Analysis and Countermeasure on Vulnerability of WPA Key Exchange Mechanism

You Sung Kang[1], KyungHee Oh[1], ByungHo Chung[1], Kyoil Chung[1], and DaeHun Nyang[2]

[1] Information Security Research Division
Electronics and Telecommunications Research Institute
Daejeon, 305-350, Korea
{youskang,khoh,cbh,kyoil}@etri.re.kr
[2] The Graduate School of Information Technology and Telecommunications
InHa University
Incheon, 402-753, Korea
nyang@inha.ac.kr

Abstract. In this paper, we analyze some weaknesses in WPA authenticator key management state machine and propose the countermeasures to overcome these problems. Our researches on IEEE 802.11i authenticator state machine that is WPA authenticator key management state machine reveal that the state machine cannot support the stable group key setting and is vulnerable to the replay attack and DoS attack. We describe 3 problems related to these vulnerabilities, propose the respective solutions and reconstruct WPA authenticator key management state machine to which the alternative solutions are applied.

Keywords: WLAN security, WPA, 802.11i, 802.1X

1 Introduction

Most of the WLAN (Wireless Local Area Network) products are based on the IEEE 802.11 standard and certified by Wi-Fi Alliance [1]. However, it is common knowledge that these products provide only limited support for confidentiality through the WEP (Wired Equivalent Privacy) protocol that contains significant flaws in the design [2]. The IEEE 802.11 TGi (Task Group i) has proposed the security architecture for IEEE 802.11 standard in order to enhance the security function [3]. In addition, Wi-Fi Alliance has released WPA (Wi-Fi Protected Access) specification as Wi-Fi security standard that is a subset of IEEE 802.11i Draft 3.0 [4]. The Wi-Fi Alliance is a nonprofit international association formed in 1999 to certify interoperability of WLAN products based on IEEE 802.11 specification. The Wi-Fi Alliance in conjunction with the IEEE 802.11 WG (Working Group), has driven an effort to bring strongly enhanced, interoperable Wi-Fi security. The result of this effort is WPA [5].

The IEEE 802.11i standard is intended to provide strong authentication, access control, key management, key establishment, and cipher algorithm. Unfortunately, our researches on IEEE 802.11i authenticator state machine that is WPA

H.-K. Kahng and S. Goto (Eds.): ICOIN 2004, LNCS 3090, pp. 915–924, 2004.

authenticator key management state machine reveal that the state machine cannot support the stable group key setting and is vulnerable to the replay attack and DoS (Denial of Service) attack. In this paper, we analyze the vulnerabilities on WPA authenticator key management state machine and propose the countermeasures to overcome these problems. We describe 3 problems and propose the respective solutions. These problems are as follows. The first is vulnerability due to the number of stations to exchange GTK, the second is vulnerability due to the reuse of ANonce when PTK update request is received, and the last is vulnerability due to the incorrect transition after timeout event. In addition, we reconstruct WPA authenticator key management state machine to clarify group key distribution procedure.

The paper is organized as follows. In section 2, the overview of WPA standard is explained briefly. Section 3 describes the technologies related to the general WLAN key establishment. In section 4, we describe the AP action in the WLAN system and analyze weaknesses of WPA key management mechanism. In addition, we explain the respective countermeasures in detail and reconstruct a new key management state machine to which the solutions are applied. Finally, section 5 concludes the paper.

2 WPA Overview

To strengthen user authentication, WPA implements IEEE 802.1X standard as a basis for access control and EAP (Extensible Authentication Protocol) as a framework for authentication message [6, 7]. This framework utilizes a central authentication server, such as RADIUS (Remote Authentication Dial In User Service) [8], to authenticate each user. After acquisition of PMK (Pairwise Master Key) from a central authentication server or PSK (Pre-Shared Key), WPA performs 4-way handshake and group key handshake to distribute PTK (Pairwise Transient Key) and GTK (Group Transient Key), respectively. The default cipher algorithm in WPA standard is TKIP (Temporal Key Integrity Protocol) with the Michael integrity check.

In IEEE 802.11, all the stations must get each PTK because an associated station is treated as a logical port. But, they must have the same GTK that is generated in the AP at the time of the first station connection. If the AP is required to update GTK, the AP must maintain both of the old GTK and a new GTK. In addition, the AP must manage the total number of stations to be sent the group key and the number of stations left to have group key updated. Therefore, the AP must have a state machine performing GTK generation, GTK setting, and GTK update. WPA Authenticator key management state machine (refer [3] section 8.5.6) performs these functions. In section 4 in this paper, we give an explanation about problems included in this state machine.

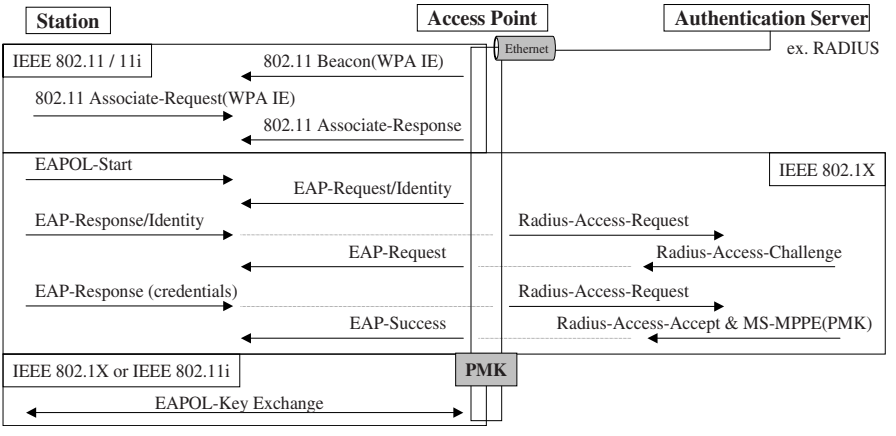

Fig. 1. PMK acquisition using IEEE 802.1X with EAP authentication

3 Key Establishment Mechanism

There are two methods for the dynamic key exchange. One is IEEE 802.1X key transmission using IEEE 802.1X authenticator key transmit state machine (refer [6] section 8.5.5). The other is WPA key exchange using WPA authenticator key management state machine. Both of two must be the next step of PMK acquisition.

3.1 PMK Acquisition

To get PMK, the AP supports two authenticated key management protocols in infrastructure mode using IEEE 802.1X with pre-shared key and with EAP authentication. Fig. 1 shows a sequence of PMK Acquisition using IEEE 802.1X with EAP authentication. EAP-TLS protocol is a typical EAP-method for getting PMK [9].

After association between a station and an AP, the exchange of EAP authentication frame happens. The second box in Fig. 1 illustrates a supplicant-initiated authentication conversation. The AP can get PMK for the associated station via MS-MPPE (Microsoft Point-to-Point Encryption) attribute as a result of IEEE 802.1X with EAP Authentication [10]. If the station is the non-WPA station the AP can use IEEE 802.1X authenticator key transmit state machine to send WEP key to the station. On the other hand, if the station is the WPA station supporting TKIP encryption the AP can use WPA authenticator key management state machine to establishment TKIP key.

3.2 IEEE 802.1X Key Transmission

According to IEEE 802.1X standard, the IEEE 802.1X authenticator key transmission state machine is an option of implementation [6]. In addition, the standard does not define an ACK of a received EAPOL-Key (EAP Over LAN) frame,

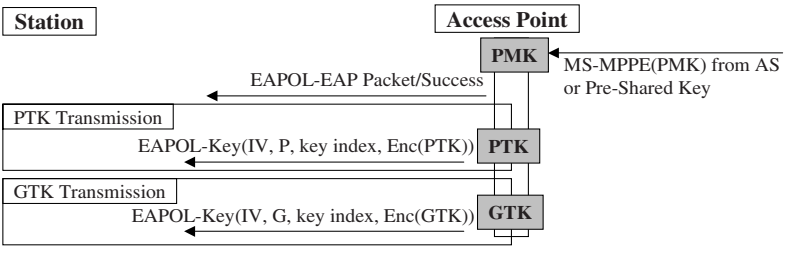

Fig. 2. IEEE 802.1X key transmission procedure

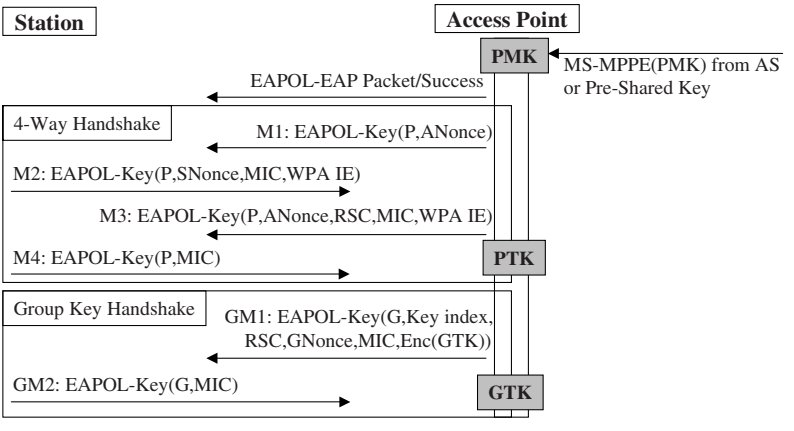

Fig. 3. WPA key exchange procedure

therefore the AP is not responsible for a complete key establishment with a non-WPA supplicant. The IEEE 802.1X key transmission procedure for non-WPA supplicant appears as illustrated in Fig. 2. After PMK acquisition, the AP sends EAP-Success frame to the station. The station receiving EAP-Success frame waits for EAPOL-Key frame. And then, the AP sends pairwise EAPOL-Key frame containing encrypted PTK and group EAPOL-Key frame containing encrypted GTK to the station sequentially. The encryption key used to encrypt the PTK or the GTK is a concatenate string of IV and PMK.

3.3 WPA Key Exchange

WPA defines the 4-way handshake for pairwise key exchange and the group key handshake for group key exchange. Fig. 3 illustrates the WPA key exchange procedure including 4-way handshake and group key handshake.

The 4-way handshake confirms the liveness of the peers communicating directly with each other over the IEEE 802.11 link, guarantees the freshness of the their shared PTK, and synchronizes the usage of the PTK to secure the IEEE 802.11 link [3]. The AP uses the group key handshake to send a new GTK to the

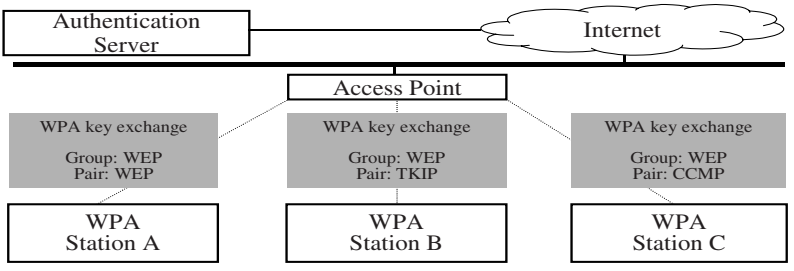

Fig. 4. WLAN system with many WPA clients

station. The PTKs are used between a single AP and a single station but the GTK is used between a single AP and all the stations authenticated to that AP. After PMK acquisition, the AP sends EAP-Success frame to the station. And then, the AP sends the first pairwise EAPOL-Key frame containing a random number called ANonce (Authenticator Nonce). The second frame comes from the station and includes SNonce (Supplicant Nonce). Next, the AP calculates PTK by means of PRF (Pseudo Random Function) using the PMK, the ANonce, and the SNonce as function parameters. After successful 4-way handshake, the AP sends group EAPOL-Key frame containing encrypted GTK to the station. The encryption key used to encrypt the GTK is a part of the preceding PTK.

4 Problems and Proposed Solutions

In a WLAN system with many WPA clients, a likely scenario is that AP supports the respective unicast keys and the common broadcast key. Fig. 4 shows the WLAN system including the WPA AP and many WPA stations.

WPA AP operating in the WPA WLAN system must support WPA key exchange procedure and may use the various cipher algorithms for unicast data. But the AP must use only one cipher algorithm and key for broadcast data. For example, if the stations supplicate the AP to exchange pairwise key and group key by using WPA authenticator key management state machine and each station uses each cipher algorithm as shown in Fig. 4, the AP must use the WEP as group cipher algorithm because the WEP is a common algorithm that all the stations can support. However, the AP uses the respective algorithm for unicast data according to the negotiation result between each station and the AP.

The WPA station employs WPA key exchange procedure shown in Fig. 3 as the key exchange procedure. The state machine related to 4-way handshake and group key handshake is WPA authenticator key management state machine. Fig. 5 shows the WPA authenticator key management state machine. According to the IEEE 802.11i specification, this state machine is responsible for group key exchange with the associated station.

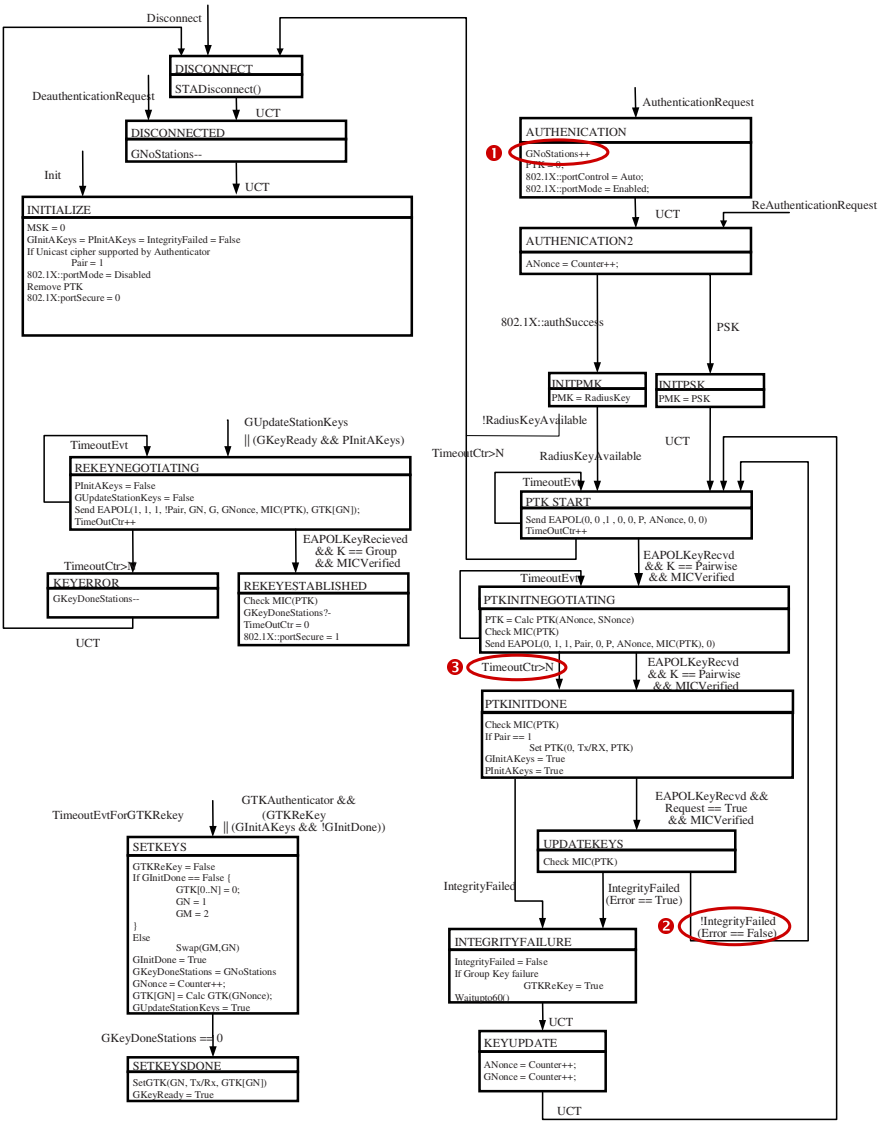

Fig. 5. Weak points in WPA authenticator key management state machine

Unfortunately, this state machine cannot support the stable group key setting and is vulnerable to the replay attack and DoS attack. In this section, 3 problems indicated by circles in Fig. 5 are described in detail and the alternative countermeasures are suggested, respectively. Fig. 6 shows the enhanced WPA authenticator key management state machine to which the alternative solutions are applied.

4.1 Vulnerability Due to the Number of Stations to Receive GTK

This weakness has a close relation to system stability. After the association of the first WPA station, this state machine will successfully support pairwise key exchange, PTK setting, group key exchange, and GTK setting. And then, the sequential WPA stations establish each PTK and the same GTK through the normal operation of this state machine. The normal operation means that the AP and the associated station acquire PMK after IEEE 802.1X authentication with EAP or PSK, the AP counts the authenticated station in the total number of stations to receive GTK, and the AP excludes the station succeeding in group key establishment from the total number of stations to receive GTK. Therefore, the AP fails to set new GTK when the AP counts the associated station in the total number of stations to receive GTK but it does not exclude the station from the number.

In Fig. 5, the variable of 'GNoStations' is the number of stations to receive GTK. This variable increases when the associated station wants the AP to be authenticated. The variable of 'GKeyDoneStations' is the number of stations left to have group key updated. In SETKEYS state, 'GKeyDoneStations' is substituted for 'GNoStations' and GTK is set in SETKEYDONE state when 'GKeyDoneStations' becomes zero.

However, a procedure with a station stays at AUTHENTICATION2 state if the AP fails to perform IEEE 802.1X authentication or the station does not request IEEE 802.1X authentication. In this case, though the variable of 'GNoStations' increases in AUTHENTICATION state the variable of 'GKeyDoneStations' for this station does not decrease because the procedure cannot reach REKEYESTABLISHED state including the operation of 'GKeyDoneStation--'. As a result of stay at AUTHENTICATION2 state, the AP fails to set new GTK.

A simple solution to resolve this problem could be to add a state transition from AUTHENTICATION2 to DISCONNECT when the authentication fails. This transition can decrease 'GNoStations' after the authentication failure. But this solution has a weak point of the processing overhead due to the disconnection and re-initialization of the station, whenever the authentication is retried.

In order to stably set the group key, we let the operation of 'GNoStaions++' be located in INITPMK state or INITPSK state as shown in Fig. 6. This modification makes the AP consider only the stations completing IEEE 802.1X authentication as an object of the operation of 'GNoStations++'. This solution can correctly control 'GNoStations' under consideration of the authentication result and does not require the additional processing overhead. In actual implementation, an indicator informing the AP that the operation of 'GNoStations++' was performed may be used. It helps the AP manage the operation of 'GNoStations++' and 'GNoStations--'.

4.2 Vulnerability Due to the Reuse of ANonce after PTK Update Request

This weakness has a close relation to the replay attack. PTK is calculated using the parameters such as PMK, ANonce, SNonce, AP hardware address, and

station hardware address. In case of the same PMK, new ANonce and new SNonce must be required to calculate new PTK. The transition line ❷ shown in Fig. 5 results from the station's PTK update request. The line directly reaches PTKSTART state from UPDATEKEYS state when the AP receives EAPOL-Key frame demanding PTK update. In other words, the existing state machine reuses ANonce when PTK update is required. The reuse of ANonce may be a potential defect such as a replay attack. For example, when an attacker who eavesdrops the previous 4-way handshake messages requests EAPOL-Key update and receives the first EAPOL-Key frame of 4-way handshake from the AP, he can successfully forge the second EAPOL-Key frame by using the previous messages because the first EAPOL-Key frame is the same frame as the previous frame.

In order to overcome this vulnerability, we let the line ❷ go through KEYUPDATE state to PTKSTART as shown in Fig. 6. If the AP receives EAPOL-Key frame demanding PTK update, ANonce increases in KEYUPDATE state. Therefore, the AP can send the first EAPOL-Key frame of 4-way handshake, containing new ANonce.

4.3 Vulnerability Due to the Incorrect Transition after Timeout Event

This weakness has a close relation to the DoS attack. The variable of 'TimeoutCtr' maintains the count of EAPOL-Key frame receive timeouts. If this value exceeds the defined number the AP must disconnect the station that is exchanging EAPOL-Key frames. However, PTKINITNEGOTIATING state is changed to PTKINITDONE in spite of the fact that the variable of 'TimeoutCtr' exceeds the limited number as shown in Fig. 5. The current incorrect transition cannot appropriately cope with the wrong EAPOL-Key frame. This problem makes a cause of the DoS attack because the AP continuously wastes its resource to process the bad EAPOL-Key frame.

In order to overcome this vulnerability, we made the AP's state be changed from PTKINITNEGOTIATING state to DISCONNECT state when the variable of 'TimeoutCtr' exceeds the limited number as shown in Fig. 6. That is, the AP disconnects the station that sends incorrect EAPOL-Key frames.

5 Conclusions and Future Works

Our researches on WPA authenticator key management state machine demonstrate that it is inappropriate to be implemented without modification. Fig. 6 shows the reconstructed WPA authenticator key management state machine to which our solutions are applied. The proposed countermeasures help the AP solve 3 problems investigated in this paper, such as the incorrect position of 'GNoStations++', the reuse of ANonce, and the incorrect treatment of timeout event.

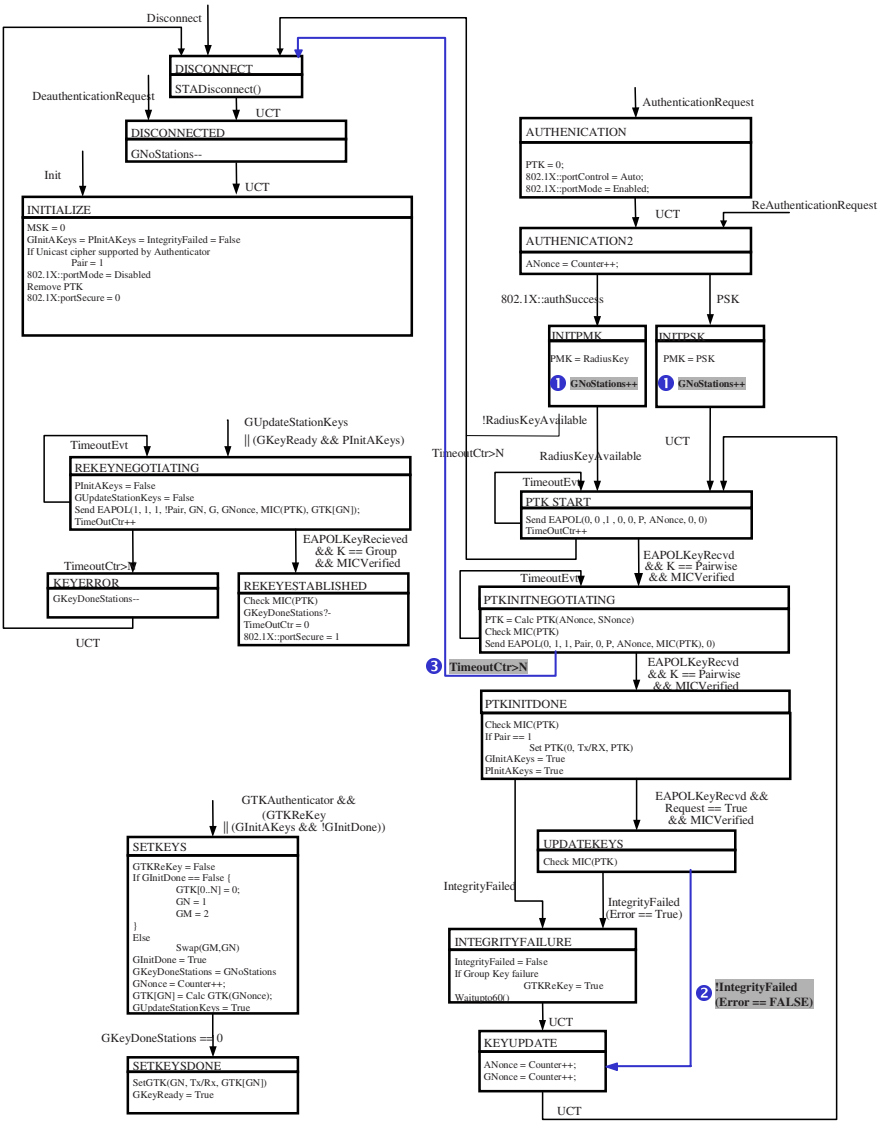

Fig. 6. Reconstruction of WPA authenticator key management state machine

The proposed state machine did not consider the functions supporting the technology related to secure hand-off or global roaming, though it can support user authentication, secure key exchange, and data confidentiality in single BSS (Basic Service Set). The IEEE 802.11 standards body is now working on significant improvements such as IAPP (Inter-Access Point Protocol) and pre-authentication [12, 13]. Therefore, the further study is expected to advance in

order to support distributed authentication for global roaming, context transfer for pre-authentication, improved cipher algorithm.

References

[1] ISO/IEC 8802-11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications. ISO/IEC 8802-11 (1999) 915
[2] J. R. Walker: Unsafe at any key size; An analysis of the WEP encapsulation. IEEE 802.11-00/362 (2000) 915
[3] IEEE 802.11: LAN/MAN Specific Requirements- Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specification: Specification for Enhanced Security. IEEE Std 802.11i/D3.0 (2002) 915, 916, 918
[4] Wi-Fi Alliance: Wi-Fi Protected Access (WPA). WPA Version 2.0 (2003) 915
[5] Wi-Fi Alliance: Overview Wi-Fi Protected Access. http://www.wi-fi.org/OpenSection/pdf/Wi-Fi_Protected_Access_Overview.pdf 915
[6] IEEE 802.1: Standard for Local and metropolitan area networks- Port-Based Network Access Control. IEEE Std 802.1X (2001) 916, 917
[7] L. Blunk and J. Vollbrecht: PPP Extensible Authentication Protocol (EAP). IETF (1998) 916
[8] C. Rigney: Remote Authentication Dial In User Service (RADIUS). IETF (2000) 916
[9] B. Aboba, D. Simon: PPP EAP TLS Authentication Protocol. IETF (1999) 917
[10] G. Pall, G. Zorn: Microsoft Point-To-Point Encryption (MPPE) Protocol. IETF (2001) 917
[11] IEEE 802.1: Standard for Local and metropolitan area networks- Port-Based Network Access Control- Amendment 1: Technical and Editorial Corrections. IEEE P802.1aa/D6.1 (2003)
[12] IEEE 802.11: Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation. IEEE Std 802.11f/D5 (2003) 923
[13] B. Aboba: IEEE 802.1X Pre-Authentication. IEEE 802.11-02/389r1 (2002) 923