Wi-Fi Protected Setup

Holy Grail?

Philippe Teuwen

NXP Representative
in Wi-Fi Protected Setup Task Groups of Wi-Fi Alliance

October 18
Hack.lu 2007

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!

By Tim Higgins for tom's networking (01/2004!)

Outline

1. Attacks: any news since hack.lu 2006?
2. A new standard
   - Overview
3. Specification
   - The big lines
   - Core protocol
   - User methods
4. Certification Program
   - Overview
5. Testing
   - Codes
6. Bibliography & Resources

Attacks: any news since hack.lu 2006?

State-of-the-art WEP cracking:

- April 2007: A. **P**yshkin, E. **T**ews and R.-P. **W**einmann publish a paper entitled "Breaking 104 bit WEP in less than 60 seconds" (proof-of-concept: **aircrack-ptw**)
  - Success probability $> 50\%$ for 40.000 frames (95% for 85.000)
  - Now directly available in **aircrack**

State-of-the-art WPA(2) cracking:

- WPA-PSK subject to dictionary attacks (nothing new but...)
- **coWPAtty** now supports rainbow tables
  - ~ 18,000 passphrases per second
  - Example: table available for 170,000 words hashed against the top 1000 most common SSIDs

Attacks: any news since hack.lu 2006?

State-of-the-art WEP cracking:

- April 2007: A. **P**yshkin, E. **T**ews and R.-P. **W**einmann publish a paper entitled "Breaking 104 bit WEP in less than 60 seconds" (proof-of-concept: **aircrack-ptw**)
  - Success probability $>$ 50% for 40.000 frames (95% for 85.000)
  - Now directly available in **aircrack**

State-of-the-art WPA(2) cracking:

- WPA-PSK subject to dictionary attacks (nothing new but...)
- **coWPAtty** now supports rainbow tables
  - ~ 18,000 passphrases per second
  - Example: table available for 170,000 words hashed against the top 1000 most common SSIDs

Outline

A new standard

Wi-Fi Protected Setup

- Wi-Fi Security:
  - 802.11i by IEEE in 2004, (WPA2) mandatory since 2006
    - Good security *IF* set up & *IF* set up properly
    - Not that easy for newbies...
- Wi-Fi Alliance response:
  - New specification for an easy setup
  - New certification program
    - Available since January 2007
    - Optional

In a (small) nutshell

Wi-Fi Protected Setup

- You bought a new Wi-Fi Protected Setup certified device
- The Network detect its presence automatically and prompts you for actionhttp://www.wireshark.org/lists/wireshark-dev/200702/msg00375.html
- You either
  - Read and Type a PIN
  - Push 2 buttons
  - "Touch" the new STA with an element of the Network
  - Plug a USB stick in the STA
- Network name and encryption information are securely transferred to the device

Outline

Specification

- "Freely" available at WFA website for US$ 99
- Extensible framework:
  - One in-band core protocol
  - Four userland methods
- Basic usage models:
  - Configure a new Network
  - Add a device to an existing Network
- Extended usage models:
  - Remove a device, Guest access, Re-keying credentials
  - Adding another AP, changing SSID etc

Outline

3 actors

Core protocol

1. AP
2. Enrollee: a new STA to be enrolled
3. Registrar
   - virtual entity located in AP
     or in any STA of the Network, wired or wireless
   - communicates with AP via UPnP

User interactions at STA and Registrar
rather than STA and AP
No need to climb up to your AP screwed to the ceiling...

EAP-like

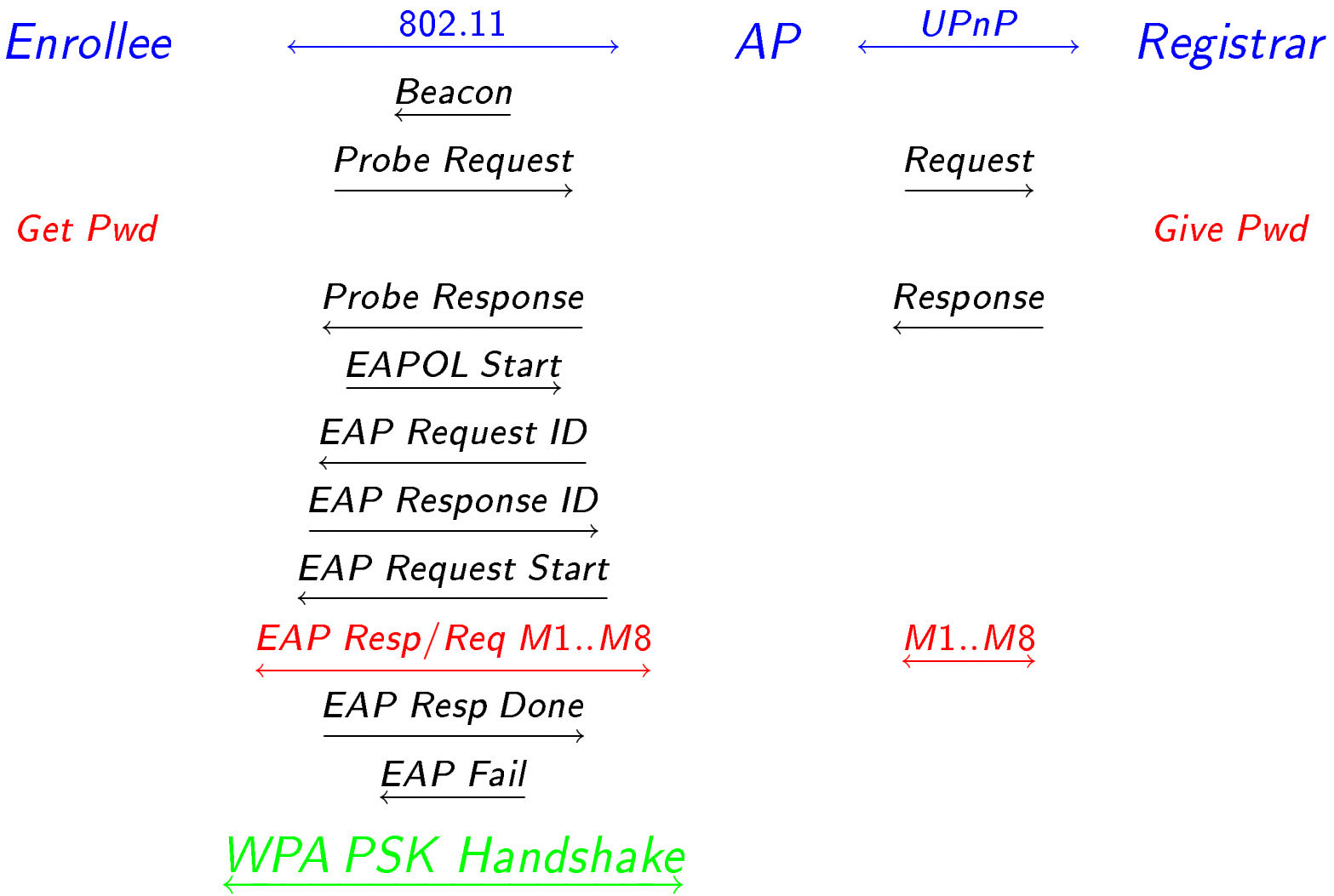
Core protocol

The trick to allow STA-Registrar communication
New pseudo EAP-extension

1. STA initiates WPA-EAP authentication
2. Magic happens
3. Halts on EAP-fail but...
   STA got the WPA-PSK!
4. STA initiates WPA-PSK handshake as usual

EAP-like

Core protocol



Magic happens

Core protocol

- Registrar got STA DevicePassword via userland
- Exchange of DH keys
- Within DH channel
  - Proof of mutual knowledge of the DevicePassword
  - Registrar transmits params to STA

Magic happens

Core protocol

- Enrollee $\longrightarrow$ Registrar:
  $M_1 = Version||N1||Description||PK_E$
- Registrar $\longrightarrow$ Enrollee:
  $M_2 = Version||N1||N2||Description||PK_R||HMAC_{AuthKey}(M_1||M_2^*)$

$PK_E = g^A \bmod p$
$PK_R = g^B \bmod p$
$AuthKey||KeyWrapKey||... =$
$kdf\left(HMAC_{SHA-256(g^{AB} \bmod p)}(N1||EnrolleeMAC||N2), ...\right)$

phil@teuwen.org

Magic happens

Core protocol

- Enrollee $\longrightarrow$ Registrar:
  $M_1 = Version||N1||Description||PK_E$
- Registrar $\longrightarrow$ Enrollee:
  $M_2 = Version||N1||N2||Description||PK_R||HMAC_{AuthKey}(M_1||M_2^*)$

$$PK_E = g^A \bmod p$$
$$PK_R = g^B \bmod p$$
$$AuthKey||KeyWrapKey||... = kdf\left(HMAC_{SHA-256(g^{AB} \bmod p)}(N1||EnrolleeMAC||N2), ...\right)$$

Magic happens

Core protocol

- Enrollee $\longrightarrow$ Registrar:

$$M_3 = Version||N2 ||HMAC_{AuthKey}(ES1||PSK1||PK_E||PK_R) ||HMAC_{AuthKey}(ES2||PSK2||PK_E||PK_R) ||HMAC_{AuthKey}(M_2||M_3^*)$$

  - PSK1 derived from 1^{st} half of DevicePassword
  - PSK2 derived from 2^{nd} half of DevicePassword

- Registrar $\longrightarrow$ Enrollee:

$$M_4 = Version||N1 ||HMAC_{AuthKey}(RS1||PSK1||PK_E||PK_R) ||HMAC_{AuthKey}(RS2||PSK2||PK_E||PK_R) ||ENC_{KeyWrapKey}(RS1) ||HMAC_{AuthKey}(M_3||M_4^*)$$

  - Enrollee can check PSK1 of Registrar

Magic happens

Core protocol

- Enrollee $\longrightarrow$ Registrar:

$$
\begin{aligned}
M_3 = \quad & Version||N2 \\
& ||HMAC_{AuthKey}\,(ES1||PSK1||PK_E||PK_R) \\
& ||HMAC_{AuthKey}\,(ES2||PSK2||PK_E||PK_R) \\
& ||HMAC_{AuthKey}\,(M_2||M_3^*)
\end{aligned}
$$

  - PSK1 derived from 1^{st} half of DevicePassword
  - PSK2 derived from 2^{nd} half of DevicePassword

- Registrar $\longrightarrow$ Enrollee:

$$
\begin{aligned}
M_4 = \quad & Version||N1 \\
& ||HMAC_{AuthKey}\,(RS1||PSK1||PK_E||PK_R) \\
& ||HMAC_{AuthKey}\,(RS2||PSK2||PK_E||PK_R) \\
& ||ENC_{KeyWrapKey}\,(RS1) \\
& ||HMAC_{AuthKey}\,(M_3||M_4^*)
\end{aligned}
$$

  - Enrollee can check PSK1 of Registrar

Magic happens

Core protocol

- Enrollee $\longrightarrow$ Registrar:

$$M_5 = Version||N2 \\ ||ENC_{KeyWrapKey}(ES1) \\ ||HMAC_{AuthKey}(M_4||M_5^*)$$

  - Registrar can check PSK1 of Enrollee

- Registrar $\longrightarrow$ Enrollee:

$$M_6 = Version||N1 \\ ||ENC_{KeyWrapKey}(RS2) \\ ||HMAC_{AuthKey}(M_5||M_6^*)$$

  - Enrollee can check PSK2 of Registrar

Magic happens

Core protocol

- Enrollee $\longrightarrow$ Registrar:

  $M_5 = Version||N2 ||ENC_{KeyWrapKey}(ES1) ||HMAC_{AuthKey}(M_4||M_5^*)$

  - Registrar can check PSK1 of Enrollee

- Registrar $\longrightarrow$ Enrollee:

  $M_6 = Version||N1 ||ENC_{KeyWrapKey}(RS2) ||HMAC_{AuthKey}(M_5||M_6^*)$

  - Enrollee can check PSK2 of Registrar

Magic happens

Core protocol

- Enrollee $\longrightarrow$ Registrar:

$$M_7 = Version||N2 \\ ||ENC_{KeyWrapKey}(ES2) \\ ||HMAC_{AuthKey}(M_6||M_7^*)$$

  - Registrar can check PSK2 of Enrollee

- Registrar $\longrightarrow$ Enrollee:

$$M_8 = Version||N1 \\ ||ENC_{KeyWrapKey}(ConfigData) \\ ||HMAC_{AuthKey}(M_7||M_8^*)$$

Magic happens

Core protocol

- Enrollee $\longrightarrow$ Registrar:

  $M_7 = Version||N2 ||ENC_{KeyWrapKey}(ES2) ||HMAC_{AuthKey}(M_6||M_7^*)$

  - Registrar can check PSK2 of Enrollee

- Registrar $\longrightarrow$ Enrollee:

  $M_8 = Version||N1 ||ENC_{KeyWrapKey}(ConfigData) ||HMAC_{AuthKey}(M_7||M_8^*)$

Outline

PIN method

Userland

1. STA displays 8-digit random PIN, freshly generated
2. User types the PIN on the Registrar

- Mandatory method of the specification
- Still ok if 4-digit PIN (for small LCD screen)
- If no display, static 8-digit PIN on a label

PIN needs to be fresh!

possibility for 3-round attack

PIN method

Userland

1. STA displays 8-digit random PIN, freshly generated
2. User types the PIN on the Registrar

- Mandatory method of the specification
- Still ok if 4-digit PIN (for small LCD screen)
- If no display, static 8-digit PIN on a label

PIN needs to be fresh!

possibility for 3-round attack

PIN method

Userland

1. STA displays 8-digit random PIN, freshly generated
2. User types the PIN on the Registrar

- Mandatory method of the specification
- Still ok if 4-digit PIN (for small LCD screen)
- If no display, static 8-digit PIN on a label

PIN needs to be fresh!

possibility for 3-round attack

Push-Button method

Userland

1. User pushes STA button
2. User pushes AP button

- Behind the scene: as if PIN=00000000
- "Some" provisions to avoid X-Mas attacks

Push & Pray...

Very dependent on actual implementation & circumstances
Probably the most popular method for newbies
Probably the most interesting method for hackers ;-)

Push-Button method

Userland

1. User pushes STA button
2. User pushes AP button

- Behind the scene: as if PIN=00000000
- "Some" provisions to avoid X-Mas attacks

Push & Pray...

Very dependent on actual implementation & circumstances
Probably the most popular method for newbies
Probably the most interesting method for hackers ;-)

NFC Password method

Userland

1. User touches Registrar with STA or STA's NFC tag
   - Out-of-band transfer of long PIN & H(Pk)

Registrar could be your next NFC-enabled Wi-Fi cell phone...

The easiest & safest way?

A priori no attack against the Network, even if static PIN

NFC Password method

Userland

1. User touches Registrar with STA or STA's NFC tag
   - Out-of-band transfer of long PIN & H(Pk)

Registrar could be your next NFC-enabled Wi-Fi cell phone...

The easiest & safest way?

A priori no attack against the Network, even if static PIN

NFC Config method

Userland

1. User touches STA with Registrar or Network's NFC tag
   - No use of the in-band core protocol,
     simple out-of-band transfer of Wi-Fi credentials

Beware of eavesdropping or reading out of the tag!

Still ok in a Home Networking context:
We trust those who enter our home
But don't take the bus with your Network tag!

Registrar could be your next NFC-enabled cell phone...

NFC Config method

Userland

1. User touches STA with Registrar or Network's NFC tag
   - No use of the in-band core protocol,
     simple out-of-band transfer of Wi-Fi credentials

Beware of eavesdropping or reading out of the tag!

Still ok in a Home Networking context:
We trust those who enter our home
But don't take the bus with your Network tag!

Registrar could be your next NFC-enabled cell phone...

USB method

Userland

- Same Password and Config modes as for NFC, with a USB memory stick

Beware of USB stick reuse!

Possible memory dump forensics if the stick was used to transfer directly the Wi-Fi settings

Initial setup

Configure Network and add external Registrar

- By default, SSID and WPA-PSK randomly generated
- Adding a wireless external Registrar:
  - Like adding a STA but the way around: we're adding an AP to the Registrar
  - Type AP PIN into the Registrar
- Adding a wired external Registrar:
  - Short UPnP handshake
- Several external Registrars allowed
- Registrar capability support optional for STAs (minimum requirement: numeric keypad)

Outline

Certification Program

- A Test Plan covering only the basic scenarios: new Network, add Registrars and STAs
- PIN method mandatory
- Push-Button method
  - optional for STAs
  - mandatory for APs (for their internal Registrar)
- (soon) NFC method optional
- External Registrar capability optional for STAs
- Visual identifier:

- Today, 139 products certified since January 2007

Outline

Codes

What googling could lead to?

- Wi-Fi Simple Config (WSC) by Intel
  - Linux Reference Implementation
  - BSD license
- SAICE Corporation bootable CD
  - Testing purpose, no support
  - WPS test application
  - Wireshark with WPS parsing
  - Available source codes & patches
- Devicescape Agent WPS
  - Free evaluation copy?
- Wireshark patch to parse WPS elements (IE & EAP)

Are we completely safe?

Just a rehearsal from hack.lu 2006

- Management frames (SSID, src and dst MAC-addresses)
- Sent in clear $\longrightarrow$ spoofable
  (e.g. spoofed Disassociation or Deauth frames),
  see airjack and Scapy
- Many ways of DoS
  (jamming, >2007 Assocs, Disassocs, Deauths,...)
- Implementation-specific issues
  (driver fuzzing with Lorcon)

Bibliography & Resources

State-of-the-Art WEP cracking

http://eprint.iacr.org/2007/120

CoWPAtty 4.0

http://www.churchofwifi.org/Project_index.asp

WPA-PSK Rainbow Tables

http://www.renderlab.net/projects/WPA-tables/

SAICE Wi-Fi Protected Setup Software Download

https://www.saice-wpsnfc.bz

Wikipedia and link to Wi-Fi Alliance WPS page

http://en.wikipedia.org/wiki/Wi-Fi_Protected_Setup

Wi-Fi Simple Config (WSC) Linux Reference Implementation

http://www.intel.com/cd/ids/developer/asmo-na/eng/247741.htm

Devicescape Agent WPS

http://www.devicescape.com/products/easy_access_landing.php

Wireshark dissector

http://www.wireshark.org/lists/wireshark-dev/200702/msg00375.html

The End

Thank you! Questions? EN/FR