SAIT

ITSC 301: Wireless Security

Module 5 – Security Risks and Threats in a WLAN

Table of Contents

- Review Lecture & Lab
- Items that affect WLAN security
- WLAN attacks
- Identify the impact to enterprises of various wireless security standards
- Identify deficiencies in temporal key integrity protocol (TKIP) encryption

Review Lecture & Lab

Review Module 4 Lecture/Lab

- Functions of a WLAN frame
- Terms used in 802.11 Layer 2 technology
- Capabilities of the IEEE 802.11 MAC
- Wireless sniffing tools to analyze Layer 2
- Troubleshoot WLAN connectivity

SAIT

Module 5: Security Risks and Threats in a WLAN

Small Group Discussion

- Brainstorm items that affect security in a wireless LAN.

Items that Affect WLAN Security

- Wireless AP placement & transmission power
- Rogue AP
- Authentication/authorization
- Vulnerabilities (protocol, encryption, authentication)
- Denial of service
- Wireless IDS/IPS and monitoring
- Prevention/detection of threats

WAP Placement & Transmission Power

- Coverage area critical to ideal AP placement
- Transmission power shouldn’t exceed regulatory limits
- Limit exposure to publicly accessible areas
    - Reduce areas of attack

Rogue AP

- Connected to your network
- Connected to the internet via cell or relay
- Denial of Service

WLAN Authentication

- Many Wi-Fi implementations lack mutual (two-way) authentication, present day attacks
  - Karma, Evil Twin
- Enterprise uses IEEE 802.1X

Wi-Fi Vulnerabilities

- MAC spoofing (easily performed)
- WEP (Deprecated by IEEE) vulnerabilities:
  - Weak IVs
    - predictability, reused, transmitted via cleartext, protocol doesn't specify how IVs are selected
  - RC4 weak keys
    - AirSnort, WEPCrack and dweputils
  - WEP Cracking (FMS, Korek, PTW)
  - Wi-Fi router key distribution isn't scalable
  - CRC32 is a checksum mechanism, not a message integrity mechanism
  - Lacks strong mutual authentication

Denial of Service: Wi-Fi

- Bombard Target network with:
  - Bogus requests, premature successful messages, failure messages, send client deauthentication
  - Abuse of Extensible Authentication Protocol (EAP)
- Injection of Network protocols:
  - Gratuitous ARP (Caffe Latte), Spanning tree (802.1D), OSPF, RIP, HSRP

Wireless IDS/IPS and Monitoring

- Prevent/detect attacks against network
- Continuous protection of wireless scope
- PCI-DSS requirement 11.1
  - Testing of wireless rogue AP quarterly or NAC or WIDS/WIPS

Prevention/Detection

- RF shielding on outer walls and windows
- DoS defense, black holing, validate handshake, rate limiting
- Hiding SSID (disable broadcast)
- MAC ID filtering (limited scale < 500 end points)
- Static IP addressing (limited scale < 500 end points)
- Implement WPA2 Enterprise, 802.1X certificate authentication with AES-CCMP, disable WEP
- Implement WIPS/WIDS

SAIT

Attacks Against WLANs

Small Group Discussion

- Explain the various attacks that can be mounted against a WLAN.

WEP Encryption Diagram

- Can you spot the flaws?

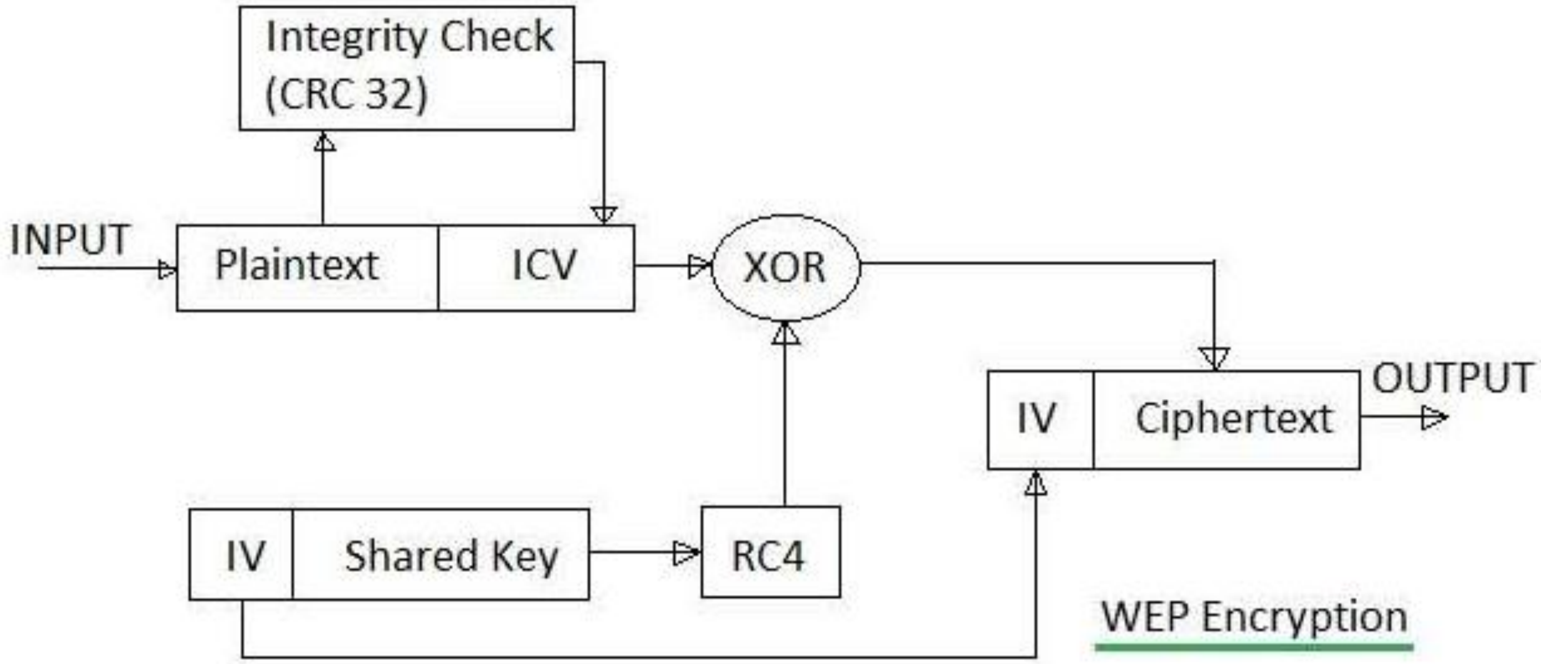


Figure 1: WEP Encryption Process Block Diagram

Source: RF Wireless World, 2012. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

WEP Weaknesses

- WEP does not prevent forgery of packets
- Easy forging of authentication messages
- WEP does not prevent replay attacks
    - Attacker can simply record and replay packets as desired and they will be accepted as legitimate
- Problem in the RC-4 algorithm (weak)
- WEP uses RC4 improperly
    - Keys used are very weak (<128) and can be brute-forced on standard computers in hours to minutes, using freely available software

WEP Weaknesses

- WEP reuses initialization vectors
    - A variety of available cryptanalytic methods can decrypt data without knowing the encryption key
- WEP allows an attacker to undetectably modify a message without knowing the encryption key
- Key management is lacking and updating is poor

Impact of Wireless Security Standards on Enterprise

Small Group Discussion

- Identify and understand the enterprise impact of security-pertinent wireless standards.

Various WLAN Standards

- 802.11z “Direct Link Setup” (client to client)
  - Universal Plug-and-Play (UPnP),
  - Devices Profile for Web Services (DPWS)
  - Zero Configuration Networking (ZeroConf).
  - These protocols let devices find other devices in a network, query their capabilities and provide some kind of automatic setup.
  - Vulnerabilities:
    - Wireless DoS
    - WPA2 PSK: key cracking

Various WLAN Standards

- 802.11ac “Gigabit over Wi-Fi” (fast)
  - Extending the air-interface concepts of 802.11n
  - Wider RF bandwidth (up to 160 MHz)
  - More MIMO spatial streams (up to eight)
  - Downlink multi-user MIMO (up to four clients)
  - High-density modulation (up to 256-QAM)

Various WLAN Standards

- 802.11af “Wi-Fi in TV White Space” – fast
  - Permits operation in TV white space of 6 MHz channels between 54 and 698 MHz between TV channels 2, 5, 6, 14–35, and 38–51
  - For mobile stations, allowed transmit power is fixed to 100 mW per 6 MHz channel, or 40 mW if an adjacent channel is in use by a primary user
  - Achievable data rate per spatial stream is 26.7 Mbit/s for 6 and 7 MHz channels and 35.6 Mbit/s for 8 MHz channels
  - With four spatial streams and four bonded channels, the maximum data rate is 426.7 Mbit/s in 6 and 7 MHz channels and 568.9 Mbit/s for 8 MHz channels

Wikipedia (2018).

Various WLAN Standards

- Bluetooth: Is it secure?
    - Limited range
    - Limited security functionality (limited string length PIN)
    - Several architectural/technical vulnerabilities

SAIT

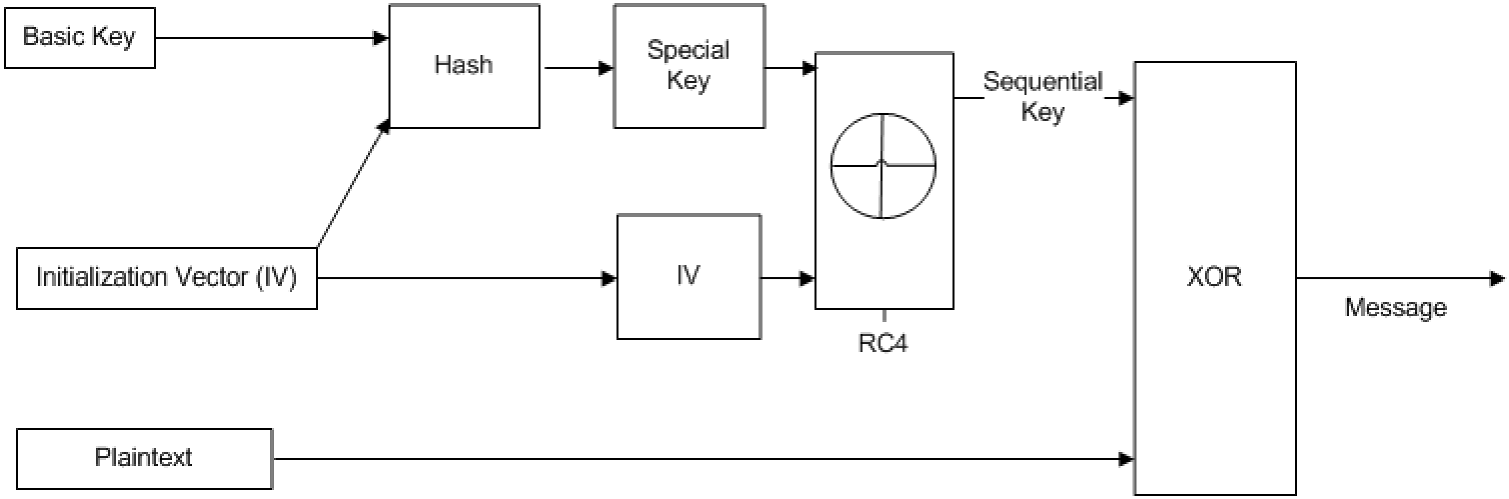
Deficiencies in Temporal Key Integrity Protocol (TKIP) Encryption

Temporal Key Integrity Protocol (TKIP)

- Created in 2002 as Wi-Fi protected access
- No longer considered secure (2009)
- Security protocol used in IEEE 802.11 networks, defined by IEEE 802.11i task group and Wi-Fi Alliance as interim solution to replace WEP w/o replacing legacy hardware
- Breaking WEP left Wi-Fi networks no viable link-layer security
- Creates three key levels: master, working, RC4

TKIP continued

- Master: shared with each client and access point, used to create working keys
- Working keys: combined with longer IV (48-bit vice 24) to form RC4 key for each packet



WPA Encryption Algorithm (TKIP)

TKIP 3 Security Feature Improvements

- Implements a key mixing function that combines secret root key with Initialization Vector (IV) before passing it to RC4 cipher
    - WEP merely concatenated the IV with root key and passed to RC4
- Sequence counter added to protect against replay attacks. Packets received out of order are rejected by the access point.
- TKIP implements a 64-bit Message Integrity Check (MIC)

Deficiencies in TKIP

- Since it uses some of the same underlying tech as WEP, it is susceptible to same attacks
  - E.g., RC4 still used

References

IEEE 802.11af. (n.d.). Retrieved June 25, 2018 from https://en.wikipedia.org/wiki/IEEE_802.11af

RF Wireless World. (2012). WEP vs WPA vs WPA2: Difference between WEP, WPA, WPA2. Retrieved from http://www.rfwireless-world.com/Terminology/WEP-vs-WPA-vs-WPA2.html

For more information, contact:
Director, Centre for Instructional Technology and Development
Southern Alberta Institute of Technology
1301 16 Ave. N.W., Calgary, AB T2M 0L4