Myths & Truths about WiFi

Asim Jaweesh
Agenda

• History
• Requirements
• Authentication methods
• Breaking authentication
• Protecting yourself
What is Wireless?

• Air as media transmission
• Different standards and technologies
• Affects our life
Myth or Truth?

WEP can protect me
WPA2 is immune to cracking
MAC filtering is applied
Hiding my WiFi name is protection
My neighbor is a good guy :)
Encryption is a good network security
Wireless Family Members

- Wi-Fi
- Bluetooth
- WiMAX
- NFC
War Chalking
Need For Speed

![Graph showing the increase in speed (Mbps) from 1997 to 2015. Key points include IEEE 802.11, 802.11g, and 802.11ac.]
Requirements

Hardware

- WiFi card
- Antenna

Software

- Device Driver
- User application
Authentication

**Wired Equivalent Privacy (WEP)**  1999

**Wireless Protected Access (WPA)**  2003

**Wireless Protected Access 2 (WPA2)**  2004
WEP

Properties
- Uses static key for encryption
- Key size of 40bit or 128bit

Attacks
- Flawed RC4 algorithm
- Fluhrer Mantin Shamir (FMs) 2001
- KoreK & chopchop 2004
- Pyshkin Tews Weinmann (PTW) 2007
- Fragmentation attack
Attack Methods

Passive

Active
Encryption & Decryption Process

Data -> Algorithm -> Cipher

 Encryption  <->  Decryption
Using WEP Encryption

User

Request for Banan WIFI

Response

Encrypted Request

Encrypted Replay

Access point

Static key

Static key
WEP Replay Attack

Attacker

Access point

Encrypted Request

Encrypted Replay

Encrypted Request

Encrypted Replay

Encrypted Replay

Encrypted Replay
My Neighbor is NOT a Good Guy
WPA

Properties
• No Static Key used
• Compatibility
• Limited key length
• Through firmware update

Attacks
• Injection
• Connection hijacking
• WPS brute force
WPA – No Static Keys

User

Access point

Probe Request-Response

Authentication, Association

Dynamic key generated first

Data encrypted with dynamic key
My Neighbor is NOT a Good Guy
WPA2

More secure algorithms
• AES
• CCMP

Attacks
• Same as WPA
• Hole 196
8.5 Keys and key distribution

8.5.1 Key hierarchy

RSNA defines two key hierarchies:

a) Pairwise key hierarchy, to protect unicast traffic
b) GTK, a hierarchy consisting of a single key to protect multicast and broadcast traffic

NOTE—Pairwise key support with TKIP or CCMP allows a receiving STA to detect MAC address spoofing and data forgery. The RSNA architecture binds the transmit and receive addresses to the pairwise key. If an attacker creates an MPDU with the spoofed TA, then the decapsulation procedure at the receiver will generate an error. GTKs do not have this property.
My Neighbor is NOT a Good Guy
Protection

On access point
- If you decide to use WEP, get out
- Just say no to WPA
- Always use WPA2

On clients
- Strong customized passphrase
- Change passphrase regularly
Myth or Truth? Revealed

- WEP can protect me
- WPA2 is immune to cracking
- MAC filtering is applied
- Hiding my WiFi name is protection
- My neighbor is a good guy :)  
- Encryption is a good network security
One more thing...
Cracking without Access Point

Request “Default”
Request “Banan WiFi”
Request “Linksys”
Request “AndroidAP”

Response “Banan WiFi”
Response “Default”
Response “AndroidAP”
Thank You 😊
Asim Jaweesh