Chapter 7.8
Security Architectures for B3G Mobile Networks

Christoforos Ntantogian
University of Athens, Greece

Christos Xenakis
University of Piraeus, Greece

ABSTRACT

The integration of heterogeneous mobile/wireless networks using an IP-based core network materializes the beyond third generation (B3G) mobile networks. Along with a variety of new perspectives, the new network model raises new security concerns, mainly, because of the complexity of the deployed architecture and the heterogeneity of the employed technologies. In this chapter, we examine and analyze the security architectures and the related security protocols, which are employed in B3G networks focusing on their functionality and the supported security services. The objectives of these protocols are to protect the involved parties and the data exchanged among them. To achieve these, they employ mechanisms that provide mutual authentication as well as ensure the confidentiality and integrity of the data transferred over the wireless interface and specific parts of the core network. Finally, based on the analysis of the security mechanisms, we present a comparison of them that aims at highlighting the deployment advantages of each one and classifies the latter in terms of: (1) security, (2) mobility, and (3) reliability.

INTRODUCTION

The evolution and successful deployment of wireless LANs (WLANs) worldwide has yielded a demand to integrate them with third generation (3G) mobile networks. The key goal of this integration is to develop heterogeneous mobile data networks, named as beyond 3G (B3G) networks, capable of supporting ubiquitous computing. Currently, the network architecture (3rd Generation Partnership Project [3GPP] TS 23.234, 2006) that integrates 3G and WLAN specifies two different access scenarios: (1) the *WLAN Direct IP Access* and (2) the *WLAN 3GPP IP Access*. The first scenario provides to a user an IP connection to the public Internet or to an intranet via the WLAN access network (WLAN-AN), while the second allows a user to connect to packet switch (PS) based services (such

as wireless application protocol [WAP], mobile multimedia services [MMS], location-based services [LBS] etc.) or to the public Internet, through the 3G public land mobile network (PLMN).

Along with a variety of new perspectives, the new network model (3G-WLAN) raises new security concerns, mainly, because of the complexity of the deployed architecture and the heterogeneity of the employed technologies. In addition, new security vulnerabilities are emerging, which might be exploited by adversaries to perform malicious actions that result in fraud attacks, inappropriate resource management, and loss of revenue. Thus, the proper design and a comprehensive evaluation of the security mechanisms used in the 3G-WLAN network architecture is of vital importance for the effective integration of the different technologies in a secure manner.

In this chapter we examine and analyze the security architectures and the related security protocols, which are employed in B3G, focusing on their functionality and the supported security services for both WLAN Direct IP Access and 3GPP IP Access scenarios. Each access scenario (i.e., WLAN Direct Access and WLAN 3GPP IP Access) in B3G networks incorporates a specific security architecture, which aims at protecting the involved parties (i.e., the mobile users, the WLAN, and the 3G network) and the data exchanged among them. We elaborate on the various security protocols of the B3G security architectures that provide mutual authentication (i.e., user and network authentication) as well as confidentiality and integrity services to the data transferred over the air interface of the deployed WLANs and specific parts of the core network. Finally, based on the analysis of the two access scenarios and the security architecture that each one employs, we present a comparison of them. This comparison aims at highlighting the deployment advantages of each scenario and classifying them in terms of: (1) security, (2) mobility, and (3) reliability.

The rest of this chapter is organized as follows. The next section outlines the B3G network architectures and presents the WLAN Direct IP Access and the 3GPP IP Access scenarios. The third section elaborates on the B3G security architectures analyzing the related security protocols for each scenario. The fourth section compares the security architectures and consequently, the two access scenarios. Finally, the fifth section contains the conclusions.

BACKGROUND

The B3G Network Architecture

As shown in Figure 1, the B3G network architecture includes three individual networks: (I) the WLAN-AN, (II) the visited 3G PLMN, and (III) the home 3G PLMN. Note that Figure 1 illustrates the architecture for a general case where the WLAN is not directly connected to the user's home 3G PLMN. The WLAN-AN includes the wireless access points (APs), the network access servers (NAS), the authentication, authorization, accounting (AAA) proxy (Laat, Gross, Gommans, Vollbrecht, & Spence, 2000), and the WLAN-access gateway (WLAN-AG). The wireless APs provide connectivity to mobile users and act like AAA clients, which communicate with an AAA proxy via the Diameter (Calhoun, Loughney, Guttman, Zorn, & Arkko, 2003) or the Radius (Rigney, Rubens, Simpson, & Willens, 1997) protocol to convey user subscription and authentication information. The AAA proxy relays AAA information between the WLAN and the home 3G PLMN. The NAS allows only legitimate users to have access to the public Internet, and finally, the WLAN-AG is a gateway to 3G PLMN networks. It is assumed that WLAN is based on the IEEE 802.11 standard (IEEE std 802.11, 1999).

On the other hand, the visited 3G PLMN includes an AAA proxy that forwards AAA information to the AAA server (located in the home 3G PLMN), and a wireless access gateway (WAG), which is a data gateway that routes users' data to