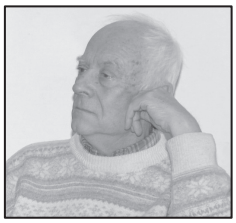

Prof. Dr. Eng. Anton POLICEC
Politechnica University of Timisoara
Electronics and Telecommunication Faculty
B-dul Vasile Pârvan Nr. 2, 300223
Timişoara, Romania

Drd. Eng. Gheorghe MÜLEC
Politechnica University of Timisoara
Electronics and Telecommunication Faculty
B-dul Vasile Pârvan Nr. 2, 300223
Timişoara, Romania
E-mail: george.mulec@rdslink.ro

Ass. Prof. Dr. Eng. Eugen MÂRZA
Politechnica University of Timisoara
Electronics and Telecommunication Faculty
B-dul Vasile Pârvan Nr. 2, 300223
Timişoara, Romania
E-mail: eugen.marza@etc.upt.ro

ANALYZING SECURITY MECHANISMS IN WLAN

NOTE: This paper was presented at the International Symposium "Research and Education in an Innovation Era", Section III, November 16-18, 2006, "Aurel Vlaicu" University of Arad, Romania.

ABSTRACT

Because of their flexibility, affordability, and ease of installation, the WLAN have become increasingly popular and widely used. Besides these advantages, inherent broadcast nature of wireless networks has raised security concerned. In this study we analyzing WLAN security standards from point of view of implementation the major security requirements in communication systems and the features and weakness of them.

KEYWORDS:

communication, WLAN, security, standard, authentication.

INTRODUCTION

The market for wireless communications has experienced incredible growth over recent years. Wireless Local Area Networks (WLANs) have quickly found a significant place and popularity in business and the computer industry alike [1]. The major benefit of WLANs is increased flexibility and mobility [2].Security risks in wireless networks are equal to the sum of the risk of operating a wired network plus the new risks introduced due to the portability of wireless devices [3].
Starting from these security requirements, we have analyzed the security standards for Wireless Local Area Networks.
There are three security standards of WLAN:

- *WEP* (Wired Equivalent Privacy) - proposed by IEEE 802.11 Task Group.
- *WPA* – (Wi-Fi Protected Access) – proposed by Wi-Fi Alliance (The Wi-Fi alliance is an alliance of major 802.11 vendors formed with the aim of ensuring product interoperability).
- *IEEE 802.11i* – (which has also come to be known as WPA2) – proposed by IEEE 802.11i task group in June 2004.

CRYPTOGRAPHY ELEMENTS

For satisfy requirements of a secure communication network the cryptography comes in. The goal of cryptography is to design, implement, deploy, and make use of cryptographic systems that are secure in some meaningful way [4].

Authentication

There are three important requirements for achieve an authentication [5]. *Mutual authentication*, *Self protecting*, *Produces session key.* In WLAN are used three types of authentication methods.

A1. Open system authentication (**Fig. 1**) – This method permit any station (STA) which wants to join a network to send an authentication request to access point (AP).

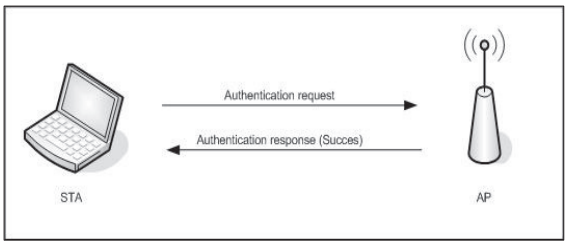

Fig. 1 – Open System Authentication

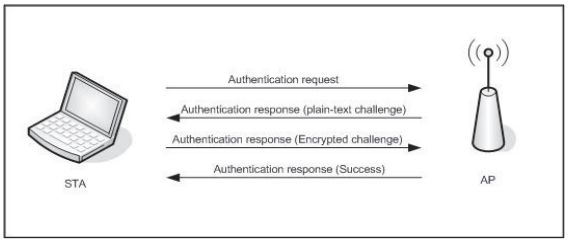

Fig. 2 – Shared Key Authentication

A2. Shared key authentication (**Fig. 2**) – This method is based on the challenge-response system. Using this method it requires that the STA and the AP be capable of using WEP and both to have a preshared key. The method doesn't produce session key, because the session key is the same with preshared key which is achieve through manual configuration for each entities involved.

A3. 802.1x authentication – Is a different approach to authentication and authorization for IEEE 802.11 that is based on the 802.1X standard, which was originally published by the IEEE in 1999, and was revised in 2001 [6].

The 802.1X standard makes use of the *Extensible Authentication Protocol* (EAP) [7] as a way of communicating authentication information between the supplicant (STA) and the Authentication Server (AS), passing through the AP – **fig. 3**.

The 802.1x port model (**Fig. 4**) is a logical model consisting of a switch with multiple logical switches, where there is one logical switch per user. The strength of IEEE 802.1x authentication lies in other authentication mechanism that is implemented above it. (ex . EAP-TLS, EAP-TTLS, etc.). When the IEEE 802.1X authentication completes successfully, the STA and the AS will share a secret, called a MSK (Master Session Key).

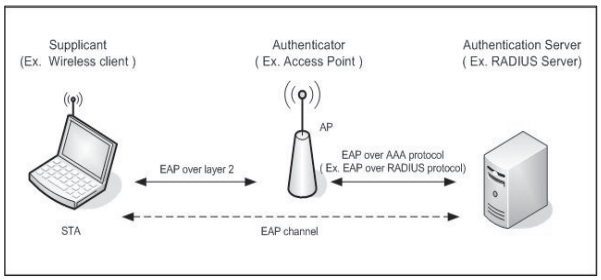

Fig. 3 – EAP protocol implementation

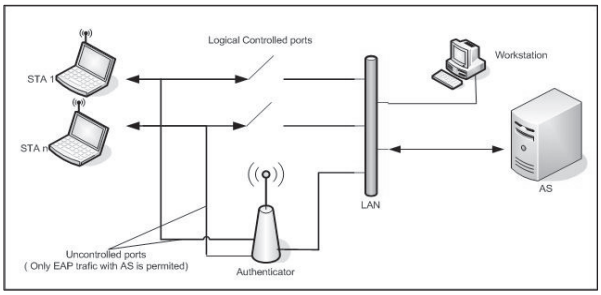

Fig. 4 – 802.1x model

Confidentiality

The confidentially is ensure by Symmetric Key Cryptography. Symmetric key Cryptography refers to the process in which the sender and the receiver use the same shared key to encrypt and decrypt messages.

Data Integrity

To ensure that a packet has not been modified in transit, WLAN uses an Integrity Check Value (ICV) field in the packet. ICV is known also as another name for Message Integrity Check (MIC). The idea behind the ICV is that the receiver should be able to detect data modifications or forgeries by calculating the ICV over the received data and comparing it with the ICV attached in the message.

SECURITY STANDARD IN WLAN

The 802.11 security architecture is compound by three security standard: WEP, WPA and 802.11i [8]. We will analyze all these standards and will accentuate on its features and weakness.

WEP – WIRED EQUIVALENT PRIVACY

It is the first security standard deployed in WLAN, when security was not very important.

Authentication with WEP

WEP support two types of authentication: Open authentication and Shared Key Authentication .Although in open authentication is no authentication at all, whoever wants to join to the network is permit. When the WEP encryption is enable, even through authentication is successful, the STA will be unable to transmit data through AP [9]. Neither has it decrypted data sent from AP.

Confidentiality with WEP

WEP uses RC4 (a stream cipher) in synchronous mode for encrypting data packets. The problem is that a stream cipher is not suitable for a wireless medium where packet loss is widespread.

Data integrity with WEP

To ensure that a packet has not been modified in transit, 802.11 use an Integrity Check Value (ICV) field in the packet. The ICV is compute with Cyclic Redundancy Check-32 bits (CRC-32) from data payload of an 802.11 packet.

The problem with the message integrity mechanism specified in 802.11 is not only that it uses a linear integrity check algorithm (CRC32) but also the fact that the ICV does not protect all the information that needs to be protected from modification.

WPA – Wi-Fi Protected Access

We consider that WPA is a bridge between WEP and 802.11i. To improve the security of 802.11 networks without requiring a hardware upgrade, the Wi-Fi alliance adopted Temporal Key Integrity Protocol (TKIP) as the security standard that needs to be deployed for Wi-Fi certification.

WPA is basically a prestandard subset of 802.11i which includes the key management and the authentication architecture (802.1X) specified in 802.11i [10].

Authentication with WPA

In a WPA environment are possible two types of authentication mechanism. The first is the same as a WEP and the second is based on the 802.1x framework.

WPA extends the two-tier key-hierarchy of WEP to a multi tier hierarchy. At the top level is still the MK, referred to as the Pair-wise Master Key (PMK) in WPA. WPA uses the PMK for deriving the Pair-wise Transient Keys (PTK) which are basically session keys. The term PTK is used to refer to a set of session keys which consists of four keys, each of which is 128 bits long.

These four keys are as follows: an encryption key for data, an integrity key for data, an encryption key for EAPoL messages and an integration key for EAPoL messages.

Confidentiality with WPA

TKIP doubles the IV size from 24 bits to 48 bits. This results in increasing the time to key collision. Actually, the IV is increased from 24 bits to 56 bits by requiring the insertion of 32 bits between the existing WEP IV and the start of the encrypted data in the WEP packet format.

Existing WEP hardware accelerators expect a 24-bit IV as an input to concatenate with a preshared key (40/104-bit) in order to generate the per-packet key (64/128-bit). This hardware cannot be upgraded to deal with a 48-bit IV and generate an 88/156-bit key. The approach, therefore, is to use per-packet key mixing, that has a key mixing function instead of simply concatenating the IV to the master key to generate per-packet key, increases the effective IV size while still being compatible with existing WEP hardware.

Data integrity with WPA

WEP used CRC-32 as an integrity check that is not a cryptographically secure integrity protocol. TKIP introduce a new ICV protocol—MICHAEL—which uses no multiplication operations and relies instead on shift and add operations. This protocol improves the CRC-32 integrity protocol. Another enhancement that TKIP makes in IV selection and use is to use the IV as a sequence counter.

IEEE 802.11i – Robust Security Network

WPA was a bridge to the final solution which was being designed by the IEEE 802.11i task group. This security proposal was referred to as the Robust Security Network (RSN) and also came to be known as the 802.11i security solution. The Wi-Fi

alliance integrated this solution in their proposal and called it WPA2.

Authentication with 802.11i

WPA had also adopted the authentication architecture specified in 802.11i completely. Therefore, the authentication architecture in WPA and 802.11i is identical.

Confidentiality with 802.11i

To provide confidentiality in 802.11i, AES is used in the counter mode. Counter mode actually uses a block cipher as a stream cipher, thus combining the security of a block cipher with the ease of use of a stream cipher.

The AES cipher is then used to encrypt the counter to produce a key stream. When the original message arrives, it is broken up into 128-bit blocks and each block is XOR-ed with the corresponding 128 bits of the generated key stream to produce the cipher-text.

The main features of AES in counter mode are: Block cipher operated as a stream cipher; Key stream can be generated before the message arrives; The various blocks of the message can be encrypted in parallel; The length of the encrypted text can be exactly the same as the length of the plain text message.

Data integrity with 802.11i

To achieve message integrity, IEEE 802.11i Task Group extended the counter mode to include a Cipher Block Chaining (CBC)-MAC Operation (CCMP). CBC-MAC XORred a plain-text block with the previous cipher block before encrypting it. This ensures that any change made to any cipher-text block changes the decrypted output of the last block and hence changes the residue. CBC-MAC is an established technique for message integrity.

CONCLUSION

WEP encapsulation is flawed at many levels and WPA is designed to patch the vulnerabilities while reusing existing hardware. WPA provides an acceptable level of security in legacy WLAN devices. WPA only requires firmware or device driver updates and is fairly easy to implement and deploy.
For using IEEE 802.11i (WPA2) is required a new hardware device with new computational capabilities. The main features of 802.11i towards WPA are that replace stream cipher (RC4) with a strong block cipher (AES) and provide a stronger integrity protection AES-based CCMP.

REFERENCES

[1] Gast M. (2002).Chapter 6: Security, Take 2: 802.1 X, 802.11 Wireless Networks: The Definitive Guide. O'Reilly. ISBN 0-596-00183-5, April.
[2] Kapp S. (2002). 802.11: leaving the wire behind. Internet Computing, IEEE. Volume 6 Issue, pages 82-85 , February.
[3] Karygiannis T& L. Owens. (2002). Draft : Wireless Network Security – 802.11, Bluetooth and Handheld Devices. USA, National Institute of Standards and Technology.
[4] W. Diffie and M. E. Hellman, "New Directions in Cryptography," IEEE Transactions on Information Theory, vol. 22, pp. 644–654, Nov. 1976.
[5] Rescorla, E., "A Survey of Authentication Mechanisms", Internet Architecture Board (IAB), work in progress, draft-iab-auth-mech-02.txt, October 2003.
[6] IEEE Std 802.1x-2001: Port Based Network Access Control, http://www.ieee802.org/1/pages/802.1x.html, June 2001
[7] 10. B. Aboba, "Extensible Authentication Protocol (EAP)." RFC 3748 (Standards Track), June 2004.
[8] "IEEE 802 Standards", http://standards.ieee.org/getieee802
[9] Gast M. (2002), Wired Equivalent Privacy (WEP), 802.11 Wireless Networks: The Definitive Guide. O'Reilly.
[10] C. He and J. C. Mitchell, "Security Analysis and Improvements for IEEE 802.11i," Proceedings of Network and Distributed System Security Symposium (NDSS), (San Diego, CA), Feb. 2005.