Available Online at http://www.recentscientific.com

CODEN: IJRSFP (USA)

International Journal of Recent Scientific Research
Vol. 8, Issue, 9, pp. 20270-20272, September, 2017

ISSN: 0976-3031

International Journal of Recent Scientific Research

DOI: 10.24327/IJRSR

Research Article

AN APPROACH TO SECURE 802.11I AUTHENTICATION PROCESS USING ONE TIME PAD CONCEPT

Mannon Mustafa Z. A and Najar, M Abdul Jawad

Department of Information Technology Central University of Kashmir

DOI: http://dx.doi.org/10.24327/ijrsr.2017.0809.0861

ARTICLE INFO

Article History:

Received 05th June, 2017
Received in revised form 21st July, 2017
Accepted 06th August, 2017
Published online 28th September, 2017

Key Words:

IEEE 802.11i; Fluxion Tool; WEP; TKIP

ABSTRACT

The paper introduces the 802.11i, IEEE 802.1x authentication protocol used in enterprise authentication mode, discuss some vulnerabilities to the existing authentication process. Finally a solution will be proposed to secure 802.11i authentication process using one time pad concept.

INTRODUCTION

The 802.11i standard enhances 802.11 with several new security mechanisms to ensure message confidentiality and integrity. Some of these mechanisms are additions, and some are complete replacements of 802.11 procedures. 802.11i also incorporates the 802.1x port authentication algorithm, another IEEE standard, to provide a framework for strong mutual authentication and key management. The additional features include the following:

1. Two new network types, called Transition Security Network (TSN) and Robust Security Network (RSN)
2. New data encryption and data integrity methods: Temporal Key Integrity Protocol (TKIP) and Counter mode/CBC-MAC Protocol (CCMP)
3. New authentication mechanisms using the Extensible Authentication Protocol (EAP)
4. Key management via security handshake protocols conducted over 802.1x

TKIP is a cipher suite and includes a key mixing algorithm and a packet counter to protect cryptographic keys. It also includes Michael, a Message Integrity Check (MIC) algorithm that, along with the packet counter, prevents packet replay and modification. TKIP and Michael are used together and are designed to work with legacy equipment, thus providing a way to secure existing networks. CCMP is an algorithm based on AES that accomplishes encryption and data integrity. CCMP provides stronger encryption and message integrity than TKIP and is preferred, but it is not compatible with the older WEP-oriented hardware. Ultimately, vendors will be required to implement CCMP to stay in compliance with the specification.

An RSN is one that allows only machines using TKIP/Michael and CCMP. A TSN is one that supports both RSN and pre-RSN (WEP) machines to operate. TSN networks have a weakness in that broadcast packets have to be transmitted with the weakest common denominator security method. Thus, if there is a device using WEP in a network, it weakens the security of broadcast traffic for all the devices. RSN is definitely preferred, and getting all networks to use CCMP exclusively would be ideal.

The authentication piece of WPA2/802.11i has two modes: Personal and Enterprise. The Personal mode requires the use of a PSK (Pre-Shared Key) and does not require users to be separately authenticated. The Enterprise mode, which requires the users to be separately authenticated based on the IEEE 802.1X authentication standard, uses the Extended EAP (Extensible Authentication Protocol). Here we will discuss enterprise mode authentication.

IEEE 802.1x authentication protocol

The authentication for 802.11i is based on 802.1x and extensible authentication protocol (EAP) [1]. IEEE 802.1x

Corresponding author:* **Mannon Mustafa Z. A
Department of Information Technology Central University of Kashmir

defines a mechanism for port-based network access control. It is based upon EAP to provide compatible authentication and authorization mechanisms for devices interconnected by IEEE 802 LANs. There are three main components in the IEEE 802.1x authentication system:

Supplicant, Authenticator, and Authentication server.

In a WLAN, the *supplicant* is usually a mobile node which wants access to an access point. The AP usually represents an *authenticator*. An authentication, authorization, and accounting (AAA) server such as the RADIUS server is the *authentication server*. The *port* in 802.1x represents the association between the supplicant and the authenticator. Both supplicant and authenticator have a port access entity that operates the algorithms and protocols associated with the authentication mechanisms. When the authenticator's *controlled port* is in unauthorized state, that is, the port is open. Messages will be directed only to the *authenticator port access entity*, which will further direct 802.1x messages to the authentication server. The authenticator port access entity will close the controlled port after the supplicant is authenticated successfully. Thus, the supplicant is able to access to other services through the controlled port. Based upon EAP, the IEEE 802.1x standard can use a number of authentication mechanisms. The authentication mechanisms are outside the scope of the IEEE 802.1x standard.

Many authentication mechanisms such as MD5, TLS,
TTLS, and PEAP can be used. The IEEE 802.1x also defines EAP over LANs (EAPOL) in order to encapsulate EAP messages between the supplicant and the authenticator [3].

Vulnerabilities of 802.1x authentication process

In the existing authentication process when the user tries to connect to any access point, she is asked to enter user name and password. Here starts the threat of vulnerabilities like fake access points, impersonation etc. All these threats arise due to the fact that the a valid user contains the credentials to get connected to the a particular access point. So the most important burden for a valid user is to safe guard his credentials and make proper use of them wisely. In this section we will discuss some of the vulnerabilities of the 802.1x authentication process and in the next section a solution will be proposed to safe guard this authentication process.

Here we will discuss only two vulnerabilities:

- Getting access via fake access points[2]
- Getting access via impersonation[4]
- Getting access via Man in the middle attack[4]

Getting access via fake access points

A fake access point or rouge access point is that access point which gives a common user an illusion that it is a valid access point by broadcasting the same SSID as the original access point has using some tools like KALI LINUX. When the user tries to connect to it thinking that it is a valid or authentic access point she gets trapped. And unknowingly enters her credentials like user name, password in to the fake interface of the fake access point, hence breaching her privacy by herself.

1. ***Fake AP (Phishing AP):*** Sometimes the attackers try to get the user credentials via phishing i.e. by broadcasting the SSID of the fake access point and waiting for any user to connect to the fake access point via there rouge SSID. Various tools are available to perform this type of phishing. In KALI LINUX this can be done using WIFIPHISHER TOOL.
   While as some times an attacker forces the user to connect to their fake access point by sending continuous deauthentication packets to the valid or legal access point. Various tools are available in kali linux to do this like FLUXION TOOL etc.
2. ***Compromised AP (Parasite AP):*** When the attacker breaks through a legal AP, the DNS server address of the compromised AP is modified to the fake DNS server address for subsequent phishing attack. All the traffics through the compromised AP are relayed to the specified AP set by the attacker. Once the user access to the compromised AP, all the network traffics are monitored by the attacker[2].
3. ***Spider AP:*** The spider AP is a new malicious AP found in 2016. Compared to Parasite AP, the attackers can use more malicious nodes and multiple times of bridge. The attacker usually set up a malicious control node hidden in the distribution box of street lamp and a malicious cloud server for data process and attacking[2].

Getting access via impersonation

Apart from using fake access points by the fake or unauthorized users to gain access to the wifi access point, there are many other ways to gain access of a legal access point. One among them is impersonation.

Impersonation can be defined as the way of getting access of an access point by an unauthorized user by first stealing the credentials of a valid by some different methods other than fake access points like shoulder sniffing, man in the middle attack which is possible on 802.1x authentication [4] etc.

A new authentication solution using one time pad

In order to make the authentication process of 802.11i secure from fake access point's the proposed solution can play an important role.

The solution is described as:

First it should be noted that the authentication server contains the cell phone number of a valid user. Also this phone number should have some user_name/ id or any other credential of user associated with it and it must be unique (what we suggest is email id of that user). Now when the supplicant tries to connect the access point, he should only enter his user_name/id or any other credential which he has already provided to the network administrator. The authenticator will send this to authentication server, which will first see this user_name/id or any other credential weather it is available or not if it is available, then the authentication server will map it to the phone number provided by that user and will send an OTP to supplicant via a different channel using SMS and also sends this OTP to authenticator. The user after receiving an OTP will enter and send it to authenticator in encrypted form using any encryption algorithm which is considered to be secure. As authenticator will be already containing this OTP it will match both if they are same it will send acknowledgement to the supplicant and permits it to get access. If OTP's will not match it will not allow the supplicant to access.

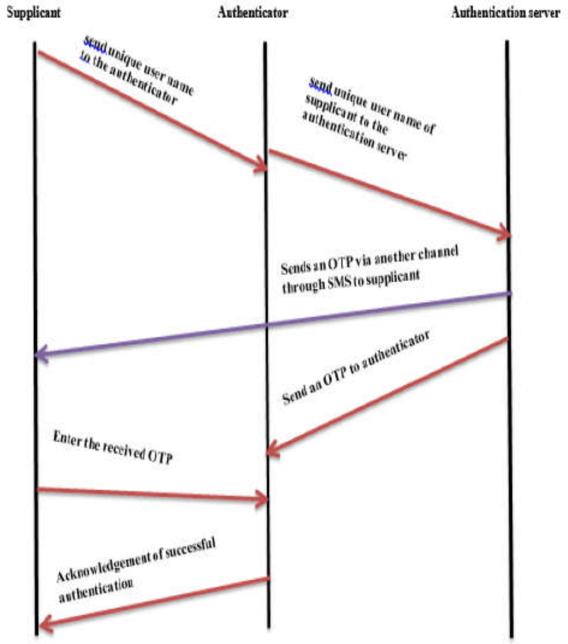
Supplicant
Authenticator
Authentication server
Send unique user name to the authenticator
Send unique user name of supplicant to the authentication server
Sends an OTP via another channel through SMS to supplicant
Send an OTP to autheaticator
Enter the received OTP
Acknowledgement of successful authentication

Fig 1 Showing authentication solution using OTP concept

Now if user got an OTP, it means that it is not a fake access point to which a valid user has connected because the OTP came to the cell phone via different channel. Hence in this way the fake access points will no longer serve for the attackers. Also other attacks of getting access by stealing user credentials can be avoided. Because if a user wants to access to authenticator via impersonation [4], he cannot as an OTP comes to the phone of a valid user and without OTP he can't get access. Also it can serve as an alarm for a valid user if she gets OTP when he is not requesting access to access point that someone is trying his credentials to get illegal access. Figure below shows the authentication using the proposed solution.

CONCLUSION

The IEEE 802.11i authentication standard suffers from various flaws and hence is easily vulnerable to various threats as discussed above. The solution proposed in this paper can overcome many vulnerabilities and makes 802.11i authentication process more secure.

References

1. Khidir M. Ali andAli Al-Khalifah "A Comparative Study of Authentication Methods for Wi-Fi Networks", Third International Conference on Computational Intelligence, Communication Systems and Networks, 2011.
2. Liu Shu-Dong, Liu Yong-lei and Jin Zhi-gang" Attack Behavioral Analysis and Secure Access for Wireless Access Point (AP) in Open System Authentication", IEEE 2017.
3. Jyh-Cheng Chen and Yu-Ping Wang "Extensible Authentication Protocol (EAP)and IEEE 802.1x: Tutorial and Empirical Experience", IEEE 2005.
4. Matthias Larisch "IEEE 802.1x authentication password exposure in WPA-Enterprise networks" github@ matthias-larisch. dehttps://github.com/Nerdy Projects/ June 22, 2014
5. Manjula Sandirigama, Rasika Idamekorala "Security Weaknesses of WEP Protocol IEEE 802.11b and Enhancing the Security With Dynamic Keys", IEEE May 2009.

How to cite this article:

Mannon Mustafa Z. A and Najar, M Abdul Jawad.2017, An Approach To Secure 802.11I Authentication Process Using one Time Pad Concept. *Int J Recent Sci Res.* 8(9), pp. 20270-20272. DOI: http://dx.doi.org/10.24327/ijrsr.2017.0809.0861

****