Wireless Authentication for secured and Efficient Communication

S.S.Riaz Ahamed

Dr., M.Tech.,Ph.D., Professor & Head, Dept of Computer Applications,
Mohamed Sathak Engg College, Ramanathapuram-623501, Tamilnadu. India.
Mobile: 9443105480. Email: ssriaz@yahoo.com

Abstract

Authentication is the process of verifying a claimed identity. In perhaps the earliest form of authentication, the person being authenticated – called the user in this article – would present a password to the authority requiring authentication – called the authenticator. If the user were able to present the correct password, he or she would be authorized to gain access to something or to receive services. For some purposes, simple password authentication can provide relatively strong security, but in order to do so, certain assumptions must hold true:

- *The user must have some assurance that the authenticator is in fact the authority in question.*
- *The communication channel between the user and the authenticator must itself be secure (user and authenticator can be sure that no one is listening).*
- *It must be highly unlikely that an attacker would be able to guess the password. Usually this is accomplished by limiting the number of wrong guesses.*

1. Introduction

In this article, we will see the Requirements for Wireless Authentication; Certificate based Authentication and Password Authentication Methods.

2. Requirements for Wireless Authentication

The following sections list requirements that an authentication method must meet (must have), additional characteristics that are highly desirable (should have), and features that may be quite useful in certain environments (may have).

2.1. REQUIREMENTS (MUST HAVES)

Mutual – It must provide mutual authentication, that is, the authenticator must authenticate the user, but the user must be able to authenticate the authenticator as well. Mutual authentication is particularly important over wireless networks because of the ease with which an attacker can set up a rogue access point. There are two possible attacks here. In one, the rogue is not connected to the target network and merely wishes to trick the user into divulging authentication credentials. In the other, the rogue is connected to the target network. The attacker may then ignore the credentials presented by the user and “authorize” network access. The user’s session may then be recorded or even altered because the attacker has been inserted in the data path.

Self-protecting – It must protect itself from eavesdropping since the physical medium is not secure. The authentication must proceed in such a way that eavesdroppers cannot learn anything useful that would allow them to impersonate the user later.

Immune to Dictionary Attacks – It must not be susceptible to online or offline dictionary attacks. An online attack is one where the imposter must make repeated tries against the authenticator “on line”. These can be thwarted by limiting the number of failed authentication attempts a user can have. An offline attack is one where attackers can make repeated tries on their own computers, very rapidly, and without the knowledge of the authenticator. Simple challenge/response methods are susceptible to offline attacks because if attackers capture a single challenge/response pair, they can try all the passwords in the dictionary to see if one produces the desired response.

Produces Session Keys – It must produce session keys that can be used to provide message authentication, confidentiality, and integrity protection for the session the user is seeking to establish. These keys will be passed to the user's device drivers to be used as WEP or TKIP keys during the ensuing session.

2.2. ADDITIONAL CHARACTERISTICS (SHOULD HAVES)

Authenticates User – It should authenticate the user rather than the user device. In that way it will be hardened against attacks against the user device. One useful way to meet this requirement would be for the method to depend on a simple secret that can easily be remembered by the user. Another way is to encase the secret in a smart card that is carried by the user and is separate from the device.

Forward Secrecy – It should provide forward secrecy. Forward secrecy means that the user's secret, whether password or secret key, cannot be compromised at some point in the future. An attacker who recorded a user's session encrypted by a key produced during authentication cannot, given knowledge of the user's secret, decrypt the recorded session. Once secure, the session data stays secure forever.

Access Points – It should work with all access points that support 802.1x with EAP authentication.

Quick and Efficient – The authentication should complete in a minimal number of protocol round trips, and computations necessary to complete the authentication should require a minimal amount of computing resources.

Low Maintenance Cost – It should be easy to administer. A method that requires the installation of a certificate on each user device, for example, is not easy to administer. Maintenance of certificate revocation lists can be a costly administrative burden.

Convenient for Users – It should be convenient enough to use that users will not balk. For example, using a certificate stored on a device, though, burdensome to administrators, is convenient for users. Smart cards, though inconvenient for users, are easier for administrators. Users don't mind typing a small, easy to remember password, but most would object to typing a long string of hex digits.

2.3. OTHER USEFUL FEATURES (MAY HAVES)

Augments Legacy Methods – It may protect a less secure, legacy method in such a way that the combination of the wireless authentication method and legacy method meet the above requirements. This feature is useful in environments with legacy authentication systems that cannot quickly be replaced.

Fast Reauthentication – It may provide a reauthentication mechanism that is less time and/or compute intensive than the legacy authentication. Of particular concern is enabling fast handoffs for mobile users. Since the time constraints on a handoff may be very tight, a reauthentication mechanism that takes few round trips or can be accomplished by a server in the service provider's domain rather than the user's home domain would be helpful. However, care should be taken that such reauthentication mechanisms provide strong security.

3. Certificate based Authentication

Today's 802.11 networks authenticate users according to the IEEE 802.1x standard. 802.1x specifies how to run the Extensible Authentication Protocol (EAP) directly over a link layer protocol.

EAP is essentially a transport protocol that can be used by a variety of different authentication types known as EAP methods. Among the EAP methods developed specifically for wireless networks are a family of methods based on public key certificates and the Transport Layer Security (TLS) protocol. These are EAP-TLS, EAP-TTLS, and PEAP.

3.1. EAP-TLS

EAP-TLS uses the TLS public key certificate authentication mechanism within EAP to provide mutual authentication of client to server and server to client. With EAP-TLS, both the client and the server must be assigned a digital certificate signed by a Certificate Authority (CA) that they both trust.

Features of EAP-TLS include:

- Fragmentation and reassembly (of very long EAP messages necessitated by the size of the certificates, if needed)
- Fast reconnect (via TLS session resumption)
- Mutual authentication (server to client as well as client to server)
- Key exchange (to establish dynamic WEP or TKIP keys)

3.2. EAP-TTLS

The Tunneled TLS EAP method (EAP-TTLS) provides a sequence of attributes that are included in the message. By including a RADIUS EAP-Message attribute in the payload, EAP-TTLS can be made to provide the same functionality as PEAP . If, however, a RADIUS Password or CHAP-Password attribute is encapsulated, TTLS can protect the legacy authentication mechanisms of RADIUS. When the TTLS server forwards RADIUS messages to the home server, it decapsulates the attributes protected by EAP-TTLS and inserts them directly into the forwarded message. Because this method is so similar to PEAP, it is being used less frequently.

Figure 1

Error! Unknown switch argument.

Source: International Engineering Consortium

3.3. PEAP

Like the competing standard TTLS, PEAP makes it possible to authenticate wireless LAN clients without requiring them to have certificates, simplifying the architecture of secure wireless LANs. Protected EAP (PEAP) adds a TLS layer on top of EAP in the same way as EAP-TTLS, but it then uses the resulting TLS session as a carrier to protect other legacy EAP methods. PEAP uses TLS to authenticate the server to the client but not the client to the server. This way, only the server is required to have a public key certificate; the client need not have one. The client and server exchange a sequence of EAP messages encapsulated within TLS messages and the TLS messages are authenticated and encrypted using TLS session keys negotiated by the client and the server.

PEAP provides the following services to the EAP methods it protects:

- Authentication of server to client (so that the protected method only needs to authenticate client to server)
- Key exchange (to establish dynamic WEP or TKIP keys)
- Fragmentation and reassembly (of very long EAP messages, if needed)
- Fast reconnect (via TLS session resumption)
- Message authentication (Imposters may neither falsify nor insert EAP messages.)
- Message encryption (Imposters may neither read nor decipher the protected EAP messages.)

PEAP is especially useful as a mechanism to augment the security of legacy EAP methods that lack one or more of the above features.

Microsoft PEAP

Microsoft PEAP supports client authentication by onlyMS-CHAP Version 2, which limits user databases to those that support MS-CHAP Version 2, such as Windows NT Domains and Active Directory.

To use Microsoft's PEAP, users must purchase individual certificates from a third-party certification authority (CA) to install on their IAS, and a certificate must be installed in the user's local computer certificate store. For wireless clients to validate the IAS certificate chain properly, the root CA certificate must be installed on each wireless client.

Windows XP, however, includes the root certificates of many third-party CAs. If the IAS server certificates correspond to an included root CA certificate, no additional wireless client configuration is required. If users purchase IAS server certificates for which Windows XP does not include a corresponding root CA certificate, they must install the root CA certificate on each wireless client.

Cisco PEAP

Cisco PEAP supports client authentication by One-Time Password support (OTP) and logon passwords. This allows support for OTP databases from vendors such as RSA Security and Secure Computing Corporation, and also supports logon password databases like LDAP, Novell NDS, and Microsoft databases. In addition, the Cisco PEAP client can protect user name identities until the TLS encrypted tunnel is established. This provides additional assurance that user names are not being broadcast during the authentication phase.

3.4. PROBLEMS WITH CERTIFICATE BASED METHODS

Despite the many advantages of certificate-based EAP types, there are some disadvantages as well.

3.4.1. Cost of Administration

The biggest down side to certificates is the cost of administration. All of the methods in this family require the authenticator to have a public key certificate signed by an authority that is recognized by the clients (the users' devices). This requires network administrators either to purchase server certificates from a commercial certificate authority (CA) or to acquire the software and expertise to create their own. Next, each device that will access the network must be configured to recognize the certificates of the authenticator and the CA. The EAP-TLS method requires all the user devices to have certificates as well. This significantly increases the cost of administration. Not only do certificates have to be created or purchased for each user device, but distribution can be a problem as well – there must be a method of securely installing the certificates on the user devices. Also, it can be difficult to maintain a Certificate Revocation List (CRL) so that the authenticator will know which certificates are good and which are not.

3.4.2. Lengthy Protocol Exchange

A second disadvantage of using a certificate-based EAP method is the number of sequential protocol exchanges (round trips) that are required between the user client and the authenticator in order to complete the authentication. For example, to authenticate a single user via EAP-MD5 protected by PEAP requires six round trips between the user station and the authenticator. Requiring a large number of protocol exchanges both lengthens the authentication delay for the user and uses more computing resources on the authenticator. Because the authentication delay is a particular problem for mobile users who must be reauthenticated when moving from one access point to another and who require a seamless handoff so as not to disrupt ongoing sessions, these methods all permit use of the TLS session resumption feature. This mitigates the handoff problem, but does not help the initial authentication.

3.4.3. Authenticates the Device Instead of the User or Requires a Smart Card

A third disadvantage is that the certificate must either be stored on the user device or on a smart card that the user carries. When certificates are stored on the user's device, it is the device that is authenticated rather than the individual user. In environments where the device cannot be sufficiently secured or where many individuals use the device, it is important to authenticate each individual user. A smart card is a way users can carry their certificates with them, but they are a source of inconvenience and require all the devices to have a card interface.

4. Password Authentication Methods

Although password authentication methods are more convenient than certificate-based methods, they still have vulnerabilities.

4.1.1. LEAP and Cisco CCX

LEAP is Cisco’s Lightweight Extensible Authentication Protocol, and is based on mutual authentication, which means that both the user and the access point must be authenticated before access onto the corporate network is allowed. Mutual authentication protects against unauthorized (or “rogue”) access points attempting to gain entry into the network. Cisco LEAP is based on a username/password scheme and is proprietary to Cisco access points. Cisco CCX (Cisco Compatible Extensions Program) provides assurance of compatibility between Cisco Aironet wireless infrastructure products and wireless client devices from third-party companies. This helps to maintain compatibility with Cisco features and protocols, including LEAP.

4.1.2. LEAP

With Cisco’s LEAP, security keys change dynamically with every communications session, preventing an attacker from collecting the packets required to decode data. The new keys generated through LEAP use a shared secret key method between the user and the access point. Because LEAP is proprietary to Cisco, it can be used only with a Cisco access point. LEAP also adds another level of security to the network by authenticating all connections to the network before allowing traffic to pass to a wireless device. Using constantly changing secret keys coupled with user authentication provides additional security for wireless data.

4.1.3. Strong Password Authentication Methods

In response to the cost and inconvenience of using certificate-based authentication methods, security researchers have developed a whole new family of authentication methods based on the use of passwords, but addressing all the deficiencies of traditional password methods. We will use the term strong password to refer to this family.

The main benefit of the strong password methods is that two parties can prove to each other that they both know a secret without revealing that secret to a third party who may be listening in on the conversation. In fact, they neither reveal the secret nor make it easier for the attacker to discover the secret. Strong password methods achieve strong authentication by using a small, easily remembered password.

At the core of these methods is a Diffie-Hellman exchange. A Diffie-Hellman exchange permits two parties to create encryption keys in such a way that an observer watching the entire session will not be able to learn the keys. Diffie-Hellman exchanges take place between web browsers and online merchants, for example, in order to encrypt personal information such as credit card numbers. If the customer and merchant have never done business before, how are they to agree on an encryption key without third parties who may be eavesdropping on the session finding out what it is? Diffie-Hellman supplies the solution.

4.1.4. The Power of SPEKE

The SPEKE method uses a series of random-looking messages exchanged between devices. SPEKE modules perform computations with these messages, then determine whether the password used at the other device was correct. When the passwords match, SPEKE puts out a shared key for each device.

To a third-party observer, SPEKE messages look like random numbers and cannot be used to verify any guesses as to what the password might be. SPEKE's additional power comes from the public key computations that are central to this method. There is no need for any long-lived public keys, private keys, or any sensitive data other than the password. SPEKE uses the Zero Knowledge Password Proof (ZKPP) authentication method to securely transmit passwords, which prevents revealing information to any participant unless they use the exact password in the protocol.

Because of this, SPEKE makes password-based authentication stronger and safer. With SPEKE, even a small or poorly chosen password receives greater protection from attack. Other security characteristics of SPEKE include:

- Complete benefits of modern cryptography using an ordinary small password
- Strong, unlimited length of key can be negotiated
- Protection from off-line attacks that crack hash-based challenge/response methods
- Client and server are authenticated simultaneously
- No other security infrastructure requirements
- No client or server certificates are required

Ease of Use

To implement SPEKE, users perform a one-time setup when installing the device driver or contacting an access point for the first time. There is no need for additional infrastructure (unlike TLS and other 802.1x authentication alternatives) to get the same level of authentication, and can be built into simple wireless access point devices.

SPEKE vs. LEAP

Cisco LEAP (Lightweight Extensible Authentication Protocol) is a proprietary protocol that may be used with Cisco access points only. It is a derivative of EAP, providing mutual authentication between client and server, but is proprietary at the access point level of the network. SPEKE is access point independent and will work with any 802.1x compliant access point. This provides maximum flexibility for mixed networks or networks that do not exclusively use Cisco WLAN infrastructure.

SPEKE vs. PEAP

Protected EAP (PEAP) provides support for one-time token authentication, password change and expire support, and database extensibility to support LDAP/NDS directories. PEAP encrypts the conversation between the EAP client and the server, and security is maintained by using a TLS channel. Mutual authentication is required between the EAP client and the server. SPEKE, however, does not require using tokens or certificates, and provides simultaneous authentication. Passwords are exchanged securely, without revealing information to third parties, and there is no need for a TLS channel.

Both the certificate-based methods and the strong password methods meet the basic requirements and may be used on wireless networks. Certificate-based methods possess some special properties that may be valuable in some environments, such as the ability to protect and augment legacy methods that may already be in use. However, the password method is much easier to set up and administer.

5. References

1. "Under the Hood: Wireless Authentication," Cisco Packet™ Magazine-Online Exclusive Archive-April 2002; available from http://www.cisco.com/warp/public/784/packet/ exclusive/apr02.html; Internet; accessed 7 November 2003.

2. Phifer, Lisa. “Cisco LEAP (Lightweight Extensible Authentication Protocol), SearchDomino (12 August 2002); available from http://searchnetworking.techtarget.com/originalContent/0,289142,sid7_gci843996,00.htmlhttp://searchnetworking.techtarget.com/originalContent/ 0,289142,sid7_gci843996,00.html; accessed 7 November 2003.
3. Wireless LAN Media Access Control (MAC) and Physical Layer (PHY) Specifications, International Standard ISO/IEC 8802-11:1999, ANSI/IEEE Std 802.11, 20 August 1999.
4. Standards for Local and Metropolitan Area Networks: Port based Network Access Control, IEEE Std 802.1X-2001, 14 June 2001.
5. L. Blunk, J. Vollbrecht, "PPP Extensible Authentication Protocol (EAP)," IETF RFC 2284, March 1998.
6. B. Aboba, D. Simon, "PPP EAP TLS Authentication Protocol," IETF RFC 2716, October 1999.
7. C. Rigney, A. Rubens, W. A. Simpson, S. Willens, "Remote Authentication Dial In User Service (RADIUS)," IETF RFC 2138, April 1997.
8. G.H. Forman and J. Zahorjan, "The Challanges of Mobile Computing," Computer, April 1994
9. D.F. Bantz, "Wireless LAN Design Alternatives," IEEE Network, March/April1994,pp.43-53.
10. H. Ahmadi, A. Krishna, and R. O. Lamaire, "Design Issues in Wireless LANs," Journal of High Speed Networks, Vol. 5, 1996, pp. 87-104.
11. T. F. La Porta, K.K. Sabnani, and R.D. Gitlin, "Challenges for Nomadic Computing: Mobility Management and Wireless Communications," Mobile Networks and Applications, Vol. 1, 1996, pp. 3-16.
12. R. Bagrodia, W.W. Chu, L. Kleinrock, and G. Popek, "Vision, Issues, and Architecture for Nomadic Computing," IEEE Personal Communications, December 1995, pp. 14-27.
13. K. Pahlavan, T.H. Probert, and M.E. Chase, "Trends in Local Wireless Networks," IEEE Communications Magazine, March 1995, pp. 88-95.
14. E. Links. W. Diepstraten and V. Hayes, "Universal Wireless LANs," Byte, May 1994, pp. 99-108.
15. B. Jabbari, et al, "Network Issues for Wireless Communications," IEEE Communications Magazine, January 1995, pp. 88-98.
16. A.K. Salkintzis and C. Chamzas, "Mobile Packet Data Technology: An Insight into MOBITEX Architecture," IEEE Personal Communications Magazine, February 1997, pp. 10-18.
17. R.H. Katz, "Adaptation and Mobility in Wireless Information Systems," IEEE Personal Communications, First Quarter 1994, pp. 6-17.

Other on-line Resources

- Wireless Network Security with IEEE 802.1X, available at:http://www.microsoft.com/ WINDOWSXP/ pro/ evaluation/ overviews/8021x.asp
- Wireless 802.11 Security with Windows XP, available at: http://www.microsoft.com/WINDOWSXP/pro/techinfo/administration/wirelesssecurity/default.asp
- Enterprise Deployment of IEEE 802.11 Using Windows XP and Windows 2000 Internet Authentication Service, available at: http://www.microsoft.com/windowsxp/pro/techinfo/deployment/wireless/default.asp
- Nokiahowto.com, http://www.nokiahowto.com/
- 3G Newsroom, http://www.3gnewsroom.com/
- Mobile IN, http://www.mobilein.com/
- Wireless Advisor, http://wirelessadvisor.com/
- Wireless Resource, http://www.alphapagingsoftware.com/
- Wireless Info Resource Center, http://www.wirc.org/
- 3G Generation, http://www.3g-generation.com/

- Wireless Researcher, http://www.wirelessresearcher.com/
- Steve Romains's Cellular Information Site, http://www.geckobeach.com/cellular/
- SprintUser.com, http://www.sprintuser.com/
- GSM Made Simple, http://www.geocities.com/henrik.kaare.poulsen/gsm.html
- Nokia 6190/Fido GSM Information, http://gsm.erc.bc.ca/
- GSM Files, http://www.gsm-files.com/
- WAP Forum, http://www.wapforum.org/
- AnywhereYouGo.com, http://www.anywhereyougo.com/
- Palowireless.com, http://www.palowireless.com/
- Phone.com Developers area, http://www.openwave.com/developers
- Ericsson's Wap Developer's Zone, http://www.ericsson.com/developerszone/index.asp
- Buzzed Mobile, http://www.buzzed.co.uk/mobile/
- Mobile Media Japan, http://www.mobilemediajapan.com/
- Thozie Info Pages, http://www.thozie.de/english/wap/
- Jumbuck.com, http://www.jumbuck.com/

Article received: 2007-10-21