

WLAN Security

Interim Solutions: TKIP and MIC

(C) Herbert Haas 2004/10/14

Content

In this chapter a detailed overview about today's WLAN security problems and solutions are presented.

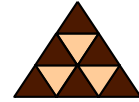
This subchapter provides an introduction into TKIP and MIC.

Objective

After completing this chapter the following tasks could be solved:

- Emphasize the basic vulnerabilities of WLAN
- Explain why WEP is insecure and give a mathematical example
- Compare WEP and TKIP/MIC
- Highlight the design flaws of the WLAN standard authentication
- Explain the design idea of 802.1x
- Compare EAP-TLS, LEAP, PEAP, EAP-TTLS, EAP-FAST with each other and emphasize important security features
- Explain the design concept of WPA and WPA2
- Implement a reliable 802.1x infrastructure over a WAN connection
- List important issues to be considered when choosing a VPN design
- Explain PSPF

802.11i

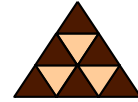


- **Two new network types**
 - ◆ **Transition Security Network (TSN)**
 - ◆ **Robust Security Network (RSN)**
- **An RSN only allows devices using TKIP/Michael and CCMP**
- **A TSN supports both RSN and pre-RSN (WEP) devices**
 - ◆ **Problem: broadcast packets have to be transmitted with the weakest common denominator security method**
 - ◆ **Consider a single client only supporting WEP**

Task Group i (TGi) was formed in March 2001 as a split from the MAC Enhancements Task Group (TGe). Its charge was to "enhance the 802.11 Media Access Control (MAC) to enhance security and authentication mechanisms." TGi finished work on the 802.11i standard, and it has been approved.

802.11i defines two WLAN network types: Transition Security Network (TSN) and Robust Security Network (RSN). RSNs only allow devices which support TKIP/Michael and CCMP. TSNs support both RSN devices and legacy pre-RSN, i. e. WEP devices. The drawback with RSN is that broadcast packets have to be transmitted with the weakest common denominator security method. If there is a device using WEP in a TSN network, it weakens the security of broadcast traffic for all the devices. RSN is definitely preferred, and getting all networks to use CCMP exclusively is the long term goal.

802.11i



**Pre-standard
802.11i
(WPA)**

- **Message Integrity Check (MIC)**
 - ◆ Nonlinear algorithm
- **Temporal Key Integrity Protocol (TKIP or “WEP2”)**
 - ◆ Also uses RC4-based WEP without the known flaws
 - Per-packet keys through IV mixing
 - Replay protection
 - ◆ Essentially a patch for WEP

**Ratified 802.11i
(WPA2)**

First WPA2 certifications
already since 1st Sept 2004

- **Counter Mode CBC MAC (CCMP)**
 - ◆ = AES + CBC-MAC
 - ◆ Replaces WEP !!!
(requires new HW support)

Recently, the **IEEE 802.11i** Security Task Group released two "informative texts" providing WEP hardening: MIC and TKIP. The IEEE 802.11 Task Group "i" is working on standardizing WLAN encryption improvements. Two new network types, called Transition Security Network (TSN) and Robust Security Network (RSN) had been defined.

The Temporal Key Integrity Protocol (TKIP), initially referred to as WEP2) is an interim solution (as part of TSN) that fixes the key reuse problem of WEP.

TKIP is a compromise on strong security and possibility to use existing hardware. Still uses RC4 but per-packet keys plus replay protection through a keyed packet authentication mechanism (Michael MIC).

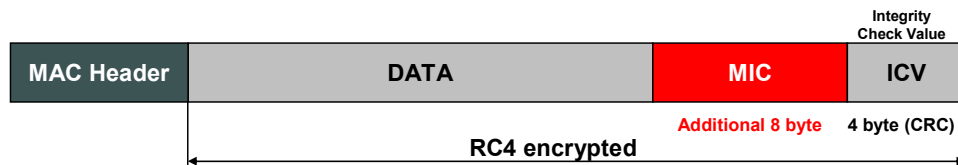
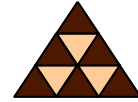
TKIP begins with a 128 bit "temporal key" shared among clients and access points. TKIP combines the temporal key with the client's MAC address and then adds a 6-byte IV to produce the key that will encrypt the data. Thus each station uses different key streams for encryption. TKIP changes keys every 10,000 packets, using a dynamic distribution method.

The IEEE plans to use the **Advanced Encryption Standard (AES)** instead of RC4 for TKIP in the long run (RSN), combined with Counter Mode - Cipher Block Chaining - Message Authentication Code (CBC MAC) to provide strong integrity and message authentication. Also the term "Wireless Robust Authenticated Protocol" (WRAP) is sometimes used synonymously for this concept.

The **Wi-Fi** specified TKIP and MIC as mandatory features of the **Wi-Fi Protected Access (WPA)** protocol, while AES should be part of WPA2.

Note: WiFi and particular vendors uses **different** TKIP/MIC algorithms, which are not compatible. Even WPA was intended to be an intermediate solution because the WiFi only picked a subset of the IEEE 802.11i working draft 3.0).

MIC (as used by WPA)



- **Encrypted checksum**
 - ♦ => Nonlinear function now
- **Uses "Michael" algorithm**
 - ♦ Much more lightweight than MD5 or SHA
- **Uses separate 64-bit key**
 - ♦ Data Integrity Key (DIK) derived from PTK after WPA key management
 - ♦ AP and STA use different MIC keys (128-bit DIK is split)

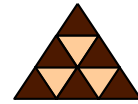
The Message Integrity Check (MIC) provides data integrity similar to CRC but provides a **non-linear** operation, the "Michael" algorithm, and is therefore not vulnerable after RC4 encryption.

The MIC is based on a **seed** value or a **secret key**, the destination and source MAC, and payload. That is, any change of these values significantly alter the MIC.

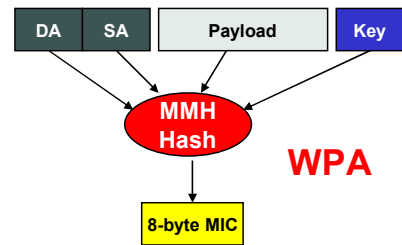
The 802.11i task group felt that other commonly used hashing algorithms such as SHA-1 were too computation-intensive to calculate on legacy hardware, so they agreed on the simpler Michael algorithm. Like many hash algorithms, Michael is calculated over the length of the packet, but all of the scrambling it does is based on shift operations and XOR additions, which are quick to calculate. Michael uses a key called the Michael key, which is derived during the WPA procedure (pairwise key).

But according to the 802.11i specification, the Michael algorithm "provides only weak protection against active attack." Therefore **MIC countermeasures** have been specified by the 802.11i: 1) logging and 2) disable and deauthenticate. If two Michael failures occur within one minute, both ends should disable all packet reception and transmission. In addition, the AP should deauthenticate all stations and delete all security associations—a rather drastic solution.

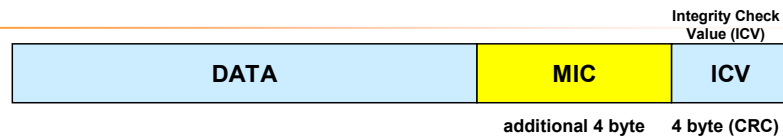
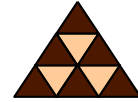
MIC Problems



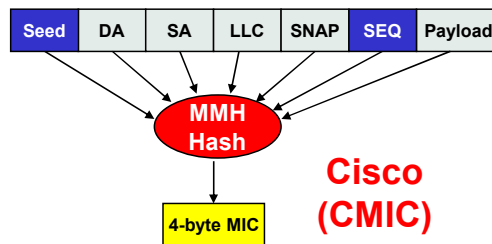
- **Michael algorithm**
 - ◆ Provides security level of only 20 bit strength
 - ◆ Attacker can construct forgery after approx 2^{19} tries (520,000 frames)
- **MIC Countermeasures**
 - ◆ Upon two MIC failures within 60 seconds, this AP disassociates *all* stations for at least 60 seconds and erases current keys in use
 - ◆ So attacker forgery trials become nearly impossible
 - ◆ Typically turned OFF (DoS!!!)



Cisco MIC (CMIC)

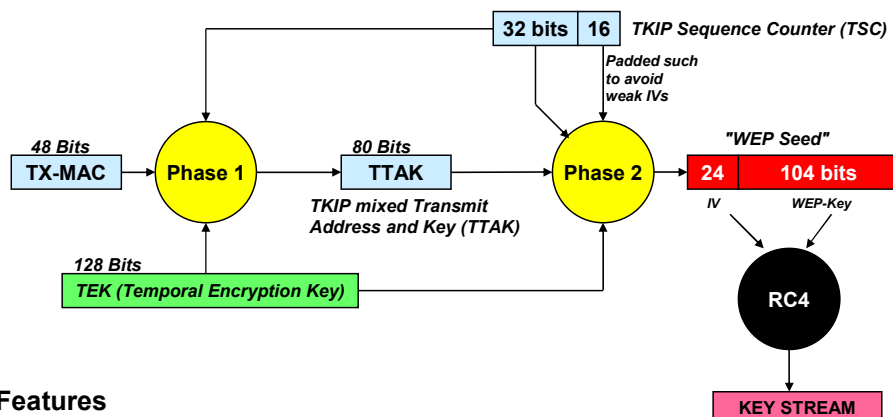


- Uses a seed value as pseudo-key
- Uses sequence number (AP verifies order)



Note: The Cisco Message Integrity Check serves the same purpose as the 802.11i MIC and is in fact stronger than Michael. It is based on Shai Halevi and Hugo Krawczyk's MMH hashing algorithm.

TKIP (As used by WPA)



- **Features**
 - ♦ Longer and unpredictable IV through IV/key mixing
 - ♦ Encrypted replay protection number (TSC)
- **WPA TKIP**
 - ♦ 48 bit IV, includes MAC
 - ♦ Fast S-box mixer
 - ♦ Fresh session keys on every association

The WPA's TKIP solution complies to the 802.11i proposals and uses fresh session keys on every association as well an 48-bit IV space. The mixing functions are based on substitution boxes (S-boxes), which are computationally very efficient, compared to other hash functions.

The **Temporal Encryption Key (TEK)** is derived from the "**Pairwise Master Key**" (PMK, also called "base key"), which has been negotiated by the WPA key management protocol. The TEK is used to securely hash a packet counter, the **TKIP Sequence Counter (TSC)**, and the transmit MAC address. A second hash stage enhances the security of the S-box principle.

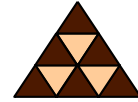
The TSC is split into 16-bit and 32-bit parts. The 16-bit part is padded to 24 bits to produce a traditional IV. The padding is done in a way that avoids the possibility of weak IV generation. Interestingly, the 32-bit part is not used for the transmitted IV generation; instead, it is utilized in the TKIP per-packet key mixing.

Phase 1 eliminates the use of the same key by all connections, and the second phase reduces the correlation between the IV and per-packet key.

The TSC starts at 0 and increases by 1 for each packet. TSCs must be remembered because they must never repeat for a given key. Each receiver keeps track of the highest value it has received from each MAC address. If it receives a packet that has a TSC value lower than or equal to one it has already received, it assumes it is a rebroadcast and drops it. Thus, packets can only arrive in sequence.

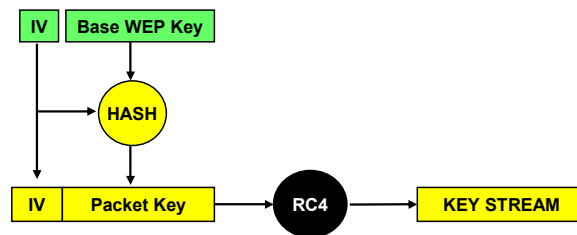
TKIP is only a SW-addon and can reuse the existing WEP hardware.

TKIP Details



- **Phase 1**
 - ♦ The high-order 32 bits of the TSC are combined with the TA and the first 80 bits of the TEK.
 - ♦ This phase of the key mixing is an iteration involving inexpensive addition, XOR, and AND operations, plus an S-box lookup reminiscent of the RC4 algorithm. These were chosen for their ease of computation on low-end devices such as APs.
 - ♦ Phase 1 produces an 80-bit value called TKIP mixed Transmit Address and Key (TTAK). Note that the only input of this phase that changes between packets is the TSC. Because it uses the high-order bits, it only changes every 64K packets.
 - ♦ Phase 1 can thus be run infrequently and use a stored TTAK to speed up processing. The inclusion of the transmitter's MAC address is important to allow a pair of stations to use the same TEK and TSC values and not repeat RC4 keys.
- **Phase 2**
 - ♦ Now the TTAK from phase 1 is combined with the full TEK and the full TSC.
 - ♦ This phase again uses inexpensive operations, including addition, XOR, AND, OR, bit-shifting, and an S-box.
 - ♦ The output is a 128-bit WEP seed that will be used as the RC4 key in the same manner as traditional WEP.
 - ♦ In the phase 2 algorithm, the first 24 bits of the WEP seed are constructed from the TSC in a way that avoids certain classes of weak RC4 keys.

Cisco TKIP ("CKIP")



- **Simple proprietary solution**
- **Still uses 24 bit IV but calculates per-packet WEP keys from IV**
 - ◆ Hash-based mixer

Because urgent security demands of the market, Cisco developed a proprietary "**Cisco KIP**" (**CKIP**), which is based on hashing the static WEP key together with the 24-bit IV to gain the actual packet key.

Also Cisco's solution provides per-packet keys, but **it is recommended to use WPA's TKIP** because:

- WPA's TKIP is computationally more efficient.
- It is more secure, because of the PMK involved.
- The dynamical RC4-key space is much bigger as compared to CKIP.
- Nearly all important vendors support WPA.



- **Against rumors, TKIP is reasonably safe!**
 - ♦ For each packet, the 48-bit IV is mixed with the 128-bit PTK to create a 104-bit RC4 key
 - There is practically no statistical correlation
 - Estimated one weak-IV per century (!)
 - ♦ Countermeasures against traffic re-injection
 - Sequence numbers + MIC
 - ♦ Robust 4-way handshake
- **Only problem: WPA-PSK**
 - ♦ Which uses a specified passphrase to PMK mapping => good passphrase required !!!
 - ♦ Otherwise dictionary attack possible

The estimated weak IV frames appearance interval with TKIP is about a century, so by the time a cracker collects the necessary 3,000 or more interesting IV frames, he or she would be 300,000 years old. [Found somewhere: CHECK!]