ITSC 301: Wireless Security

Module 6 – Minimizing Security Risks in a Wireless LAN

Table of Contents

Review Lecture & Lab

Module 5: Review Lecture & Lab

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

Module 6: Common Wireless Security Solutions

Module 6: EAP Capabilities and Features

Small Group Discussion

- Explain the functions, features and capabilities of common wireless security solutions, including:
  - LEAP
  - PEAP
  - EAP-TTLS
  - EAPFAST
  - EAP-TLS

EAP Function

- EAP-only message formats
- Authentication framework frequently used in wireless networks and point-to-point connections
- WPA and WPA2 standards have adopted IEEE 802.1X with 100 EAP types as official authentication mechanism

Capabilities and Features: LEAP

- Lightweight Extensible Authentication Protocol
  - Uses a modified version of MS-CHAP
  - Creates dynamic WEP keys and mutual authentication (between a wireless client and a RADIUS server)
  - Allows for clients to re-authenticate frequently
  - Upon each successful authentication, client acquires a new WEP key (in hope that WEP keys don't live long enough to be cracked)

    (Wikipedia, 2018)
  - May be configured to use TKIP instead of dynamic WEP

LEAP Security Considerations

- Well-known security weaknesses involving offline password cracking
- An authentication protocol in which user credentials are not strongly protected
- Automated tools like ASLEAP demonstrate the simplicity of getting unauthorized access

(Wikipedia, 2018)

Capabilities and Features: PEAP

- Protected Extensible Authentication Protocol
  - Similar in design to EAP-TTLS
  - Correct deficiencies in EAP
  - EAP assumed a protected communication channel, such as that provided by physical security, so facilities for protection of EAP conversation not provided
  - Uses server-side public key certificates to authenticate server
  - EAP-MSCHAPv2 and EAP-GTC refer to the inner authentication methods which provide user or device authentication
  - Third authentication method commonly used with PEAP is EAP-SIM

(Wikipedia, 2018)

Capabilities and Features: EAP-TTLS

- EAP Tunneled Transport Layer Security
  - An EAP protocol that extends TLS
  - Client can, but does not have to be authenticated via a CA-signed PKI certificate to the server
  - After server is securely authenticated to the client via its CA certificate (and, optionally, the client to the server), the server can use established secure connection (“tunnel”) to authenticate the client
  - Can use an existing and widely deployed authentication protocol and infrastructure

(Wikipedia, 2018)

Capabilities and Features: EAP-FAST

- EAP Flexible Authentication via Secure Tunneling
  - Designed to address the weaknesses of LEAP while preserving the “lightweight” implementation
  - Server certificates optional
  - Uses a Protected Access Credential (PAC) to establish a TLS tunnel in which client credentials are verified

(Wikipedia, 2018)

EAP-FAST Vulnerability

- An attacker can intercept the PAC and use that to compromise user credentials
  - Mitigated by manual PAC provisioning or by using server certificates for the PAC provisioning phase

(Wikipedia, 2018)

Capabilities and Features: EAP-TLS

- EAP Transport Layer Security
  - Requires client-side X.509 certificates without giving the option to disable the requirement, even though the standard does not mandate their use
  - Requirement for client-side certificate gives EAP-TLS its authentication strength
  - A compromised password is not enough to break into EAP-TLS-enabled systems
  - Highest security available: when client-side certificate “private keys” are housed in smart cards

(Wikipedia, 2018)

Module 6: Attacks Against WEP Encryption

Small Group Discussion

- WEP attacks

Various WEP Wireless Attacks

- Key-recovery attacks
  - Karma – Takes advantage of WLAN probing technique of clients trying to associate with stations in their preferred network list and then impersonates that legitimate WLAN SSID luring the client to connect
  - Evil Twin – Sets up a fake WiFi AP to be same as target (channel and SSID) used to gather pre-shared key or certificate to MITM
  - FMS – Initialization vector is transmitted unprotected with the packets, so the attacker initially also knows the first three bytes of the per packet key for all packets.
  - Korek – Uses 16 additional correlations between the first l bytes of an RC4 key, the first two bytes of the generated keystream, and the next keybyte K[l].
  - PTW – Creates two methods to attack WEP, one to guess keybyte, one to guess rootkey using 35,000 to 40,000 packets for 50% success probability

Various WEP Wireless Attacks

- Packet-building attacks
  - Chopchop – Interactively decrypts the last m bytes of plain text of an encrypted packet by sending m 128 packets on average to the network
  - Fragmentation – Sends a single packet in up to 16 fragments. Uses the 8 bytes of keystream we know to broadcast a packet containing 64 bytes of known text in 16 fragments.

Module 6: Attacks Against WPA2-PSK Networks

Small Group Discussion

- WPA2-PSK attacks

WPA/WPA2 Attacks

- WPA/WPA2
  - Beck and Tews (inject traffic -QoS features)
  - Ohigashi-Morii (inject traffic – in all modes)
  - Michael (inject traffic – in all modes)
  - Hole196 (man-in-the-middle, inject trac, DoS attack)
  - Dictionary attack (key recovery)
  - Reaver (WPA Password attack)
  - Krack (WPA2 by forcing nonce reuse)
  - CoWPAtty (Offline WPA dictionary attack)
  - Fluxion (Evil AP)
  - Airbash (WPA PSK capture)

Module 6: Attacks Against Enterprise WPA2 Networks

Small Group Discussion

- WPA2-Enterprise Attacks

WPA/WPA2 Attacks

- WPA/WPA2
  - Beck and Tews (inject traffic -QoS features)
  - Ohigashi-Morii (inject traffic – in all modes)
  - Michael (inject traffic – in all modes)
  - Hole196 (man-in-the-middle, inject trac, DoS attack)
  - Dictionary attack (key recovery)
  - Reaver (WPA Password attack)
  - Krack (WPA2 by forcing nonce reuse)
  - CoWPAtty (Offline WPA dictionary attack)
  - Fluxion (Evil AP)

Module 6: WiFi DoS Attacks

Small Group Discussion

- Evaluate WiFi DoS attacks

WEP/WPA2 DoS Attacks

- WEP
  - Omerta,
  - essid_jack,
  - wlan_jack,
  - fata_jack,
  - void11

- WPA/WPA2
  - Hole196 (man-in-the-middle, inject trac, DoS attack)
  - Fluxion (Evil AP)

References

Extensible Authentication Protocol. (n.d.). Retrieved July 3, 2018 from Wikipedia: https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#EAP-TTLS

Lightweight Extensible Authentication Protocol. (n.d.). Retrieved July 3, 2018 from Wikipedia: https://en.wikipedia.org/wiki/Lightweight_Extensible_Authentication_Protocol

Protected Extensible Authentication Protocol. (n.d). Retrieved July 3, 2018 from Wikipedia: https://en.wikipedia.org/wiki/Protected_Extensible_Authentication_Protocol

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