available at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

OSNP: Secure wireless authentication protocol using one-time key

Y.L. Huang[a,*], P.H. Lu[a], J.D. Tygar[b], A.D. Joseph[b]

[a]Dept. of Electrical & Control Eng., National Chiao-Tung Univ., Hsinchu, Taiwan
[b]Dept. of Electrical Eng. & Computer Sciences, Univ. of California, Berkeley, USA

ARTICLE INFO

Article history:
Received 8 March 2009
Received in revised form
26 April 2009
Accepted 15 May 2009

Keywords:
802.11 WLAN security
Handover security
Handover authentication
Mutual authentication
Inter-domain authentication
EAP-based protocol
SWOON experiments

ABSTRACT

Handover security and efficiency have become more and more important in modern wireless network designs. In this paper, we propose a new protocol using the one-time key for user authentication. The proposed protocol can support both intra-domain and inter-domain authentications efficiently. Our protocol requires five messages for intra-domain initial authentication; three for subsequent authentication; and five for handover authentication. No authentication server is needed during handover, and our design reduces the computing load on the authentication server. We show an integration and implementation of EAP from 802.1X and our protocol, giving an easy way to apply our protocol on existing 802.11 wireless networks. The proposed protocol is realized and verified on the SWOON secure wireless testbed.

1. Introduction

To enhance the security in wireless networks, IEEE 802.11i (Ieee, 2003) defines a new security model for 802.11 a/b/g networks, specified new standards for authentication, encryption and message integrity, and implemented 802.1X (Ieee, 2001) for user authentication and key distribution. 802.1X is a port-based network access control mechanism that provides an extensible authentication protocol (EAP) (Aboba et al., 2004) and can be used in conjunction with other popular authentication protocols, such as TLS, PEAP, CHAP, etc.

There are many EAP methods supporting 802.11i authentication, including EAP-TLS (Ppp Eap, 1999), EAP-FAST (The Flexible Authentication, 2007), and LEAP (Macnally, 2001). EAP-TLS and EAP-FAST are used with public-key cryptography for authentication. Compared to symmetric-key systems, public-key systems and certificates ensure stronger security, but require more computational power. LEAP, a symmetric-key authentication protocol, requires less computational power and thus takes less response time when performing user authentication. However, LEAP is vulnerable to several attacks (Baek et al., 2004) such as weak encryption keys. To balance the efficiency and security, an efficient authentication is required for wireless networks, especially for roaming users.

In 2007, Zrelli et al. (Zrelli and Shinoda, 2007) presented an integration of the Kerberos protocol with EAP framework, called EAP-Kerberos. Kerberos (Neuman et al., 2005) is well known for its symmetric-key cryptography, strong per-person key and inter-domain authentication. However, it is still

* *Corresponding author*. Tel.: +886 3 5131476; fax: +886 3 5715998.
E-mail addresses: ylhuang@cn.nctu.edu.tw (Y.L. Huang), watil.eceforever@gmail.com (P.H. Lu), doug.tygar@gmail.com (J.D. Tygar), adj@eecs.berkeley.edu (A.D. Joseph).
0167-4048/$ – see front matter © 2009 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2009.05.009

inefficient in the WLAN environment because users need to use proxies to get tickets from the Kerberos Key Distributed Center (KDC). In other words, in Kerberos, KDC is involved in the handover of a roaming user.

In this paper, we propose a handover authentication protocol for WiFi (802.11) networks. Our protocol does not require a public key infrastructure and can be integrated with the 802.1X (Ieee, 2001) Extensible Authentication Protocol (EAP) (Aboba et al., 2004). The novel contributions of this paper are:

- We propose an efficient authentication protocol supporting handover authentication without a trusted of third-party.
- We integrate the proposed protocol with the EAP framework so that it can be applied to wireless network authentication with only minor efforts.
- We implement the proposed protocol and verify it using the SWOON testbed, a secure wireless network emulation testbed. We also compare it with other EAP methods in terms of communication, computation and storage costs.

The rest of this paper is organized as follows. Related research is detailed in Section 2. We present our authentication protocol and the integration with EAP in Sections 3 and 4, respectively. Section 5 compares our system to others, and Section 6 concludes the paper. In the Appendix, we use BAN logic (Burrows et al., 1989) and a possible enhancement (Shieh et al., 1999) to formally prove that our protocol can reach the goals of mutual authentication.

2. Related work

2.1. *Network authentication protocols*

This section summarizes the characteristics and drawbacks of some related authentication protocols.

- Kerberos

  Kerberos (Neuman et al., 2005) was developed as a solution to network security problems, such as replaying, eavesdropping and sniffing packets. In Kerberos V5, six messages are required for initial intra-domain authentication. The number of message required for inter-domain authentication depends on the number of KDCs between the visited and home domains.

- One-Time Password/Kerberos

  Since the traditional password authentication is vulnerable to dictionary and playback attacks, in 2005, Cheng et al. (Xiao-rong et al., 2005) presented a new authentication method that integrates the Kerberos protocol and a one-time password (OTP) system. The main idea of OTP authentication is to add random factors during the initial login process and make the password used vary from time to time. Similar to the Kerberos protocol, the OTP/Kerberos protocol requires three steps to authenticate a user: authentication by the KDC, request of tickets from the Ticket-Granting Server (TGS) and access to the server (S). On the client, the OTP is generated by hashing the user's secret passphrase and the seed from the KDC. By encrypting and decrypting messages with the OTP, the user and server mutually authenticate each other. However, to generate an OTP for authentication requires seven messages in the first step mentioned above. In other words, OTP/Kerberos increases the communication cost for authenticating a user, resulting in longer user authentication times, which is not practical for roaming users in wireless networks.

- Secure Authentication Protocols

  In the last decade, many secure authentication protocols (Shieh et al., 1999; Chien, 2003; Liang and Wang, 2004; Hwang, 2005) were proposed to solve the issues of Kerberos. Among these protocols, Secure Network Protocol (SNP) (Shieh et al., 1999) is one of the few protocols that has real deployment for years. SNP is a symmetric-key based protocol providing an efficient way for both intra- and inter-domain authentication. Compared to Kerberos, fewer messages are required in SNP to authenticate client identity. For intra-domain authentication, SNP takes four messages to authenticate client identity and one more optional message for mutually authenticating the server. For inter-domain authentication, it takes seven messages for initial authentication, regardless of the number of hops between the visited and home domains. Only two messages are required for subsequent authentication when requesting the same service. To simplify the design, SNP replaces timestamps with nonces, reducing the need for time servers. For faster authentication, a master key is shared by the authentication server (AS) and the service servers (S). The unchanged master keys can make the system vulnerable to various attacks.

2.2. *EAP-based authentication protocols*

EAP is an authentication framework used in various networks, such as wireless LANs and Point-to-Point connections (PPP). EAP provides some common functions and a negotiation of the desired authentication methods, such as EAP-MD5, EAP-OTP, EAP-TLS, etc. In wireless LANs, EAP authentication methods are normally supported with Remote Authentication Dial-In User Service (RADIUS) (Remote Authentication Dial, 2000). RADIUS is also a client/server protocol that enables remote access servers to communicate with a centralized authentication server to authenticate dial-in users. It also authorizes their access to the requested services. The RADIUS server supporting various EAP methods then becomes the major authority of wireless networks. This section summarizes EAP authentication methods supporting strong authentication for roaming users in wireless LANs.

- EAP-TLS

  EAP-TLS (Ppp Eap, 1999) is a popular EAP method for securing wireless LANs with RADIUS. The mobile node and RADIUS server must have certificates to mutually authenticate each other. EAP-TLS is resilient to man-in-the-middle attacks. However, it requires a trusted-third party (Certificate Authority) to support authentication between the