SECURING WIRELESS LOCAL AREA NETWORKS BASED ON IEEE 802.1X AND X.509 CERTIFICATES

Bogdan CRAINICU

Abstract

Deploying a secure WLAN is an especial challenge, because there are a number of extremely risks. These risks will have to be thwarted by the use of stronger security mechanisms while keeping an adequate level of network performance. The 802.1X authentication standard provides a method to protect the network behind the access point based on Extensible Authentication Protocol (EAP). Moreover, in order to strengthen the security solution, a Public Key Infrastructure (PKI) scheme that uses X.509 certificates and Certificate Authority (CA) is added.

Introduction

Wireless LAN (WLAN) by its nature broadcasts data over an area that it cannot be always physically controled. Communication over such a wireless infrastructure is potentially insecure and can be eavesdropped and spoofed. Therefore, wireless security aspects, including data confidentiality, integrity, mutual authentication, as well as key management, have become a serious concern.

Based on the EAP (Extensible Authentication Protocol), IEEE 802.1X standard specifies a general method for the provision of port-based network access control, providing compatible authentication and authorization mechanisms for devices interconnected by IEEE 802 LANs. The authentication is usually done by a third-party entity, such as a RADIUS server.

But IEEE 802.1X [9] has some limitations and in order to get a high level of data protection we need additional security functions [6], [7]. An X.509-based public key infrastructure (PKI) provides one of the best solution in establishing a party's identity, defining a model for strong authentication [8].

IEEE 802.1X

Today WLANs are facing a set of high demanding security requirements. The addition of IEEE 802.1X authentication to the WLAN security framework provides a method to protect network behind the access point against intruders.

The IEEE 802.1X standard [9] states that Port Access Control provides an optional extension of preventing unauthorized access and it is achieved by the network device enforcing authentication of supplicants that attach to the network device's controlled ports (supplicant – an entity at one end of a point-to-point LAN segment that seeks to be authenticated by an authenticator attached to the other end of that link). Moreover, the operation of Port Access Control relies on assumption that the Ports on which it operates offer a point-to-point connection between a single supplicant and a single authenticator – the authentication decisions are made on a per-port basis [9].

The rapid acceptance of 802.1X consists in the flexibility of the Extensible Authentication Protocol (EAP [1]) that may be implemented in a number of differnet ways. 802.1X encompasses a range of EAP authentication methods, such as: MD5, TLS, TTLS, LEAP, PEAP, SecurID, SIM and AKA. Through the use of EAP, support for a

number of authentication schemes may be added: Kerberos, Smart Cards, Public Key Encryption, One Time Passwords.

A WLAN in infrastructure topology, which includes an 802.1X authentication mechanism, features an access point (authenticator), an authentication server (RADIUS [2] or DIAMETER [3]) and at least one supplicant. When EAP is run over a LAN, EAP packets are encapsulated by EAP over LAN (EAPOL) messages. Usually, the EAPOL messages are transmitted between the supplicant and the access point (authenticator), and the RADIUS or DIAMETER protocol occurs between the access point (the authenticator) and the RADIUS or DIAMETER server. Also, [4] defines RADIUS support for EAP, where the authenticator or access server forwards EAP packets to and from the RADIUS server, encapsulated within EAP-Message attributes; this has the advantage of allowing the authenticator to support any EAP authentication method, without the need for method-specific code, which resides on the RADIUS server.

[5] specifies the Diameter EAP application that carries EAP packets between a Network Access Server (NAS) working as an EAP Authenticator and a back-end authentication server; the Diameter EAP application is based on the Diameter Network Access Server Application.

When the supplicant tries to connect to the WLAN, it sends a request to the authenticator; the authenticator receives the request and creates a virtual port with the supplicant. Further, the authenticator sends/receives authentication information to/from the authentication server. In the case of supplicant's acceptance, the authenticator changes the virtual port with the supplicant to an authorized state allowing network access to that supplicant. If there takes place mutual authentication, then supplicant has to check the authentication server's credentials.

X.509 Certificates

X.509-based PKI provides a strong authentication mechanism. The core of X.509 describes standard formats for public key certificates and a certificate path validation algorithm [10]. The X.509 specifications define a framework for obtaining and trusting privilege attributes of an entity in order to determine whether or not they are authorized to access a particular resource.

X.509 certificates can be used to authenticate communication peers and protect messages inside the company's network. PKI using X.509 certificates establishes a common basis of trust, with the requirement of safeguarding the private key associated with the X.509 certificate.

Providing strong verification between two applications, the X.509 architecture does not rely on data encryption; therefore, the specific separation of authentication from confidentiality offers advantages in terms of performance and availability for applications that requires only authentication, but do not require confidentiality.

Combining IEEE 802.1X with X.509 Certificates

[6] suggests a solution based on 802.1X and X.509 certificates for ad-hoc wireless networks, with a CA server under RADIUS server. For a WLAN infrastructure and/or ad-hoc mode, the our proposed prototype includes a CA server and DIAMETER protocol instead of RADIUS server. In some cases, DIAMETER offers more secure

authentication, authorization and accounting (AAA) than RADIUS. In fact, DIAMETER is an enhanced version of the RADIUS protocol and its security is provided by IPSEC or TLS. The DIAMETER base protocol provides important facilities such as error handling, message delivery reliability, handling of user sessions and accounting.

The authentication mechanism relies on EAP-TLS protocol, which is not a password-based authentication method, but it is a certificate-based authentication model. Thus, both server (DIAMETER) and client (supplicant) applies for X.509 certificates. For the case of more CA servers, users obtain all CA certitifcates, after these CA servers mutually authenticate each other [6], [11].

Conclusions

This paper proposes a WLAN authentication mechanism based on DIAMETER proocol. The X.509 certificates issued by a CA server in a public key infrastructure (PKI) are used to verify the credentials of comunnication peers. Moreover, in the context of IEEE 802.1X authentication framework, strong mutual authentication is achieved using EAP-TLS. Future work will concentrate on comparing the performance of different EAP methods both for infrastructure mode and ad-hoc mode.

REFERENCES:

[1] Aboba B., Blunk L., Vollbrecht J., Carlson J., Levkowetz H., "Extensible Authentication Protocol (EAP)", Request for Comments: 3748, Network Working Group, 2004
[2] Rigney C., Willens S., Rubens A., Simpson W., "Remote Authentication Dial In User Service (RADIUS)", Request for Comments: 2865, Network Working Group, 2000
[3] Calhoun P., Loughney J., Guttman E., Zorn G., Arko J., "Diameter Base Protocol", Request for Comments: 3588, Network Working Group, 2003
[4] Aboba B., Calhoun P., "RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)", Request for Comments: 3579, Network Working Group, 2003
[5] Eronen P., Hiller T., Zorn G., "Diameter Extensible Authentication Protocol (EAP) Application", Request for Comments: 4072, Network Working Group, 2005
[6] Chia Hsing Tung, Yi Quan Chen, Zhi Mou Chen, and Shuoh Ren Tsai, "Implementation of Security Mechanism for Adhoc Wireless Networks Based on X.509 and IEEE 802.1X", Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing - Volume 01, 2006, pages: 562 - 563
[7] Shunman Wang, Ran Tao, Yue Wang, and Ji Zang, "WLAN and it's security problems", Proceedings of the Fourth International Conference on Parallel and Distributed Computing, Applications and Technologies, 2003, pages: 241 - 244
[8] Public-Key Infrastructure (X.509) (pkix) Charter, www.ietf.org/html.charters/pkix-charter.html
[9] IEEE Std 802.1X-2004, 802.1X - IEEE Standard for Local and metropolitan area networks - Port-Based Network Access Control, http://www.ieee802.org/1/pages/802.1x.html

[10] ITU-T Recommendation X.509, X.509 (08/2005), Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks http://www.itu.int/rec/T-REC-X.509/en
[11] Zengwei Lan, Han Zhen, Changxiang Shen, "Hierarchy-distribution combined PKI trust model", Proceedings of the IEEE Region 10 Conference on Computers, Communications, Control and Power Engineering, 2002, Volume 1, pages: 121 - 124