Chapter XII
Architecture and Protocols for Authentication, Authorization, and Accounting in the Future Wireless Communications Networks

Said Zaghloul
Technical University Carolo-Wilhelmina – Braunschweig, Germany

Admela Jukan
Technical University Carolo-Wilhelmina – Braunschweig, Germany

ABSTRACT

The architecture, and protocols for authentication, authorization, and accounting (AAA) are one of the most important design considerations in third generation (3G)/fourth generation (4G) telecommunication networks. Many advances have been made to exploit the benefits of the current systems based on the protocol remote authentication dial in user service (RADIUS)protocol, and the evolution to migrate into the more secure, robust, and scalable protocol Diameter. Diameter is the protocol of choice for the IP multimedia subsystem (IMS) architecture, the core technology for the next generation networks. It is envisioned that Diameter will be widely used in various wired and wireless systems to facilitate robust and seamless AAA. In this chapter, we provide an overview of the major AAA protocols RADIUS and Diameter, and we discuss their roles in practical 1xEV-DO network architectures in the three major network tiers: access, distribution, and core. We conclude the chapter with a short summary of the current and future trends related to the Diameter-based AAA systems.

INTRODUCTION

Many 3G cellular providers consider the architecture for the authentication, authorization, and accounting (AAA) system as one of the most important functional blocks for the success of service delivery. Typically, users are authenticated when requesting a service and only after successful authentication they are authorized to use the service. Once the user is granted access to the service, the network generates accounting messages based on the user's activity. Currently, the remote authentication dial in user service (RADIUS) protocol is the most widely deployed protocol in cellular networks to perform subscriber AAA. Since RADIUS is susceptible to various security threats, a standard developed by the Internet Engineering Task Force (IETF), called Diameter, was proposed to substitute RADIUS in the future. Unlike its predecessor RADIUS, Diameter offers reliable and secure communication enabling seamless roaming among operators and support of auditability, capability negotiation, and peer discovery and configuration. Diameter augments its reliable transmission capabilities by defining failover mechanisms and thus embraces two crucial elements for the robust communication of sensitive billing and authentication messages. Since most of the current equipment and radio standards only support RADIUS for authentication, it is evident that cellular network operators will be running both protocols in the near future. Therefore, it can not be sufficiently emphasized that prudent decisions need to be made when designing AAA systems with multiple protocols in mind at the three major tiers: access, distribution, and core.

The purpose of this chapter is to address the specific aspects of the AAA system architecture of these three major tiers. Given the broadness of the scope and the myriad of the existing AAA standards, we sharpen our focus on a reference 3G cellular network architecture which we define and show in Figure 1. As can be seen from Figure 1, a typical AAA system in 3G architectures is characterized by three distinctive architectural elements: (1) radio access network (RAN), (2) distribution network based on mobile IP (MIP), and (3) a multimedia domain (MMD)[1] based core including both IP multimedia system (IMS) networks and Internet access deployments. The RAN, based on one of the 1x carrier evolution data only (1xEV-DO) standards/revisions for wireless transmission, consists of various base stations (BSs) and radio network controllers (RNCs). The distribution network consists of the MIP elements, that is, the packet data serving node (PDSN) playing the foreign agent's (FA) role and the home agent (HA). It is worth observing that this architecture has a hierarchical nature, where multiple BTSs are governed by a single RNC and multiple RNCs are covered by a single PDSN region. Finally, at the core, we have the IMS elements, including it standardized elements such as the call session control functions (CSCF) and home subscriber servers (HSS) enabling robust applications and services such as gaming, presence, voice over IP (VoIP), and so forth.

Upon receiving a mobile subscriber call, the RNC authenticates the subscriber's request by communicating with the access network AAA (AN-AAA) over the RADIUS-based A12 interface. Once authenticated, the RNC contacts the PDSNs through the A10/A11 interface (3rd Generation Partnership Project 2 [3GPP2] A.S0008-B, 2006). Note that since the A12 interface is RADIUS based, a translation agent (TA) needs to be used to translate the RADIUS requests to Diameter for authentication. In Figure 1, we illustrate that the AAA contacts an Oracle-based users' database to authenticate the incoming calls. We assume that the TA, AAA, and the AN-AAA are collocated in the same physical platform for simplicity. For higher reliability, RNCs usually connect to multiple AAAs (one primary and another secondary AAAs) to allow redundancy to admit users into the system in case of AN-AAA connectivity problems.

Once admitted, the mobile node (MN) starts a point-to-point (PPP) session with the PDSN. During the process of PPP establishment, the PDSN advertises itself as a MobileIP FA and challenges the user. The user then replies with a Mobile IP registration request that answers the PDSN's challenge. The PDSN forwards this information to the AAA. The AAA validates the user's response