
WPA2
Are we safe?
WPA(2) Auth
Overview
WPA-PSK
WPA-EAP
Going further
WPS
mPSKs
Bibliography

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

sid@rstack.org
phil@teuwen.org

Wi-Fi securities and attacks
Dumb security
WEP
WPA
WPA2
Are we safe?
WPA(2) Auth
Overview
WPA-PSK
WPA-EAP
Going further
WPS
mPSKs
Bibliography

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

sid@rstack.org
phil@teuwen.org

Wi-Fi securities and attacks
Dumb security
WEP
WPA
WPA2
Are we safe?
WPA(2) Auth
Overview
WPA-PSK
WPA-EAP
Going further
WPS
mPSKs
Bibliography

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

sid@rstack.org
phil@teuwen.org

Wi-Fi securities and attacks
Dumb security
WEP
WPA
WPA2
Are we safe?
WPA(2) Auth
Overview
WPA-PSK
WPA-EAP
Going further
WPS
mPSKs
Bibliography

Active attacks

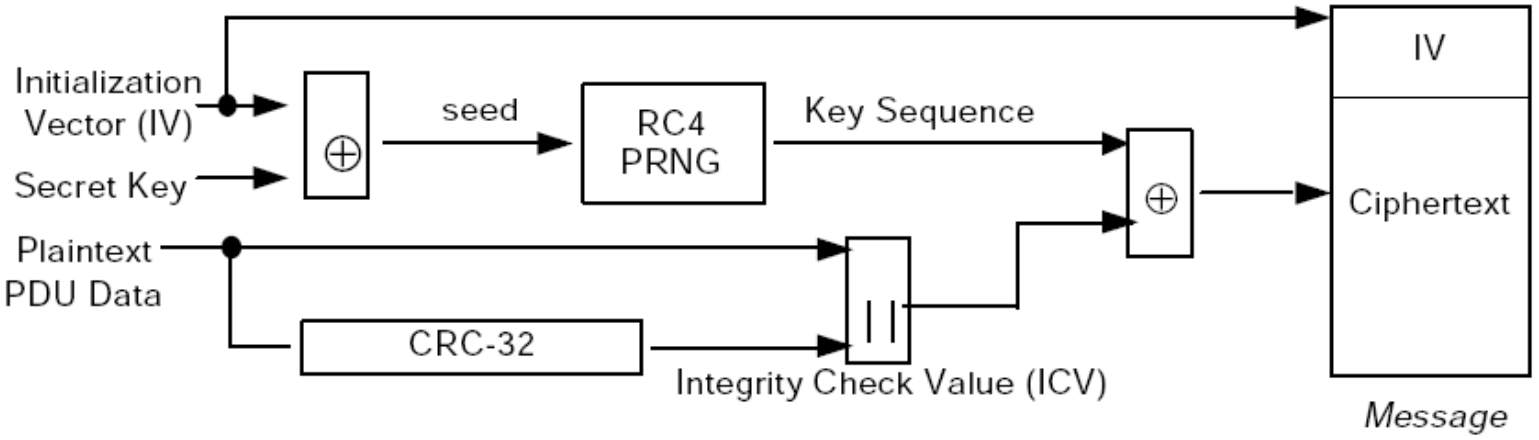
- Replay attacks
  - Goal is to provoke traffic to help data collection
  - WEP: no replay protection, no need to decrypt, nature of packet easily guessable by its length
  - Most obvious: ARP Replay (look for length=68 and dest.addr=ff:ff:ff:ff:ff:ff), this is what **aireplay** does
- Known plaintext 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

sid@rstack.org
phil@teuwen.org

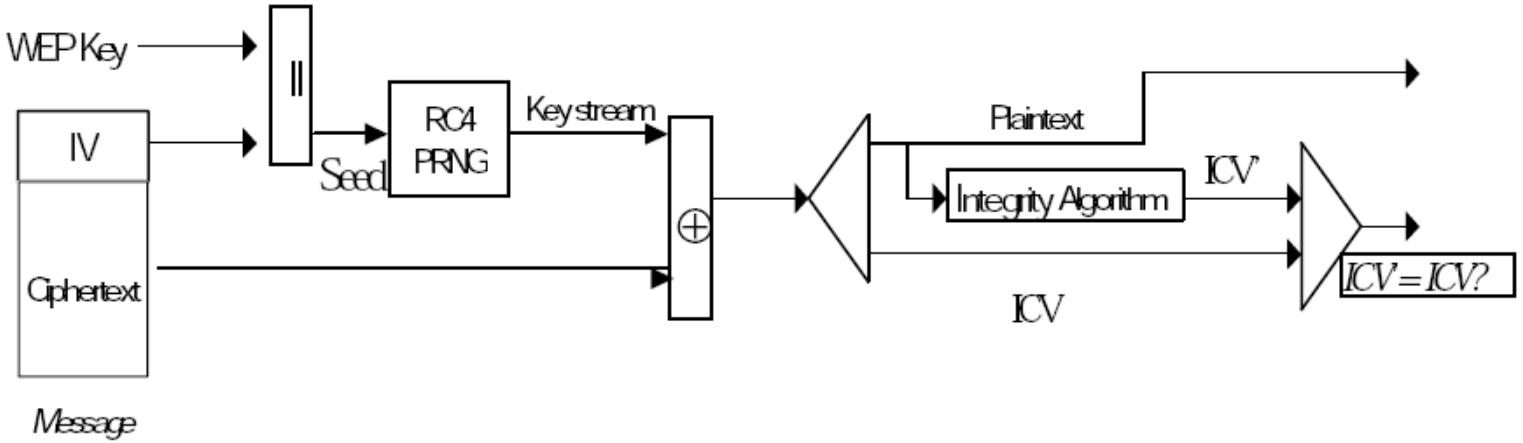
Wi-Fi securities and attacks
Dumb security
WEP
WPA
WPA2
Are we safe?
WPA(2) Auth
Overview
WPA-PSK
WPA-EAP
Going further
WPS
mPSKs
Bibliography

WEP Internals

Bundling:



Unbundling:



Not enough?

New attack based on fragmentation, by Bittau, Handley and Lackey[1]

- Known plaintext attack not that practical
  - Need to recover X bytes to send ≤X-byte long packets
  - We want the keystream faster and more reliably
- Easy guess: first 8 bytes is LLC/SNAP header
  - We can send 4 bytes of data + 4 bytes of CRC, but 4 bytes is even not a complete LLC header :-(
  - Use a 802.11 feature: fragmentation (up to 16) with the same IV/keystream
  - So we can forge arbitrary packets of 4*16=64 bytes after sniffing one single arbitrary packet!
- Decrypt an arbitrary packet?
  - Send the packet over Internet by prepending (in fragments) a new IP header ⇒ decrypt in real-time

[1] The Final Nail in WEP's Coffin http://tapir.cs.ucl.ac.uk/bittau-wep.pdf

Not enough?

New attack based on fragmentation, by Bittau, Handley and Lackey[1]

- Known plaintext attack not that practical
  - Need to recover X bytes to send ≤X-byte long packets
  - We want the keystream faster and more reliably
- Easy guess: first 8 bytes is LLC/SNAP header
  - We can send 4 bytes of data + 4 bytes of CRC, but 4 bytes is even not a complete LLC header :-(
  - Use a 802.11 feature: fragmentation (up to 16) with the same IV/keystream
  - So we can forge arbitrary packets of 4*16=64 bytes after sniffing one single arbitrary packet!
- Decrypt an arbitrary packet?
  - Send the packet over Internet by prepending (in fragments) a new IP header ⇒ decrypt in real-time

[1] The Final Nail in WEP's Coffin `http://tapir.cs.ucl.ac.uk/bittau-wep.pdf`

Not enough?

New attack based on fragmentation, by Bittau, Handley and Lackey[1]

- Known plaintext attack not that practical
  - Need to recover X bytes to send ≤X-byte long packets
  - We want the keystream faster and more reliably
- Easy guess: first 8 bytes is LLC/SNAP header
  - We can send 4 bytes of data + 4 bytes of CRC, but 4 bytes is even not a complete LLC header :-(
  - Use a 802.11 feature: fragmentation (up to 16) with the same IV/keystream
  - So we can forge arbitrary packets of 4*16=64 bytes after sniffing one single arbitrary packet!
- Decrypt an arbitrary packet?
  - Send the packet over Internet by prepending (in fragments) a new IP header ⇒ decrypt in real-time

[1] The Final Nail in WEP's Coffin `http://tapir.cs.ucl.ac.uk/bittau-wep.pdf`

Not enough?

New attack based on fragmentation, by Bittau, Handley and Lackey[1]

- No Internet?
  - Broadcast fragments and listen the reconstruction
    34 fragments later, a new 1500-byte keystream
    We can now forge any arbitrary packet
  - Broadcast the full packet non-fragmented again and again 2^{24}(~16M) times $\Rightarrow$ build a dictionnary
- Specific keystream to break e.g. source IP in an ARP?
  - Inverted Chopchop: 8 bytes, +1, +1...
  - Send the 256 guesses in // with multicast IPs
- Proof-of-concept:
  - **wesside** by A. Bittau makes **aircrack** more powerful

[1] The Final Nail in WEP's Coffin `http://tapir.cs.ucl.ac.uk/bittau-wep.pdf`

sid@rstack.org
phil@teuwen.org

Wi-Fi securities and attacks
Dumb security
WEP
WPA
WPA2
Are we safe?
WPA(2) Auth
Overview
WPA-PSK
WPA-EAP
Going further
WPS
mPSKs
Bibliography

Not enough?

New attack based on fragmentation, by Bittau, Handley and Lackey[1]

- No Internet?
  - Broadcast fragments and listen the reconstruction
    34 fragments later, a new 1500-byte keystream
    We can now forge any arbitrary packet
  - Broadcast the full packet non-fragmented again and again 2^{24} (~16M) times $\Rightarrow$ build a dictionnary
- Specific keystream to break e.g. source IP in an ARP?
  - Inverted Chopchop: 8 bytes, +1, +1...
  - Send the 256 guesses in // with multicast IPs
- Proof-of-concept:
  - **wesside** by A. Bittau makes **aircrack** more powerful

[1] The Final Nail in WEP's Coffin `http://tapir.cs.ucl.ac.uk/bittau-wep.pdf`

sid@rstack.org
phil@teuwen.org

Wi-Fi securities and attacks
Dumb security
WEP
WPA
WPA2
Are we safe?
WPA(2) Auth
Overview
WPA-PSK
WPA-EAP
Going further
WPS
mPSKs
Bibliography

Not enough?

New attack based on fragmentation, by Bittau, Handley and Lackey[1]

- No Internet?
  - Broadcast fragments and listen the reconstruction
    34 fragments later, a new 1500-byte keystream
    We can now forge any arbitrary packet
  - Broadcast the full packet non-fragmented again and again 2^{24} (~16M) times $\Rightarrow$ build a dictionnary
- Specific keystream to break e.g. source IP in an ARP?
  - Inverted Chopchop: 8 bytes, +1, +1...
  - Send the 256 guesses in // with multicast IPs
- Proof-of-concept:
  - **wesside** by A. Bittau makes **aircrack** more powerful

[1] The Final Nail in WEP's Coffin `http://tapir.cs.ucl.ac.uk/bittau-wep.pdf`

Outline

1. Wi-Fi securities and attacks
   - Dumb security
   - WEP (Wired Equivalent Privacy)
   - WPA (Wi-Fi Protected Access)
   - WPA2
   - Are we safe?
2. WPA(2) Authentication mechanisms
   - Overview
   - WPA-PSK (Pre-Shared Key)
   - WPA-EAP (Extensible Authentication Protocol)
3. Going further for Home Networks
   - WPS
   - mPSKs
4. Bibliography & Resources

sid@rstack.org
phil@teuwen.org

Wi-Fi securities and attacks
Dumb security
WEP
WPA
WPA2
Are we safe?
WPA(2) Auth
Overview
WPA-PSK
WPA-EAP
Going further
WPS
mPSKs
Bibliography

WPA TKIP

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

sid@rstack.org
phil@teuwen.org

Wi-Fi securities and attacks
Dumb security
WEP
WPA
WPA2
Are we safe?
WPA(2) Auth
Overview
WPA-PSK
WPA-EAP
Going further
WPS
mPSKs
Bibliography

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 TK
- "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...

sid@rstack.org
phil@teuwen.org

Wi-Fi securities and attacks
Dumb security
WEP
WPA
WPA2
Are we safe?
WPA(2) Auth
Overview
WPA-PSK
WPA-EAP
Going further
WPS
mPSKs
Bibliography

Outline

1. Wi-Fi securities and attacks
   - Dumb security
   - WEP (Wired Equivalent Privacy)
   - WPA (Wi-Fi Protected Access)
   - WPA2
   - Are we safe?
2. WPA(2) Authentication mechanisms
   - Overview
   - WPA-PSK (Pre-Shared Key)
   - WPA-EAP (Extensible Authentication Protocol)
3. Going further for Home Networks
   - WPS
   - mPSKs
4. Bibliography & Resources

sid@rstack.org
phil@teuwen.org

Wi-Fi securities and attacks
Dumb security
WEP
WPA
WPA2
Are we safe?
WPA(2) Auth
Overview
WPA-PSK
WPA-EAP
Going further
WPS
mPSKs
Bibliography

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

sid@rstack.org
phil@teuwen.org

Wi-Fi securities and attacks
Dumb security
WEP
WPA
WPA2
Are we safe?
WPA(2) Auth
Overview
WPA-PSK
WPA-EAP
Going further
WPS
mPSKs
Bibliography

Outline

1. Wi-Fi securities and attacks
   - Dumb security
   - WEP (Wired Equivalent Privacy)
   - WPA (Wi-Fi Protected Access)
   - WPA2
   - Are we safe?
2. WPA(2) Authentication mechanisms
   - Overview
   - WPA-PSK (Pre-Shared Key)
   - WPA-EAP (Extensible Authentication Protocol)
3. Going further for Home Networks
   - WPS
   - mPSKs
4. Bibliography & Resources

sid@rstack.org
phil@teuwen.org

Wi-Fi securities and attacks
Dumb security
WEP
WPA
WPA2
Are we safe?
WPA(2) Auth
Overview
WPA-PSK
WPA-EAP
Going further
WPS
mPSKs
Bibliography

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 (e.g. spoofed Disassociation or Deauthentication frames),
  see airjack and Scapy
- So, still many ways of DoS (jamming, >2007 Assocs, Disassocs, Deauths, PS-Polls)

sid@rstack.org
phil@teuwen.org

Wi-Fi securities and attacks
Dumb security
WEP
WPA
WPA2
Are we safe?
WPA(2) Auth
Overview
WPA-PSK
WPA-EAP
Going further
WPS
mPSKs
Bibliography

Are we safe?

(assuming that WPA2 is bullet-proof)

- Implementation-specific issues
  - Driver fuzzing with Lorcon
  - Black Hat 2006 and ToorCon 2006 demos
  - Intel Centrino vulnerability
  - Apple: 3 vulnerabilities in Airport
  - NDAs, speaches, retractations, where is the fuzz? ;-)
- Other tools
  - pen tool wicrawl

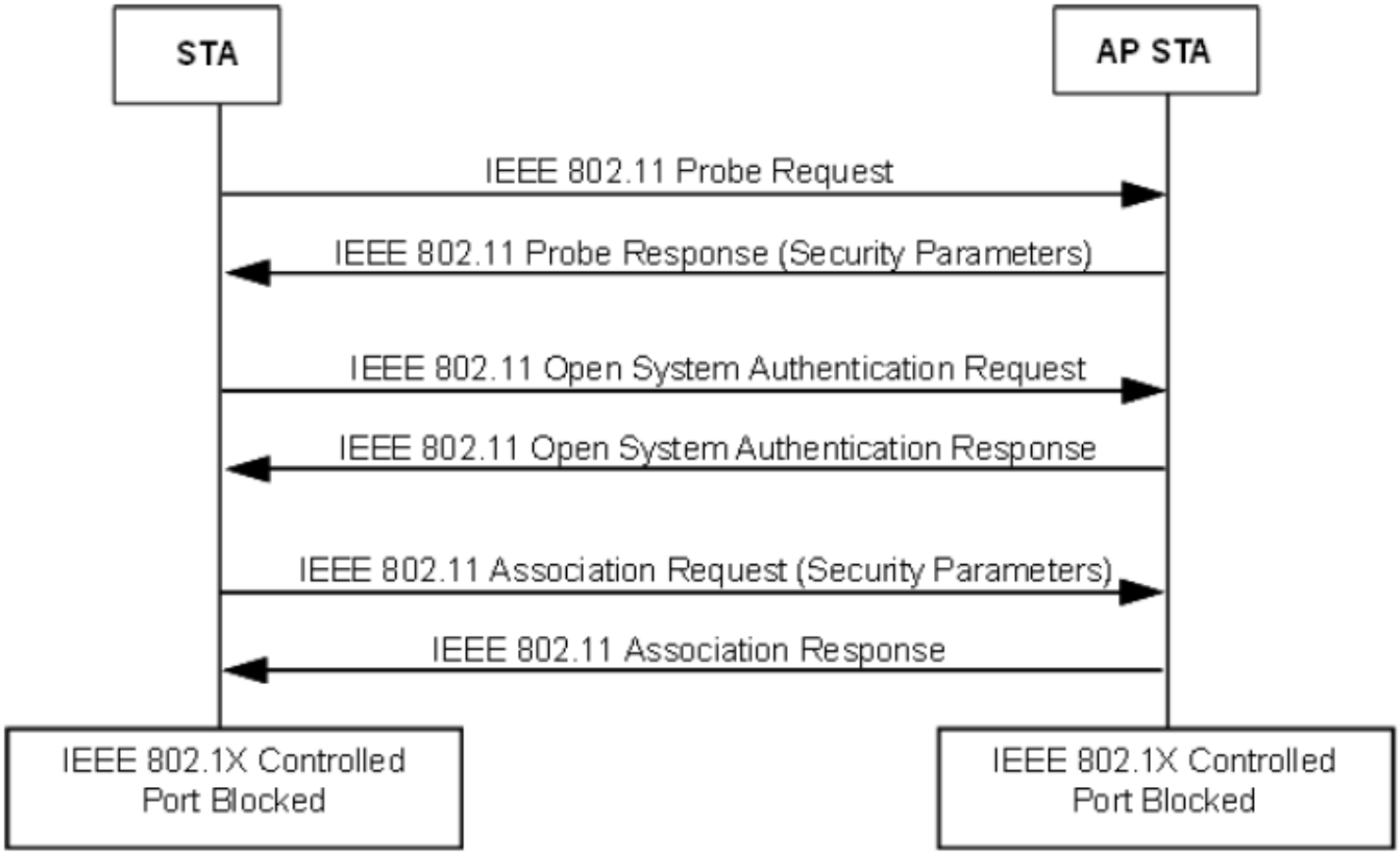
sid@rstack.org
phil@teuwen.org

Wi-Fi securities and attacks
Dumb security
WEP
WPA
WPA2
Are we safe?
WPA(2) Auth
Overview
WPA-PSK
WPA-EAP
Going further
WPS
mPSKs
Bibliography

Outline

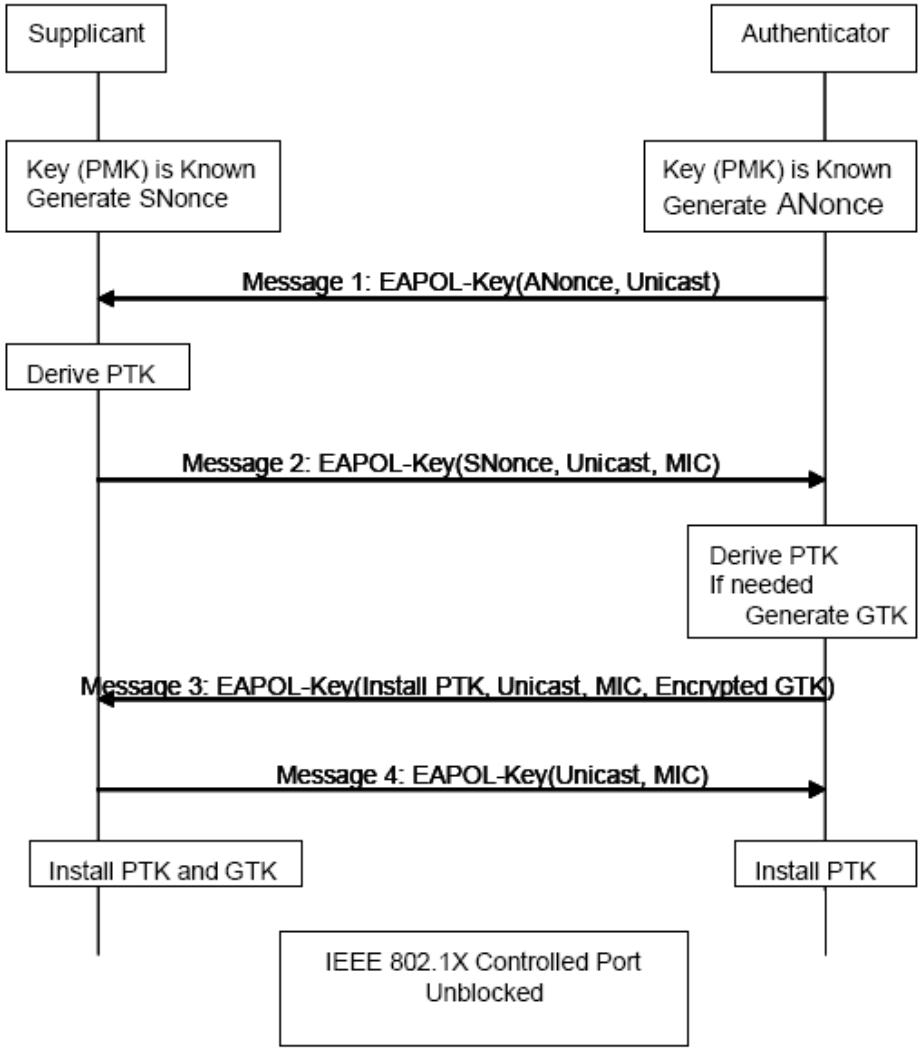
1. Wi-Fi securities and attacks
   - Dumb security
   - WEP (Wired Equivalent Privacy)
   - WPA (Wi-Fi Protected Access)
   - WPA2
   - Are we safe?
2. WPA(2) Authentication mechanisms
   - Overview
   - WPA-PSK (Pre-Shared Key)
   - WPA-EAP (Extensible Authentication Protocol)
3. Going further for Home Networks
   - WPS
   - mPSKs
4. Bibliography & Resources

WPA(2) Authentication



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

WPA(2) 4-Way Handshake



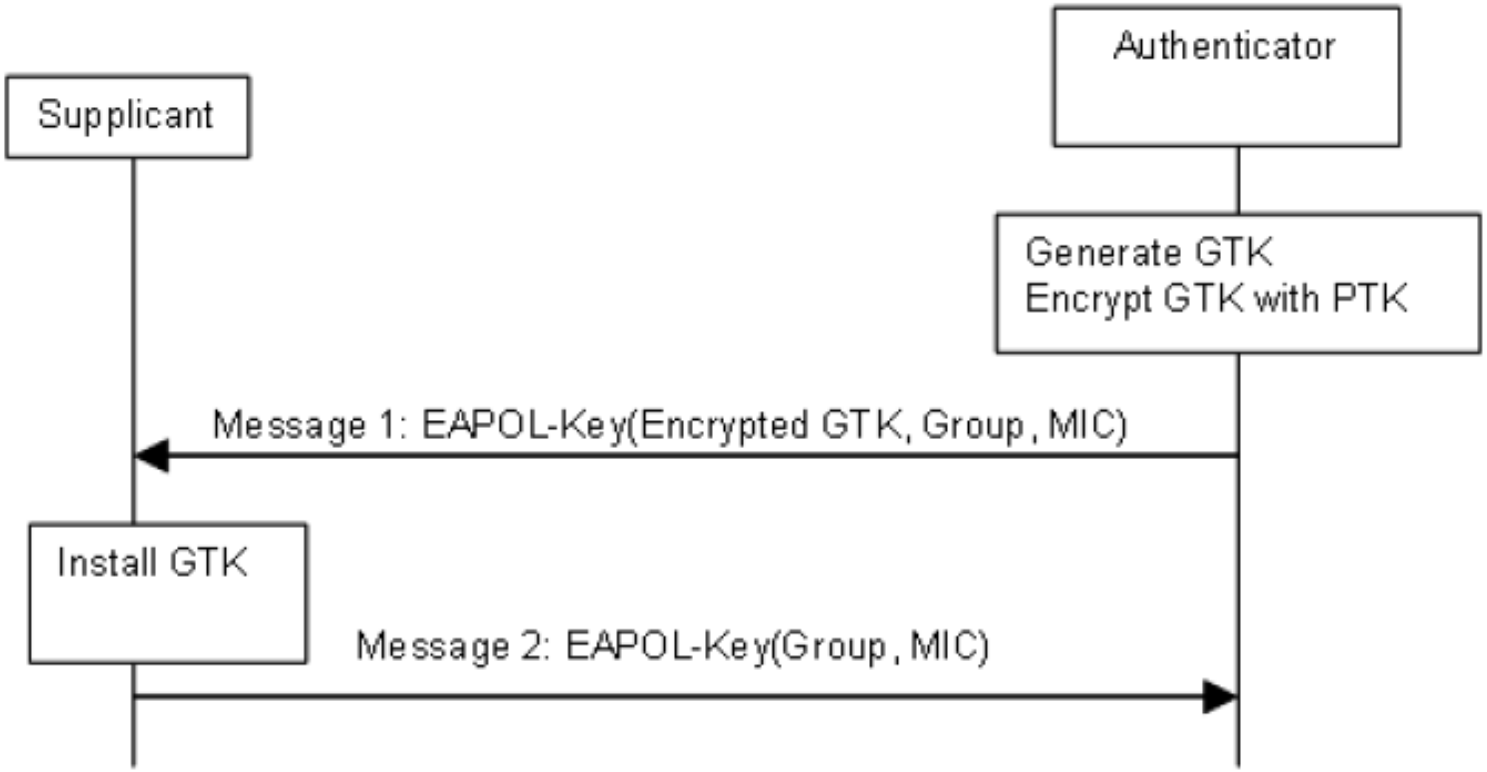
For WPA, group keys are shared in a separate handshake

sid@rstack.org
phil@teuwen.org

Wi-Fi securities and attacks
Dumb security
WEP
WPA
WPA2
Are we safe?
WPA(2) Auth
Overview
WPA-PSK
WPA-EAP
Going further
WPS
mPSKs
Bibliography

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

sid@rstack.org
phil@teuwen.org

Wi-Fi securities and attacks
Dumb security
WEP
WPA
WPA2
Are we safe?
WPA(2) Auth
Overview
WPA-PSK
WPA-EAP
Going further
WPS
mPSKs
Bibliography

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)

sid@rstack.org
phil@teuwen.org

Wi-Fi securities and attacks
Dumb security
WEP
WPA
WPA2
Are we safe?
WPA(2) Auth
Overview
WPA-PSK
WPA-EAP
Going further
WPS
mPSKs
Bibliography

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

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

- 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

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

- 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

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

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

Outline

1. Wi-Fi securities and attacks
   - Dumb security
   - WEP (Wired Equivalent Privacy)
   - WPA (Wi-Fi Protected Access)
   - WPA2
   - Are we safe?
2. WPA(2) Authentication mechanisms
   - Overview
   - WPA-PSK (Pre-Shared Key)
   - WPA-EAP (Extensible Authentication Protocol)
3. Going further for Home Networks
   - WPS
   - mPSKs
4. Bibliography & Resources

sid@rstack.org
phil@teuwen.org

Wi-Fi securities and attacks
Dumb security
WEP
WPA
WPA2
Are we safe?
WPA(2) Auth
Overview
WPA-PSK
WPA-EAP
Going further
WPS
mPSKs
Bibliography

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..63B) or PSK (256b)
- PSK = PBKDF2(passphrase, ssid, ssidlength, 4096, 256)
- PMK ≡ 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
- Dictionary attacks (Cowpatty, WPA Cracker and Aircrack)

passphrase ⇒ PSK ⇒ PMK ⇒ PTK ⇒ MK ⇒ MIC

sid@rstack.org
phil@teuwen.org

Wi-Fi securities and attacks
Dumb security
WEP
WPA
WPA2
Are we safe?
WPA(2) Auth
Overview
WPA-PSK
WPA-EAP
Going further
WPS
mPSKs
Bibliography

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..63B) or PSK (256b)
- $\text{PSK} = \text{PBKDF2}(\text{passphrase}, \text{ssid}, \text{ssidlength}, 4096, 256)$
- $\text{PMK} \equiv \text{PSK}$!!
- 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
- Dictionary attacks (Cowpatty, WPA Cracker and Aircrack)

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

sid@rstack.org
phil@teuwen.org

Wi-Fi securities and attacks
Dumb security
WEP
WPA
WPA2
Are we safe?
WPA(2) Auth
Overview
WPA-PSK
WPA-EAP
Going further
WPS
mPSKs
Bibliography

WPA-Personal

alias WPA-PSK

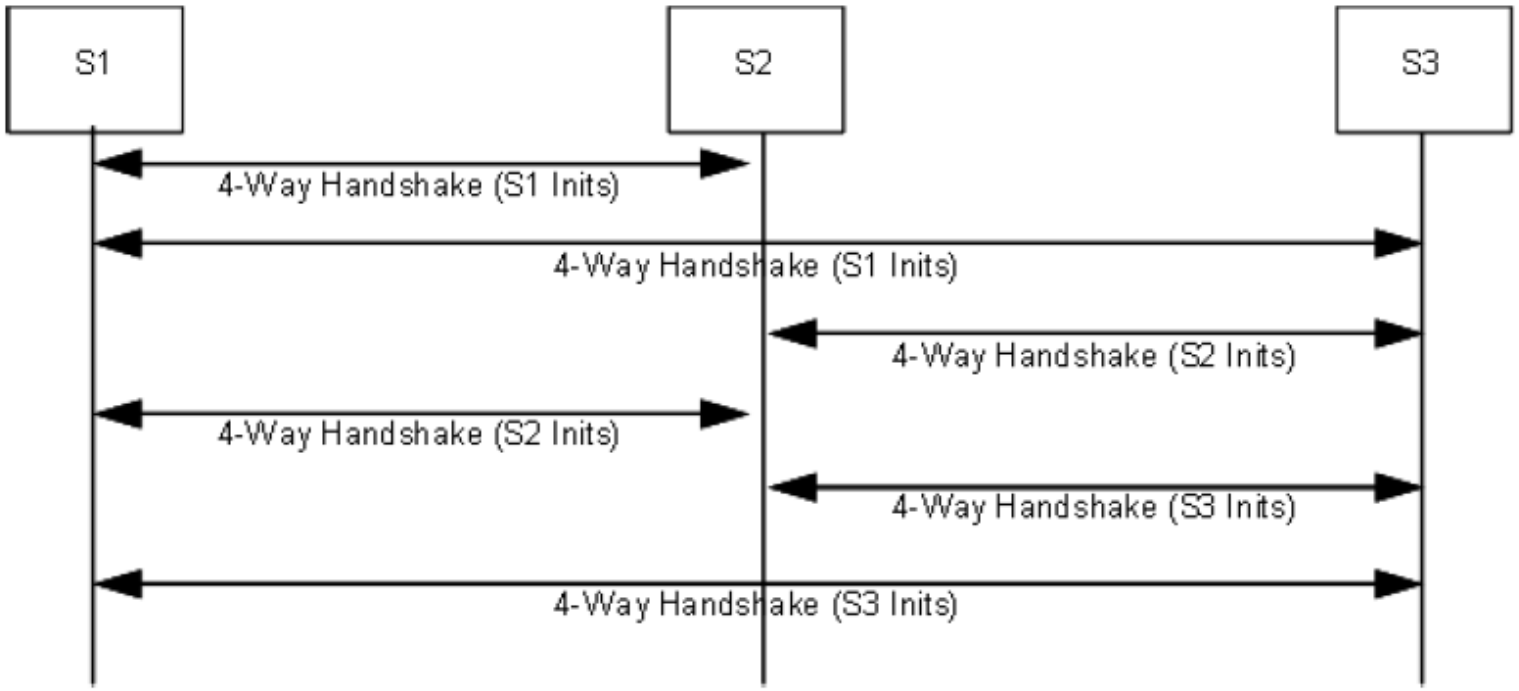
- For those who cannot afford a 802.1X server
- But TinyPEAP and hostapd could change this...
  - *Still relevant for non-PC devices, typically in Home Networks*
- One common passphrase (8..63B) or PSK (256b)
- $\text{PSK} = \text{PBKDF2}(\text{passphrase}, \text{ssid}, \text{ssidlength}, 4096, 256)$
- $\text{PMK} \equiv \text{PSK}$!!
- 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
- Dictionary attacks (Cowpatty, WPA Cracker and Aircrack)

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

sid@rstack.org
phil@teuwen.org

Wi-Fi securities and attacks
Dumb security
WEP
WPA
WPA2
Are we safe?
WPA(2) Auth
Overview
WPA-PSK
WPA-EAP
Going further
WPS
mPSKs
Bibliography

WPA(2) IBSS 4-Way Handshakes



N*(N-1) 4-Way handshakes for N STAs!
Twice more than pairs because each STA propagates its own GTK
Remember, this doesn't prevent any participant to sniff others ;-)

sid@rstack.org
phil@teuwen.org

Wi-Fi securities and attacks
Dumb security
WEP
WPA
WPA2
Are we safe?
WPA(2) Auth
Overview
WPA-PSK
WPA-EAP
Going further
WPS
mPSKs
Bibliography

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...)

sid@rstack.org
phil@teuwen.org

Wi-Fi securities and attacks
Dumb security
WEP
WPA
WPA2
Are we safe?
WPA(2) Auth
Overview
WPA-PSK
WPA-EAP
Going further
WPS
mPSKs
Bibliography

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!

sid@rstack.org
phil@teuwen.org

Wi-Fi securities and attacks
Dumb security
WEP
WPA
WPA2
Are we safe?
WPA(2) Auth
Overview
WPA-PSK
WPA-EAP
Going further
WPS
mPSKs
Bibliography

Outline

1. Wi-Fi securities and attacks
   - Dumb security
   - WEP (Wired Equivalent Privacy)
   - WPA (Wi-Fi Protected Access)
   - WPA2
   - Are we safe?
2. WPA(2) Authentication mechanisms
   - Overview
   - WPA-PSK (Pre-Shared Key)
   - WPA-EAP (Extensible Authentication Protocol)
3. Going further for Home Networks
   - WPS
   - mPSKs
4. Bibliography & Resources

sid@rstack.org
phil@teuwen.org

Wi-Fi securities and attacks
Dumb security
WEP
WPA
WPA2
Are we safe?
WPA(2) Auth
Overview
WPA-PSK
WPA-EAP
Going further
WPS
mPSKs
Bibliography

WPA-Enterprise

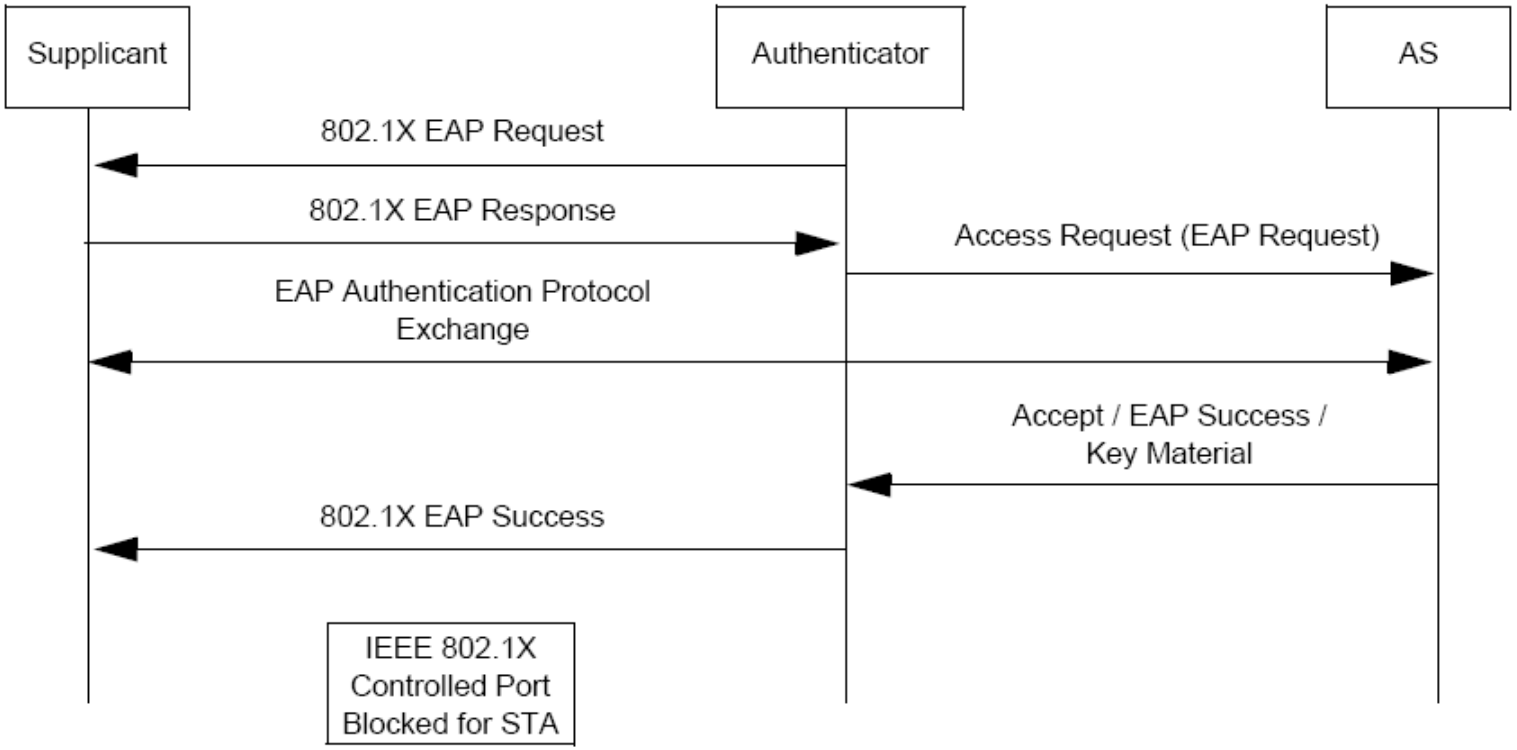
alias WPA-EAP, incl. 802.1X

- 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
- Don't use EAP-LEAP (Cisco) anymore!
  Cf e.g. THC-LEAPcracker and asleap

sid@rstack.org
phil@teuwen.org

Wi-Fi securities and attacks
Dumb security
WEP
WPA
WPA2
Are we safe?
WPA(2) Auth
Overview
WPA-PSK
WPA-EAP
Going further
WPS
mPSKs
Bibliography

WPA(2) EAP Authentication



sid@rstack.org
phil@teuwen.org

Wi-Fi securities and attacks
Dumb security
WEP
WPA
WPA2
Are we safe?
WPA(2) Auth
Overview
WPA-PSK
WPA-EAP
Going further
WPS
mPSKs
Bibliography

EAP Methods

Many methods on top of the 5 Wi-Fi certified ones

- 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.
  - Requires a RADIUS Authentication Server (or 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

sid@rstack.org
phil@teuwen.org

Wi-Fi securities and attacks
Dumb security
WEP
WPA
WPA2
Are we safe?
WPA(2) Auth
Overview
WPA-PSK
WPA-EAP
Going further
WPS
mPSKs
Bibliography

EAP Methods

Many methods on top of the 5 Wi-Fi certified ones

- 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.
  - Requires a RADIUS Authentication Server (or 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

1. Wi-Fi securities and attacks
   - Dumb security
   - WEP (Wired Equivalent Privacy)
   - WPA (Wi-Fi Protected Access)
   - WPA2
   - Are we safe?
2. WPA(2) Authentication mechanisms
   - Overview
   - WPA-PSK (Pre-Shared Key)
   - WPA-EAP (Extensible Authentication Protocol)
3. Going further for Home Networks
   - WPS
   - mPSKs
4. Bibliography & Resources

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.

sid@rstack.org
phil@teuwen.org

Wi-Fi securities and attacks
Dumb security
WEP
WPA
WPA2
Are we safe?
WPA(2) Auth
Overview
WPA-PSK
WPA-EAP
Going further
WPS
mPSKs
Bibliography

Secure and easy setup

Numerous proprietary attempts, among others:

- Push-Button
  - 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 cost-effective, non PC-centric, etc!

sid@rstack.org
phil@teuwen.org

Wi-Fi securities and attacks
Dumb security
WEP
WPA
WPA2
Are we safe?
WPA(2) Auth
Overview
WPA-PSK
WPA-EAP
Going further
WPS
mPSKs
Bibliography

Secure and easy setup

Numerous proprietary attempts, among others:

- Push-Button
  - 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 cost-effective, non PC-centric, etc!

sid@rstack.org
phil@teuwen.org

Wi-Fi securities and attacks
Dumb security
WEP
WPA
WPA2
Are we safe?
WPA(2) Auth
Overview
WPA-PSK
WPA-EAP
Going further
WPS
mPSKs
Bibliography

Secure and easy setup

Numerous proprietary attempts, among others:

- Push-Button
  - 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 cost-effective, non PC-centric, etc!

sid@rstack.org
phil@teuwen.org

Wi-Fi securities and attacks
Dumb security
WEP
WPA
WPA2
Are we safe?
WPA(2) Auth
Overview
WPA-PSK
WPA-EAP
Going further
WPS
mPSKs
Bibliography

Secure and easy setup

Numerous proprietary attempts, among others:

- Push-Button
  - 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 cost-effective, non PC-centric, etc!

sid@rstack.org
phil@teuwen.org

Wi-Fi securities and attacks
Dumb security
WEP
WPA
WPA2
Are we safe?
WPA(2) Auth
Overview
WPA-PSK
WPA-EAP
Going further
WPS
mPSKs
Bibliography

Secure and easy setup

Easy setup is now a Wi-Fi priority
Dedicated Wi-Fi Simple Config Task Groups in charge of specifying a solution
For the first time, Wi-Fi Alliance had to write a spec by itself
You'll hear soon about the new certification program:

Wi-Fi Protected Setup

Under embargo till $6^{th}$of November, 2006, 8 a.m. ET :-(

sid@rstack.org
phil@teuwen.org

Wi-Fi securities and attacks
Dumb security
WEP
WPA
WPA2
Are we safe?
WPA(2) Auth
Overview
WPA-PSK
WPA-EAP
Going further
WPS
mPSKs
Bibliography

Wi-Fi Protected Setup

Already publicly available infos:

- Wi-Fi Alliance®
  - AUSTIN, TEXAS - August 16, 2006 - The Wi-Fi Alliance today announced Wi-Fi Protected Setup™ as the name for its upcoming consumer ease-of-use program, formerly code named "Wi-Fi Simple Config". Slated for launch in Q4 of this year, the program is planned as an optional certification based on a standardized method for security setup in home Wi-Fi networks.
- Google search for "Wi-Fi+Simple+Config" ⇒Intel
  - Linux Reference Implementation under BSD
  - Mention optional NFC method
- DeviceScape
  - Free evaluation copy?
  - Mention PIN & Push-Button method

sid@rstack.org
phil@teuwen.org

Wi-Fi securities and attacks
Dumb security
WEP
WPA
WPA2
Are we safe?
WPA(2) Auth
Overview
WPA-PSK
WPA-EAP
Going further
WPS
mPSKs
Bibliography

Outline

1. Wi-Fi securities and attacks
   - Dumb security
   - WEP (Wired Equivalent Privacy)
   - WPA (Wi-Fi Protected Access)
   - WPA2
   - Are we safe?
2. WPA(2) Authentication mechanisms
   - Overview
   - WPA-PSK (Pre-Shared Key)
   - WPA-EAP (Extensible Authentication Protocol)
3. Going further for Home Networks
   - WPS
   - mPSKs
4. Bibliography & Resources

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!

sid@rstack.org
phil@teuwen.org

Wi-Fi securities and attacks
Dumb security
WEP
WPA
WPA2
Are we safe?
WPA(2) Auth
Overview
WPA-PSK
WPA-EAP
Going further
WPS
mPSKs
Bibliography

Multiple PSKs support

Scenario:

- STA wants to join AP
- 1st message from AP: go on...
- 2nd 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 PMK and sends 3rd message to STA

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

sid@rstack.org
phil@teuwen.org

Wi-Fi securities and attacks
Dumb security
WEP
WPA
WPA2
Are we safe?
WPA(2) Auth
Overview
WPA-PSK
WPA-EAP
Going further
WPS
mPSKs
Bibliography

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
- 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

sid@rstack.org
phil@teuwen.org

Wi-Fi securities and attacks
Dumb security
WEP
WPA
WPA2
Are we safe?
WPA(2) Auth
Overview
WPA-PSK
WPA-EAP
Going further
WPS
mPSKs
Bibliography

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
- 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

sid@rstack.org
phil@teuwen.org

Wi-Fi securities and attacks
Dumb security
WEP
WPA
WPA2
Are we safe?
WPA(2) Auth
Overview
WPA-PSK
WPA-EAP
Going further
WPS
mPSKs
Bibliography

Bonus

- Nice attack to extract PSK from a roaming client
  - Sniff and seek a Probe Req from a station (ok we don't know yet if it's for WPA(2)-PSK)
  - Setup RogueAP with this SSID, announce capa WPA(2)
  - Station attemps to connect, run until you get 2^{nd} msg from 4-Way HS
  - We got everything to try to break the passphrase offline
  - Reconduct RogueAP attack with the right PSK

passphrase $\Rightarrow$ PSK $\Rightarrow$ PMK $\Rightarrow$ PTK $\Rightarrow$ MK $\Rightarrow$ MIC

Enhancement for theta44.org 's Karma suite?

sid@rstack.org
phil@teuwen.org

Wi-Fi securities and attacks
Dumb security
WEP
WPA
WPA2
Are we safe?
WPA(2) Auth
Overview
WPA-PSK
WPA-EAP
Going further
WPS
mPSKs
Bibliography

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

Beginner's Guide to Wireless Auditing (driver fuzzing)

http://securityfocus.com/infocus/1877

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

sid@rstack.org
phil@teuwen.org

Wi-Fi securities and attacks
Dumb security
WEP
WPA
WPA2
Are we safe?
WPA(2) Auth
Overview
WPA-PSK
WPA-EAP
Going further
WPS
mPSKs
Bibliography