Wi-Fi (In)Security
All Your Air Are Belong To…

Raúl Siles
raul@taddong.com
November 16, 2010

TINAPT-TYOANTU-WEP

This Is Not Another Presentation To Tell You Once Again Not To Use WEP
Waka Waka

- **WAKA** (Wi-Fi Access, Kontrol & Attacks)
  - All your air are belong to… ¿?
  - How to enhance your Wi-Fi security posture?
Outline

- “I don’t have any wireless…”
- Wi-Fi signal range
- Open Wi-Fi networks
  - Hotspots & VPNs
- WEP
- WPA(2)-PSK
  - PSK cracking
- WPA(2)/TKIP
- WPA2-Enterprise
- 802.11n
- DoS
- Wi-Fi Alliance Roadmap
- WIDS
  - Forensics, HoneySpot
- Wi-Fi Clients
  - Deficiencies
  - Privacy & targeted attacks
  - PNL, karma & geolocation
  - Wi-Fi drivers
- Wi-Fi Defenses

How relevant Wi-Fi connectivity is for your business today?
How to enhance your Wi-Fi security posture?

- Network architecture (basic security principles…)
  - Defense-in-depth, layered architecture, inbound & outbound filtering, WLAN isolated segment, layer-2 isolation & controls, assessments…

- Wi-Fi infrastructure
  ★ Technology
    - 802.11, WPA2, 802.1x, EAP, RADIUS…
  - Controllers and APs
  ★ Wi-Fi intrusion detection (WIDS)
  ★ Wi-Fi (mobile) clients

Wi-Fi Technologies
“I don’t have any wireless…”

Are You Sure?

• Your policy says so…
  … but what is the reality?
• “Authorized” devices:
  – Desktops, laptops, mobile devices…
  – Missconfigured AP’s or controllers
• Rogue devices (AP’s & clients)
• Real-world visibility: Wi-Fi assessments
  – Even in PCI DSS Wireless Guideline (quarterly)

Same scenario with “I only have WPA2-Enterprise…”
Rogue Devices

- The traditional cheap AP
  - Productivity and flexibility
- Wi-Fi clients acting as APs (& adhoc)
  - Soft or virtual APs, in mobile devices too!
  - Linux & Mac OS X (they are Unix… ah!)
  - Windows 7: Wireless Hosted Net (WPA2-PSK/AES)
    - AP and STA roles simultaneously
    - Enterprise security posture (new entry points)
    - Daily feature and threat perception

```cmd
netsh wlan set hostednetwork mode=allow ssid=linksys key=...
```
Where Does My Signal Go?

- Evaluate where your network is visible from? (sniffing, injection & assoc.)
  - Where is the attacker located? “Parking”
- Shared facilities and out to the street
- **Wi-Fi Signal Assessments**
- Adjust TX power and antennas
- What’s the maximum distance for a bidirectional 802.11b network?
  - World record 😊

Defcon 13: WiFi Shootout 2005
(802.11b distance record)

124.9 miles
200.96 Km

New records in 2007, but it made the point !!!!

www.wifi-shootout.com
Defcon WiFi Shootout 2005
(Line of Sight (LoS) limitation)

• How far is the horizon?

• Distance to the horizon in nautical miles = 1.17 times the square root of your height of eye (above the surface of the water - ft)
• Distance = 1.17 × √h(src) + 1.17 × √h(dst)
• A nautical mile is 1.15 miles = 1.85 km

http://www.boatsafe.com/kids/distance.htm

Defcon WiFi Shootout 2005
(Orography)

Las Vegas: ≈ 7716 ft (2352 m)
St. George: ≈ 4800 ft (1463 m)
Free Wi-Fi HotSpots

Open Wi-Fi Networks

- Internet everywhere (can not live w/o it)
- You don’t have an open network in your infrastructure but what about your users…
  - … & What about the “guest” Wi-Fi network?
- Traffic capture (Confidentiality)
  - “I’m just accessing public info…”
- Traffic manipulation (GAME OVER!)
Firesheep

- HTTP session hijacking (Sidejacking)
- Firefox add-on (>= 3.6.10) + Winpcap
  - Eric Butler & Ian Gallagher
  - Windows & Mac OS X (& Linux in the future)
  - October 2010 - ToorCon 12 (not new but…)
- Unencrypted web-apps (auth is not enough) on unsecure/open Wi-Fi networks (hub)
  - Facebook, Twitter, Dropbox, Wordpress…
- BlackSheep: detect Firesheep

http://codebutler.com/firesheep
http://www.zscaler.com/blacksheep.html

Firesheep in Action
Airpwn

- Defcon 12 (2004) by Toast (LORCON(2))
- Airpwn: Content Injection (∼ HTTP)
  - Open & WEP networks
  - Man-in-the-Air (MitA): race condition (win)
  - Any unencrypted content
  - XSS + CSRF (+ BeEF + Metasploit)
    - Client vulnerabilities (web browser & plug-ins)
  - Software updates (Ippon – Defcon 17, 2009)
- Clients switching from secure to insecure networks all the time

http://airpwn.sourceforge.net

Airpwn in 2010

- Airpwn-MSF
  - State retained across security boundaries
    - Web browser caching mechanism
    - “RFC 1918 blues” (Robert Hansen)
  - Malicious web content (JS) injected, cached and (afterwards) reloaded from local cache
    - Persistent attacks (“Cache-control” & “Expires”)
  - Full HTTP headers + DOM control (stager)
    - Single HTTP request/response (no HTTPS)

“Wi-Fi Security… Depression…”
BlackHat DC 2010 – Mike Kershaw
Wi-Fi & VPN

• VPN in the hands of the user (timing)
  – IPSec, SSL, SSH…
• Layer-2 authentication & encryption?
• Is the VPN connection established? (DoS)
• Common Wi-Fi hotspot setup (open net)
  – Web-based captive portal page (HTTP)
  – HTTP exploitation (pre-VPN)
  – Layer 2/3: ARP, DHCP & DNS spoofing/poisoning

The “Future” of Hotspots

• WPA2-Enterprise
• Same username/password (shared)
  – ! crypto keys per-user OR
  – Create guest accounts on demand (expiration)
• Digital certificate validation
  – Custom CA (up to the user) 😐
  – Public CA (attacker gets another cert from the same CA) 😐
  – Manual digital certificate fingerprint verification
WEP

- Wired Equivalent Privacy (WEP)
  - Decryption & full access to network
  - User awareness: false sense of security… (key)

- You don’t have WEP in your infrastructure but what about your users… (CEO)
- We learned lots of lessons… or not?
  - We need to learn from the past
- “Hello… Telecom Service Providers”
  - SOHO: Still the case nowadays 😊

Legacy devices: Wi-Fi credit card readers, VoIP phones, handhelds…

WEP Timeline


802.11a
802.11b
1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010

(WPA-PSK)

Sophisticated attacks tools + WEP chop-chop

PTW (< 60 secs)
2007-04-01

WEP cloacking Caffe-latte...
WPA(2)-PSK (1)

- Easy of use & setup (≈ WEP)
- Pre-**Shared** Key (PSK)
- Something shared… it’s not secret!
  - Open, WEP & WPA(2)-PSK
- Key length: >= 8 chars; +20 chars in spec
- PMK (master key) derived from PSK
  - SSID acting as a seed + computationally high
  
  \[ PMK = PBKDF2(PSK, SSID + length, 4096\text{ HMAC-SHA1}) \]

WPA(2)-PSK (2)

- Per-user keys accessible to any user sharing PSK if the 4-way handshake is captured
  
  \[ PTK = \text{Derived\_from}(PMK, \text{@AP, @STA, Apn, STAn}) \]

- Vendors & Service providers: WPA(2)-PSK
  - SSID (follows a well-known pattern)
  - WPA key derived from SSID (e.g. MiFi Verizon)
    - Obscure algorithms (discovered by the community)
  - WPA key derived from XX and MAC (e.g. WLAN_XX)
  - Eases process & allows brute-force (Rainbowtables)
WPA(2)-PSK Handshake Details

• Gathering the WPA(2)-PSK handshake
  – Only two packets are required (“-2”) vs. 4-way
  – Client attacks (out of range of target network)

Cowpatty (>= 4.5)

http://www.willhackforsushi.com/?p=284

WPA(2)-PSK Rainbow Tables

• Church Of Wifi rainbow tables
  – 1000 most popular SSID’s (Wigle)
  – 1 million word dictionary
    • Real passwords from Mark Burnett & Kevin Mitnick
      plus other dictionary words (processed)
  – 40 GB rainbow tables
• FPGA’s (3 days x 15 arrays) & coWPAtty
• Torrent (a must for any serious pen-tester)

http://www.churchofwifi.org/Project_Display.asp?PID=90
WPA(2)-PSK Cracking

- Enhancing the cracking speed by HW
- NVIDIA GPUs (CUDA technology) + ATI
  - October 2008
  - Up to 10K times faster than CPU
  - Multi GPU
- Patent-pending product
- Still based on the quality of dictionaries
  - Variations, combinations, permutations...

http://www.elcomsoft.com/ewsa.html

WPA(2)-PSK Cracking by Numbers

Latest NVIDIA’s boards (Fermi chipset) missing, e.g. NVIDIA Tesla S2050/S2070, claimed to surpass everything before, in late 2010.
WPA Cracker (1)

- “In the cloud” WPA(2)-PSK cracking
- For pen-testers and security auditors or…
- Dictionary attacks (custom. for WPA)
- 400 CPU cluster & 136 million word dict.
- 5 days to 20 minutes for $35 (ratio 1:360)
  - $17 half-cluster
- Dictionaries: (digits: [0-9]{8} – 100 million)
  - English (new 284M – $40 - 55min) & German

http://www.wpacracker.com

WPA Cracker (2)

- PCAP: WPA 4-way handshake (<10MB) + beacon frame
  - SSID (≈ ESSID)
  - E-mail address
- Similar service: Recover WPA (by e-mail)
  - For free (you pay only if key is found): £15
  - From 100-200 million words (English)
  - 5 mins – 24h (“Powerful Super Computer”)
  - Advanced: 700M (or your own dict) + fee £5

http://www.recoverwpa.com
WPA(2)/TKIP - Enterprise/PSK

- TKIP: Temporary solution (5-years) – 2003
- TKIP + WMM (QoS, .11e) = Built-in DoS
  - Vulnerability in the replay protection
  - Michael MIC failures
- TKIP chop-chop attack (CRC-32) – Nov’08/Aug’09
  - Perhaps, the start of a new era…
  - Decrypt traffic from AP to STA
  - Mic failure = knowledge of one new byte
  - ARP packet in 14-17 mins
  - Inject packets (<= 7)
  

WPA2-Enterprise

- WPA2/AES-CCMP + 802.1x/EAP
- Per-user:
  - Mutual authentication (x509 digital certs)
  - Traffic segregation (crypto keys)
  - Replay protection (data frames)
  - Strong data protection (AES-CCMP)
- Authentication based on user credentials…
- Proprietary inter-client protections (L2)
  - Doesn’t work against direct injection
WPA2/EAP Authentication

• Layer-2 network access authentication
  – Wireless: 802.1x + EAP(OL)
  – Wired: RADIUS + EAP
• Supplicant + Authenticator + Auth. server
• Common setup:
  – TLS: requires digital cert on auth. server
  – PEAP (Win - MS-CHAPv2) and TTLS (others)
  – RADIUS HMAC-MD5 on wired side (secret)
• Recommended: EAP-TLS (PKI)

WPA2/EAP Authentication Failures

• Digital certificate validation
  – Misconfigured clients or non-security aware users accepting… invalid certs (CA & CN)
  – Default: verifies CA, prompts user for server (!CN)
  – Any cert from CA (or CAs)
  – User decision!
• Attacker replaces whole setup, same SSID, and gets access to inner authentication
FreeRADIUS-WPE

- RADIUS impersonation vulnerabilities
  - Wireless Pwnage Edition (WPE)
  - Shmoocon 2008 - J. Wright & B. Antoniewicz
  - FreeRADIUS patch to…
  - PEAP/TTLS (Access to inner auth: user/pass)
    - Username + Challenge/Response
    - Fixed challenge (Rainbowtables)
- Deploy securely: Selected CA only, specify CNs of RADIUS servers, ! prompt user

http://www.willhackforsushi.com/?page_id=37

WPA2-Enterprise Hole 196 (1)

- First public vulnerability on WPA2-Enterprise
  - BlackHat & Defcon 2010, MD Sohail Ahmad
- “If something is shared, it is not secret!”
- GTK (Group Temporal Key) shared by all clients
  - Broadcast & multicast traffic
- Injection of such traffic

WPA2-Enterprise Hole 196 (2)

- Insider attack
  - Only legitimate users get the GTK
  - Stealthier MitM attacks (WIDS)
    - ARP poisoning (Can you cope with it nowadays?)
  - Client-based detection (ARP poisoning)
  - Another (new) DoS: increase packet number (PN) field

- Associated research:
  - Layer 3 (IP) unicast packets in layer 2 bcast or mcast
  - One-way attacks on Wi-Fi PSPF (Publicly Secure Packet Forwarding, aka "client isolation")
  - E.g. Windows Vista/7 (TCP)

New 802.11n Risks

- “I want more bandwidth!”
- RF spectrum overlaps: 2.4Ghz & 5 Ghz
  - 20 vs 40 Mhz channels (WIDS)
- 802.11n high-throughput (HT) networks
  - QoS mandatory: !TKIP (not standard but...)
- Signal range increased (MIMO): redesign
- 802.11n HT greenfield mode (vs. mixed mode)
  - WIDS + audit tools?

DoS

- 802.11 management and control frames
  - No authentication, encryption or integrity
- Easy DoS attacks (deauth & disassoc)
- 802.11w (published 2009-09-11)
  - Management frames security (key + MIC)
  - Deauth & disassoc frames only
  - Proprietary solutions (Cisco MFP)
- Physical layer: RF jammer & noise

Wi-Fi Alliance Roadmap:
Looking For a WPA2-only World

- History of Wi-Fi technology availability:
  - WEP since 1999 & TKIP since 2003
- 2011: TKIP not allowed in APs alone (…+AES)
  - WPA2/AES by default (vs. open)
- 2012: TKIP not allowed in STAs
- 2013: WEP not allowed in APs (…still PoS)
- 2014: (Press release?)
  - TKIP+AES not allowed in APs (WPA2/AES only)
  - WEP not allowed in STAs

WEP & TKIP not allowed in Wi-Fi certified devices
So… How 2014 Will Look Like?

- WPA2/AES by default: what is the key?
  - Wi-Fi Protected Set-up (WPS)
    http://www.wi-fi.org/wifi-protected-setup
- What about open networks? Still allowed!!
- Two worlds: Secure and (In)Secure
  - Open vs. WPA2/AES (still with PSK)
- 802.11n: AES only
  - Backward compatibility mode: 802.11g

Wi-Fi Intrusion Detection Systems
WIDS
Wi-Fi Detection

- Wireless Intrusion Detection System (WIDS)
  - 802.11-based attacks (mgmt, control & data)
  - Identify 802.11 layer 1 & 2 malicious activities
  - Locating the culprit (“Where’s Waldo?”)
- Complements your NIDS (TCP/IP-based)
- WIPS?
- Lack of an open-source WIDS 😞
  - “Snort-Wireless”
Do Not Become the Next TJX…

• TJX (2007):
  – One of the biggest thefts of credit card data made public
  – Marshalls department store in St. Paul Minnesota WEP-protected WLAN compromised
  – Initial estimates between 45.7 million and 200 million payment card numbers revealed
  – 451,000 drivers licenses and SS#'s also compromised
  – Forrester Research estimates the cost of the breach could surpass 1 billion dollars in 5 years
  – 8 Gbytes of Internet outbound traffic (info leak) in 7 months
  – Discovered after 1,5 years of 1st attack

Wireless Forensics
Tapping the Air

• How do you manage Wi-Fi security incidents?
  – The nightmare of (legal) Wi-Fi evidence collection
• RF & air modulations
• Multi-channel eavesdropping
• Mobile clients, roaming and signal range
• Amount of captured data (yours/others), performance, GPS, antennas,
• Dealing with encryption + merging/analysis
• Commercial products (15 cards 11b/g + more)

HoneySpot: Wi-Fi Honeypot

• Honeypot + Hotspot = HoneySpot
  – January, 2008 (still work “in-progress” 😃)
• Research the state-of-the-art of real-world wireless attacks
• History, definition, and taxonomy
• Architecture, design, and deployment of wireless honeypots
  – Modules: WC, WAP, WMON, WI, WDA


Wi-Fi Clients
Wi-Fi Client Deficiencies (1)

- What type of network are you connecting too? It has a lock, so it must be secure ;)
  - Mobile devices
    - iPhone
    - Mac OS X (says WEP or WPA before entering key)

Think about other Wi-Fi clients too: printers, VoIP phones, AV…

Wi-Fi Client Deficiencies (2)

- What type of network are you connecting too? It has a lock, so it must be secure ;)
  - Mobile devices
    - Windows Mobile 6.x
    - Windows XP/V/7 provide details in advance
  - Cannot disable connect auto if known net in range

Unless you configure the Wi-Fi network manually
Combining Different Wireless Technologies: WiFi & Bluetooth

- Bluetooth: the address is like a secret
- Wi-Fi: the address is disclosed on every 802.11 packet (even with 802.11i/w)
- Is there any relationship between the Wi-Fi & Bluetooth addresses?
  - Consecutive numbering by the manufacturer
  - An attacker can obtain the “secret” Bluetooth BD_ADDR through Wi-Fi
  - E.g. Probe requests or (switched off) TAD-2010-002 (WM 6.1 & 6.5)

Wi-Fi Privacy and Targeted Client Attacks

- Wi-Fi technology is chatty and commonly tied to the user or personal environment
- How do Wi-Fi clients work? (PNL)
- Wi-Fi clients periodically search for their preferred networks (PNL) by name
- Attacker can eavesdrop Wi-Fi communications looking for unique names
  - Management frames (not encrypted)
- Wi-Fi client & user privacy compromised
Hidden networks and the PNL

• How do Wi-Fi APs work?
• What is more secure?
  1. A hidden or non-broadcasting network
  2. A visible or broadcasting network
• Still a very common best practice for home and business Wi-Fi environments
• What do you want to “protect”?
  – Wi-Fi clients or infrastructure (APs)
• Discovering the undiscoverable 😊

Kismet(-Newcore)
Nowadays, this is the default behavior for main OS:
- Windows XP SP3, Vista & 7
- Mac OS X
- Linux

But what about new players…

PNL on Mobile Devices

- Vulnerability: TAD-2010-003 - Thanks PNL!! 😊
  - Security threat known since 2005
  - Protection in Windows XP since January 2007
  - “Do we learn from the past?”
- High impact & targeted attacks
  - Unique SSID helps to identify the user
  - SSID set could allow fingerprinting the user
  - Targeted and privacy attacks
  - Victim connects to attacker’s Wi-Fi network
- Wi-Fi interface keeps the previous state (turned off)

Karma-like Attacks

- Wi-Fi client(s) asking for known networks?
- “Is <SSID> here?”… Here I am! 😊
  - Mobile: known networks are auto-joined (no option)
- Out of range (or strongest signal wins)
- Karma or airbase-ng
  - WEP key attacks (Caffe-Latte, Hirte, Shared), WPA(2)-PSK key attacks & full fake AP
- The attacker is the network & the Internet
  - Mail servers, web servers & everything
- Karmetasploit: MSF + Karma/Airbase

aircrack-ng.org & http://theta44.org/karma/index.html
TAD-2010-003 & Microsoft

• “However, because of the low severity impact of the information disclosed combined with the fact that the attack would be untargeted (i.e. the attacker cannot force the mobile device to disclose the PNL), Microsoft would not issue a public security update to address this issue.”
• Low severity impact? (attacker & victim sharing layer-2)
• I do not need to force the device to disclose the PNL, it does on its own 😊
• Windows Phone 7 not vulnerable (MS says)
  – “Good” business model
• Let’s see how targeted this can be…

Wi-Fi Client PNL

Nowadays, this is the default and only behavior for main OS connecting to hidden networks:
- Windows XP SP3, Vista & 7
- Mac OS X
- Linux
- Mobile devices
What if I capture this traffic during a flight?
- HTC HD2 (WM 6.5)
Eavesdropping Wi-Fi Network Names (Probe Requests)

Wigle (Wireless Geographic Logging Engine) - Network

SSID: “SX551D84D20”
Where do you live or work (or hang out)?

Mr. iPhone… Where Is My PNL?

- When you connect to a Wi-Fi network it goes into the PNL
- A different story is how it leaves the PNL and how…
- “Forget this Network” only available when in range
  - Go back where the network is! 😊
  - Still on iPhone 3.x, 4.x (2G & 3G)
Google Street View Scandal

“...a mistake...” of the data collection software

Google Street View Summary

- Collecting data while Street View imagery vehicles were cruising streets in +30 countries
  - Improve geo-location database for location-based mobile applications (during 3 years, 600 GB)
- “…entire e-mails and URLs were collected along with some passwords” (3rd-party analysts say)
- Law: Headers or payload? PII?
  - Delete the data or keep it (country-based) or both 😊
- Are you concerned about your open Wi-Fi networks… Google, your neighbor(S) or both?

Google Street View… and more 😊

- What is this data used for? Mobile Apps…
  - Google Geolocation API:
    - HTTP POST + JSON object to REST API
    - Create a script or use a web interface (Samy)

Or, you can simply test the Location by entering a router MAC address:

Do you remember our friend “SX551D84D20”? BSSID = 00-01-e3-d8-4d-20

http://www.samy.pl/mapxss/?mac=00-01-e3-d8-4d-20

Google Geolocation API

[Google Maps image]
Wi-Fi Driver Attacks

- IEEE 802.11 specification
  - 802.11-2007 (1233 pages)
  - 802.11a/b/d/g/h/i/j/e + n (536 pg) + w (111pg)
- Firmware and/or SW implementation
  - Humans make mistakes = vulnerabilities
  - Layer-2 attacks (AP & STA) and ring-0


"You think that’s air you’re breathing now?"

Morpheus to Neo during the scene when he was teaching him in the virtual dojo on board the ship The Nebuchadnezzar
Tools, Tools, and… More Tools
More advanced, easy to use, and damaging

Wi-Fi Defenses
Wi-Fi Technology

- Detect & knock rogue devices
- Limit your signal range
- WPA2-Enterprise (AES-CCMP+EAP/TLS) - !TKIP
  - If WPA2-PSK: random key > 20 chars (63) – shared
  - MAC address filtering (Joe neighbor vs. overload)
- Protect RADIUS traffic (IPSec) + != secrets
- Full client cert validation (EAP) + ! prompt user
  - Strong user credentials
- WIDS + Wi-Fi forensics + new technologies: 11n
- Plan for the worse: DoS backup

Wi-Fi Clients

- Switch off the Wi-Fi interface if not in use
- Do not connect to open/WEP networks
  - VPN and “100% fully” protected clients (HotSpots)
- Manage the Wi-Fi client
  - Avoid automatic connection to known Wi-Fi networks
  - Auto disable if not connection in X sec (mobile)
  - Avoid adhoc (P2P) networks & unknown APs
- Manage the PNL (clean up) – Group Policy
  - Privacy or anonymity attacks & Karma-like attacks
- Update your Wi-Fi drivers & Wi-Fi client application or supplicant (& all client SW)
References

• Taddong’s Blog (Wi-Fi posts)
  – http://blog.taddong.com/search/label/Wi-Fi
• RaDaJo Blog (Wireless posts)
  – http://www.radajo.com/search/label/Wireless
• Raul Siles’ Wi-Fi webpage:
    (I know it needs a few updates… 😊)
• Twitter: @taddong

Questions? 😊