IDEA GROUP PUBLISHING

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

ITP5138

This paper appears in *Managing Modern Organizations Through Information Technology*, Proceedings of the 2005 Information Resources Management Association International Conference, edited by Mehdi Khosrow-Pour.

WLAN Client Authentication

Göran Pulkkis, Kaj J. Grahn and Jonny Karlsson

Arcada Polytechnic, Jan-Magnus Janssons plats 1, 00550 Helsingfors, Finland, {goran.pulkkis, kaj.grahn, jonny.karlsson@arcada.fi}

ABSTRACT

This paper is an overview of client authentication in Wireless Local Area Networks (WLANs). Security policy issues for WLAN client authentication are briefly discussed. WLAN access management based on the WLAN security standards IEEE 802.11/WEP, IEEE 802.11X/EAP, IEEE 802.11i/WPA and 802.11i/WPA2 is surveyed. Special attention is paid to implementations of certificate based client authentication. Newly proposed WLAN authentication protocols such as Statistical One-bit Lightweight Authentication (SOLA) and Protocol for carrying Authentication for Network Access (PANA) are also presented.

INTRODUCTION

The implementation of client authentication mechanisms is essential when designing Wireless Local Area Networks (WLANs). WLANs are by nature easy to access since they are based on open air connections. Physical security measures, such as security personnel, identity cards and door locks, which eliminate most intruders in wired Local Area Networks (LANs) are not effective in WLANs. An intruder with a mobile device and a Network Interface Card (NIC) can easily access an unprotected WLAN from anywhere within the WLAN radio range, even from outside a building, where WLAN access points are installed. The purpose of this paper is to discuss strengths and weaknesses of different WLAN user authentication protocols and their implementations. Both existing and proposed future protocols are discussed.

WLAN SECURITY POLICY ISSUES FOR CLIENT AUTHENTICATION

In a tutorial published in November 2002 basic WLAN security policy rules were proposed (Geier 2002). Several rules, like

- Activate Wired Equivalence Privacy (WEP) at the very least
- Utilize dynamic key exchange mechanisms
- Disable APs during non-usage periods
- Assign “strong” passwords to Access Points (Aps)
- Don’t broadcast Service Set Identifiers (SSIDs)
- Don’t use default SSID names
- Reduce propagation of radio waves outside the facility
- Deploy access controllers
- Monitor for rogue APs
- Control the deployment of WLANs

are related to client authentication.

WLAN ACCESS MANAGEMENT BASED ON IEEE 802.11 STANDARDS

There are two kinds of authentication mechanisms defined by the 802.11 standards: open system and shared key authentication. Service Set Identifier (SSID) and Media Access Control (MAC) authentication are also commonly used (Wireless LAN Security, 2004). MAC address authentication is not specified in the 802.11 standard but is supported by many WLAN hardware vendors to strengthen the access control.

Open system authentication allows any client to authenticate to a WLAN as long as it passes through a possible MAC address filter. This authentication mechanism is very vulnerable, since all authentication packets, including MAC addresses, are transmitted without encryption and MAC addresses are easily “spoofed”.

SSIDs are normally broadcasted by WLAN APs. This means that intruders can easily access open system WLANs with the use of a mobile device and a NIC. Some AP vendors support disabling SSID broadcasts but an SSID can still be easily determined by sniffing probe response frames from an AP.

Shared key authentication is based on static WEP keys, which are manually configured in to every AP and client in a WLAN. Freely available packages that allow attackers to discover the WEP key can be found on the Internet, see (Sourceforge, 2001).

IEEE 802.11i and Wi-Fi Protected Access (WPA) provide a more secure shared key based authentication mechanism, called Pre-Shared Key (PSK). WPA in PSK mode is, like WEP, also based on manually entered passwords, but the same key is not used for both authentication and data encryption like in WEP. (Edney, 2003)

CLIENT AUTHENTICATION BASED ON IEEE 802.1X STANDARD

IEEE 802.1X, specified in (IEEE, 2001), is a standard defining a client/server based access control and authentication protocol to prevent unauthorized clients from connecting to a network through publicly accessible network ports. Originally, IEEE 802.X was designed for LANs but is today also used for WLANs. IEEE 802.1X is required in the recently ratified WLAN security standards 802.11i/WPA and 802.11i/WPA2.

The principle of 802.1X is shown in Fig. 1. In case of a WLAN, the 802.1X components consist of:

- supplicant (wireless client)
- authenticator (wireless access point)
- authentication server (typically Remote Authentication Dial-in User Service (RADIUS)

Until a supplicant is successfully authenticated on the authentication server the authenticator only permits authentication messages between the supplicant and the authentication server through the uncontrolled port at the authenticator system. After successful authentication the supplicant is granted network access through the authenticator system’s controlled port. Authentication methods and authentication message exchange methods are defined by the Extensible Authentication Protocol (EAP). The authentication messages are known as EAP over LAN (EAPOL) messages, see Fig. 2.

Username/Password Based Client Authentication

IEEE 802.1X provides username/password based client authentication through various authentication protocols supported by EAP. Examples of such protocols are: EAP-MD5, EAP-LEAP, EAP-TTLS and EAP-PEAP. EAP-MD5 (Message Digest 5) is the least secure EAP type due to the lack of support for mutual authentication and is therefore not accepted in the IEEE 802.11i standard.

The Lightweight EAP Protocol (LEAP) requires mutual authentication between the supplicant and the authenticator. The Tunneled Transport

Figure 1. Principle of IEEE 802.1X Access Control

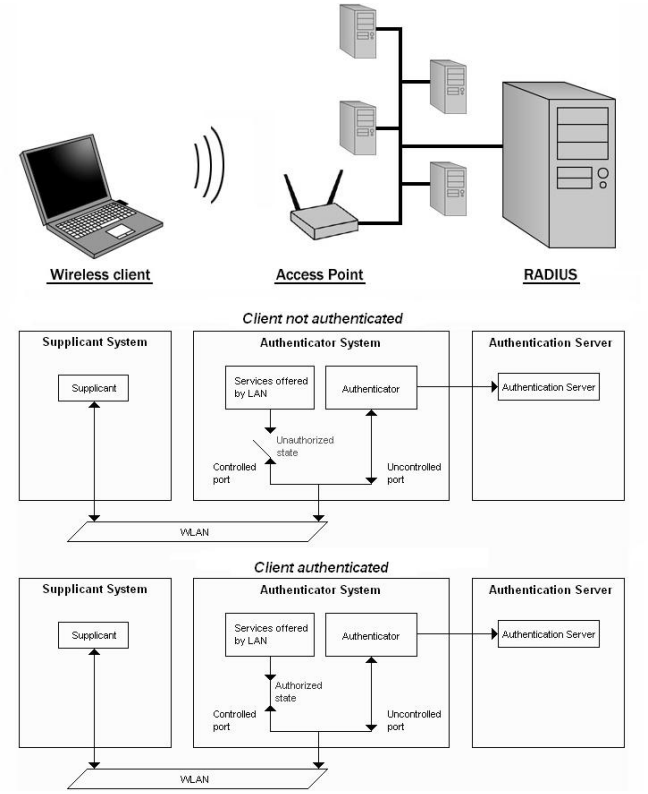
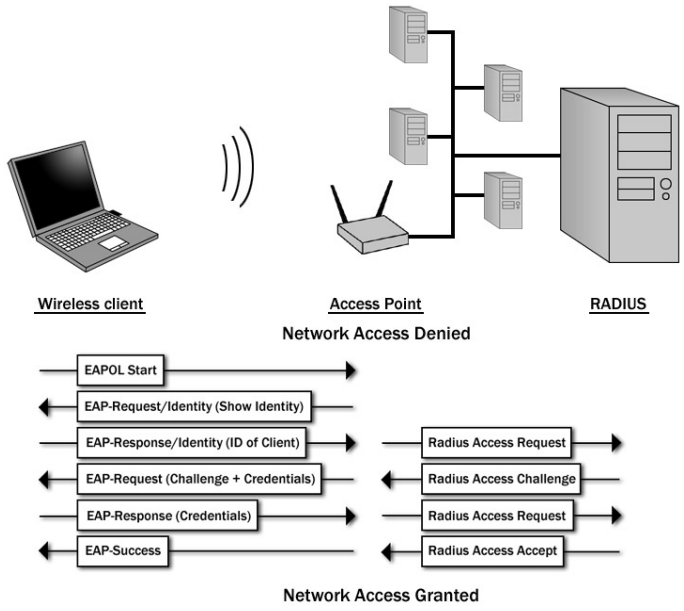


Figure 2. EAPOL Messages



Layer Security (TTLS) and the Protected EAP (PEAP) protocol also provides mutual authentication but differs from LEAP in the way how the network is authenticated on the supplicant. TTLS and PEAP utilize Public Key Interface (PKI) and require authentication servers to use certificates for server authentication. Once an authentication server is authenticated, username/password based user authentication can be performed and the authentication messages are securely transmitted through an encrypted Transport Layer Security (TLS) tunnel.

Certificate Based Client Authentication

The strongest authentication protocol provided by EAP is the Transport Layer Security (TLS) protocol. TLS requires both client- and server side certificates and EAP authentication messages are encrypted and thus protected from eavesdroppers. However, the maintenance of such an authentication framework is complicated due to the need of a PKI infrastructure including certification services, maintenance of Certificate Revocation Lists (CRLs), and trust management. Another important issue is the way a user keeps and protects the private key. For this purpose there are both soft token and hardware token solutions.

Soft Tokens

A X.509 certified private key stored in a soft token practically means that the private key is attached to a file stored on the computer's hard disc. The private key file can alternatively be stored in a floppy disc or USB memory stick which is more secure since a user can carry such a device and is thus easier to control and protect. The private key in a file certificate is usually protected with a pass phrase that is known only by the key owner.

Hardware Tokens

X.509 certified private keys stored in hardware tokens is a more secure and practical solution than storing them in files. A hardware token can be an electronic identity smartcard or an USB token/smartcard. Hardware tokens are protected by PIN codes to protect the private key. A Finnish Electronic Identity (FINEID) smartcard (Finnish, 2004) and a USB based smartcard Aladdin Etoken (Aladdin, 2004) have been tested in a research WLAN environment in Arcada Polytechnic (Arcada, 2004).

- FINEID Smartcard: It was stated that a FINEID smartcard cannot as such be used for EAP-TLS authentication since it's certificate doesn't meet the TLS protocol's and the MS Windows' certificate requirements. The problem was solved by developing a Secure Socket Layer (SSL) protected web based smartcard certificate enrolment interface to which users can log in and authenticate to, using their original FINEID citizen certificate and enrol a new smartcard certificate to be used for WLAN authentication. The web enrolment interface was originally developed by Tampere University of Technology (FEIDHE, 2004) and modified by Arcada Polytechnic for WLAN authentication purposes.
- Aladdin Etoken: The Aladdin Etoken is simpler to prepare for WLAN authentication purposes compared to a FINEID smartcard since private keys and certificates can be imported directly using the Windows XP Certificate Import Wizard. In other words, a X.509 certified private key can be, generated and stored in PKCS#12 file format and as such imported to the USB token. The certificate requirements for the Aladdin Etoken are the same as for the FINEID smartcard except that the maximum length of the private key is 1024 bit, while FINEID cards support 2048 bit keys.

Trust Management

Introduction and use of definitions for credentials, trust levels, trust relationships and security policies are components of trust management. In large infrastructure WLAN environments trust management is based on cryptographic techniques such as PKI.

In PKI, public keys are generated, distributed, and certified by CAs, RAs (Registration Authorities) and directory services (Housley, 2001). These entities can be used to establish a hierarchy or chain of trust. Entities that are unknown to each other in a WLAN, such as a user and an authentication server, individually establish a trust relationship with the CA that has issued and signed the user and/or server certificate.

The simplest trust model is the Single Point mode with only one CA. All users in this environment can trust each other, since all their certificates

are issued and signed by that particular CA that they all trust. PKI implementations for large network environments are however based on the hierarchical trust model with one root CA and a number of underlying CAs. (Housley, 2001)

The trust model in EAP-TLS consists of two parts: a client trusting server and a server trusting client. In the client, a root CA must be configured to be trusted. By using this root CA the client is able to validate the authentication server assumed that the configured root CA has signed or is a part of the server certificate's CA chain. Correspondently a similar configuration is required on the authentication server in order to make it possible for the server to authenticate the client. (Aboba, 1999).

Mobile Phone SIM Card Based Authentication

Utilization of mobile phones and their Subscriber Identity Module (SIM) cards for user authentication in WLANs is an emerging area. EAP-SIM is a new authentication protocol, provided by EAP, allowing users to authenticate to a WLAN using the GSM mobile phone authentication network. Recently, EAP-SIM based user authentication is provided by mobile operators in several hotspot WLAN environments. In an EAP-SIM environment the operator provides access to the GSM network through a standard WLAN 802.1X configuration and an additional GSM/MAP/SS7 (Global System for Mobile Communications /Mobile Application Part/Signalling System 7) gateway. During the authentication process, the authentication server passes the user's SIM card authentication information to the GSM authentication centre through the GSM/MAP/SS7 gateway. The GSM triplets are then retrieved and used to authenticate the client. The EAP-SIM client software, on the supplicant, retrieves authentication information from the SIM card, i.e. by connecting the SIM card to a SIM card reader attached to the client computer, or by connecting to the mobile phone over a Bluetooth connection. Whether the GSM triplets are successfully validated by the SIM card and the EAP-SIM client software on the client side, the authentication server requests the wireless AP to grant network access to the user. (EAP-SIM, 2004).

A new type of mobile phone SIM card is presently entering the market. SETEC, see (SETEC, 2003), was the first vendor to manufacture this type of SIM card which they call PKI eSIM™. Apart from basic mobile phone SIM card functionality the PKI eSIM™ card provides the possibility of storing keys and certificates which can be used for user authentication and digital signatures. Some operators already offer PKI SIM services for their customers, see for example (Sonera, 2004). PKI SIM cards with integrated citizen certificates, provided by the Finnish Population Register Centre (Finnish, 2004), will be available by the end of 2004. This opens the possibility of using mobile phones as authentication tokens in certificate based WLAN client authentication.

Authentication Server and User Data Base

The authentication server, which is typically a RADIUS server, works as a backend server providing authentication service to an authenticator. The RADIUS server maintains a database of users authorized to access the WLAN. Some RADIUS servers, i.e. freeRADIUS (freeRADIUS, 2004), also include support for storing WLAN user credentials in external databases such as Lightweight Directory Access Protocol (LDAP).

NEW WLAN AUTHENTICATION PROTOCOLS

Recent WLAN security standards WPA and IEEE 802.11i provide trustworthy authentication of WLAN clients and APs as well as integrity and confidentiality of data communication between authenticated WLAN clients and APs. The same security features can also be obtained by the IPSec protocol for a WLAN with a single AP in an access router.

End-to-end security in client/server applications requires security protocols like VPN, TLS and Secure Shell (SSH). However, to prevent unauthorized use of APs, any end-to-end security solution must be combined with unambiguous identification of authorized WLAN clients. Required security is obtained by securing the hop between the client and the AP with WPA or IEEE 802.11i in all client/server applications. A drawback of this solution is the high computational load in the WLAN client. Data packets already encrypted with the used end-to-end security protocol must be encrypted once more with the strong encryption algorithm in WPA or IEEE 802.11i. To fulfill necessary WLAN access control requirements a computationally light protocol, SOLA (Statistical One-bit Lightweight Authentication), has been proposed for mutual authentication of a WLAN client and an AP (Johnson, 2002).

Another approach to avoid computationally expensive redundant strong encryption of data communication between a WLAN client and an AP for end-to-end protected client/server applications is to use a network level authentication protocol, which is a carrier of the actual authentication protocol. Such an authentication protocol, PANA (Protocol for carrying Authentication for Network Access), is presently being developed by an IETF Internet Working Group (PANA Working Group, 2004).

SOLA

The principle of SOLA (Statistical One-bit Lightweight Authentication) is simple. A WLAN client and an AP use the encryption key of a successful key agreement to generate the same random bit sequence. The sending side adds the next bit in the generated bit sequence to the MAC header of each transmitted data frame. The communication overhead of SOLA is very low, since only one bit is added to each data frame. The probability that an intruder guesses a sequence of n bits correctly is 2^{-n}. (Johnson, 2002)

Synchronization Requirements

A SOLA implementation also requires a synchronization algorithm for advancing the bit choice from the generated sequence for the next data frame, because data frames and acknowledgement frames can be lost in the data link level communication between a WLAN client and an AP. An algorithm for synchronizing SOLA bit sequences, when acknowledge frames from an AP to a WLAN client are lost, is presented in (Johnson, 2002). An enhanced version of this synchronization algorithm is presented in (Wu, 2004).

Evaluation

The functionality of the synchronization algorithm of SOLA has been proved by simulating sessions between two mobile devices with TCP data sources of an FTP application. The failure rate (ratio of data packets with wrong identification bit to the total number of checked data packets) was measured as a function of

- the drop probability of acknowledgement data (ACK) packets
- the drop duration (number of dropped successive ACK packets)

The simulation gave

- failure rates of 8…20% for a drop probability of 10 % and drop durations of 1…6
- failure rates of 16…40% for a drop probability of 20 % and drop durations of 1…6

For a "guessing the authentication bit" attack the simulation gave the failure rate 50%. The simulation shows that

- the SOLA synchronization algorithm recovers drop probabilities up to 20% and
- reveals "guessing the authentication bit" attacks. (Johnson, 2002)

The security of the SOLA protocol is also evaluated in (Johnson, 2002) for

- "Denial-of-Service" attacks based on transmission of "failed" ACK packets

- "Overwrite" attacks, based on changing data packet content and other header bits than the SOLA synchronization bit
- "Man-in-Middle"-attacks.

All these attacks except the "overwrite" attack are detected as abnormal failure rates of the SOLA synchronization algorithm. An "overwrite" attack is however detected by the IPSec protocol for client/server applications with VPN based end-to-end security.

In the WLAN research community it has been proposed to include SOLA in the IEEE 802.11 standard even if SOLA is still a research prototype under development in three universities (Wu, 2004).

PANA

PANA (Protocol for carrying Authentication for Network Access) is a client/server network layer protocol, where

- the client implementation is called PANA Client (PaC)
- the server implementation is called the PANA Agent (PAA), which communicates with an Authentication Server (AS). AS can for example be a RADIUS server
- the access control is implemented by an Enforcement Point (EP).

PANA is a carrier of existing authentication protocols like EAP. No new authentication protocol is introduced by PANA. (Protocol, 2004)

In a typical WLAN deployment of PANA shown in Fig. 3 (PANA Framework, 2004)

- PaC is installed in each WLAN client
- PAA is installed in AR (Access Router)
- EP is installed in the AR, if the WLAN client connects to a VPN
- EP is installed in each AP, when WPA or IEEE 802.11i link layer security with WPA or IEEE 802.11i is required. In this case Pre-Shared Key mode is used, since PANA is responsible for WLAN client authentication.

PANA is presently an Internet Draft level IETF protocol. An open source implementation of PANA is still already available (PANA Functional, 2004).

CONCLUSIONS

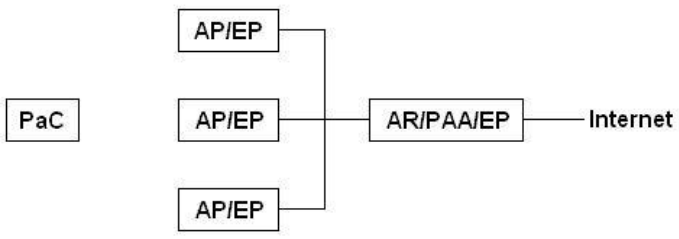
Security risks and threats are higher in a WLAN, compared to wired LANs, since OSI layers 1 and 2 are open for eavesdropping, intrusion and information content manipulation attacks. Therefore, network administrators must be well aware of the security threats and how security can be managed.

Standard organizations such as IEEE, IETF and the Wi-Fi Alliance are developing new reliable security standards to address WLAN vulnerabilities. WEP included serious security flaws due to the use of static encryption keys and the lack of user authentication mechanisms.

IEEE 802.11i, ratified in June 2004, is expected to address all the security flaws in WEP and to eliminate the need of using third party standards such as IPSec. A snapshot version of 802.11i, WPA, is today available in most WLAN equipment. WLAN products with full 802.11i support have been available since fall 2004. WPA and 802.11i provide reliable access management mechanisms through the 802.1X standard and the use of dynamic keys to provide strong data encryption.

New client authentication protocols like PANA and SOLA are being developed to overcome functional and efficiency shortcomings of present WLAN client authentication methods.

Figure 3. PANA Wireless LAN Model (PANA Framework, 2004)



REFERENCES

Aboba, B. and Simon, D. (1999). *PPP EAP TLS Authentication Protocol.* RFC 2716. IETF. Retrieved, Septemeber 28, 2004, from http://www.ietf.org/rfc/rfc2716.txt

Aladdin Knowledge Systems Portal. (2004). Retrieved September 30, 2004, from http://www.ealaddin.com/

Arcada Polytechnic Web Portal. Retrieved October 4, 2004 from http://www.arcada.fi/web/index_eng.php

EAP-SIM Authentication Method for Converging Worlds of Mobile Telephony and Wirleless LAN. Retrieved September 30, 2004, from http://www.mtghouse.com/Whitepaper_EAP-SIM_112003B.pdf

Edney, J. and Arbaugh, W. A. (2003) *Real 802.11 Security: Wi-Fi Protected Access and 802.11i.* Addison Wesley.

FEIDHE pilots. (2004). Retrieved September 30, 2004, from http://www.csc.fi/suomi/funet/middleware/english/summary.html

Finnish Electronic Identity Card Portal. (2004). Retrieved September 30, 2004 from http://www.fineid.fi.

freeRADIUS Portal. Retrieved August 31, 2004, from http://www.freeradius.org.

Geier, J. *The Guts of WLAN Security Policy.* Tutorial. November 2002, Retrieved August 29, 2004 from http://www.wi-fiplanet.com/tutorials/article.php/1499151

Housley, R. and Polk, T. (2001). *Planning for PKI: Best Practices Guide for Deploying Public Key Infrastructure.* John Wiley & Sons, Inc.

IEEE Standard for Local and metropolitan area networks – Port-Based Network Access Control. IEEE Std 802.1X-2001, 2001, ISBN 0-7381-2626-7

Johnson, H., Nilsson, A., Fu, J., Wu, S. F., Chen, A. and Huang, H., SOLA: A one-bit identity authentication protocol for access control in IEEE 802.11, GLOBECOM 2002 - IEEE Global Telecommunications Conference, vol. 21, no. 1, November 2002, pp. 777-781

PANA Framework (2004, July), draft-ietf-pana-framework, Retrieved August 31, 2004, from http://www.ietf.org/internet-drafts/draft-ietf-pana-framework-01.txt

PANA Functional Architecture Version 1.0.0, Retrieved August 31, 2004, from http://diameter.sourceforge.net/pana/

PANA Working Group Web Page, Retrieved August 31, 2004, from http://www.ietf.org/html.charters/pana-charter.html

Protocol for Carrying Authentication for Network Access (PANA) (July 2004), draft-ietf-pana-pana-05, Retrieved August 31, 2004, from http://www.ietf.org/internet-drafts/draft-ietf-pana-pana-05.txt

SETEC Portal. (2003). Retrieved September 30, 2004 from http://www.setec.fi/

Sonera Portal. (2004). Retrieved, Retrieved September 30, 2004 from http://www.sonera.fi/

Sourceforge Project wepcrack (2001). Retrieved December 12, 2003, from http://sourceforge.net/projects/wepcrack.

Wireless LAN Security. Retrieved 16.8.2004 from http://www.tdap.co.uk/uk/archive/access/access(bluesocket_0212).html

Wu, F., Johnson, H., and Nilsson, A. (2004, May-June). SOLA: Lightweight Security for Access Control in IEEE 802.11. *IT Professional,* 6(3), 10-16.