ASIAN JOURNAL OF PHARMACEUTICAL AND CLINICAL RESEARCH

INNOVARE ACADEMIC SCIENCES
Knowledge to Innovation

Special Issue (April)

Online - 2455-3891
Print - 0974-2441

Full Proceeding Paper

ADVANCED ENCRYPTION AND EXTENDED AUTHENTICATION FOR WIRELESS LOCAL AREA NETWORKS

EMIL SELVAN GSR[1], GAYATHRI N[1], RAKESH KUMAR S[2], ANKUSH RAI[3], JAGADEESH KANNAN R[3]

[1]Department of Computer Science and Engineering, Thiagarajar College of Engineering, Madurai, Tamil Nadu, India. [2]Department of Bannari Amman Institute of Technology, Sathyamangalam, Erode, Tamil Nadu, India. [3]Department of Computer Science and Engineering, Thiagarajar College of Engineering, Madurai, Tamil Nadu, India, VIT University, Chennai, Tamil Nadu, India. Email: emil@tce.edu

Received: 28 December 2016, Revised and Accepted: 10 May 2017

ABSTRACT

Wireless networking technology is becoming increasingly popular but, at the same time, has introduced many security issues. Wired equivalent privacy (WEP) standards are followed in wireless local area networks for providing security. However, WEP is fatally crippled by the fact that WEP keys are the same for all users, all sessions, never change, and its poor implementation of the RC4 encryption scheme. The authentication mechanism is based on a simple challenge-response protocol. The main problem with the previously used method was same key was used for both encryption and authentication. But, the proposed authentication is by means of certificates using extensible authentication protocol and a session key is transferred after successful authentication between mobile node and server. This session key is then used for encrypting messages using advanced encryption standard between mobile node and server.

Keywords: Wireless local area network, Wired equivalent privacy, 802.11, Wi-Fi-protected access, Wi-Fi-protected access 2, Extensible authentication protocol, RADIUS, RC4, Advanced encryption standard, Authentication.

 DOI: http://dx.doi.org/10.22159/ajpcr.2017.v10s1.19987

INTRODUCTION

Most enterprises are becoming more aware of security and therefore they need more than just usernames and passwords. A new authentication protocol, called the extensible authentication protocol (EAP), was therefore designed. Security has been considered an important issue in Wi-Fi networks from the beginning. Consequently, early versions of the IEEE 802.11 wireless local area network (WLAN) standard (802.11) have already featured a security architecture, which is called wired equivalent privacy (WEP) [1]. Even when WEP is implemented, the well-publicized weaknesses of WEP add only minimal protection against the casual hacker. The only solution to this problem is to implement an official WLAN with real WLAN security while banning users from implementing their own wireless networks. Providing a convenient and secure alternative is the only way to enforce this ban on personal wireless networking.

WEP is a link-layer security protocol that is specified, but not required, by the 802.11 standard [2]. WEP is based on the RC4 stream cipher, a symmetric cipher where the same key is used for both encryption and decryption. RC4 is the most widely used stream cipher in software applications. These vulnerabilities create the potential for active and passive attacks that could allow attackers to decrypt traffic or inject unauthorized data into a network. The term "wired equivalent" denotes that the security provided by WEP is intended to be roughly equivalent to what one would expect in a WLAN. WLANs, of course, can be protected by numerous physical mechanisms, unlike wireless transmissions. WEP uses a symmetric scheme in which the same key and algorithm are used for both encryption and decryption of data [3]. For encryption, advanced encryption standard (AES), highly regarded cryptographic algorithms that go far beyond the RC4 stream cipher used by WEP, is used while EAP [4] acts as the authentication mechanism and the combination of the two makes it possible to resolve the biggest liability of WEP, static user and static session keys. User authentication is now mutually assured, WEP keys can now be centrally managed with policies and keys can be distributed securely.

In this study, we will examine the problems with WEP, the solution with AES and EAP, and the concepts and design configuration of an enterprise worthy WLAN.

Section 1 of this study describes the problem with WEP, Section 2 presents the comparison of AES with RC4, we discuss the evaluation methodology of EAP-transport layer security (TLS) and certificates in Section 3, and finally, we conclude with Section 4.

PROBLEM WITH WEP

During the inception of the 802.11 standards for wireless networking, a fundamental issue of wireless security needed to be resolved. Since the physical layer of wireless networking uses radio signals through the open air waves and not electrical signals through closed wires, there was no physical security of the wireless signal compared to that afforded by wired networking [5-9]. WEP was created to address this fundamental liability. It was supposed to give wireless networks the equivalent privacy of wired networks using 40 and 104 bit encryption. Unfortunately, for whatever reason, their effort resulted in a WEP that was not so private. However, there exist massive weaknesses in WEP due to its poor implementation of the RC4 encryption scheme. Freeware applications such as Air Snort and WEP crack to first passively capture a data sample (100-1000 MBs) and crack WEP using non-brute force techniques in as little as a few hours. This means that anyone with a laptop and a 60 dollar 802.11b adapter can get behind our firewall with minimal time and effort even when maximum encryption is enforced.

Since the 802.11 [10] standard has no facility to centrally manage or distribute keys, WEP is fatally crippled by the fact that WEP keys are the same for all users, all sessions, and never change [6]. Attempting to manually change the WEP key is highly impractical due to the fact that it requires us to manually communicate to every wireless user what the new WEP key is so that they can manually enter it into their WEP settings. The final result is a WEP standard that is worthless for anything other than casual home web surfing.

There are two basic security problems in WLANs: First, due to the broadcast nature of radio communications, wireless transmissions can be easily eavesdropped. Second, and more importantly, connecting to the network does not need physical access to the network access point (AP); therefore, any device can try to illegitimately use the services provided by the network. WEP attempts to solve the first problem by encrypting messages. The second problem is addressed by requiring the authentication of the mobile stations (STAs) before allowing their connection to the network. The authentication of the STA is based on a simple challenge-response protocol. Once authenticated, the STA communicates with the AP by encrypted messages. The key used for encryption is the same as the one used for authentication. The encryption algorithm specified by WEP is the RC4 stream cipher [6]. Stream ciphers produce a long pseudorandom byte sequence out of a short secret seed value; this pseudorandom sequence is then XORed to the clear message (byte by byte) to generate the encrypted message. WEP works in the same way. The sender (the STA or the AP) of a message M initializes the RC4 algorithm with the secret key and XORs the pseudorandom sequence K produced by RC4 to M. The receiver of the encrypted message M, K, uses the same secret key to initialize the RC4 algorithm, which will then produce the same pseudorandom sequence K. Then, K is XORed to the encrypted message to obtain the clear message: $(M \oplus K) \oplus K=M$. WEP appends an initialization vector (IV) to the secret key before initializing the RC4 algorithm, where the IV changes for every message. This ensures that the RC4 algorithm produces a different pseudorandom sequence for every message. Integrity of the message is guaranteed with the help of cyclic redundancy check (CRC) [11,12].

The discovered flaws are instructive; there are many pitfalls in protocol design.

Integrity protection

WEP "integrity" does not provide integrity

- CRC is linear, so stream cipher XOR can change cipher text and CRC so that checksum remains correct. Such introduced errors go undetected, this requires no knowledge of the plain text.
- CRC is designed to detect random errors.
- It is not designed to detect intelligent changes.

Confidentiality

When using a stream cipher, it is essential that each message is encrypted with a different pseudorandom sequence. In WEP, but the problem is that the IV is only 24-bit long, which means that there are only approximately 17 million possible IV values. If any ever repeats, confidentiality is at risk. The total collapse of WEP is caused by the inappropriate use of the RC4 cipher.

PERFORMANCE COMPARISON OF AES WITH RC4

Block ciphers are an important and omnipresent building block of modern cryptography. In August 2000, the block cipher Rijndael was selected for the AES. The AES is a Federal Information Processing Standard (FIPS), specifically, FIPS Publication 197, that specifies a cryptographic algorithm for use by the US Government organizations to protect sensitive, unclassified information. The National Institute of Standards and Technology anticipates that the AES will be widely used on a voluntary basis by organizations, institutions, and individuals outside the US Government.

- AES can be represented mathematically does not mean it is simple to solve. Other algebraic problems remain intractable.
- Shortcut attacks against RC4 [7]:
  - n=5, state can be recovered in 242 steps versus key space of 2160.
  - 230 bytes to distinguish RC4 versus random.
  - 2nd byte has bias. 200 streams needed to RC4 from random.
  - 1st byte has bias. 1700 first bytes needed to distinguish RC4 from random.

However, AES [8,9] has no known shortcut attacks. Table 1 compares different encryption schemes.

- Existence of distinguishing attack means we cannot naively use RC4 to securely build other things.
- Shortcut attacks, even academic ones, are sufficient to rule out the cipher for long-term use. RC4→AES. They chose AES for long-term solution instead of RC4 [13].
- For wireless situation, they found AES flexible enough.
- RC4 speed is <2 times (1.77x) AES speed in software:
  - AES-128 runs at 62 MB/seconds
  - RC4 runs at 110 MB/seconds
  - Speed difference in software may not be that dramatic.
- AES is efficient in hardware also.
- AES uses less energy for smaller packets. RC4 uses less energy for larger packets. Fig. 1 compares encryption throughput with packet size for AES and RC4.

AUTHENTICATION USING CERTIFICATES (EAP-TLS)

WEP authentication mechanism

The authentication of the STA is based on a simple challenge-response protocol consisting of the exchange of four messages. First, the STA signals that it wants to authenticate itself (authenticate request). In response to this, the AP generates a random challenge and sends it to the STA (authenticate challenge). The STA encrypts the challenge with a secret key known only to the STA and the AP and sends the result back to the AP (authenticate response). The AP now decrypts the STA's response. If the decryption results in the same random value that the AP sent to the STA, it concludes that the response was generated by the STA (since no one else knows the key to generate a correct response)

Table 1: Comparison of different encryption schemes

Feature	WEP	WPA	WPA2
Cipher	RC-4	RC-4	AES
Key length	40 or 104 bits	128 bits encryption 64 bits	128 bits
IV size	24 bits	48 bits	48 bits
Per-frame key	Concatenated	Mixing function	Not needed
Data integrity	CRC-32 ICV	MIChael	CCM
Header integrity	None	MIChael	CCM
Relay protection	None	IV sequence	IV sequence
Key management	Static shared key	Pre-shared key	Pre-shared key

WEP: Wired equivalent privacy, WPA: Wi-Fi-protected access, IV: Initialization vector, CRC: Cyclic redundancy check

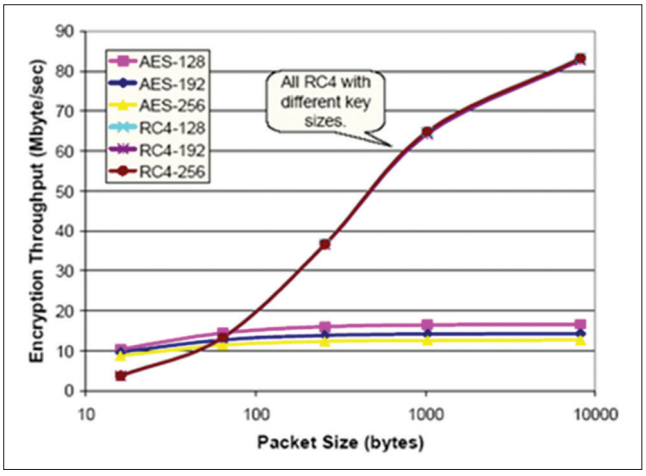


Fig. 1: Encryption throughput

and thus, the STA is authenticated. Otherwise the authentication fails. Based on the result of the authentication, the AP decides whether it can grant access to the network or not, and informs the STA about its decision. Once authenticated, the STA communicates with the AP by encrypted messages. The key used for encryption is the same as the one used for authentication [14-16].

WEP design flaws

Authentication in WEP has several problems. First of all, authentication is not mutual, meaning that the AP does not authenticate itself to the STA. Second, the authentication and the encryption mechanisms use the same secret key. This is not desirable since an attacker can exploit the weaknesses of both the authentication and the encryption methods to break the secret key. Having different keys for different functions is a better security engineering practice. The third problem is that the STA is authenticated only at the time when it tries to connect to the network. Once the STA is associated to the AP, anyone can send messages in the name of that STA by spoofing its medium access control address.

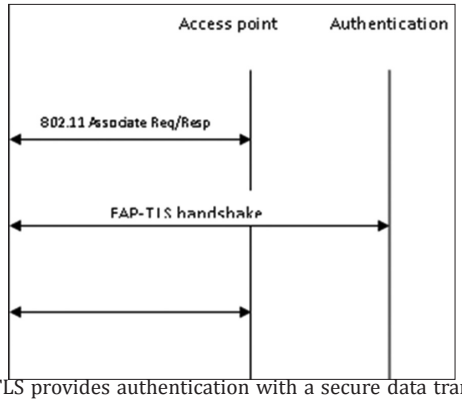
Authentication certificates (EAP)

EAP-TLS is an open standard that is supported by nearly every vendor [10]. TLS is the next version of the secure socket layer (SSL) standard. Its strength is that it is the most widely supported implementation of EAP and it requires the use of public key infrastructure (PKI). PKI makes EAP-TLS extremely secure with the use of asymmetric public and private keys on the RADIUS and client side. Cost of implementing EAP-TLS is almost negligible if we use Microsoft RADIUS and PKI technology [17]. This is because Microsoft's Internet Authentication Service (IAS) RADIUS is bundled with the Windows 2000 server operating system and is as stable as any other solution in my experience. Since Microsoft recommends the implementation of IAS on a domain controller, there is neither cost of an extra server nor are there additional licensing costs. The required PKI can be addressed by implementing the certificate authority service also bundled with Windows 2000 server, and deployment of client certificates can be automated by Microsoft Active Directory Group Policies. Deployment, licensing, and server costs are kept to a minimum. Bottom line, if we spend the time to learn and build the required infrastructure, we will get one of the most opened, secure, and least expensive solutions. The only additional burden over LEAP requirements is setting up a PKI in our organization. But, keep in mind that a PKI is extremely useful and can be used for many other things such as L2TP VPN, EFS encrypted folders, digital code signing, email signing and encryption, and SSL web pages. Fortunately, this is just a one-time setup, and once EAP-TLS is fully implemented, it is almost completely maintenance free and transparent to the user.

A conversation in EAP-TLS consists of the following:

Initially, EAP negotiation between the authenticator (AP) and the station. The AP sends an EAP-response/identity to the station, who will respond with an EAP-response/identity packet containing the stations' user ID.

- At this point, the AP passes the EAP packet from the station through the authentication server (AS) residing behind the AP. At this stage, the AP behaves as a pass-through device since the security conversation occurs between the station and client with the AS.
- When the AS [13] receives the identity of the station, it sends back a EAP-TLS/start packet, which signifies the start of the TLS handshake encapsulated using EAP.
- The station, acting as a client, replies by sending an EAP-response packet, where the data field encapsulates one or more TLS records containing the client_hello handshake message.
- The AS in turn replies with a EAP-request packet whose data field encapsulates one or more TLS records, including a server_hello handshake message. Additional parameters include the servers' TLS certificates, server_key_exchange data, certificate request (from the client), cipher suites, and others.



- EAP-TLS provides authentication with a secure data transfer over WLAN, thereby overcoming shortcoming of WEP which did not have mutual authentication.

Configuration certificates for EAP

When we use EAP with a strong EAP type such as TLS with smart cards or certificates, both the client and the server use certificates to verify their identities to each other. Certificates must meet specific requirements to allow the server and the client to use them for successful authentication.

One such requirement is that the certificate must be configured with one or more purposes that are specified in enhanced key usage (EKU) extensions that correlate to the certificate use. For example, a certificate used for the authentication of a client to a server must be configured with the client authentication purpose. Similarly, a certificate used for the authentication of a server must be configured with the server authentication purpose. When certificates are used for authentication, the authenticator examines the client certificate to find the correct purpose of object identifier in its EKU extensions. For example, the object identifier for the client authentication purpose is 1.3.6.1.5.5.7.3.2.

We can customize certificates issued by certificate services, including both how certificates are issued and what they contain, using certificate templates. In certificate templates, we can use a default template, such as the computer template, to define the template that the CA uses to assign certificates to computers. We can also create a certificate template and assign purposes in EKU extensions to the certificate. By default, the computer template includes the client authentication purpose and the server authentication purpose in EKU extensions. The certificate template that we create can include any purpose for which the certificate will be used. For example, if we use smart cards for authentication, we can include the smart card logon purpose in addition to the client authentication purpose. When using IAS, we can configure IAS to check certificate purposes before granting network authorization. IAS can check additional EKUs and issuance policy purposes (also known as certificate policies).

EAP-TLS is a new fast re-authentication architecture that employs a secure three-party key distribution protocol which reduces the number of message exchanges during the network access control process.

CONCLUSION

It is clear that WEP encryption does not provide sufficient wireless network security and can only be used with high-level encryption solutions. Wi-Fi-protected access (WPA) [17] is a secure solution for upgradeable equipment not supporting WPA2, but WPA2 will soon be the standard for wireless security. We presented the operation of WEP and described its weaknesses. We also described the authentication, access control, and key management mechanisms of WLAN. In this study, we have described the possible measures for the comparison of the AES candidates. We believe that the real question in the AES process is how to compare speed and efficiency to security, i.e., which of them to prefer and how to choose their relative importance. AES is secure and elegant. We prove that AES encryption provides more security in 802.1x

framework than RC4 algorithms. Furthermore, efficient authentication can be provided using certificates in TLS which we conclude to be better than all other mechanisms used previously.

REFERENCES

1. No. 802. Working Group Home Page. Available from: http://www.grouper.ieee.org/groups/802/1/index.html.
2. IEEE Standard 802. Standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications; 11-1999.
3. IEEE Standard 802. 1X-2001. IEEE Standard for Local and Metropolitan Area Networks, Port-based Network Access Control. October; 2001.
4. Blunk L, Vollbrecht J. RFC 2284. PPP Extensible Authentication Protocol (EAP). IETF, March; 1998.
5. The Limits on Wireless Security, 802. 11 in early 2002 by James Voorhees. January, 30; 2002. Available from: http://www.rr.sans.org/wireless/limits.php.
6. Prasithasanagre P, Krishnamurthy P. Analysis of Energy Consumption of RC4 and AES Algorithms in Wireless LANS. IEEE GLOBECOM; 2003.
7. Fluhrer S, Mantin I, Shamir A. Weaknesses in the Key Scheduling Algorithm of Rc4. 8th Eighth Annual Workshop on Selected Areas in Cyptography, August; 2001.
8. Anderson R, Biham E, Udsen L. Serpent: A Proposal for the Advanced Encryption Standard. NIST AES Proposal, June; 1998.
9. Martin-Lopez R, Gomez AF, Bernal F. Secure three-party key distribution protocol for fast network access in EAP-based wireless networks. Comput Netw 2010;54(15):2651-73.
10. Eissa MM, Ihab AA, Abdel-Latif KM. Wi-Fi protected access for secure power network protection scheme. Int J Electr Power Energy Syst 2013;46(1):414-24.
11. Rai A. Dynamic data flow based spatial sorting method for groups: Software based autonomous parallelization. Recent Trends Parallel Comput 2014;1(1):15-8.
12. Rai A. Shell implementation of neural net over the UNIX environment for file Management: A step towards automated operating system. J Oper Syst Dev Trends 2014;1(2):10-4.
13. Jindal P, Singh B. RC4 Encryption-A Literature Survey. In: Proceedings of the International Conference on Information and Communication Technologies, ICICT 2014, 3-5 December; 2014.
14. Rai A. Automation of community from cloud computing. J Adv Shell Program 2014;1(1):21-3.
15. Rai A. Dynamic pagination for efficient memory management over distributed computational architecture for swarm robotics. J Adv Shell Program 2014;1(2):1-4.
16. Rai A, Ramanathan S, Kannan RJ. Quasi Opportunistic Supercomputing for Geospatial Socially Networked Mobile Devices. Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), 2016 IEEE 25th International Conference on. IEEE; 2016.
17. Pacheco de Carvalhoa JA, Veiga H, Pacheco CF, Reis AD. Performance Evaluation of Laboratory Wi-fi Ieee 802. 11a Wpa Point-to-Multipoint Links. CENTERIS 2013-Conference on Enterprise Information Systems; 2013.