Chapter XIII
Authentication, Authorisation, and Access Control in Mobile Systems

Josef Noll
University Graduate Center – UniK, Norway

György Kálmán
University Graduate Center – UniK, Norway

ABSTRACT

Converging networks and mobility raise new challenges towards the existing authentication, authorisation, and accounting (AAA) systems. Focus of the research is towards integrated solutions for seamless service access of mobile users. Interworking issues between mobile and wireless networks are the basis for detailed research on handover delay, multi-device roaming, mobile networks, security, ease-of-use, and anonymity of the user. This chapter provides an overview over the state of the art in authentication for mobile systems and suggests extending AAA mechanisms to home and community networks, taking into account security and privacy of the users.

INTRODUCTION

Today's pervasive computing environments raise new challenges against mobile services. In future visions, a converged user access network is projected. This means, that one network will be used to deliver different services, for example, broadcast TV, telephony, and Internet. Composed from mobile (e.g., Universal Mobile Telecommunications System [UMTS]), wireless (IEEE 802.11, IEEE 802.16, IEEE 802.20), and wired (cable, Asymmetric Digital Subscriber Line [ADSL]), these networks hide the border between the telecom, broadcast, and computer networks. The common service enables roaming terminals, which can access services independently of the currently used networking technology. Market players in both areas transform into wireless service providers across access networks. Telecom provide packet switched data and mobile services over the fixed network, while Internet service providers run voice over IP (VoIP) and video on demand (VoD) over mobile networks.

The changing environment also changes the management plane of the underlying networks. Providers on converged networks have to change their accounting and billing methods and need to redefine their business models. While commercial

players demonstrate early examples, research in the AAA area focuses on providing a backplane for the upcoming ubiquitous services run over converged networks.

BACKGROUND

The AAA methods employed in current networks were developed for a single type of network, resulting in two different systems, one for telecommunication services and one for computer networks. This chapter addresses AAA in global system for mobil communications (GSM) and UMTS and computer network solutions based on Internet Engineering Task Force (IETF) standards.

The computer networks provide a unified AAA access, and research focuses on extending the existing methods to be suitable for telecommunication services. Extensions for Remote Authentication Dial In User Service (RADIUS) and Diameter are proposed. RADIUS is the current de facto standard for remote user authentication. It uses Universal Datagram Protocol (UDP) as transport. Authentication requests are protected by a shared secret between the server and the client, and the client uses hash values calculated from this secret. The requests are sent in plaintext except for the user password attribute. The Diameter protocol provides an upgrade possibility as compared to RADIUS. While enhancing the security through supervised packet transmission using the transmission control protocol (TCP) and transport layer encryption for reducing man-in-the-middle attacks, it lacks backward compatibility.

Both methods have a different background. The computer networks targeted the person using a computer in a fixed network environment, while mobile systems addressed a personal device in a mobile network. Thus a challenge for telcos is to enhance seamless network authentication towards user authentication for service access. Most companies are also Internet service providers (ISPs), this would be a natural unification of their AAA systems.

A generic approach is taken by extension of the Extensible Authentication Protocol (EAP) family. Development efforts of the Internet and telecommunication world were united on EAP. This protocol family has the potential for becoming the future common platform for user authentication over converged networks. EAP is a universal authentication framework standardised by IETF, which includes the authentication and key agreement (AKA) and Subscriber Identity Module (SIM) methods. EAP-AKA is the standard authentication method of UMTS networks.

Beside the fundamental differences of communication and computer networks, mobility is the key issue for both. Network services should not only be accessible from mobile terminals, but they should be adapted to the quality of service (QoS) requirements of a mobile/wireless link. Improvements of AAA methods are of fundamental importance for mobility, providing fast handover, reliable and secure communications on a user-friendly and privacy protecting basis.

Subscriber Authentication in Current Networks

In GSM networks, the integrated AAA is used for any type of user traffic. The authentication is just one way the user has to authenticate himself/herself towards the network.

To be more precise, the user is authenticated with a PIN code towards the SIM in the mobile phone, then the device authenticates itself towards the network. Device authentication instead of user authentication can hinder the upcoming personalised services because it is hiding the user behind the device. In UMTS, the authentication of the device is two-way. A device can also check the authenticity of the network with the help of keys stored on the SIM.

Integration of the mobile authentication with different external services is not widespread. The telecom providers have some internal services, which can authenticate the subscriber based on the data coming from the network. Credentials could be basically the CallerID, the Temporary International Mobile Subscriber Identity (TIMSI) or other data transformed with a hash function. Access control and authorisation is more an internal