3GPP TSG SA WG3 Security — SA3#36 **S3-040916**
November 23-26, 2004
Shenzhen, China

Title: **Correction WRAP to CCMP**

Source: **CCSA/ZTE Corporation**
Agenda item: **WLAN-IW**
Document for: **Approval**

1 Introduction

WLAN interworking security specification TS 33.234 Annex A.1.3 mentioned three WLAN link layer encryption protocols, WEP, TKIP, and WRAP. WRAP is an option in early draft version of IEEE802.11i (e.g. D3.0). But it's removed from the last specification.
In IEEE 802.11i/D3.0 Draft[1], there are two sections, *i.e.*, addressing WRAP and CCMP respectively,

8.3.3 Wireless Robust Authenticated Protocol (WRAP) *47*
8.3.4 The Counter-Mode/CBC-MAC protocol (CCMP) *54*

In IEEE 802.11i-2004 final version[2], only CCMP is kept,

8.3.3 CTR With CBC-MAC Protocol (CCMP) *57*

In order to reflect the change in TS 33.234, it is necessary to delete the content of WRAP, and add the description of CCMP.

2 Proposal

Section A.1.3 is modified as follows:

A.1.3 Encryption and integrity protection

The air-link protection in IEEE 802.11 occurs in the MAC layer. This means that all layer-2 data frames, including LAN broadcasts, are protected. The 802.11-1999 standard specifies the Wired Equivalent Privacy (WEP) for encryption and integrity protection. The 802.11i task group is specifying two new encryption/integrity-protection protocols, the Temporal Key Integrity Protocol (TKIP) and the ~~Wireless Robust Authenticated Protocol (WRAP)~~CTR with CBC-MAC Protocol(CCMP). The 802.1X/EAP authentication mechanism can in principle be used with any of the three encryption protocols but configuration can restrict the number of allowed encryption protocols in a cell.
In order to be backwards compatible, an 802.11i-capable cell could support several encryption protocols simultaneously. For example, to support legacy stations a manually configured shared WEP key may need to be used for those stations. This key will then also be used as broadcast/multicast key for 802.11i-capable stations that instead use unique pair-wise keys for unicast traffic.

WEP

The IEEE 802.11-1999 Standard specified the Wireless Equivalent Privacy (WEP). WEP uses RC4 with a 40-bit key and 24-bit initialisation vector (IV) for encryption. RC4 is a stream cipher where a seed is used as input to the RC4 PRNG, which produces an output bit string, that is XOR'ed with the plaintext to produce the ciphertext. For WEP the seed to the RC4 PRNG is the key concatenated with the IV. The key is shared between the communicating parties and the IV is transmitted in clear text in each packet. Message integrity is provided using a CRC checksum that

is added to the payload and then encrypted together with the rest of the payload. WEP does not protect against replay.
Since the publication of the standard, several shortcomings of WEP have been discovered. Attacks to retrieve the WEP key and to modify the payload have been described. One weakness is the seed derivation. With RC4 it is important that each packet has a different RC4 seed. The RC4 seed in 802.11-1999 is constructed by concatenating the IV and the 40-bit key but the standard did not contain specifications to ensure uniqueness of <key,IV> pairs.
Today, WEP is not considered useful.

TKIP

The Temporal Key Integrity Protocol (TKIP) is a new protocol that will fix the known problems with WEP. TKIP uses the same ciphering kernel as WEP (RC4) but adds a number of functions:

- 128-bit encryption key;
- 48-bit Initialisation Vector;
- New Message Integrity Code (MIC);
- Initialisation Vector (IV) sequencing rules;
- Per-packet key mixing algorithm that provides a RC4 seed for each packet;
- Active countermeasures.

The purpose of TKIP is to provide a fix for WEP for existing 802.11b products. It is believed that essentially all existing 802.11b products can be software-upgraded with TKIP (all major 802.11 vendors participate in the 802.11i standardisation).
The TKIP MIC was designed with the constraint that it must run on existing 802.11 hardware. It does not offer very strong protection but was considered the best that could be achieved with the majority of legacy hardware. It is based on an algorithm called Michael that is a 64-bit MIC with 20-bit design strength. Details can be found in IEEE Std 802.11i [6].
The IV sequence is implemented as a monotonically incrementing counter that is unique for each key. This makes sure that each packet is encrypted with a unique <key, IV> pair, i.e. that an IV is not reused for the same key. The receiver shall also use the sequence counter to detect replay attacks. Since frames may arrive out of order due to traffic-class priority values, a replay window (16 packets) has to be used.
A number of "weak" RC4 keys have been identified for which knowledge of a few number of RC4 seed bits makes it possible to determine the initial RC4 output bits to a non-negligible probability. This makes it easier to crypto analyse data encrypted under these keys. The per-packet mixing function is designed to defeat weak-key attacks. In WEP, the IV and the key are concatenated and then used as seed to RC4. In TKIP, the cryptographic per-packet mixing function combines the key and the IV into a seed for RC4.
Because the TKIP MIC is relatively weak, TKIP uses countermeasures to compensate for this. If the receiver detects a MIC failure, the current encryption and integrity protection keys shall not be used again. To allow a follow-up by a system administrator the event shall be logged. The rate of MIC failure must also be kept below one per minute, which means that new keys shall not be generated if the last key update due to a MIC failure occurred less than a minute ago. In order to minimize the risk of false alarms, the MIC shall be verified after the CRC, IV and other checks have been performed.
TKIP is an interim solution to support 802.11i on legacy hardware. It is not considered as secure as the AES solution (~~WRAP~~CCMP) but very much better than WEP.

~~WRAP (AES)~~

~~The Wireless Robust Authenticated Protocol (WRAP) is the long-term solution and is based on the Advanced Encryption Standard (AES). AES is a block cipher that can be used in different modes of operation. In 802.11i, two modes have been discussed: Offset Codebook (OCB) and Counter-~~

~~mode with CBC-MAC (CCM). These two modes use AES differently to provide encryption and message integrity. OCB is a mode that provides both encryption and integrity in one run. CCM uses the Counter-mode for encryption and CBC-MAC for integrity. It is currently undecided if both or only one of the modes will be included in the final 802.11i spec. Both modes have been submitted to NIST as proposed block cipher modes.~~
~~The AES implementation requires hardware support and the majority of legacy 802.11b products will thus not be able to run WRAP.~~

CCMP(AES)

The CTR with CBC-MAC Protocol (CCMP) is the long term solution and is based on the Advanced Encryption Standard(AES). AES is a block cipher that can be used in different modes of operation. In 802.11i, Counter mode with CBC-MAC(CCM) is adopted. CCM based on AES can provide robust encryption and message integrity. CCM uses the Counter mode for encryption and CBC MAC for integrity.
The AES implementation requires hardware support and the majority of legacy 802.11 series products (802.11a, b, g and etc.) will thus not be able to run CCMP.

3 Reference

[1] IEEE 802.11i/D3.0, November 2002, “Draft Supplements to Standard for Telecommunications and Information Exchange Between Systems – LAN/MAN Specific Requirements-Specific requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Specification for Enhanced Security”.
[2] IEEE Std 802.11i, June 2004: "IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems – Local and Metropolitan Area Networks - Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and physical layer (PHY) specifications - Amendment 6: Media Access Control (MAC) Security Enhancement".