WLAN Security

- WLAN Security Standards
- WEP
- IEEE 802.1X
- Wi-Fi Protected Access (WPA)
- 802.11i
- Layered Security for Wireless Networks
What Do I have to know?

- Mode
  - Infrastructure mode
  - Ad-hoc mode
  - Radio link

- User group
  - Open user group
  - Restricted access

- Equipment
  - End user equipment
  - Radio equipment
  - Infrastructure equipment

- What we have to protect?
Components of a WLAN Infrastructure

- WLAN Management
- Security Infrastructure
  - AAA - Server
  - Firewall / VPN
  - Intrusion Detection
- Distribution System
- Access Point
- Client
- Radio Interface
What can we do? - Security Infrastructure

- MAC access control lists
  - Static MAC list on access points
  - Central RADIUS server

- Packet filter
  - Firewall

- Protection on application level
  - Application proxy
  - Intrusion detection system
  - Isolation of critical servers
  - …
Network Architecture

Multiple Base Station and Multiple Channel Network
## War Driving

<table>
<thead>
<tr>
<th>MAC</th>
<th>SSID</th>
<th>Name</th>
<th>Chan</th>
<th>Vendor</th>
<th>Type</th>
<th>WEP</th>
<th>SNR</th>
<th>Signal+</th>
<th>Noise-</th>
<th>SNR+</th>
<th>Latitude</th>
</tr>
</thead>
<tbody>
<tr>
<td>00045A0E3EA0</td>
<td>linksys</td>
<td>6</td>
<td>Linksys</td>
<td>AP</td>
<td></td>
<td>-91</td>
<td>-100</td>
<td>9</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>00045AE838CB</td>
<td>linksys</td>
<td>6</td>
<td>Linksys</td>
<td>AP</td>
<td></td>
<td>-84</td>
<td>-102</td>
<td>15</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>00022D2C82DA</td>
<td>2c82da</td>
<td>1</td>
<td>Agere (...)</td>
<td>AP</td>
<td>Yes</td>
<td>-75</td>
<td>-99</td>
<td>21</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>000124F05623</td>
<td>default</td>
<td>6</td>
<td>Linksys</td>
<td>AP</td>
<td></td>
<td>-95</td>
<td>-98</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>00045A0E3A4A</td>
<td>linksys</td>
<td>6</td>
<td>Linksys</td>
<td>AP</td>
<td></td>
<td>-71</td>
<td>-104</td>
<td>32</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>00045AD770F</td>
<td>ANY</td>
<td>6</td>
<td>Linksys</td>
<td>AP</td>
<td>Yes</td>
<td>-90</td>
<td>-101</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>00045AE85F93</td>
<td>linksys</td>
<td>6</td>
<td>Linksys</td>
<td>AP</td>
<td></td>
<td>-88</td>
<td>-102</td>
<td>13</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>00045A0F2264</td>
<td>linksys</td>
<td>6</td>
<td>Linksys</td>
<td>AP</td>
<td></td>
<td>-87</td>
<td>-98</td>
<td>11</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>00062550331E</td>
<td>linksys</td>
<td>6</td>
<td>Linksys</td>
<td>AP</td>
<td></td>
<td>-89</td>
<td>-99</td>
<td>9</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>00045AE81743</td>
<td>peggyp</td>
<td>3</td>
<td>Linksys</td>
<td>AP</td>
<td></td>
<td>-81</td>
<td>-100</td>
<td>17</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>00030A000D54</td>
<td>aa</td>
<td>11</td>
<td>AP</td>
<td>Yes</td>
<td></td>
<td>-82</td>
<td>-99</td>
<td>17</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0030F1102D35</td>
<td>WLAN</td>
<td>11</td>
<td>AP</td>
<td>Yes</td>
<td></td>
<td>-85</td>
<td>-99</td>
<td>14</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>00022D3F21CE</td>
<td>3f21ce</td>
<td>1</td>
<td>Agere (...)</td>
<td>AP</td>
<td>Yes</td>
<td>-85</td>
<td>-100</td>
<td>15</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>00045AD00E47</td>
<td>linksys</td>
<td>6</td>
<td>Linksys</td>
<td>AP</td>
<td>Yes</td>
<td>-91</td>
<td>-98</td>
<td>7</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0030651C568A</td>
<td>Office</td>
<td>1</td>
<td>Apple</td>
<td>AP</td>
<td>Yes</td>
<td>-93</td>
<td>-96</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0040964569DC</td>
<td>NEUSTAR</td>
<td>6</td>
<td>Cisco</td>
<td>AP</td>
<td>Yes</td>
<td>-90</td>
<td>-100</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0040964576BD</td>
<td>NEUSTAR</td>
<td>6</td>
<td>Cisco</td>
<td>AP</td>
<td>Yes</td>
<td>-90</td>
<td>-99</td>
<td>9</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>003065030058</td>
<td>Better then Windows</td>
<td>6</td>
<td>Apple</td>
<td>AP</td>
<td>Yes</td>
<td>-89</td>
<td>-95</td>
<td>6</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>00045ACE3A63</td>
<td>pchan</td>
<td>6</td>
<td>Linksys</td>
<td>AP</td>
<td></td>
<td>-88</td>
<td>-101</td>
<td>11</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>00601DF0438E</td>
<td>sproq</td>
<td>3</td>
<td>Agere (...)</td>
<td>AP</td>
<td>Yes</td>
<td>-88</td>
<td>-99</td>
<td>11</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>000625504834</td>
<td>Falcos</td>
<td>10</td>
<td>AP</td>
<td></td>
<td></td>
<td>-80</td>
<td>-101</td>
<td>18</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>00409632DE23</td>
<td>luckgoose</td>
<td>4</td>
<td>Cisco</td>
<td>AP</td>
<td></td>
<td>-93</td>
<td>-100</td>
<td>7</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0030AB0B617A</td>
<td>Roming</td>
<td>6</td>
<td>Delta N...</td>
<td>AP</td>
<td>Yes</td>
<td>-86</td>
<td>-97</td>
<td>11</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>004096485D54</td>
<td>leesburg2</td>
<td>6</td>
<td>Cisco</td>
<td>AP</td>
<td>Yes</td>
<td>-63</td>
<td>-100</td>
<td>36</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>00409659F7BE</td>
<td>1SU</td>
<td>6</td>
<td>Cisco</td>
<td>AP</td>
<td></td>
<td>-58</td>
<td>-102</td>
<td>40</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>00409659D4EF</td>
<td>1SU</td>
<td>6</td>
<td>Cisco</td>
<td>AP</td>
<td></td>
<td>-57</td>
<td>-100</td>
<td>42</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>004096486D0F</td>
<td>leesburg2</td>
<td>1</td>
<td>Cisco</td>
<td>AP</td>
<td>Yes</td>
<td>-85</td>
<td>-100</td>
<td>13</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
WLAN Security Standards

- **Preshared KEY**
  - WEP Static Key
  - WEP Dynamic Key

- **802.1X**
  - EAP
  - WPA

- **802.11i**
  - AES-CCMP
  - TKIP

- **RADIUS (Auth.)**
- **RADIUS (AAA)**

- **CMS**

- **Secure Roaming**
- **Trust Relation**

- **802.11f SLP**

**Time**

- **WPA**
- **WPA v.2**

Colors:
- Yellow: IEEE standard
- Pink: IETF standard
- Blue: WiFi Alliance

Definitions:
- CMS: Cryptographic Message Syntax
- TKIP: Temporal Key Integrity Protocol
- AAA: Authentication, Authorization, Accounting
- SLP: Service Location Protocol
- EAP: Extensible Authentication Protocol
- RADIUS: Remote Authentication Dial In User Service
WEP (Wired Equivalent Privacy) – WEP Encryption

Steps:

a) Use CRC-32 to calculate the ICV (Integrity Check Value) over the plaintext message (for packet authentication)

b) Concatenate the ICV to the plaintext

c) Choose a random IV (Initialization Vector, 3 bytes, selected for each packet) and concatenate it to the secret key (13 bytes)

d) Input the secret key + IV into the PRNG (Pseudo Random Number Generator) to produce a pseudo-random key sequence

e) Encrypt the plaintext + ICV by doing a bitwise XOR with the pseudo random key sequence under RC4 to produce the cipher text

f) Communicate the IV to the peer by placing it in front of the cipher text
WEP (Wired Equivalent Privacy) – WEP Decryption

Steps:

a) Concatenate the IV of the incoming message to the secret key.

b) Generate the key sequence (same as for sender) using the pseudo-random noise generator.

c) Decrypt the incoming message. Combining the cipher text with the proper key sequence yields the original plaintext and ICV.

d) Verify the decryption by performing the integrity check algorithm on the recovered plaintext and comparing the output ICV'.

e) If ICV' is not equal to ICV, the received message is in error, and an error indication is sent to the MAC management and back to the sending station.
Weaknesses of WEP

WEP has well known flaws in the encryption algorithms

- RC4 used to derive the XOR sequence for the message
- As with all stream ciphers, **RC4 is easily broken if the same key is used twice**. This problem is usually solved by hashing the key with a unique initialization vector (IV) each time it is used, and sending the IV along with the message.

- IV is generated for each packet, generation of IV is weak
- IV consists of 3 bytes only and is generated by the WLAN card HW

WLAN Security Standards

- Pre Share KEY
- WEP Static Key
- WEP Dynamic Key
- EAP
- 802.1X
- RADIUS (Auth.)
- RADIUS (AAA)
- AESS-CCMP TKIP
- AES-CCMP TKIP
- 802.11i
- CMS

- WPA
- WPA v.2
- Time

- IEEE standard
- IETF standard
- WiFi Alliance

CMS: Cryptographic Message Syntax
AAA: Authentication, Authorization, Accounting
EAP: Extensible Authentication Protocol
TKIP: Temporal Key Integrity Protocol
SLP: Service Location Protocol
RADIUS: Remote Authentication Dial In User Service
IEEE 802.1X – Basic Concepts

Port-based Access Control

Port Access Entity (PAE) operates algorithms and protocols associated with authentication mechanisms for device port

- Supplicant
- Authenticator
- Authentication Server

Authenticator accepts EAPOL packets from Supplicant, forwards EAP packets to Authentication Server over higher layer protocol like RADIUS

Authenticator forwards Authentication Server EAP packets over EAPOL to Supplicant

EAPOL: Extensible Authentication Protocol over LAN
802.1X Architecture in WLAN System

Suppliant PAE
(WLAN Client)

EAPOL (EAP Over LAN)
(Ethernet, Token Ring, 802.11)

Authenticator
PAE
(WLAN AP)

Service

Authentication Server
• RADIUS
• Diameter

EAP in RADIUS
(Encapsulated EAP messages, typically on RADIUS)

WLAN

Mobile Communication Networks Andreas Mitschele-Thiel, Florian Evers 15-Jan-13 14
802.1X – Controlled Port and Uncontrolled Port

- Protocol exchanges between Authenticator and Authentication Server conducted via Controlled or Uncontrolled Port

- **Controlled Port** accepts packets from authenticated devices

- **Uncontrolled Port** only accepts 802.1X packets
  
  Uncontrolled Port used for exchanging Extensible Authentication Protocol (EAP) over LAN packets, EAPOL, with Supplicant

- Uncontrolled Port and Controlled Port considered same *point of attachment* to the LAN
802.1X – EAP Authentication Types

EAP-MD5 Challenge

- Earliest authentication type, CHAP (Challenge-Handshake Authentication Protocol) password protection on a WLAN
- Base-level EAP support among 802.1X devices, one-way authentication (MD5 not generally used anymore)
**EAP-TLS (Transport Layer Security)**

- Certificate-based (X.509), mutual authentication of client and network (PKI)
- **Client-side and server-side certificates** to perform authentication
- Dynamically generated user- and session-based keys
- Certified by WPA and WPA2

![Diagram of EAP-TLS Authentication Process]

**PrK: Private Key**
**PuK: Public Key**
**Certificate (s)/(r): The certificate of supplicant/RADIUS server**
802.1X – EAP Authentication Types

EAP-LEAP (Lightweight Extensible Authentication Protocol)
- Cisco’s proprietary EAP authentication type
- Mutual authentication (user name + password hash)
- Provides security during credential exchange, credentials include username and password
- Encrypts data transmission using dynamically generated WEP keys
- Risk of dictionary attacks due to use of passwords

EAP-TTLS (Tunneled TLS)
- Extension to EAP-TLS
- Certificates to authenticate server side
- Legacy methods to authenticate client side (no client certificates needed)
- Option of using simple authentication protocols (tunneled!)
  - clear text passwords or
  - challenge-response passwords authentication
- TTLS ‘packs’ this authentication protocol inside of TLS tunnel (hence the term ‘tunneled’)
- Similar security properties as EAP-TLS, i.e. mutual authentication and a shared secret for WEP session key
802.1X – Example of Session Authentication

(Ethernet, Token Ring, 802.11)

Access blocked

EAPOL (EAP Over LAN)

EAPOL-Start

EAPOL (EAP-Request/Identity)

EAPOL (EAP-Response/Identity)

EAPOL (EAP-Request)

EAPOL (EAP-Response)

Derive Pairwise Master Key (PMK)

EAPOL (EAP-Success)

EAP in RADIUS

Radius-Access-Request ()

Radius-Access-Challenge ()

Radius-Access-Request ()

Radius-Access-Accept ()

Access allowed
802.1X – MAC Layer Key

MAC layer **encryption keys** generated as part of authentication process (EAP) between Supplicant and Authentication Server (different from authentication key!)

Encryption keys will be used by chosen data encryption algorithm, e.g. RC4 for WEP, Rijndael for AES

- 802.1X used to direct encryption keys down to MAC layer on both Authenticator and Supplicant
- Two sets of encryption keys are generated during authentication:
  - **Pairwise Master Key** (PMK, session key) (256 bits, shared secret)
    PMK is unique to association between individual Supplicant and Authenticator
  - **Groupwise Key** (Group Key)
    Group Key is shared among all Supplicants connected to same Authenticator
## EAP - Summary

<table>
<thead>
<tr>
<th>EAP Authentication Type</th>
<th>EAP – MD5</th>
<th>EAP – TLS</th>
<th>EAP – LEAP</th>
<th>EAP – TTLS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mutual Authentication</td>
<td>no</td>
<td>supported</td>
<td>supported</td>
<td>supported</td>
</tr>
<tr>
<td>Server Authentication</td>
<td>none</td>
<td>Public Key (Certificate)</td>
<td>Password Hash</td>
<td>Public Key (Certificate)</td>
</tr>
<tr>
<td>Supplicant Authentication</td>
<td>Password Hash</td>
<td>Public Key (Certificate)</td>
<td>Password Hash</td>
<td>Password Hash</td>
</tr>
<tr>
<td>Dynamic WEP</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Security Risks</td>
<td>Identity exposed, Dictionary attack, Man-in-the-Middle (MitM) attack, Session hijacking</td>
<td>Identity exposed</td>
<td>Identity exposed Dictionary attack</td>
<td>MitM attack?</td>
</tr>
</tbody>
</table>
802.1X – Summary

- Intended to provide strong authentication, access control and key management
- Wireless terminal is Supplicant and Access Point is Authenticator
- Authentication initiated by Supplicant or Authenticator
- Authentication occurs at system initialization time
- EAP to exchange authentication messages
- RADIUS as authentication server
- Different authentication methods
  - Password
  - MAC address
  - Certificate-based authentication (TLS, etc.)

![Diagram of Port Based Network Access Control]
Wi-Fi Protected Access (WPA)

- Flaws in WEP: weak encryption, static encryption keys, lack of key distribution method
- IEEE 802.11i: standard for enhanced wireless security
  - addresses weak data encryption and user authentication within existing 802.11 standard
- WPA: joint effort between Wi-Fi Alliance and IEEE (trade mark)
  - subset of 802.11i (draft 3.0, without AES)
- WPA2: full 802.11i

WPA = 802.1X + Temporal Key Integrity Protocol (TKIP)

- 802.1X employs EAP for authentication
- RC4-TKIP is used for encryption and dynamic key distribution
WPA – Data Encryption

WPA

- uses Temporal Key Integrity Protocol (TKIP)
  => stronger data encryption
- addresses known vulnerabilities in WEP

TKIP

- based on RC4 stream cipher algorithm
- supplements WEP cipher engine with 4 new algorithms:
  - extended 48-bit Initialization Vector (IV) and IV sequencing rules (compared to the shorter 24-bit WEP IV)
  - new per-packet key mixing function
  - derivation and distribution method – re-keying
  - Message Integrity Check (MIC) ensures messages haven’t been tampered with during transmission
Temporal Key Integrity Protocol (TKIP) – Encryption

**DA** – Destination Address

**ICV** – Integrity Check Value

**MPDU** – Message Protocol Data Unit

**MSDU** – MAC Service Data Unit

**MIC** – Message Integrity Check

**SA** – Source Address

**TA** – Transmitter Address

**TKIP** – Temporal Key Integrity Protocol

**TSC** – TKIP Sequence Counter

**TTAK** – Result of phase 1 key mixing of **Temporal Key** and **Transmitter Address**

**WEP** – Wired Equivalent Privacy

**WEP IV** – Wired Equivalent Privacy Initialization Vector

**Michael**: Message Integrity Code for the Temporal Key Integrity Protocol
TKIP – Decryption

MIC Key

TA

TK

TKIP TSC

Unmix TSC

TKIP TSC

Phase 1 key mixing

TTAK

Phase 2 key mixing

WEP Seed

WEP Decapsulation

DA + SA + Priority + Plaintext MSDU

Michael

MIC'

MIC

MIC = MIC'?

Ciphertext MPDU

Out-of-sequence MPDU

In-sequence MPDU

Reassemble

Plaintext MPDU

MSDU with failed TKIP MIC

Countermeasures

Michael

DA + SA + Priority + Plaintext MSDU

Reassemble

Plaintext MPDU

MIC

MIC = MIC'?

Ciphertext MPDU

Out-of-sequence MPDU

In-sequence MPDU

WEP Decapsulation
TKIP – Encryption Details

TKIP enhances the WEP encapsulation process with the following additional steps:

1. TKIP computes the MIC over the MSDU source address, destination address, priority, and data, and appends the computed MIC to the MSDU. TKIP discards any MIC padding prior to appending the MIC.

2. If needed, IEEE 802.11 fragments the MSDU with MIC into one or more MPDUs. TKIP assigns a monotonically increasing TSC value to each MPDU, taking care that all the MPDUs generated from the same MSDU use counter values from the same 16-bit counter space.
   - (TKIP Sequence Counter (TSC) - Combination of extended 48-bit IV and IV sequence counter, extends life of Temporal Key, eliminates need to re-key Temporal Key during single association.)

3. For each MPDU, TKIP uses the key mixing function to compute the WEP seed.

4. TKIP represents the WEP seed as a WEP IV and RC4 key, and passes these with each MPDU to WEP for encapsulation of either the plaintext MPDU or the plaintext MPDU and the MIC. WEP uses the WEP seed as a WEP default key, identified by a Key ID associated with the temporal key.

5. TKIP calculates the ICV for each plaintext MPDU Data Field.

Informative Note:

When the TSC space is exhausted, the choices available to an implementation are to replace the temporal key with a new one or to end communications. Reuse of any TSC value compromises already sent traffic. Note that retransmitted packets reuse the TSC without any compromise of security. The TSC is large enough, however, that TSC space exhaustion should not be an issue.
TKIP – Decryption Details

TKIP enhances the WEP decapsulation process with the following additional steps:

1. Before WEP decapsulates a received MPDU, TKIP extracts the TSC sequence number and Key ID from the WEP IV and the Extended IV. TKIP discards a received MPDU that violates the sequencing rules, and otherwise uses the mixing function to construct the WEP seed.

2. TKIP represents the WEP seed as a WEP IV and RC4 key and passes these with the MPDU to WEP for decapsulation.

3. If WEP indicates the ICV check succeeded, the implementation reassembles the MPDU into an MSDU. If the MSDU reassembly succeeds, the receiver verifies the MIC. If MSDU reassembly fails, then the packet is discarded.

4. The MIC verification step recomputes the MIC over the MSDU source address, destination address, priority, and MSDU data (but not the MIC field), and bit-wise compares the result against the received MIC.

5. If the received and the locally computed MIC are identical, the verification succeeds, and TKIP shall deliver the MSDU to the upper layer. If the two differ in any bit position, then the verification fails, the receiver shall discard the packet, and shall engage in appropriate countermeasures.

**Michael** (Message Integrity Code for the Temporal Key Integrity Protocol):

To defend against active attacks, TKIP includes a MIC, named Michael. Michael offers only weak defenses against message forgeries, but it constitutes the best that can be achieved with the majority of legacy hardware. "802.11i-D6.0.doc"
WPA – User Authentication

WPA supports two authentication methods:

- **802.1X and EAP authentication**
  - enterprise environments
  - centralized authentication server
  - mutual authentication required to prevent user from joining rogue network

- **Pre-Shared Key authentication** (PSK)
  - home or office environment
  - no centralized authentication server (RADIUS) or EAP framework needed
  - easy configuration
WPA – Pre-Shared Key Authentication (PSK)

- Pre-shared key
  - requires home or office user to manually enter password (Master Key) in Access Point or Wireless Gateway and same password in each PC
- devices with matching password join the wireless network
- manually configured WPA password used as temporal key for TKIP
WLAN Security Standards

- Pre Share KEY
- 802.1X
- WEP Static Key
- EAP
- WEP Dynamic Key
- WPA
- AES-CCMP TKIP
- 802.11i
- Secure Roaming
- CMS
- RADIUS (Auth.)
- RADIUS (AAA)
- 802.11f SLP
- Trust Relation
- CMS: Cryptographic Message Syntax
- TKIP: Temporal Key Integrity Protocol
- AAA: Authentication, Authorization, Accounting
- SLP: Service Location Protocol
- EAP: Extensible Authentication Protocol
- RADIUS: Remote Authentication Dial In User Service

Time

IEEE standard
IETF standard
WiFi Alliance
WPA - Summary

- Wi-Fi Protected Access effectively addresses WLAN security requirements and provides immediate and strong encryption and authentication solution
- forward compatible with the full 802.11i standard
- replaces WEP as standard Wi-Fi security mechanism
- initial release of WPA (WPAv1) addresses
  - infrastructure-based 802.11 networks
  - no support of AES
- final WPA standard (WPAv2 = IEEE 802.11i)
  - support for ad-hoc (peer-to-peer) networks
  - full adoption of 802.11i standard, including AES
IEEE 802.11i – Robust Security Network (RSN)

802.11i:

- enhanced wireless security standard
- known as Robust Security Network (RSN)
- developed by IEEE Taskgroup i (TGi)

- addresses weaknesses of WEP based wireless security
  => replaces WEP
- security solution for legacy 802.11 hardware and new hardware
  (AES support)
- addresses infrastructure-based and ad-hoc (peer-to-peer) based
  802.11 wireless security requirements

802.11i is fully supported by WPA2
802.11i (RSN) – Encryption Protocols

- **Counter Mode with CBC-MAC Protocol (CCMP)** based on Advanced Encryption Standard (AES)
  - counter mode: use of counter to periodically change key
  - CBC: Cipher Block Chaining, i.e. ciphering of current block (16 bytes) is based on previous blocks in addition to key
- **TKIP** targeted at legacy 802.11 hardware
- **CCMP** targeted at future 802.11 hardware
- **Transitional Network**: RSN supporting simultaneous use of TKIP and CCMP
  => temporary solution till all hardware supports CCMP
- **802.11i specifies both TKIP and CCMP**
  - true RSN uses only CCMP
  - CCMP mandatory for 802.11i (RSN)
  - TKIP optional
AES Encryption Protocol

- Latest encryption technology, replaces
  - Data Encryption Standard (DES) and
  - Triple Data Encryption Standard (3DES)
  for all government transactions

- Uses fixed 128-bit encryption key length and uses same key for encryption and decryption (for 802.11)

- Same temporal encryption key, AES(K), used in AES encryption blocks for both MIC calculation and packet encryption

- Like TKIP, AES temporal encryption key derived from Pairwise Master Key (PMK)

Disadvantage

AES-ready hardware is not compatible with WEP
=> Legacy hardware can not be used for AES
CCMP MPDU Format

<table>
<thead>
<tr>
<th>MAC Header</th>
<th>CCMP Header</th>
<th>Data (PDU)</th>
<th>MIC</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>8 octets</td>
<td>&gt;= 1 octets</td>
<td>8 octets</td>
</tr>
</tbody>
</table>

CCMP processing expands the original MPDU size by 16 octets:

- 8 octets for the **CCMP Header** and
- 8 octets for the **Message Integrity Code (MIC)**.

The CCMP Header is constructed from the PN, ExtIV and Key ID fields.

**PN** is a 48 bit sequence counter represented as an array of 6 octets. PN5 is the most significant octet of the PN and PN0 is the least significant.

Note that CCMP does not use the WEP ICV.

The ExtIV field, bit 5, of the Key ID octet signals that the CCMP Header extends the MPDU by an additional 4 octets to the 4 octets added by the WEP format. The **ExtIV** bit (Extended IV) is always set to 1 for CCMP.

**Rsvd** denotes reserved fields.
CCMP encrypts the payload of a plaintext MPDU and encapsulates the resulting ciphertext using the following steps:

1. **Increment the Packet Number** (PN), to obtain a fresh PN for each MPDU where the Packet Number shall never repeat for the same temporal key (TK). Note that retransmitted packets are not modified on retransmission.

2. The fields in the MAC header are used to **construct the Additional Authentication Data** (AAD) for the CCM mode. The CCM algorithm provides integrity protection for the fields included in the AAD. MAC Header fields that may change when retransmitted are muted by being masked to 0 in the AAD.

3. Construct the **CCM Nonce block** (pseudo random number) from the PN, A2 and the Priority of the MPDU where A2 is MPDU Address2.

4. **Construct the CCMP Header** encoding the new PN and the Key ID into the 8 octet.

5. **CCM originator processing** uses the temporal key (TK), AAD, Nonce and MPDU data to form the ciphertext and MIC.

6. The Encrypted MPDU is formed by combining the original MAC Header, the CCMP header, the encrypted Data and the MIC.
CCMP Decapsulation Process

Steps of the decapsulation process:

1. The Encrypted MPDU is parsed to construct the AAD and Nonce values. The MIC is extracted for use in the CCM integrity checking.
2. The AAD is formed from the MAC Header of the Encrypted MPDU.
3. The Nonce value is constructed from A2, the PN, and Priority.
4. The CCM recipient processing uses the temporal key (TK), AAD, Nonce, MIC and MPDU ciphertext data to recover the MPDU plaintext data as well as check the integrity of the AAD and MPDU plaintext data.
5. The received MAC Header and the MPDU plaintext data from the CCM recipient processing may be concatenated to form a Plaintext MPDU.
6. The decryption processing prevents replay of MPDUs by validating that the PN in the MPDU is greater than the replay counter (PN') maintained for the session.
802.11i (RSN) – Summary

- **802.11i (RSN)** addresses security concerns for legacy hardware and new hardware.
- Security solution providing robust data encryption and user authentication.
- Addresses security requirements of infrastructure-based and ad-hoc-based 802.11 systems.
### WiFi Protected Access (WPA) – Overview

<table>
<thead>
<tr>
<th></th>
<th>WPA</th>
<th>WPA2</th>
</tr>
</thead>
</table>

PSK: Pre-shared key
Layered Security for Wireless Networks

1. Wireless deployment and policies

2. Wireless Access control

3. Perimeter Security

4. Application Security

Routing:
- eth0:1 10.4.0.254
- eth0:2 10.5.0.254
- eth0:3 10.6.0.254
- eth0:4 10.7.0.254
- eth1 10.1.0.254
- eth2 10.8.0.254
- eth2 10.9.0.254
- eth1 10.3.0.254
- eth0 10.0.0.254

Corresponding Node

WLAN Management

Access Point

Radio Interface

WLAN Accesspoint

AAA - Server

Firewall / VPN

Intrusion Detection

Security Infrastructure

Distribution System

Client

Radio Interface
Layered Security for Wireless Networks

Level 1: Wireless deployment and policy

- The foundation on which a secure environment is created
- Deploy the minimum number of APs needed for adequate coverage
- Set AP transmit power to the lowest practical level
- Verify broadcast coverage in and around facility
Layered Security for Wireless Networks

Level 2: Wireless access control (device access control)
- Configure highest level of encryption (WPA2 with CCMP)
- Do not broadcast SSID!
- Verify MAC address upon device connection

1. Wireless deployment and policies
2. Wireless access control

Diagram: Network topology with access points and switches, showing network addresses and connections.
Layered Security for Wireless Networks

Level 3: Perimeter Security

- User authentication
- Install an Intrusion Prevention / Detection System (IPS) and Firewalls
- Encrypt WLAN traffic using VPN (layer 2 or 3)
- Direct all traffic through VPN server and configure clients appropriately
- Maintain and enforce VPN routing and access policies

1. Wireless deployment and policies

2. Wireless Access control

3. Perimeter Security
Layered Security for Wireless Networks

Level 4: Application Security (end-to-end security)

- Implement application-level user-authentication system (above layer 4)
- Maintain and enforce permissions and password policies
- Install vendor patches as they become available

1. Wireless deployment and policies

2. Wireless Access control

3. Perimeter Security

4. Application Security
Layered Security for Wireless Networks – Summary

<table>
<thead>
<tr>
<th>Common wireless threat</th>
<th>Level 1 Wireless deployment and policies</th>
<th>Level 2 Wireless access control</th>
<th>Level 3 Perimeter security</th>
<th>Level 4 Application security</th>
</tr>
</thead>
<tbody>
<tr>
<td>unauthorized user</td>
<td></td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>unauthorized devices</td>
<td></td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>MAC spoofing</td>
<td></td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>man-in-the-middle attacks</td>
<td></td>
<td>√</td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>replay attacks</td>
<td></td>
<td></td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>DoS attacks</td>
<td></td>
<td>√</td>
<td>√</td>
<td></td>
</tr>
</tbody>
</table>

Each level contributes to the security of the network.
The more levels incorporated into a WLAN, the more secure the WLAN will be.
## Summary

<table>
<thead>
<tr>
<th>ESSID</th>
<th>Authentication Method</th>
<th>Authenticator</th>
<th>Authentication Type/Protocol</th>
<th>Encryption Key/Protocol</th>
<th>Encryption Algorithm</th>
</tr>
</thead>
<tbody>
<tr>
<td>One-way Auth.</td>
<td>AP</td>
<td></td>
<td>Pre-Shared (Plain Text)</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>MAC Filter</td>
<td>One-way Auth.</td>
<td>AP/RADIUS</td>
<td>Pre-Shared (Plain Text)</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>WEP</td>
<td>One-way Auth.</td>
<td>AP</td>
<td>Pre-Shared (Challenge)</td>
<td>Static WEP Key</td>
<td>RC4</td>
</tr>
<tr>
<td>802.1X</td>
<td>Mutual Auth.</td>
<td>RADIUS</td>
<td>EAP</td>
<td>Dynamic WEP Key</td>
<td>RC4</td>
</tr>
<tr>
<td>WPA</td>
<td>Mutual Auth.</td>
<td>RADIUS</td>
<td>EAP</td>
<td>TKIP</td>
<td>RC4</td>
</tr>
<tr>
<td>802.11i (WPA2)</td>
<td>Mutual Auth.</td>
<td>RADIUS</td>
<td>EAP</td>
<td>CCMP</td>
<td>AES</td>
</tr>
</tbody>
</table>
## Grade of WLAN Security Mechanisms

<table>
<thead>
<tr>
<th>Mechanism</th>
<th>Encryption</th>
<th>Authentication</th>
<th>Security Class</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN (incl. personal firewall) + 802.11i</td>
<td>VPN: 3DES o. AES</td>
<td>VPN: Certificates</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>WLAN: s.b.</td>
<td>WLAN s.b.</td>
<td></td>
</tr>
<tr>
<td>IEEE 802.11i or WPA2 + IEEE 802.1X</td>
<td>AES-CCMP</td>
<td>EAP-TLS</td>
<td>2</td>
</tr>
<tr>
<td>IEEE 802.11i WPA + IEEE 802.1X</td>
<td>RC4-TKIP</td>
<td>EAP-TLS</td>
<td>3</td>
</tr>
<tr>
<td>IEEE 802.11i or WPA2 + IEEE 802.1X</td>
<td>AES-CCMP</td>
<td>EAP-PEAP/ EAP-TTLS</td>
<td>4</td>
</tr>
<tr>
<td>IEEE 802.11i WPA + IEEE 802.1X</td>
<td>RC4-TKIP</td>
<td>EAP-PEAP/ EAP-TTLS</td>
<td>5</td>
</tr>
<tr>
<td>IEEE 802.11i or WPA2 + PSK</td>
<td>AES-CCMP</td>
<td>-</td>
<td>6</td>
</tr>
<tr>
<td>IEEE 802.11i or WPA + PSK</td>
<td>RC4-TKIP</td>
<td>-</td>
<td>7</td>
</tr>
<tr>
<td>WEP</td>
<td>RC4</td>
<td>-</td>
<td>8</td>
</tr>
</tbody>
</table>

Source: Technische Richtlinie 03103, v1, BSI
Mobility and WLAN Security

- **Layer 3 Mobility**
  - Mobility by means of DHCP
  - Mobile IP
  - Tunneling approaches

- **Roaming between WLAN-installations**
  - Roaming and WEP
  - Roaming and authentication by means of MAC-addresses
  - Roaming with VPN
  - Roaming with IEEE 802.11i and WPA

A lot of challenges and issues to solve!
Links

The Unofficial 802.11 Security Web Page
http://www.drizzle.com/~aboba/IEEE/

IEEE Std 802.1x Standard

WiFi Protected Access
http://www.wifialliance.com/OpenSection/protected_access.asp

IEEE Std 802.11i/D10.0
http://grouper.ieee.org/groups/802/11/private/Draft_Standards/11i/P802.11i-D10.0.pdf

Technische Richtlinie 03103, Version 1.0, Bundesamt für Sicherheit in der Informationstechnik, 2005
http://www.bsi.bund.de