Chapter XLIX
Extensible Authentication (EAP) Protocol Integrations in the Next Generation Cellular Networks

Sasan Adibi
University of Waterloo, Canada

Gordon B. Agnew
University of Waterloo, Canada

ABSTRACT

Authentication is an important part of the authentication authorization and accounting (AAA) schemes and the extensible authentication protocol (EAP) is a universally accepted framework for authentication commonly used in wireless networks and point-to-point protocol (PPP) connections. The main focus of this chapter is the technical details to examine how EAP is integrated into the architecture of next generation networks (NGN), such as in worldwide interoperability for microwave access (WiMAX), which is defined in the IEEE 802.16d and IEEE 802.16e standards and in current wireless protocols, such as IEEE 802.11i. This focus includes an overview of the integration of EAP with IEEE 802.1x, remote authentication dial in user service (RADIUS), DIAMETER, and pair-wise master key version (2PKv2).

INTRODUCTION

Extensible authentication protocol (EAP) is a universally accepted authentication mechanism, frequently used in different wireless technologies. Although the applications of EAP protocol are not limited to wireless local area networks (LANs), they could be used for authentication in wired-based LAN applications. However EAP is most often used in wireless LANs. The integrations of EAP and other security protocols and mechanisms often result in strong security frameworks.

These integrations are often established with other security protocols and mechanisms, such as transport layer security (EAP-TLS), message digest 5 (EAP-MD5), privacy key management (PKM-EAP), and so forth.

The organization of the sections of this chapter is as follows: Section II will discuss details about the EAP-IEEE 802.1x interactions. Section III is dedicated to remote authentication dial in user service (RADIUS) and DIAMETER in the authentication/authorization schemes. Section IV talks about the IEEE 802.1x-EAP functions implemented in Wi-Fi (IEEE 802.11i) and introductions to EAP-MD5, lightweight extensible authentication protocol (LEAP), EAP-TLS (TTLS) and protected extensible authentication protocol (PEAP). Section V presents the PKMv2-EAP scheme in worldwide interoperability for microwave access (WiMAX) (IEEE 802.16) followed by section VI, which is a configured testbed for a WiMAX system. Sections VII and VIII contains conclusions and references respectively.

EAP AND IEEE 802.1X

Based on RFC 3748 (Aboba, Blunk, Vollbrecht, Carlson, & Levkowetz, 2004), EAP runs on top of IEEE 802.1x (Figure 1), therefore 802.1x is the key issue to understanding the EAP. IEEE 802.1x offers a strong framework for authenticating and controlling user traffic for protecting networks. IEEE 802.1x also offers dynamically varying encryption keys. IEEE 802.1x uses EAP in both wired and wireless LANs and supports multiple authentication methods, such as Kerberos, one-time passwords, and public key certificates. Our main focus is on wireless technologies.

IEEE 802.1x initially starts the communications by an attempt to connect with an authenticator (i.e., an 802.16 or 802.11 access point [AP]) to authenticate an unauthenticated supplicant. The AP responds back by enabling a port for passing only EAP packets between the clients to the authentication server, which is usually located on the wired side of the AP. The AP blocks all other traffic (i.e., HTTP and dynamic host configuration protocol [DHCP] packets), until the AP (authenticator) is able to verify the client's identity using an authentication server (e.g., DIAMETER or RADIUS). Once authenticated, the AP opens the client's port for the rest of traffic types.

To better understand how 802.1x operates, the interactions mentioned in Table 1a usually happen between various 802.1x elements.

As showed in Figure 1, EAP is an important component of an 802.1x-based infrastructure. EAP improves the authentication scheme provided by the point-to-point protocol (PPP) (RFC 1661). EAP provides PPP with a generalized framework for

Figure 1. 802.1x authentication components (Adapted from Kwan, 2003)

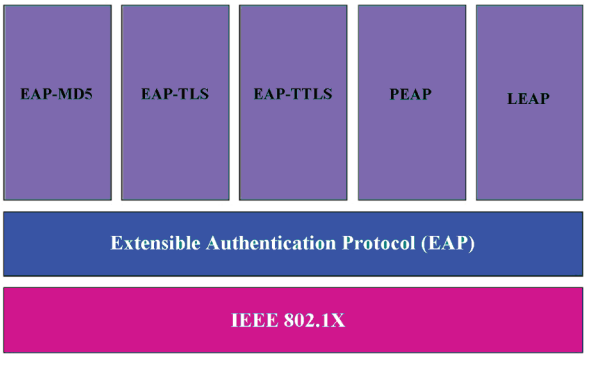

Figure 2. Different layers of 802.1x (Adapted from Leira, 2005)