Security Analysis and Authentication Improvement for IEEE 802.11i Specification

Xinyu Xing, Elhadi Shakshuki, Darcy Benoit
Jodrey School of Computer Science
Acadia University
Wolfville, Nova Scotia, Canada
{085094x, elhadi.shakshuki, darcy.benoit}@acadiau.ca

Tarek Sheltami
Computer Engineering Department
King Fahd University of Petroleum and Minerals
Dammam, Saudi Arabia
tarek@kfupm.edu.sa

Abstract—The IEEE 802.11i amendment has been finalized to address the security issues in wireless local area networks. A prodigious amount of research has demonstrated that the IEEE 802.11i specification is sufficient to prevent unauthorized access and use. In this paper, we analyze the IEEE 802.11i wireless networking amendment with respect to data confidentiality, integrity, mutual authentication and availability. Our analysis indicates that a number of serious threats have still not been addressed by the 802.11i amendment. This includes DoS attacks, insider attacks, offline guessing attacks, etc. Furthermore, configuring security features on a commercial Wi-Fi network is moderately-to-very difficult. Towards this end, this paper proposes an improved authentication mechanism which adopts asymmetric cryptography and thus accomplishes link-layer frame protection. Through our further analysis and discussion, we conclude that the proposed mechanism not only prevents potential security threats but also accomplishes autonomic security configuration without human intervention.

Keywords—IEEE 802.11i; WEP; WLANs; Asymmetric cryptography

I. INTRODUCTION

A Wireless Local Area Network (WLAN) enables access to computing resources for devices that are not physically connected to a network. Although WLANs work over a fairly limited range, they effectively enhance user mobility by acting as an extension of the wired local network. In a wired LAN, an adversary has to gain physical access to the LAN by compromising a host on the LAN. In contrast to a Wired LAN, an attacker simply needs to be within the range of the WLAN infrastructure to gain access. In addition, highly sensitive directional antennas can be utilized to extend the effective range of the WLAN beyond the standard range. Therefore, establishing wireless robust security networks has become a principal concern.

Prior to the IEEE 802.11i amendment, original IEEE 802.11 specification has a prodigious amount of security weaknesses [1][10][11]. To address these weaknesses, IEEE 802.11 specification defined two mechanisms (open system authentication and shared key authentication) to validate the identities of wireless devices attempting to gain access to a WLAN. Neither of these alternatives provides effectively secure protection. Open authentication is a null authentication mechanism which does not provide identity verification. The shared key authentication is based on a unilateral challenge-response mechanism known as Wired Equivalent Privacy (WEP), which is a simple authentication mechanism. Recently, researchers have indicated that shared key authentication has already exposed to several security issues [2][3][4]. Due to the significant deficiencies of shared key authentication, the IEEE 802.11i amendment was ratified in June 2004. The IEEE 802.11i amendment introduced the concept of a Robust Security Network (RSN). An RSN is defined as a wireless security network that only allows the creation of Robust Security Network Associations (RSNA). As the definition depicted in [5], an RSNA is a logical connection between communicating IEEE 802.11 entities established through the IEEE 802.11i key management scheme, called the 4-Way Handshake, which is a protocol that validates that both entities share a pairwise master key (PMK), synchronizes the installation of temporal keys, and confirms the selection and configuration of data confidentiality and integrity protocols. The entities obtain the PMK in one of two ways—either the PMK is already configured on each device, in which case it is called a pre-shared key (PSK), or it is distributed as a side effect of a successful EAP authentication instance, which is a component of IEEE 802.1X port-based access control. The PMK serves as the basis for the IEEE 802.11i data confidentiality and integrity protocols that provide enhanced security over the flawed WEP. The configuration of a wireless network with robust security features is considered a complicated and time-consuming task. Although the IEEE 802.11i amendment introduced a great number of security enhancements, most common security objectives (including confidentiality, integrity, availability and access control) are still under serious threats. More details are provided in Section 2.

The main aim of this paper is to propose an improved authentication mechanism to accomplish autonomic security configuration and enhance wireless security. The remainder of the paper is organized as follows. Section 2 analyzes the data confidentiality and integrity protocols of IEEE 802.11i amendment and describes potential threats. Section 3 proposes an enhanced authentication mechanism and discusses how to
automatically configure wireless network security. Section 4 provides a brief overview of the related works. Section 5 concludes the paper and provides our future plan.

II. SECURITY ANALYSIS

In order to analyze the IEEE 802.11i amendment, it is essential to provide a brief introduction to 802.11i. Following the introduction, we outline and discuss security issues that are overlooked by the IEEE 802.11i specification.

A. IEEE 802.11i Amendment

The IEEE 802.11i amendment allows for enhanced security features beyond WEP and the simple IEEE shared key challenge-response authentication. Its authentication process involves three entities, namely: Station (STA), Access Point (AP) and Authentication Server (AS). Generally, a successful authentication process means that the station and the access point verify each other’s identity and generate some shared secret for subsequent secure data communication. The authentication server can be implemented either in an access point, or through a separate server. As depicted in Fig. 1, it consists of six distinct phases: 1) discovery phase, 2) authentication and association phase, 3) EAP/802.1x/RADIUS authentication, 4) 4-way handshake, 5) group key handshake, and 6) secure data communication.

1. Discovery Phase: the access point periodically advertise its IEEE 802.11i security policy in a certain channel through the Beacon frame. Station passively monitors the Beacon frame and uses the frame to identify the access point.

2. Authentication and association phase: the station selects one access point from the list of available access points and attempts to authenticate and associate with that access point. However, this authentication requires to be supplemented by further mutual authentication.

3. EAP/802.1x/RADIUS authentication: the station and the authentication server perform mutual authentication and thus some common secret (i.e. Master Session Key - MSK) is generated between the station and the authentication server. This step does not exist if a static Pre-Shared Key (PSK) is pre-installed over the station and the access point, as shown in Fig. 2.

4. 4-way Handshake: the station and the access point utilize a handshake scheme to confirm the existence of the PMK (see Fig. 3), verify the selection of the cipher suite and derive a fresh Pairwise Transient Key (PTK). PTK is shared between the station and the access point.

5. Group Key Handshake: due to the requirement of multicast applications, the access point is able to generate and distribute a fresh Group Temporal Key (GTK) to the stations.

6. Secure Data Communication: by using PTK or GTK, the station and the access point construct a secret transmission channel and thus accomplish robust data confidentiality.

B. Vulnerability to Insider Attack

One of the primary threats to wireless local area networks is insider attack. Due to the fact that distributing various PSKs in a large network might be infeasible, a great number of vendors adopt a single PSK for every station. Thus, this may give rise to...
a potential security threat. For instance, an insider adversary is able to easily sniff and store all the messages generated at the 4-way-handshake stage. Since all the stations in the same WLAN share a unique PSK, the insider adversary is able to easily calculate the PTK. An adversary can use the shared PSK and first two handshake messages, including the MAC address and nonce of the station and access point, i.e. SA, AA, SNonce and ANonce - through a Pseudo Random Function with output length X (PRF-X) to derive the fresh PTK, say, $PTK = PRF-X(PSK," pairwisekeyexpansion" ||min(AA,SA)||max(AA,SA)||min(ANonce, SNonce)||max(ANonce, SNonce))$.

C. Vulnerbaility to Offline Guessing Attack

Even though the PSK is unique for each station, a potential threat still exists. An adversary is capable to use the PSK by capturing and analyzing 4-way-handshake messages. It is not difficult for an adversary to sniff and store those handshake messages. The attacker needs to use some passive wireless network eavesdropping analyzers, such as Kismet [13] and Wireshark [14], to capture handshake messages. Based on these captured handshake messages, the adversary extracts security-related value, including MAC address and nonce of access point and station i.e. AA, SA, ANonce and SNonce, respectively. In order to accomplish offline guessing attack, the attacker has to cache the Message Integrity Code (MIC), sequence number (sn) and payload (msg1,2,3,4) of handshake messages. Due to the fact that MIC is calculated by using PTK to encrypt nonce, sequence number and message payload (see Equation (1)), the attacker is able to use authentication message copies, guess and verify the PTK in an offline environment.

$$MIC_{ptk} = \{nonce, sn, msg\}.$$ (1)

An adversary can also utilize the pre-computed hash of all passwords, like rainbow tables [12], to accelerate the process of offline guessing attack. For instance, a demo at ShmooCon [15] showed that applying a hash file, pre-computed on a much more powerful machine led to the testing of 18,000 keys per second. In addition, the coWPAtty in a separate project has pre-computed a password list of 170,000 words against the top 1000 most common SSIDs in the Wigle.net database to give an adversary a place to start.

D. No Protection for Management Frames

The IEEE 802.11i amendment does not provide a protection mechanism for management frames. In contrast to regular data frames encrypted by Temporal Key Integrity Protocol (TKIP) or Cipher Block Chaining MAC Protocol (CCMP), 802.11 management frames are always transmitted in an unsecured manner. Even though a WLAN adopts high level security policy, management frames are always under unauthenticated and unsecured threats. Based on this drawback, a prodigious amount of attacks are launched such as Denial-of-Service attack, masquerading attack and man-in-the-middle attack, etc. By exploiting unprotected management frames, an adversary can simply conduct a DoS attack either by flooding abundant management frames or transmitting forged management frames (such as deauthentication and disassociation) to disable service to legitimate users.

E. No Protection for Null Data Frames

Some WLAN vendors use null data or QoS null data frames, which contain an empty frame body, to carry special control information to another station. For example, a station commonly sends an access point a null data frame to indicate a change in sleep state by setting the power management bit in the frame control field appropriately. This situation usually occurs after a station being in power save mode has been awaken to receive buffered frames from the access point. Furthermore, the null data frame is able to notify the access point to start buffering frames again for that station because the station is going back to sleep.

Another use of null data frames is part of active scanning. The station sends a null data frame to the access point to indicate the sleep state prior to performing active scanning, which is the process of looking for access points on different channels for the purpose of possible roaming. The access point then buffers frames for the station while the station scans other RF channels. While on another channel, the client cannot receive frames from the access point. Because the IEEE 802.11i amendment does not provide effective protection for null data frames, an adversary can exploit the security deficiency of the null data frame to send forged null data frames to steal buffered frames. Furthermore, a DoS attack based on virtual jamming can be launched. An adversary can update the NAV field in a null data frame and thus mislead stations cannot gain access to the channel.

F. No Protection for EAPOL Frames

An outline of the EAP/802.1x/RADIUS authentication sequence is shown in Fig. 4. During the authentication procedure, all the EAPOL frames are out of protection since a RSNA has not been established. Therefore, a great number of attacks may occur at the EAP/802.1x/RADIUS stage. For instance, an adversary can passively eavesdrop and cache sensitive traffic (eg. access account). In addition, an adversary is capable of inserting some messages with moderate equipment (such as a station with a common wireless network interface card and some relevant software) and thus launching a DoS attack. As it does in the case of EAPOL-related DoS attacks, an adversary injects either a forged EAPOL-logoff frame to force a legitimate station out of service, or a forged EAPOL-failure frame to disconnect a station from an existing session. In addition, adversaries are able to spoof a station to disconnect from an authentication session by sending a premature EAPOL-success frame.

G. Denial-of-Service Attack

In addition to the aforementioned security threats, there is another potential security issue at the 4-way-handshake stage. As shown in Fig. 3, the first handshake message does not involve MIC filed to accomplish integrity protection. Therefore, an adversary can flood forged initialized messages and thus derive inconsistent keys between the station and access point [6][7][8].
III. AUTONOMIC CONFIGURATION AND SECURITY IMPROVEMENT

Since the IEEE 802.11i amendment needs to maintain backward compatibility with the IEEE 802.11 state machine, open system authentication – null authentication is still allowed at the authentication and association stage. In order to address the potential security threats described in section 2, we propose an improved authentication mechanism based on asymmetric cryptography.

Figure 4. EAP message flow

A. Authentication based on Asymmetric Cryptography

The proposed authentication mechanism installs a pair of public-private keys, which can be achieved by using a Certificate-Authentication-signed (CA-signed) certificate or a self-signed certificate. Furthermore, each access point is able to accomplish automatic public key updates. The procedure of the proposed authentication can be described, at an abstract level, as follows.

[Frame 1: STA → AP]
AA, AAN, ATSN, Timestamp

[Frame 2: AP → STA]
SPA, AccSC, ATSN+1, Certificate,
Ticket{AA, Timestamp, MIC}

[Frame 3: STA → AP]
AA, ATSN+2, Ticket{AA, Timestamp, MIC},
{Pre-session Key}PK

[Frame 4: AP → STA]
SPA, ASC

Following the discovery phase frame exchange, the station first sends an authentication request frame to perform asymmetric-cryptography authentication. This request frame encapsulates the MAC address, Authentication Algorithm Number (AAN) and Authentication Transaction Sequence Number (ATSN). Second, the access point responds with an authentication response frame. If the MAC address in the request frame is in a list of registered stations, Access State Code (AccSC) filed will be set to “success”. In addition, the response frame encapsulates a certificate of access point and a ticket. The ticket consists of three elements: the MAC address of Station, the timestamp shown in the request frame that the access point received and a MIC. Based on the response frame that it received, the station verifies the identity of access point and generates a pre-session key encrypted through public key of access point. Third, the station sends the access point a frame that encapsulates the encrypted pre-session key and ticket. Finally, while receiving the ticket and pre-session key, the access point verifies the ticket through the timestamp and MIC. If it is valid, the access point calculates the symmetric session key and response a frame containing an Authentication State Code (ASC) with the value “success”. On the contrary, either an expired ticket or an inconsistent MIC triggers a response frame with authentication failure claims. In this procedure, the fresh session key is derived from the pre-session key through a Pseudo Random Function, say, session-key=PRF(pre-session-key, timestamp, public-key, AA, SPA “asymmetriccryptographauthenticaion”). Also, the PMK can be calculated through an exclusive or operation, say, PMK=session-key ⊕ PBKDF(passphrase, ssid, ssidLength, 4096, 256).

B. Protection for Management Frames

Based on the proposed authentication mechanism, unicast, multicast and broadcast management frames can be effectively protected. For a unicast management frame, a Message Authentication Code (MAC) is computed through a cryptographic hash function and is attached to the tail of the frame. Before accepting the frame, either the station or access point checks the MAC. If the frame fails to be decrypted, the station or access point will drop the frame. Similarly, an access point can also protect broadcast or multicast frames by signing these frames with its pre-session key. Therefore, any attempt to copy, forge or reply a frame invalidates the MAC or signature.

C. Protection for Null Data Frames

The IEEE 802.11i amendment does not provide any protection for null data frames and QoS null data frames, since no payload is carried by null data frames. To address the potential threat described in Section 2, a Pseudo Random Number Generator (PRNG) is presented to achieve the protection for null data frames. Most PRNG algorithms can produce sequences which are uniformly distributed. In addition, PRNG algorithms possess a large state space. For instance, a 128-bit seed is able to generate 32-bit pseudo-random number and the period of the number sequence is around $2^{128}$. In our authentication mechanism, each access point or station has a PRNG. After the pre-session key is derived, an access point performs a negotiation with the stations (the negotiation procedure is under the protection of pre-session key) and initializes a seed and thus generates a 32-bit pseudo random number. The number is used as a key which is attached with a null data frame. Because the key is tagged...
only in one null data frame and will be changed in the next null data frame, any attempt to forge and reply a null data frame is of no use.

D. Protection for EAPOL and Handshake Frames

Although the IEEE 802.11i amendment provides some protection schemes for regular data frames, these protections just occur after a successful EAP/802.1x/RADIUS authentication. Therefore, all the EAPOL frames and partial handshake frames are always out of effective protection. In contrast to the 802.11i amendment, our proposed authentication mechanism accomplishes EAPOL-frames and handshake-frame protection by using session-key encryption and decryption.

E. Autonomic Configuration

Currently, in order to access to a robust security wireless network, a user has to manually patch his/her wireless devices and ensure his wireless access points and network adapters are also properly configured. However, it is a complicated and time-consuming task for most of wireless network users. For example, in an airport scenario, a Windows XP user has to obtain the shared secret (passphrase) either from the Ethernet service counter or from a webpage based application. After the user attains his/her access account and passwords, he needs to disconnect the current session, set up security-related parameters through control panel and reconnect to a Wi-Fi Protected Access (WPA) channel. By using our authentication mechanism based on asymmetric cryptography, a user can simply obtain his/her passphrase and complete the WPA authentication for the reason that the negotiated passphrase is under the protection of pre-session key.

IV. RELATED WORKS

Over the past few years, an increasing amount of attention from industry and academia has focused on security protocols over wireless networks. In [9], Mano et al. proposed a lightweight enhancement to the WPA 4-way handshake and thus tackled the issues of a potential insider attack. This 4-way-handshake improvement is accomplished through implementation of the Diffie-Hellman key exchange method. However, research has proven that the Diffie-Hellman key exchange protocol is vulnerable to a man-in-the-middle attack. Furthermore, this proposed improvement does not provide any effective protection for null data frames and management frames. Recently, the IEEE 802.11w proposal was presented which provides protection in three categories: 1) protection for unicast management frames, 2) generic broadcast management frames, and 3) de-authentication/disassociation frames. Although 802.11w promises to patch security issues to stop the information leakage and reduce some basic DoS attacks, the security offered by 802.11w can only occur after EAP/802.1x/RADIUS authentication and 4-way handshake. Partial management frames which are announced before the EAP/802.1x/RADIUS authentication are still left out of the protection scope. In addition, 802.11w does not support any protection scheme for null data frames. Currently, the most common security solution (which is being used in many airports, business centers and hotel rooms) is the captive portal technique. This technique forces an unauthenticated user to see a special web page. During the authentication procedure, the browser is redirected to a web page which may require authentication or payment. However, a captive portal is not desirable for wireless devices that do not support HTTP services.

V. CONCLUSION AND FUTURE WORKS

This paper analyzed the IEEE 802.11i amendment and identified its potential threats. Based on our analysis, an improved authentication mechanism is proposed. This mechanism adopts an asymmetric cryptography approach to accomplish effective protection in six categories, which included protection for management frames, null data frames and EAPOL frames as well as protection from some basic DoS attacks, offline guessing attacks and insider attacks. Furthermore, our proposed authentication mechanism is able to allow stations to configure themselves automatically. In the future, we plan to investigate asymmetric-cryptograph authentication mechanism trends toward reducing the number of authentication frames and utilizing formal security analysis.

REFERENCES