Edith Cowan University
Research Online

Australian Information Security Management Conference

Security Research Institute Conferences

2008

Securing a wireless network with EAP-TLS: perception and realities of its implementation

Brett Turner
Edith Cowan University

Andrew Woodward
Edith Cowan University

Originally published in the Proceedings of the 6th Australian Information Security Management Conference, Edith Cowan University, Perth, Western Australia, 1st to 3rd December 2006.
This Conference Proceeding is posted at Research Online.
http://ro.ecu.edu.au/ism/56

Securing a wireless network with EAP-TLS: perception and realities of its implementation

Brett Turner
Andrew Woodward
Secau
Edith Cowan University,
Perth, Western Australia
b.turner@ecu.edu.au

Abstract

In the arena of wireless security, EAP-TLS is considered one of the most secure protocols. However since its inception the uptake has been poor and the investigation into the reasons for this are sparse. There is an industry perception that EAP-TLS is complex as well as difficult to configure and manage. One of the major barriers is in the use of public key infrastructure and the perceived difficulties in its application. The paper discusses why it is seemingly difficult to implement and how this may differ from the reality of its implementation. This premise is investigated using Windows Server 2003 to provide an argument that is in contradiction to the perception. This paper demonstrates that the processes with which the technology can now be applied have significantly improved through automation of public key infrastructure configuration and deployment.

Keywords

EAP-TLS, public key infrastructure, certificates, wireless security

INTRODUCTION

Securing a wireless network has been a barrier to its use since its inception, from the early issues reported with wired equivalent privacy (WEP) (Walker, 2000; Fluhrer *et al*, 2001), through to the introduction of WPA and subsequent release of vulnerability with the implementation of the temporal key integrity protocol (TKIP). The release of the final version of the 802.11i extension saw WPA2 introduced by manufacturers, which does offer a high level of security through the use of 8021.x RADIUS and EAP for authentication, and the and AES for encryption. Unfortunately, there is also a reasonably high level of both technological knowledge, as well as hardware required to implement these new security features.

Whilst these security issues may have delayed enterprise level deployment of wireless networks, it appeared to do little restrict or prevent its use by smaller organisations and individuals (Yek and Bolan 2004). A more recent survey of the central business district in the Perth, Western Australia, conducted by the authors of this paper showed that a much smaller number of users had unsecured access points than revealed in the 2004 survey of the same area. What was of concern however was the relatively high use of WEP. Given that breaking WEP is a trivial task that can be completed in minutes (Bittau *et al*, 2006), it's use as a security measure in a corporate environment should cease. The TKIP method of protecting a wireless LAN is already subject to offline dictionary attack, with tools such as coWPAtty (Wright, 2006). In addition, there are recent reports indicating that TKIP used by WPA personal mode has been partially cracked (Resende, 2008). Effectively, this means that the only real method of adequately securing a wireless network is to use the enterprise mode provided by WPA2. This also means coming to terms with the increased technological and financial burden associated with its implementation. More specifically, this means implementing EAP-TLS authentication, and the use of digital certificates.

One of the biggest strengths of EAP-TLS is its leverage of public key infrastructure (PKI), or certificates. In EAP-TLS, certificates are used on the server and on the client [supplicant] to validate the identities of each to the other for mutual authentication. The client certificate requirement has also been seen as a "major concern [for implementation] due to their sheer numbers." (Ou, 2005). Taking that concern even beyond the impression that statement implies of huge efforts involved in distributing the certificate to supplicants, "client-side certificate required a PKI server infrastructure (rare for most organizations) to be in place ahead of time or expensive third-party certificates, it automatically excluded EAP-TLS as a feasible option for most organizations" (Ou, 2005). This identifies a number of distinct perceived barriers to the uptake of EAP-TLS to be discussed. It is the purpose of this paper to investigate the perceptions held by some in industry surrounding EAP-TLS and challenge their validity.

AUTHENTICATION FOR WIRELESS NETWORKS USING 802.1X / EAP

Extensible Authentication protocol [EAP] is an arbitrary authentication mechanism that is used to authenticate a remote connection. As an extension of the Point to Point Protocol [PPP] it views many forms of network connections (ie: wired ports, Virtual Private Network [VPN], wireless connections) that are not immediately seen as such as remote connections. EAP is negotiated at the connection phase with the exact method negotiated between the authenticator and the client (Microsoft, 2006).

The IEEE 802.1x authentication system is a means for authenticating and controlling user access to a protected network, as well as dynamically varying encryption keys. 802.1X works in conjunction with an extensible authentication protocol (EAP), and an authenticator, usually RADIUS, to both the wired and wireless LAN media (Edney and Arbaugh 2004). It consists of three parts:

1. The Supplicant – the client wishing to join the network
2. An authentication server – an authentication system, usually RADIUS
3. An authentication device – an intermediary between the server and client, usually an access point

It supports multiple authentication methods including Kerberos, one-time passwords, certificates, and public key authentication. In wireless networks, the process involves a four way handshake as shown in Figure 1. Client authentication with 802.1x works in the following manner:

1. The supplicant sends an authentication request to the authentication device.

2. The authentication device responds with a request to the supplicant to provide authentication and blocks all other traffic

3. The supplicant sends an its identity response to the authentication server

4. The authentication server receives and verifies the supplicants' response. If successful an accept message is sent to the authenticating device, if unsuccessful a failure message is sent.

5. If the authentication server accepts the supplicant, then the authentication device will transition the client's port to an authorized state, unblock traffic and forward additional traffic.

Figure 1: The four way handshake process used to authenticate clients in a wireless network using 802.1x (Craiger 2002).

There are many different types of EAP, which can be used in conjunction with the 802.1x system. These include: protected EAP (PEAP), lightweight EAP (LEAP), EAP with transport layer security (EAP-TLS), tunnelled transport layer security (EAP-TTLS), and EAP message digest (EAP-MD-5) (Intel 2008).

The different types of EAP available can be summarised as:

- The MD5 method is not common as it only performs one way authentication, and it does not support WEP key automation, meaning that considerable administration is required.
- The TLS method is very secure, but requires that client certificates for all wireless users. Maintenance of this PKI system would also require extra administration.
- The TTLS overcomes the problem of certificates by tunnelling the TLS. However, there is a charge for both supplicant and authentication software.

- The LEAP system was developed by CISCO for use with their equipment only. Although this has now been licensed to other manufacturers, vulnerabilities have been demonstrated, and if used, a strong password policy must be enforced.
- EAP-FAST can be used in instances where strong passwords cannot be used, and certificates are also an unwanted option.
- PEAP is to EAP-TTLS in that it does not require client certificates. PEAP was developed by Cisco, Microsoft and RSA.

A summary of the different EAP types in terms of their key features can be found in Table 1.

Table 1: The different EAP types available for use with 802.1x in a wireless environment (Intel 2008)

EAP type / Features	**MD5**	**TLS**	**TTLS**	**PEAP**	**FAST**	**LEAP**
Client certificate	no	yes	no	no	no	no
Server certificate	no	yes	no	yes	no	no
WEP management	no	yes	yes	yes	yes	yes
Rogue AP detection	no	no	no	no	yes	yes
Authentication	One-way	Mutual	Mutual	Mutual	Mutual	Mutual
Ease of deployment	Easy	Difficult	Medium	Medium	Medium	Medium
WiFi Security	Poor	Very high	High	High	High	High (strong password required)

EAP-TLS AND HOW IT IS USED

EAP-TLS is based on and is similar to Secure Sockets Layer [SSL] and VPN. While TLS can be used with pre-shared keys, it is designed to be used with certificates. With certificates passwords are never transmitted over the network in any form, instead certificates are exchanged and the chain of trust is validated. Encryption methods and session keys are then negotiated and securely transmitted using a Public Key Encryption [PKE] technique such as the Diffie-Hellman algorithm. From this point, only those security principals that possess the private keys matching the exchanged public keys are able to participate in the conversation (Microsoft, 1999, 2008).

Public Key Infrastructure [PKI] is the key component in a secure implementation of EAP-TLS. A PKI is a system to make available Public Key Encryption [PKE] (and related services) and, in the context with which this paper is concerned with, associate these with a security principal through a Certificate Authority [CA]. Through the use of PKI a certificate can be traced back to a CA who confirms the identity of the security principal seeking authentication or validation.

The process by which a wireless client authenticates to a wireless network using EAP-TLS can be seen in Figure 2.

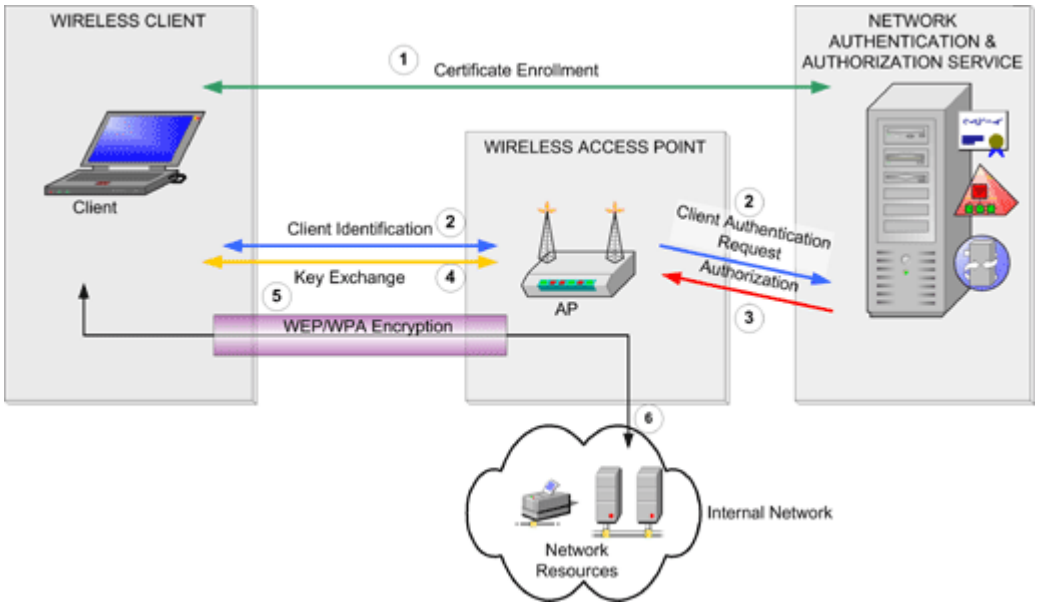

Figure 2: 802.1x EAP-TLS implementation for a wireless network (Microsoft, 2004)

BARRIERS TO EAP-TLS USE

Third party Certificate Authority

The essence of the third party certificate authority [CA] argument lies in a perception that the certificate for some reason must be issued from a third party CA, otherwise known as a Trusted Third Party [TTP], such as VeriSign or Thawte. This perception can be motivated by issues surrounding other uses for PKI such as online commerce where external liability is a reassurance. With that perception the effort or expense involved in getting a certificate issued from a TTP becomes a point of contention. SSL certificates from TTP start around two hundred and fifty dollars (and go up past the fifteen hundred dollar figure) for one year for one certificate depending on the provider, they need to be renewed and care needs to be taken in preserving their validity.

Expense of PKI

Regardless of if you use an external or internal CA, EAP-TLS requires the presence of a PKI. Certificates are core to the highest levels of data transport security such as EAP-TLS, SSL and VPN. While some of these can be implemented with other mechanisms such as shared secrets, their true potential and capabilities are not brought to bear without the use of certificates. The issue of PKI being a difficult and expensive technology to implement is such that many organisations would rather scale back than implement it (White, 2006).

Some of these perceptions come from the way the technology has been presented in the past. For example one of Microsoft's earlier guides, Securing Wireless LANs with Windows 2003 was over 300 pages and recommended such procedures as an offline root CA and performing all operations to a CA (such as installation or revocation of certificates) with witnesses present. Many of the best practices of PKI recommend layered, hierarchical approaches with dedicated purposed hosts and dire warnings of what could happen if a compromise occurred, usually if the one failed to heed said recommendations (Posey, 2006).

Effort of supplicant configuration

In EAP-TLS both the server and the client require a certificate. While this is not such a huge burden for the server(s) which are few, the potential exists for the number of supplicants to be considerably higher. Given this image it is easy to understand how this could be a daunting task given some means of manual distribution. In fact it could be argued that manual installation of the certificate on the supplicant is the only means of ensuring the integrity of the certificate.

The perception of this particular issue is widespread enough that EAP-TLS has been extended to remove the requirement of the supplicant certificate. EAP-TTLS was created to enable a supplicant to use more traditional methods of authentication with a more secure means of transmitting said means of authentication (Ou, 2005). However, by removing the supplicant certificate and thus mutual authentication, EAP-TTLS is more susceptible to exploits such as man-in-the-middle (MitM) attacks (WIPO, 28 June, 2004).

Another perception is that the wireless configuration of the supplicant for EAP-TLS, not being as simple as some other wireless security methods, needs to be done for each machine and as such creates a large overhead for manual handling and administration of these supplicants. This particular point could be seen as a nuisance for a small organisation without a huge supplicant base but could well be an unjustifiable use of costly resources for a large enterprise with a considerable fleet.

SOLUTIONS TO IMPLEMENTATION BARRIERS

The impressions of difficulty mentioned here are discussed in the context of a Windows 2003 Domain environment implementation with Windows XP SP2 as the client. All the software components needed to implement come included in this environment without additional cost. The hardware used was a Cisco 1100 Access Point [AP] which supports EAP authentication methods.

Third party Certificate Authority

The core issue with the perception that a TTP is required lies in the nature of certificates themselves. Certificates are in essence the public key of a security principal in a container signed by the private key of a trusted third party, in this case a TTP. This allows anyone with the public key of the CA to validate that the certificate is signed by the CA and that the public key and credentials associated with that certificate are trustable.

The irony here is that to trust an initially un-trustable source (the supplicant) that they are who they say they are, they are vouched for by a third party who's word is trusted for no other reason than they say they should be trusted. This dichotomy is overlooked in public applications because the root certificates of these providers are included in the Trusted Root Certification List of most operating systems and web browsers, most notably in Windows. This prevents unsightly messages of unknown CA certificates which have been known to dissuade users from using secure sites, especially casual browsers from online stores where 'too hard' means 'go somewhere else' (Posey, 2006). This also means in the case on online transactions that the liability resulting from the failure of a certificate to secure details such as credit card numbers, for whatever reason, can potentially be either shared or divested to the TTP.

Bringing a third party to the table to resolve an internal communications issue is a strange decision, especially if it is to only solve the issue of confused users seeing an unfamiliar message when an unknown CA is encountered for the first time. This problem is easily resolvable in a Windows 2003 domain as root certificates for CA's can be distributed into the local certificate stores of machines with group policy. By using your own CA and disseminating its root public certificate to the workstations Trusted Root Certification List through group policy, this allows a trustworthy PKI without the involvement of a third party.

When talking about certificates for internal use, especially for the purpose of securing the communications of a network, an internal CA makes more sense. This is an authority that the organisation trusts because they have essentially invested that trust in themselves and that, unlike a TTP, the organisation has complete control over. This type of CA is internal to the circle of trust. The questions that should be asked are 'What is the purpose of this CA? What are we going to use this for?' This perception is often a problem of not asking the right questions about how the certificates are to be used or not understanding what certificates really are.

Expense of PKI

The perception that a PKI is immensely expensive, difficult to implement and manage comes from the point that most documentation does not offer clear advice. They are generally written for enterprise level implementations and either skip the question of what purpose the PKI will be used for is or if they do, do not explain how to evaluate the risks involved in simplifying their recommendations. Instead things are mentioned such as cost, potential liability, disaster and unrecoverable data. With phrases like "treat your certificate authority the way that you would treat a nuclear warhead; protect it at all costs." (Posey, 2006). how can uncertainty and doubt not follow for any average organisation?

A PKI can be simple or elaborate, cheap or expensive and come with minimal or onerous overheads. Although it is a case of the more trustworthy and secure you want your PKI to be, the more you will pay this has to be balanced against the purpose and cost of compromise. For small organisations wanting to implement wireless security, EAP-TLS is not something that need be extravagant as long as the compromises are understood and it is far preferable than having an unsecured wireless network or even worse, the false belief in the implementation of a protocol with well known vulnerabilities.

For many organisations, a PKI with the sole purpose of securing network traffic can be implemented with a single, online root CA. With a Windows 2003 Server host this is a free, additional service that can be installed. This can be piggybacked upon a server that has other roles even though it is strongly recommended against in CA circles (Posey, 2006) again, because only the theoretical best practices are considered instead of the purpose.

Effort of supplicant configuration

Distribution of certificates and configuration of the wireless component of the supplicant can be completely automated through Group Policy [GP] in a Windows 2003 Domain. Through the use of a Group Policy Object [GPO], a selection of security principals can be configured to request a certificate, what type of certificate they will request, if they should automatically request a new one when the current one expires and from what CA they should request it from. The root CA can also be added into the Trusted Root Certification List through this method and the wireless configuration can be done through the Wireless Network (IEEE 802.11) Policies. This creates an automated implementation of PKI with minimal overhead by using simple, over the wire methods.

As for control over dissemination of certificates, again we must come down to the purpose the PKI will serve. Through the use of GP and proper use of GPOs, certificates can be configured to be automatically issued to only those security principals that we desire and simply possessing a valid certificate in no way translates to a right to use the network.

This leaves as the last issue to be addressed here the potential of interception of the public/private key pair in transmission as it is issued. For most implementations of EAP-TLS this level of caution is not only unnecessary, it plays into the perception by trading off usability for a level of security that is usually not reflected in the rest of the network. While the certificates can be technically intercepted while transmitted over the wired network, it should be questioned that if this is a viable risk then why are these same wired networks not secured? This may well be a valid concern in some networks where data is of a nature that requires precautions of this level but most do not. To use this as evidence of difficulty and thus justification for an implementation of a method of lesser calibre is flawed reasoning.

CONCLUSION

Public Key Infrastructure is an often misunderstood technology. It is viewed in the light of its most heavy applications, given the weight of its heaviest burdens and thus comes with the sternest of warnings. Because of these perceptions its heavy dependence on certificates, EAP-TLS often inherits these onerous expectations. Practices which are accepted as good practice for Public Key Infrastructure in general or in the most prolific arenas of its use are not challenged in the other areas certificates can be used for. The preconceived notions often prevent those questions that should be asked, from being asked. What is this being used for? How secure does this need to be? Are the highest recommendations really needed or can this be simplified?

EAP-TLS in a Windows 2003 Domain is not a difficult method to implement, with Certificate Server and other essential software tools immediately available for no additional cost, so long as the wireless access points supports EAP authentication methods. A basic implementation of EAP-TLS does not need an elaborate Public Key Infrastructure. Group policy can be used to configure supplicants centrally and have that configuration pushed out automatically. Group policy can also solve the problem of issuing certificates to each supplicant and combined with an internal certificate authority allows for complete management of the solution.

The questions that are left to be answered come from the core of why these perceptions exist. Is there a shortfall in the fundamental understanding of what certificates are, or what they can be used for by those that could use them? Is the gap in communication of practices flawed such that ‘best practices’ are seen as ‘only practices’? Is there a lack of knowledge of what tools are available for implementation and management? Future research will look at determining answers to the se questions and to create a framework or best practice for implementation of PKI based EAP usage for wireless networks for small business and other organisations who should be employing this security measure but who are not doing so.

REFERENCES

Bittau, A., Handley, M. & Lackey, J. (2006). The Final Nail in WEP’s Coffin. In The 2006 IEEE Symposium on Security and Privacy, pp 386-400

Chen, J.C. & Wang, Y.P (2005). Extensible authentication protocol (EAP) and IEEE 802.1x: tutorial and empirical experience. Communications Magazine, IEEE Volume 43, Issue 12, Page(s): supl.26 - supl.32. Retrieved June 7, 2008, from http://0-ieeexplore.ieee.org.library.ecu.edu.au/iel5/35/33162/01561920.pdf?tp=&isnumber=33162&arnumber=1561920

Craiger, J.P. (2002). *802.11, 802.1x, and Wireless Security*. Retrieved 10/9/05 from http://www.sans.org/rr/whitepapers/wireless/171.php

Edney, J. & Arbaugh, W.A. (2004) *Real 802.11 security: Wi-Fi protected access and 802.11i*. Pearson, Boston

Fluhrer, S., Mantin, I. & Shamir, A. (2001) Weaknesses in the key scheduling algorithm of RC4. In *Selected Areas In Cryptography.* (Vol. 2259, pp. 1-24). Springer: Berlin

Groom, R. (n.d.). PEAP and EAP. Retrieved June 7, 2008, from http://bizsecurity.about.com/od/mobilesecurity/a/peapeap.htm

Intel. (2005). The Alphabet Soup of EAP types - MD5, LEAP, PEAP, FAST, TLS and TTLS. Retrieved September 15th 2008 from http://www.intel.com/support/wireless/wlan/sb/CS-008413.htm

Microsoft (1999). RFC 2716 - PPP EAP TLS Authentication Protocol. Retrieved June 10, 2008 from http://www.faqs.org/rfcs/rfc2716.html

Microsoft (2004). Chapter 3: Secure Wireless LAN Solution Architecture. Retrieved June 10, 2008 from http://www.microsoft.com/technet/security/prodtech/windowsserver2003/pkiwire/PGCH03.mspx?mfr=true

Microsoft. (2005). Medium Business Solution for Remote Connectivity. Retrieved June 7, 2008, from http://www.microsoft.com/technet/solutionaccelerators/smbiz/mits/rc/mit_rc_2.mspx

Microsoft. (2006). Implementing and Administering Security in a Microsoft Windows 2003 Network.

Microsoft. (2008). RFC 5216, The EAP-TLS Authentication Protocol. Retrieved June 10, 2008 from http://tools.ietf.org/html/rfc5216

Ou, G. (2005). Understanding the updated WPA and WPA2 standards. Retrieved June 7, 2008, from http://blogs.zdnet.com/Ou/?p=67

Posey, B. (2006). Determining Whether an in House or an External Certificate Authority is More Appropriate for Your Company. Retrieved June 7, 2008, from http://www.windowsecurity.com/articles/InHouse-External-Certificate-Authority-More-Appropriate.html

Resende, P. (2008). Researchers Crack WPA Security for Wireless Networks. Retrieved 6th November 2008 from http://www.mobile-tech-today.com/story.xhtml?story_id=012000EWAAJO

Thawte. (n.d.) SSL Web Server Certificates. Retrieved June 11, 2008 from

https://www.thawte.com/ssl-digital-certificates/ssl/index.html?click=main-nav-products-webserver

VeriSign. (n.d.). Secure Site Pro: True 128-bit SSL Certificates. Retrieved June 11, 2008 from http://www.verisign.com/ssl/buy-ssl-certificates/secure-site-pro-ssl-certificates/index.html

Walker, J. (2000). Unsafe at any key size; an analysis of the WEP encapsulation. Retrieved June 10th 2008 from http://md.hudora.de/archiv/wireless/unsafew.pdf

Wang , Y.P., Chen, J.C. & Liu, Y.W. (November 11, 2004).Design and Implementation of WIRE1x. Retrieved June 7, 2008 from http://www.ccrc.nthu.edu.tw/tech/2005101.pdf

White, A. (2006). The Key to Secure Remote Computing. Communications News, Nokomis: Dec 2006. Vol. 43, Issue 12, pg. 32.

Woodward, A. & Turner, B. (2008).

World Intellectual Property Organization [WIPO]. (2004). (Wo/2005/002131) Two-Factor Authenticated Key Exchange Method and Authentication Method using the same, and Recording Medium Storing Program Including the same. Retrieved June 7, 2008 from http://www.wipo.int/pctdb/en/wo.jsp?IA=WO2005002131&wo=2005002131&DISPLAY=DESC

Wright, J. (2006). coWPAtty. Retrieved 10th June 2008 from http://wirelessdefence.org/Contents/coWPAttyMain.htm

Yek, S. & Bolan, C. (2004). An analysis of security in 802.11b and 802.11g wireless networks in Perth, W.A. 5th Annual Information Warfare and Security Conference, Perth, Western Australia 2004

COPYRIGHT

Brett Turner & Andrew Woodward ©2008. The author/s assign Edith Cowan University a non-exclusive license to use this document for personal use provided that the article is used in full and this copyright statement is reproduced. Such documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. The authors also grant a non-exclusive license to ECU to publish this document in full in the Conference Proceedings. Any other usage is prohibited without the express permission of the authors.