Wireless Security

Sheetal Joseph
CISSP, CEH
Tech Mahindra
sheetalj@techmahindra.com

OWASP
22nd September 2008

Copyright © The OWASP Foundation
Permission is granted to copy, distribute and/or modify this document
under the terms of the OWASP License.
Roadmap

- Wireless Overview
- Wireless Security Standards
- Exploiting Wireless Vulnerabilities
- Wireless Best Practices
Wireless - The World of Convenience!

• User mobility
  • Reduced cost
  • Flexibility and convenience
  • Increase the productivity

• Wireless devices use Radio Frequency (RF) technology to facilitate communication.

• Various types of wireless communication solutions use different frequencies, most regulated by governments.
Wireless Standards

- **802.11b** – Transmits at 2.4 GHz, sends data up to 11 Mbps using direct sequence spread spectrum modulation. 100-150 feet range.
- **802.11a** – Transmits at 5 GHz and send data up to 54 Mbps using orthogonal frequency division multiplexing (OFDM). 50-75 feet range. **Not** interoperable is 802.11b.
- **802.11g** – Combines features of both standards (a,b), 2.4 GHz frequency, 54 Mbps Speed, 100-150 feet range and **is** interoperable with 802.11b.
- **802.11i** – Improves WEP encryption by implementing Wi-Fi Protected Access (WPA2). Data encryption with Advanced Encryption Standard (AES).
- **802.11n** – 600 Mbps speed by adding multiple-input multiple-output (MIMO) and Channel-bonding/40 MHz operation to the physical (PHY) layer, and frame aggregation to the MAC layer. 802.11n uses WPA and WPA2 to secure the network.
Latest Wireless Hacks

- Email sent before the Ahmedabad & Delhi bombings sent via a hacked wireless connection

- TJX theft tops 45.6 million card numbers
Types of Attacks

- **Identity theft (MAC spoofing)** - Cracker is able to listen in on network traffic and identify the MAC address of a computer and attack after spoofing the same.

- **Man-in-the-middle attacks** - Cracker entices clients to log into a computer set up as an AP. Once this is done, the hacker connects to a real AP through another wireless card offering a steady flow of traffic.

- **Denial of service** - Cracker continually bombards a targeted AP with bogus requests, premature successful connection messages, failure messages, and/or other commands.
Wireless Security Goals

- **Access Control** - Ensure that your wireless infrastructure is not mis-used. This calls for Efficient Key Management.

- **Data Integrity** - Ensure that your data packets are not modified in transit.

- **Confidentiality** - Ensure that the contents of your wireless traffic is not learned. Proper Encryption mechanisms need to be implemented.
Wireless Security Standards

**802.11i (WPA-2)**
- Will require hardware upgrade
- Uses new cipher (AES)
- Provides final 802.11i standard
- Offers forward compatibility with WPA

**802.11+WPA**
- Uses today’s hardware
- Replaces WEP (but not the cipher)
- Incorporates key features of 802.11i
- Includes firmware upgrade

**802.11i+802.1x**
- Uses today’s hardware
- Adds authentication through software upgrade
- Leverages a RADIUS server with EAP

**802.11 (WEP)**
- Uses today’s hardware
- Offers sufficient security for home use
- Can use proprietary WEP enhancements
- Can be augmented with VPN in enterprise and high-traffic environments
Description of WEP Protocol

WEP relies on a **secret key** (64 bit/128 bit) which is shared between the sender and the receiver.

**SENDER**: Mobile station (e.g., Laptop with a wireless ethernet card)

**RECEIVER**: Access Point (e.g., base station)

- **Secret Key** is used to encrypt packets before they are transmitted
- **Integrity Check** is used to ensure packets are not modified in transit.

The standard does not discuss how shared key is established.

In practice, most installations use a **single key** which is shared between all mobile stations and access points.
CHAP Authentication

Supplicant

Authenticator

username

challenge

response

Accept/reject
How WEP works

IV → key → RC4 → encrypted packet

original unencrypted packet → checksum
Deficiencies of WEP

- IV is too short and not protected from reuse.
- The per packet key is constructed from the IV, making it susceptible to weak key attacks.
- No effective detection of message tampering (message integrity).
- No built-in provision to update the keys in all wireless clients connected to the access point.
- No protection against message replay.
Radius: An additional layer in the security
WPA (Wi-Fi Protected Access)

- IEEE 802.1X authentication server- LEAP, EAP/TLS, PEAP
  or
  PSK (Pre-Shared Key)

- RC4 stream cipher, with a 128-bit key and a 48-bit initialization vector (IV).

- Temporal Key Integrity Protocol (TKIP)

- Message Integrity Code (MIC) Michael to ensure data Integrity
802.1x
- Port-based access control
- Mutual authentication via authentication server

1. Request access
2. Limit access to authentications server
3. Issue challenge
4. Answer challenge
5. Validate response
6. Allow access to network
7. Use other Network devices

Client inaccessible network devices
WPA - PSK

- No RADIUS server required
- A Shared secret key is used.
- That PSK is usually generated by combining the WLAN's name (Service Set Identifier, SSID) with a passphrase (an ASCII string, 8-63 characters.)
- A passphrase less than 64 characters can be insecure
- Management is handled on the AP
  - Vulnerable to dictionary attacks
Temporal Key Integrity Protocol

- Fixes the flaw of key reuse in WEP
- Comprised of three parts, guarantees clients different keys
  - 128-bit temporal key, shared by clients and APs
  - MAC of client
  - 48-bit IV describes packet sequence number
- Increments the value of the IV to ensure every frame has a different value
- Changes temporal keys every 10,000 packets
- Uses RC4 like WEP, so only software or firmware upgrade required
Michael Message Integrity Check (MMIC)

- Message Integrity Code (MIC) - 64-bit message calculated using “Michael” algorithm inserted in TKIP packet to detect content alteration

- Message is concatenated with the secret key and the result is hashed

- Protects both data and header

- Implements a frame counter, which discourages replay attacks
WPA

- Confidentiality: Per-packet keying via TKIP
- Message Authenticity: Michael algorithm
- Access Control and Authentication: IEEE 802.1x - EAP/TLS
Deficiencies of WPA

- **Dictionary Attack on WPA-PSK** - The weak passphrases users typically employ are vulnerable to dictionary attacks.

- **DoS Attacks** - Due to inevitable weaknesses of Michael, TKIP will shut down the network for one minute if two frames are discovered that fail the Michael check after passing all other integrity checks that would have caught noisy frames.
WPA2 – 802.11i

- 802.1x for authentication.

- CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) to provide confidentiality, integrity and origin authentication.

- AES replaces RC4 w/TKIP
# A Comparison

<table>
<thead>
<tr>
<th></th>
<th>WEP</th>
<th>WPA</th>
<th>WPA2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cipher</strong></td>
<td>RC4</td>
<td>RC4</td>
<td>AES</td>
</tr>
<tr>
<td><strong>Key Size</strong></td>
<td>40 bits</td>
<td>128 bits</td>
<td>128 bits</td>
</tr>
<tr>
<td><strong>Key Life</strong></td>
<td>24 bit IV</td>
<td>48 bit IV</td>
<td>48 bit IV</td>
</tr>
<tr>
<td><strong>Packet Key</strong></td>
<td>Concatenated</td>
<td>Mixing Function</td>
<td>Not Needed</td>
</tr>
<tr>
<td><strong>Data Integrity</strong></td>
<td>CRC - 32</td>
<td>Michael</td>
<td>CCM</td>
</tr>
<tr>
<td><strong>Header Integrity</strong></td>
<td>None</td>
<td>Michael</td>
<td>CCM</td>
</tr>
<tr>
<td><strong>Replay Attack</strong></td>
<td>None</td>
<td>IV Sequence</td>
<td>IV Sequence</td>
</tr>
<tr>
<td><strong>Key Management</strong></td>
<td>None</td>
<td>EAP - Based</td>
<td>EAP - Based</td>
</tr>
</tbody>
</table>
Exploiting Vulnerabilities

1. Locating a wireless network
2. Attaching to the Found Wireless Network
3. Sniffing Wireless Data
We need a special holiday to honor the countless kind souls with unsecured networks named 'linksys'.

Source: [http://www.xkcd.com](http://www.xkcd.com)
Strip Number: 466
Trivia

• More than 320 wi-fi networks were open and unsafe near
  • Mumbai Airport / Andheri.
  • Major regions of central Mumbai are dominated by Netgear devices.
  • Major western region of Mumbai is dominated by Linksys devices.
  • Thane, surprisingly had over 170 hotspots.

• These were active insecure / open access points / networks.

Locating a wireless network

There are two tools that are commonly used in this regard:

- **NetStumbler** – This Windows based tool easily finds wireless signals being broadcast within range
Locating a wireless network (contd)

- **Kismet** – Kismet will detect and display SSIDs that are not being broadcast which is very critical in finding wireless networks.
Attaching to the Found Wireless Network

If the wireless network is using authentication and/or encryption, you may need one of the following tools.

- **Airodump-ng** - packet capture program, collects authentication handshake

- **Aireplay-ng** - de-authenticator /packet injection program
Attaching to the Found Wireless Network (contd)

- **CowPatty** – Brute force tool for cracking WPA-PSK.

- **Aircrack-ng** - To crack PSK using authentication handshake

- **Airdecap** - Decrypts WEP/WPA capture files
Sniffing Wireless Data

- **Wireshark** – Ethereal can scan wireless and Ethernet data and comes with some robust filtering capabilities. It can also be used to sniff-out 802.11 management beacons and probes and subsequently could be used as a tool to sniff-out non-broadcast SSIDs.
Recommendations for Securing Your Home Wireless Network

- Change the router’s default passwords.
- Change the SSID name and disable SSID broadcast.
- Setup MAC filters to limit which computers can connect.
- Turn on WPA or WPA2 encryption.
- If you are using WPA-PSK, ensure passphrase is 64 character with no dictionary word.
- Review your wireless logs.
- Watch for upgrades from the manufacturer.
- Practice good computer security.
Recommendations for securing Enterprise Networks

1. Define, monitor and enforce a wireless security policy

   • Policy should cover all 802.11 and Bluetooth wireless devices
   • Define wireless policies for mobile workers
   • Ensure wireless devices are not used until they comply with the wireless security policy

2. Take a complete inventory of all Access Points and 802.11 devices in the airwaves

   • Eliminate rogue Access Points and unauthorized user Stations.
Recommendations for securing Enterprise Networks (Contd)

3. Define secure configurations for Access Points and user stations
   - Change default setting
   - Disable SSID broadcast
   - Turn-off “ad-hoc” mode operation

4. Define acceptable encryption and authentication protocols
   - Use strong authentication (802.1x with EAP recommended)
   - Use strong encryption with at least 128-bit keys (WPA2, WPA recommended)
   - Deploy a layer-3 Virtual Private Network (VPN) for wireless communication
5. Monitor the airwaves to identify suspicious activity

- Deploy a Wireless Intrusion Detection System (IDS) to identify threats and attacks
- Detect and terminate unauthorized associations in a timely manner
- Monitor wireless assets for policy violations
- Log, analyze, and resolve incidents in a timely manner
- Gather and store wireless activity information for forensic analysis
References

- http://www.ethicalhacker.net/content/view/16/24/
- http://cache-www.intel.com/cd/00/00/01/77/17769_80211_part2.pdf
- Wikipedia!
Questions :-?
Thank You!
Types of EAP

- LEAP - Cisco proprietary, uses username/password to authenticate against RADIUS
- TLS - RFC 2716, uses X.509 certificates for authentication on both Supplicant and Authenticator
- TTLS - Developed by Funk Software, Authenticator uses a certificate to identify itself, Supplicant can use username/password
- PEAP - Authenticator uses certificate, Supplicant can use username/password
Four-way Key Handshake

1. EAPOL-Key (ANonce)
   - Derive Pairwise Transient Key (PTK) using ANonce and SNonce

2. EAPOL-Key (SNonce, MIC)
   - Derive PTK using ANonce and SNonce
   - Supply Group Transient Key (GTK)

3. EAPOL-Key (MIC, Encrypted GTK)

4. EAPOL-Key (MIC)
   - Install PTK and GTK
   - Install PTK

Encrypted data can now be sent / received

PTK ← PRF-X (PMK, "Pairwise key expansion",
Min(AA, SA) || Max(AA, SA) || Min(ANonce, SNonce) || Max(ANonce, SNonce))