PA197 Secure Network Design
9. WiFi Networks and Security

Eva Hladká, Luděk Matyska

Faculty of Informatics

18 April 2017

Content

Need for AA in WiFi

- WiFi networks use shared media
  - impossible to "hide" the traffic from a neighbor
- Basic risks
  - an unauthorized client can get network access
  - an unauthorized access point (AP) can get client's traffic
  - an unauthorized AP can jam the network
- Remedy
  - proper authentication
  - strict authorization
  - full encryption

Basic architecture

- Stations
  - access points (concentrators)
  - clients
- Basic service set (BSS)
  - a set of all stations that communicate through the shared medium
  - all stations in BSS share an SSID (Service Set IDentifier)
  - independent BSS
    - ad hoc network
    - no access point
  - infrastructure BSS
    - at least one access point
    - the common Wi-Fi setup
    - MAC address of the AP is the BSSID of this set

Basic architecture II

- Extended service set (ESS)
  - set of connected BSSs
  - access points in ESS connected through a distribution system
- Distribution system
  - connects access points
  - concept used for roaming
  - can be wired or wireless
    - wireless usually based on WDS or MESH protocols

Simple security mechanisms

- SSID hiding
  - "security by obscurity"
  - easy to overcome
- MAC filtering
  - weak, attacker can eavesdrop the MAC of authorized client
- Static IP addressing
  - client must know its IP
  - weak against sophisticated attacker
- Limited AP power
  - decreases the perimeter of the network
  - extremely weak
- None of these actually protects the Wi-Fi network
  - see also discussion following the article `http://www.pcworld.com/article/2052158/5-wi-fi-security-myths-you-must-abandon-now.html`

Protocols overview

- 802.1X protocol
  - IEEE standard for port-based network access control
  - provides authentication mechanism for attaching to LAN or WLAN
    - defined for shared media networks, also e.g. Ethernet
  - defines encapsulation of Extensible Authentication Protocol (EAP) over 802
  - EAP derivatives: LEAP, PEAP
- Wired Equivalent Privacy (WEP)
  - introduced 1999
- Wi-Fi Protected Access (WPA) and 802.11i
- All these protocols cover authentication and encryption
  - authentication usually indirect, through shared secret (e.g. password)

WEP

- Wired Equivalent Privacy
- Introduced 1999, deprecated 2004
- Basic features
  - stream cipher RC4: confidentiality
  - CRC-32 checksum: integrity
- 64 bit WEP (WEP-40)
  - 40 bit key concatenated with 24 bit initialization vector
- 128 bit WEP (WEP-104)
  - 104 bit key
- Also 152 and 256 bit versions exist
- Weak protocol
  - too short key
    - possible to recover RC4 key in a minute in busy network
  - single shared key
    - problems with several users
    - expensive disconnecting a user from a network

WEP authentication

- A shared key authentication
  - client sends an authentication request
  - AP replies with a clear-text challenge
  - client encrypts it and sends back
  - AP decrypts and confirms

  The same pre-shared key is used for authentication and encryption
- Open System authentication
  - no authentication, pre-shared keys are used only for payload

  Stronger than shared key, as no pair of (plain,encrypted) text is sent over the network

WPA

- WiFi Protected Access
- Data encryption based on 802.11 standard
- Includes TKIP and 802.1X mechanisms
  - dynamic key encryption
  - mutual authentication
- Temporal Key Integrity Protocol (TKIP)
  - per-packet key construction and distribution
    - new unique encryption key periodically generated for each client
  - message integrity code
  - 48 bit initialization vector
  - one-way hash instead of XOR
- WPA-Personal
  - Pre-shared Key (WPA-PSK)
  - does not require authentication server
- WPA-Enterprise
  - uses authentication server (e.g. RADIUS) and EAP

WPA2

- Full 802.11i
- Stronger data protection and network access control
- Counter Cipher Mode with block chaining message authentication code Protocol (CCMP)
  - replaces TKIP
  - uses AES
- WPA2-PSK and WPA2-Enterprise
  - analogous to WPA-PSK and WPA-Enterprise
- Combined with WPS (Wi-Fi Protected Setup)
  - introduced for home users for a simpler setup of WPA and WPA2
  - flaw discovered in December 2011
    - brute-force attack to get WPA/WPA2 pre-shared keys through revealing WPS PIN
    - WPA/WPA2 without WPS not vulnerable
- WPA2 currently the obligatory standard for all equipment certified by Wi-Fi Alliance

EAP

- Extensible Authentication Protocol
  - defined in RFC 3748, updated in RFC 5247
  - widely used in wireless networks
- A framework
  - more than 40 different authentication methods defined
  - requirements for methods described in RFC 4017
- Many specific extensions

EAP Extensions

- LEAP
  - lightweight EAP, introduced by CISCO, never directly accepted by Microsoft
- EAP-TLS
  - see RFC 5216
- EAP-TTLS/MSCHAPv2
  - tunneled EAP-TLS
- EAP-POTP
  - Protected One-Time Password
  - see RFC 4793
- EAP-PSK
  - pre-shared key
  - see RFC 4764
- EAP-PWD
  - shared password, used e.g. in Android 4.0
  - see RFC 5931

EAP Extensions II

- EAP-FAST
  - Flexible Authentication via Secure Tunneling
  - CISCO, successor of LEAP, to overcome its flaws
  - see RFC 4851
- EAP-SIM
  - EAP for GSM Subscriber Identity Module
  - see RFC 4186
- EAP-AKA
  - Authentication and Key Agreement for Universal Mobile Telecommunications System (UMTS)
  - see RFC 4187
- EAP-EKE
  - Encrypted Key Exchange
  - secure mutual authentication using short passwords, Diffie-Hellman variant of EKE
  - see RFC 6124
- and many other

EAP-TLS

- EAP-Transport Layer Security
  - IETF open standard
- Required client side certificate
  - although attempts to remove this requirement exists
- No password
- Practically unbreakable without access to client's private key
  - use of smart cards/tokens on the client side

EAP Encapsulation

- EAP only defines message format
- Needs an encapsulation of the actually used transport protocol
- PEAP
  - Protected EAP
    - uses TLS tunnel
  - joint development of CISCO, Microsoft and RSA Security
  - combined with specific authentication methods
    - MSCHAPv2 and GTC methods most popular
- Point-to-Point Protocol (PPP)
  - the origin of EAP
  - to replace CHAP and PAP authentication protocols
- 802.1X
  - EAP over LAN (EAPOL)
  - includes supplicant, authenticator, authentication server

Types of attack

- Access control attacks
- Confidentiality attacks
- Integrity attacks
- Authentication attacks
- Availability attacks
- See `http://searchsecurity.techtarget.com/feature/A-list-of-wireless-network-attacks` for list of tools for each attack
- Another distinction between passive and active attacks
  - passive usually means no traffic is directly injected

Passive Attacks

- Eavesdropping the network traffic
  - simple on unencrypted traffic
- WEP password cracking
  - uses eavesdropping
  - Aircrack tool easily available
  - for principles see Fluhrer, Mantin, Shamir: Weaknesses in Key Scheduling Algorithm of RC4 (`http://www.crypto.com/papers/others/rc4_ksaproc.pdf`)
- MAC spoofing
  - stealing MAC address of an authorized user (or AP)
- Twin AP
  - setup of an AP with the same SSID
  - a specific version of phishing attack
  - could be used also for man in the middle attack
    - intercept TCP and/or SSL/SSH tunnels

Active Attacks

- DoS attacks
  - availability attacks
  - to prevent correct use of the Wi-Fi network
- Authentication attacks
  - packet injection, not only eavesdropping

DoS Attacks

- Signal jamming (see later)
- 802.11 use
  - control frames
    - continuous transmit mode blocks other stations
    - Queensland DoS
  - forged de-authenticate frames
    - disconnect an individual station
    - Death DoS
  - malicious associate frames
    - exhaust AP resources
- Similar attacks through 802.1X packets
  - e.g. EAP logoff flood, EAP start flood

WEP attacks

- Based on reused key attack for stream ciphers (RC4 in WEP)
- Principle
  - assume two messages A and B, both encrypted with the same key K.
  - the stream cipher produces a string of bits $C(K)$, the encrypted messages are
    $E(A) = A \mathrm{xor} C$
    $E(B) = B \mathrm{xor} C$
  - attackers captures $E(A)$ and $E(B)$, from which he can compute $A \mathrm{xor} B$ (equal to $E(A) \mathrm{xor} E(B)$)
  - if one of A or B is known, the decryption is straightforward; if none is known, but structure (e.g. plain text, ARP packet, ...) is known, it takes just few moments on a computer to find the result

WEP attacks II

- ARP request replay attack
  - steps
    - attacker listens for ARP packet
    - it retransmits it back to AP
    - AP repeats ARP, but with new IV
    - this is repeat, used to capture different IVs
  - the captured IVs used for password cracking
- A similar approach is to send known plain text to the victim
  - e.g. an ICMP packet

  and to capture its encrypted version

WPA short packet spoofing

- Only for TKIP-based WPA
  - paper describing this attack released in November 2008
- Principles
  - TKIP includes Message Integrity Check (MIC) hashing algorithm
  - MIC is based on a weak algorithm
    - legacy from WEP
  - If more than 2 MIC failures occur in 60 second interval, both AP and client shut down for 60 s
  - attack reveals one byte of a message per each 60 s
- TKIP keys are not compromised
- Able to decrypt TKIP frame sent from AP to the client (but not vice versa)
- With enabled QoS, attacker can inject up to 15 arbitrary frames for every decrypted packet
  - ideal to decrypt ARP request followed by ARP poisoning

WPA2 password attack

- WPA2 is cryptographically secure against eavesdropping
  - no WEP-like password crack possible through traffic observation
- However, handshake packets could be used for offline cracking
  - the structure of handshake packet is known
- Attacker needs to capture handshake packet
  - passive: waiting till somebody connects in
  - active: using forged de-authenticating packet
    - victim automatically tries to reconnect
    - sending the waiting for handshake packets
- Attackers uses captured handshake packets for offline cryptanalysis (passphrase revelation)

Hole196

- An insider attack
  - discovered by AirTight Networks in 2010 (see `http://www.airtightnetworks.com/WPA2-Hole196`)
  - affects both WPA and WPA2
- An insider attack
  - attacker must be authenticated within the SSID
- Does not reveal any keys
  - does not compromise the AES encryption

Hole196 II

- Principle
  - resembles Man-in-the middle attack
  - steps
    1. attackers creates ARP frame with IP address of the default gateway but with attacker's MAC address and sends this packet directly to the victim, using the common group key for broadcast (shared by all clients and AP in a BSS)
    2. victim receives the frame and updates its routing table
    3. victims sends next data frame with gateway address of attacker; the data are encrypted by victim's unicast key
    4. the packet is received by AP, decrypted by shared victim's unicast key and encrypt with attacker's unicast key; the packet is sent to attacker
    5. attacker decrypts the packet; victim's traffic is exposed to the attacker
- If client isolation is used, the attack reduces to DoS
  - client isolation means that no two clients could communicate directly, bypassing AP and its security measures

Signal Jamming

- A specific form of active DoS attack
  - usually create noise to interfere with signal
- Obvious jamming
  - random noise: taken as atmospheric noise
  - random pulse
  - stepped stones: against single AM/FM
  - spark: short often burst
  - gulls, wobbler, recorded sounds: against voice transmission
  - preamble jamming
- Subtle jamming
  - no noise generation
  - disrupted/bogus control information

Summary

- Wi-Fi network poses security challenge
  - shared broadcast medium
  - easy to eavesdrop
  - easy to inject frames/packets
  - easy to jam
- Users and data protection a natural part of Wi-Fi protocols
- Many frameworks and protocols
  - also a lesson in protocol weaknesses
- Passive and active attacks abundant
  - from packet capturing through password cracking to data decryption
- Wi-Fi networks a battlefield for network security
- Next session: (Wireless) personal area networks