International Journal of Information & Computation Technology.
ISSN 0974-2239 Volume 4, Number 13 (2014), pp. 1299-1303
© International Research Publications House
http://www. irphouse.com

Secure Initial Access Authentication in WLAN

Konduru Sandhya (CNIS)

Sree Vidyanikethan Engineering College, Andhra Padesh

ABSTRACT

Nowadays, with the rapid increase of WLAN-enabled mobile devices and the more widespread use of WLAN, it is equally important to have a more efficient initial link setup mechanism. 802.11i is an IEEE standard designed to provide enhanced MAC security in wireless networks. The authentication process involves three entities: the supplicant, the authenticator, and the authentication server. A 4-Way Handshake must be made between the supplicant and the authenticator to derive a pairwise key and/or group key for subsequent data transmissions.

Security is a serious concern because the wireless medium is open for public access within a certain range. In fact, it has been suggested that 802.11 is highly susceptible to malicious denial-of-service (DoS) attacks targeting its management and media access protocols. The attack involves forging initial messages from the authenticator to the supplicant to produce inconsistent keys in peers. In this paper one solution is proposed based on various considerations to avoid DoS.

Keywords WLAN, 802.11i, Authentication, 4-Way Handshake, Denial-of-Service, MAC.

INTRODUCTION

A **wireless local area network** (**WLAN**) links two or more devices using some wireless distribution method, and usually providing a connection through an access point to the wider Internet. This gives users the ability to move around within a local coverage area and still be connected to the network. IN recent years, wireless local area networks (WLAN) technology continues to gain increasing popularity for its good mobility, high bandwidth, and flexibility. Users can easily access a variety of network applications through WLAN, for example, face book, Twitter, e-mail, and online music and videos.

In order to provide secure data communications over wireless Links, the 802.11 Task Group proposed the Wired Equivalent Privacy (WEP) to encrypt the data stream and authenticate the Wireless devices. However, significant deficiencies have been found. To repair the problems, an authentication mechanism based on EAP/802.1X/RADIUS has been developed to replace the poor Open System authentication and Shared Key authentication in WEP. The authentication process combines 802.1X authentication with key management procedures to generate a fresh pairwise key and/or group key, Message Integrity Code (MIC), followed by data transmission sessions.

This paper gives the some idea how to mitigate the DoS attacks when using WLAN. In this paper section 2 gives brief explanation on IEEE 802.11i, section 3 gives idea on 4-way handshake and possibility of attacks in the process of handshake. Section 4 shows the already implemented solution for attacks. Section 5 is the proposed solution which is an alternative to above solution.

IEEE 802.11i :

IEEE 802.11i-2004 or **802.11i** standard specifies security mechanisms for WLAN. Provides Confidentiality, Authentication, and Key Management. It replaced the short Authentication and privacy clause of the original standard with a detailed Security clause.

The new security standard, 802.11i, which was ratified in June 2004, fixes all WEP weaknesses. It is divided into three main categories:

1. Temporary Key Integrity Protocol (TKIP)
2. Counter Mode with CBC-MAC Protocol (CCMP)
3. 802.1X Port-Based Network Access Control.

802.11i also has an extended key derivation/management.

EAP

Extensible Authentication Protocol (EAP) is just the transport protocol optimized for authentication, not the authentication method itself. It is an authentication framework which supports multiple authentication methods. EAP runs directly over data link layers such as Point-to-Point Protocol (PPP), without requiring IP.

EAP-TLS

Creates a Transport Layer Security (TLS) session within EAP, between the Supplicant and the Authentication Server. Both the server and the client(s) need a valid certificate, and therefore a PKI. This method provides authentication both ways.

DOS ATTACKS

In computing, a **Denial-Of-Service (DoS) attack** is an attempt to make a machine or network resource unavailable to its intended users. The main motive of attacker is to prevent legitimate users from information or services. This is done by flooding with useless traffic.

The possible Dos attacks in 802.11i 4-way are Probe Request Flood, Authentication Request Flood, Association Request Flood, De-Authentication Attack, De-Association Attack, Media Access Attack.

DoS in 4-way handshake

During the 4-way handshake the PTK inconsistency is caused between the Authenticator and Supplicant. This leads to blocking of protocol execution, authenticator timeout and subsequent de-authentication of supplicant. To avoid this all the nonce's and corresponding PTKs are need to be kept by supplicant. This ultimately leads to DoS attack.

The general process of 4-way handshake done between Authenticator and Supplicant is shown in below figure:

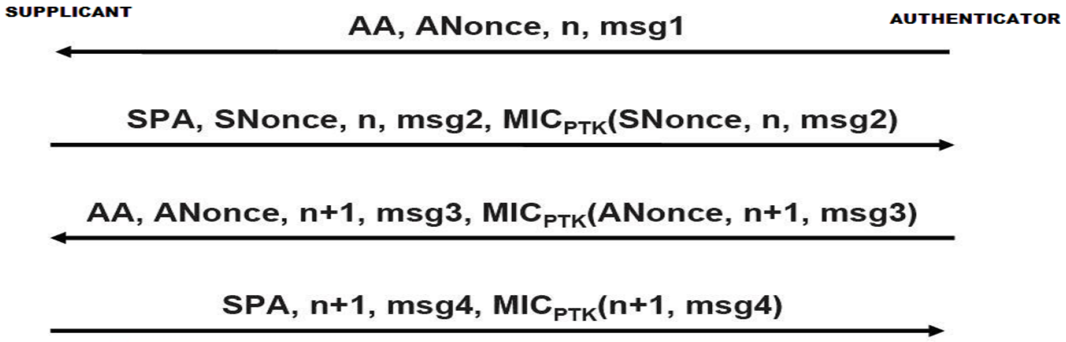
SUPPLICANT
AUTHENTICATOR
AA, ANonce, n, msg1
SPA, SNonce, n, msg2, MIC_PTK(SNonce, n, msg2)
AA, ANonce, n+1, msg3, MIC_PTK(ANonce, n+1, msg3)
SPA, n+1, msg4, MIC_PTK(n+1, msg4)

Figure 1: 4-Way Handshake

The attacker can make PTK inconsistency with simple one-message attack by impersonating the authenticator, composing the initial message and sends to supplicant. The attacker forges the message and sends to supplicant in the middle of 4-way handshake. This attack arises from the vulnerability of Initial message.

Message 1: **S** ← **A**
AA, ANonce, n, Msg1
Message 2: **S** ← **A**
SPA, SNonce, n, Msg2, MIC$_{PTK}$(SNonce, n, Msg2)
Message 1': **S** ← **Attacker**
AA, ANonce', n, Msg1
{ Supplicant derives PTK' by generating ANonce' and SNonce'**}**
Message 3: **S** ← **A**
AA, ANonce, n+1, Msg3, MIC$_{PTK}$ (ANonce, n+1, Msg3)
{Protocol blocked with PTK,
PTK' inconsistency, MIC not verified}

Figure 2: DoS in 4-Way Handshake

The subsequent handshake is blocked due to different PTK value than the one in authenticator; this is because the supplicant calculates the new PTK to the nonces for newly received message. By monitoring the network traffic or by just flooding the message with some frequency the attacker determines the appropriate time to send out message.

IMPLEMENTED SOLUTION

Possible repair is, MIC derived from PMK can be added to message, this will prevent the forging the messages from attacker. Message sent by authenticator is still distinguishable by secure bit with the message sent by attacker. To solve this problem 802.1x authentication process dynamically generates PMK. Static PMK is relatively used for long time message is still vulnerable to replay attacks. To defend against replay attacks authenticator should maintain a monotonically increasing sequence counter.

The replayed messages are detected by supplicant by comparing the counter of a received message against the counter of the largest numbered previous message. Clock time counter is added to message format, eliminating the possible problem of counter rollover. This do not influences on other parts of standard and this specific sequence counter is also consistent with its usage in the group key handshakes. No need to worry about clock time synchronization.

ALTERNATE SOLUTION

Alternative to clock time counter there is a possibility to use timestamps. One way to prevent replay attacks and countermeasure for DoS is to attach a timestamp to messages sent between authenticator and supplicant. The supplicant can confirm that the timestamp is within an acceptable range and will reject any messages missing the timestamp or reporting too old. This cannot confirm that the communication is only processed once as it can be repeated within the timeframe, but it forces a malicious attacker to work quickly. To make sure the message is only accepted once a nonce (pseudo-random string) can be added to messages to be only one time, with other messages sharing the same nonce to be discarded.

CONCLUSION

With the rapid increase of the WLAN-enabled mobile devices, the current WLAN security standard IEEE 802.11i is challenged for its low efficiency. In IEEE 802.11i 4-way handshake we find and analyze DoS attack on Message1 in protocol. To generate a shared PTK between supplicant and authenticator only one active handshake must be allowed at any time by this protocol. Upon analysis this leads to vulnerabilities, allows an attacker to block the handshake by simply inserting one forged message. Attack can only be performed between Message1 and Message3 of 4-way handshake.

The repair is implemented with a some change; a MIC calculated from the PMK can be added to *Message 1* to prevent the attacker from forging *Message 1*. This remedy also requires a monotonically increasing sequence counter to be implemented in the authenticator side to prevent replay attacks. The local clock time counter of the authenticator appears to be a simple increasing counter that would do the job. We in this paper will use the timestamps as counters to prevent from attacks. This would be the alternate solution to clock time counters.

REFERENCES

[1] Adoba, B., and Simon, D. PPP EAP TLS authentication protocol. *RFC 2716*, October, 1999.

[2] AusCERT AA-2004.02. Denial of Service vulnerability in IEEE 802.11 wireless devices. May 13, 2004. Available at

[3] X. Li, J. Ma, and Y. Shen, “An efficient WLAN Initial Authentication Protocol,” Proc. IEEE Global Comm. Conf. (Globecom’12), 2012.

[4] Aura, T., and Nikander, P. Stateless Connections. In *Proceedings of International Conference on Information and Communications Security (ICICS’97)*, pages 87-97, Beijing,

[5] Bellardo, J., and Savage, S. 802.11 Denial-of-Service attacks: real vulnerabilities and practical solutions. In *Proceedings of the USENIX Security Symposium*, pages 15-28, August, 2003.

[6] IEEE p802.11i/D10.0. Medium Access Control (MAC) Security Enhancements, Amendment 6 to IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications. April, 2004.

[7] C. Rigney , S. Willens, A. Rubens, and W. Simpson, “Remote Authentication Dial in User Service (RADIUS),” RFC 2865, June 2000.

[8] C. He, J.C. Mitchell, “Analysis of the 802.11i 4-Way Handshake,” Proc. Third ACM Workshop Wireless Security (Wisec’04), pp. 43-50, 2004.