WiFi Basics & Security

original slides by
Matthias Vallentin
vallentin@net.in.tum.de

Outline

- 802.11 ("WiFi") Basics
  - Standards: 802.11{a,b,g,h,i}
  - CSMA/CA
- WiFi Security
  - WEP
  - 802.11i
  - DoS
### IEEE 802 family

#### 802.11 standards

<table>
<thead>
<tr>
<th>Year</th>
<th>802.11</th>
<th>802.11b</th>
<th>802.11a/h</th>
<th>802.11g</th>
<th>802.11n</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency</td>
<td>2.4 GHz</td>
<td>2.4 GHz</td>
<td>5 GHz</td>
<td>2.4 GHz</td>
<td>5 GHz</td>
</tr>
<tr>
<td>Transfer rate</td>
<td>2 MBit/s</td>
<td>11 MBit/s</td>
<td>54 MBit/s</td>
<td>54 MBit/s</td>
<td>~600 MBit/s</td>
</tr>
<tr>
<td>Acceptance</td>
<td>veraltet</td>
<td>stark verbreitet</td>
<td>gering verbreitet</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Security</td>
<td>-</td>
<td>WEP</td>
<td>WEP</td>
<td>WEP, WPA</td>
<td>-</td>
</tr>
</tbody>
</table>

802.11i is an Amendment
802.11 operational modes

- **Infrastructure mode**
  - Access Point (AP) interface to wired network
  - Basic Service Set (BSS) contains
    - Wireless hosts
    - Access Point (ad hoc mode: only hosts)

- **Ad hoc mode**
  - no access points
  - nodes can only transmit to other nodes within link coverage
  - nodes organize themselves

Wireless link characteristics

Differences to wired link ....

- **Decreased signal strength**: radio signal attenuates as it propagates through matter (path loss)
- **Interference from other sources**: standardized wireless network frequencies (e.g., 2.4 GHz) shared by other devices (e.g., phone); devices (motors) interfere as well
- **Multipath propagation**: radio signal reflects off objects ground, arriving at destination at slightly different times

.... make communication across (even a point to point) wireless link much more “difficult”
Wireless network characteristics

Multiple wireless senders and receivers create additional problems (beyond multiple access):

- Hidden terminal problem
  - B, A hear each other
  - B, C hear each other
  - A, C cannot hear each other means A, C unaware of their interference at B

Signal fading:
- B, A hear each other
- B, C hear each other
- A, C cannot hear each other interfering at B

IEEE 802.11 multiple access

- 802.11 Carrier Sense Mulitple Access – “listen” before sending
  - To avoid collisions with ongoing transmissions
- 802.11: no Collision Detection (CD)!
  - Would require parallel sending (own data) and receiving (sensing collisions) → expensive!
  - Not all collisions can be detected anyhow → hidden node, signal fading
- Goal: avoid collisions:
  - CSMA/C(ollision)A(voidance)
802.11 MAC Protocol: CSMA/CA

802.11 Sender

1. if (sense channel idle for DIFS)
   transmit entire frame (no CD)
2. if (sense channel busy) {
   start random backoff timer
   timer counts down while channel idle
   transmit when timer expires
   if (no ACK) {
     increase random backoff interval
     repeat 2
   }
}

802.11 Empfänger

if (frame received OK)
   return ACK after SIFS

ACK necessary due to hidden terminal problem

Avoiding collisions (more)

idea: allow sender to "reserve" channel rather than random
access of data frames: avoid collisions of long data frames

- sender first transmits small request-to-send (RTS) packets to BS
  using CSMA
  - RTSs may still collide with each other (but they're short)
- BS broadcasts clear-to-send CTS in response to RTS
- RTS heard by all nodes
  - sender transmits data frame
  - other stations defer transmissions

Avoid data frame collisions completely using small reservation packets!
Outline

- 802.11 ("WiFi") Basics
  - Standards: 802.11{a,b,g,h,i}
  - CSMA/CA
- WiFi Security
  - WEP
  - 802.11i
  - DoS
WiFi security

- Wireless security
  - Confidentiality
  - Authenticity
  - Integrity
  - Availability

- Do the existing security protocols (WEP, WPA, WPA2) address these aspects?

IEEE 802 Familie
**Wired Equivalent Privacy (WEP)**

- Part of the 802.11 standard
  - **Goal**: secure the MAC layer
- Design goals:
  - **Confidentiality**
  - **Access Control**
  - **Data Integrity**: via checksum (CRC32)
- **Stream Cipher**
  - **RC4** ("arcfour")
  - Input-Parameters:
    - initialization vector \( v \) and secure key \( k \)
    - Key stream: \( RC4(v,k) \) (\( v \) is also known as seed)

---

**WEP**

![Diagram of WEP process]

- **Keystream** \( RC4(v,k) \)
- WEP-KEY
- IV
- verschlüsselt

---

1. 100
2. 010
3. =
4. 110
WEP (2)

Plaintext

Message | CRC

XOR

Keystream = RC4(v,k)

\[ v = IV = \text{Initialization Vector} \]

(Clear text)

Attacks on WEP

- Bruteforce
- Key stream reuse
  - IV dictionary
- Weak IVs
- Frame injection
- Fragmentation attack
Key stream reuse

- Reuse of an already used key stream $RC4(v,k)$
- Key stream space: $24 \text{ bit} = 2^{24} \text{ IVs}$
- Attacker can decode packets encrypted with the same key stream
- With even just one valid key stream an attacker can send arbitrary frames into the network
  - 802.11b has no protection against replay attacks

\[
RC4(v,k) \quad \text{Plaintext} = \text{Ciphertext}
\]

Key stream reuse (2)

- **IV dictionary**: stores all IVs together with their corresponding key stream
- With a full dictionary an attacker can decode all traffic
- How to get valid key streams?
  - *Shared Key Authentication* (deprecated)
  - *Known plaintext*
  - *Fragmentation attack*
    - Relaying broadcast frames
    - *Chop-Chop* (key stream “guessing”)

\[
RC4(v,k) = P \quad C
\]
Weak IVs

- Private key $k$ computable
  - "weak" IVs: reveal a byte of the private key $k$
  - Known RC4 weakness
  - 4 years (!) prior to the publication of WEP
- Vendors offered hardware patches: filter weak IVs
  - Aggravates problem: reduces key stream space: $< 2^{24}$
  - Legacy host can compromise whole network

Frame injection

- Additional classes of weak IVs are known
  - Up to 13% reveal a key byte
- Vendor decided to ignore it (no further IV-filters)
  - Still needs $\approx 500.000 - 1.000.000$ packets for successful attack $\Rightarrow$ "long" waiting times
- Speedup of attack possible via WEP frames replay
  - Only frames that imply an answer e.g.: ARP request (recognizable via fixed size)
- Vendor solution: EAP with fast re-keying
  - EAP = Extensible Authentication Protocol
    - Authentication Framework, no special authentication mechanism
    - ca. 40 methods: EAP-MD5, EAP-OTP, EAP-GTP, ... , EAP-TLS, ...
Fragmentation attack

- New real-time attack, robust against frequent re-keying enables
  - Sending of data into WEP network
  - Decryption of WEP data
- Approach: 802.11 can be used against WEP
  - 802.11 specifies fragmentation on MAC layer
    - Each fragment is individually encrypted
    - Multiple fragments can be send with the same key stream
    - Max. 16 fragments, due to 4 bit field for FragNo

802.11 Fragmentation

Original plain-text & CRC.

Data | CRC32
---|---
abcd | efgh | 1234

Fragments & CRC.

abcd | 1983 | efgh | 1914

Keystream (IV x).

\[
\begin{align*}
\text{abcd} & \oplus 1234 & = & \text{efgh} & \oplus 5678 \\
\end{align*}
\]

Encrypted frags.

\[
\begin{align*}
x & \oplus 2911 & = & x & \oplus 1337 \\
\end{align*}
\]
Fragmentation attack (2)

- 8 bytes of known plaintext in each frame*
  - 802.11 Frames use LLC/SNAP encapsulation (constant/known header)
  - Ether type = IP or ARP
  - => 8 bytes of key stream are known
    • $P = RC4(v,k)$
  - (8 - 4) x 16 = 64 bytes data can be injected immediately via fragmentation
    - 4 bytes for CRC (therefore 8 - 4)

Fragmentation attack (3)

- Why does it help?
  - Can speedup other attacks (e.g.: weak IV)
  - Key stream attacks
    • determine 8 bytes of key stream
    • extend key stream: send long broadcast frames in several fragments and decode answers from AP ($P = RC4(v,k)$). Repeat until 1500 bytes (MTU) of the key stream are known
    • IV Dictionary:
      - Send 1500 byte broadcasts
      - AP is likely to rely packet
      - Determine key stream for this packet and via this all further key streams
    • Decode packets with known key streams
  - Decode packets in real-time...
Fragmentation attack (4)

- Decoding of packets in *real-time*
  - Requirement: Internet connectivity
  - Attacker can use AP for decoding
  - With 802.11 fragmentation one can add an additional IP-header in front of the original packet
  - Original packet is contained in last fragment
    - AP reassembles, decodes the packet and sends it to the spoofed IP address

```
IV Data
\begin{array}{c}
\text{Encrypted payload.} \\
\hline
\text{IP header} & \text{payload frags.} \\
\text{IP Header} & \text{seib ello} \\
\end{array}
```

802.11 termini
### 802.11 security

<table>
<thead>
<tr>
<th></th>
<th>WEP</th>
<th>WPA</th>
<th>WPA2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Algorithm</strong></td>
<td>RC4</td>
<td>RC4</td>
<td>AES-CTR</td>
</tr>
<tr>
<td><strong>Key length</strong></td>
<td>64/128 bit</td>
<td>128 bit</td>
<td>128 bit</td>
</tr>
<tr>
<td><strong>IV-length</strong></td>
<td>24 bit</td>
<td>48 bit</td>
<td>48 bit</td>
</tr>
<tr>
<td><strong>Data integrity</strong></td>
<td>CRC-32</td>
<td>Michael</td>
<td>CBC-MAC</td>
</tr>
<tr>
<td><strong>Header integrity</strong></td>
<td>-</td>
<td>Michael</td>
<td>CBC-MAC</td>
</tr>
<tr>
<td><strong>Authentication</strong></td>
<td>Shared Key</td>
<td>802.1X</td>
<td>802.1X</td>
</tr>
<tr>
<td><strong>Key-management</strong></td>
<td>-</td>
<td>802.1X</td>
<td>802.1X</td>
</tr>
<tr>
<td><strong>Replay-attack protection</strong></td>
<td>-</td>
<td>IV-Sequenz</td>
<td>IV-Sequenz</td>
</tr>
</tbody>
</table>

### 802.11i - RSNA overview

- 3 entities for Robust Security Network Association (RSNA)
  - Supplicant (WLAN client)
  - Authenticator (access point)
  - Authentication server (almost always a RADIUS server)

- 6 connection phases until data exchange
  - Phase 1: Network and Security Capability Discovery
  - Phase 2: 802.11 Authentication and Association
  - Phase 3: EAP/802.1X/RADIUS Authentication
  - Phase 4: 4-Way Handshake
  - Phase 5: Group Key Handshake
  - Phase 6: Secure Data Communication

- More complex than WEP (luckily its also safer :)}
802.11i weaknesses

- PSK dictionary brute force attack
- Security level rollback attack
- Reflection attack

802.11i PSK brute force

- PSK = PMK = PBKDF2
  (passphrase, SSID, SSIDlength, 4096, 256)

- PSK = Pre-Shared Key
- PMK = Pairwise Master Key
- PBKDF2 = methods from PKCS#5 v2.0
- SSID = Service Set Identity
- SSIDlength = length of the SSID
- 4096 = number of hashes
- 256 = output length
Security level rollback attack

- Transient Security Network (TSN): Compatibility modus for heterogeneous environments
  - Idea: use for soft migration to WPA2
  - Enables Pre-RSNA and RSNA connections
- Attacker simulates a Pre-RSNA authenticator
  - Send spoofed Probe-Requests / Beacons
  - Security reduces to the weakest component
  - Fallback to WEP :(

Security level rollback attack

![Diagram showing the rollback attack process](image-url)
Reflection attack

- Attacker is Supplicant and Authenticator in one node
  - 4-Way-Handshake (4WH) as authenticator
  - 4WH as Supplicant with same parameters
- Responses from second 4WH can be used as valid data for the first 4WH
  - No mutual authentication
  - Encrypted data can be saved (e.g.: for offline analysis)
- Attack only works in ad hoc mode
  - With infrastructure mode Supplicant and Authenticator are always different nodes
Denial-of-Service (DoS)

- Frequency Jamming (PHY)
- Deauthentication/disassociation frame spoofing
- CMCA/CA – no protection for management frames
  - Ignore standard: e.g.: no “backoff”
  - Virtual carrier-sensing (RTS with large NAV)
- ARP-Cache poisoning
- 802.1X
  - EAP-{Start, Logoff, Failure} Spoofing
  - EAP identifier only 8 bit: send more than 255 Authentication Request at the same time
  - DoS too easy (not addressed by 802.11i!)
  - DoS attack can easy further attack (Session-Hijacking, MitM)

Conclusion

- WiFi is ubiquitär / pervasive
- Continuous improvements of the standards
- Security aspects
  - Shared medium (!)
  - Forget about WEP
  - Use secure protocols (SSH, IMAPS, HTTPS) over WLAN
  - Use good WPA/WPA2 pass phrases $\rho$ ($\rho \notin$ dictionary)
  - DoS (still) too easy
  - If important use cable :)
Course overview

- Introduction
  - Attacks and threats, cryptography overview
  - Authentication (Kerberos, SSL)
- Applications
  - Web, email, ssh
- Lower layer network security
  - IPsec, firewalls, wireless
- Monitoring / information gathering
  - Intrusion detection, network scans
- Availability
  - Worms, denial of service, network infrastructure