Digital Identity in Current Networks

Kumbesan Sandrasegaran
University of Technology, Sydney, Australia

Xiaoan Huang
University of Technology, Sydney, Australia

INTRODUCTION

The daily activities of humans and business are increasingly depending on the usage of (digital) identity for interaction with other parties and for accessing resources. Current networks use a number of digital-identity management schemes. For example, in the public switched telephone network (PSTN), a telephone number is simply used as the digital identity of a user. Most of the digital-identity management schemes are effective only within their networks and have limited support for interoperability. In the hybrid network environment of next-generation networks (NGNs), new digital-identity management models are expected to be proposed for digital-identity management.

The rest of the chapter is focused on the introduction of digital identity, the digital-identity schemes used in current telecommunication networks, and the future trends.

BACKGROUND

What is Digital Identity?

We define the identity of an individual as the set of information known about that person. With the development and widespread use of digital technologies, humans have been able to communicate with each other without being physically present. Digital identity is the means that an entity (another human or machine) can use to identify a user in a digital world. The aim of digital identity is to create the same level of confidence and trust that a face-to-face transaction would generate. Some selected definitions for digital identity are as follows.

Digital ID World ("What is Digital Identity?" 2003):

"A Digital Identity is the representation of a human identity that is used in a distributed network interaction with other machines or people. The purpose of the Digital Identity is to restore the ease and security human transactions once had, when we all knew each other and did business face-to-face, to a machine environment where we are often meeting each other for the first time as we enter into transactions over vast distances."

Field Elliot (2002)

"A Digital Identity is an assurance by one end of a digital conversation (such as a Web Services transaction) that the other end of the conversation is being conducted on behalf of a specific human, company, or other entity."

Composition of Digital Identity

Digital identity is comprised of two basic elements: the actual identity of the entity (something that can be observed by human senses), and the credentials or what are used to prove the identities. Credentials can take the following forms (Reed, 2002).

- **Something that the entity knows:** An example is a password or any piece of knowledge that the entity knows.
- **Something the entity has or possesses:** An example would be a magnetic swipe card used for entry into a room, elevator, or so forth.
- **Something the entity is:** Examples of parts of an entity include fingerprints and eye scans. These attributes are the most difficult to copy or impersonate.

Profile

A profile consists of data needed to provide services to a user once his or her identity has been verified. A user profile could include what an entity can do, what he or she has subscribed to, and so on. Profiles are important to digital identity as they represent records and other data about users that can be stored external to the actual entity itself.

Usage of Digital Identity

Authentication

One of the important uses of digital identity is authentication, where an entity must prove digitally that it is the entity that it claims to be ("What is Digital Identity?" 2003). It is at this stage that the credentials of digital identity are used.

The simplest form of authentication is the use of a user name and a corresponding password.

Authorisation

Once an entity is authenticated, a digital identity is used to determine what that entity can do. This is where the profile of a digital identity is required. For example, while both an administrator and a user are authenticated to use a computer, the actions that each may do with that resource are determined by the authorisation.

Accounting

Accounting involves the recording and logging of entities and their activities within the context of a particular organisation, Web site, and so forth. Effective accounting processes enable an organisation to track unauthorised access when it does occur.

DIGITAL IDENTITY IN CURRENT NETWORKS

Digital Identity in Mobile Networks

One of the evolution paths of mobile networks is from the global system for mobile communications (GSM) to general packet radio service (GPRS), and to the universal mobile telecommunication system (UMTS). Figure 1 shows the architectures of the GSM, GPRS, and UMTS networks. In GSM/GPRS, users connect to the mobile core networks via the base-station subsystem. The mobile switching centre (MSC) and visitor location register (VLR) in the core network are the main entities used for the CS domain. The serving GPRS support node (SGSN) and gateway GPRS support node (GGSN) are the main entities used for the PS domain. In UMTS, the new radio network controller (RNC) takes charge of connecting users with the SGSN or MSC and VLR. A number of RNCs form the UMTS terrestrial radio access network (UTRAN).

Digital-Identity Composition in Mobile Networks

There are three broad aspects of digital-identity composition in mobile networks.

Identity and Communication Management

In identity and communication management, each subscriber has to be uniquely identified. The unique addressing codes are described below (Kaaranen, 2001).

- **International Mobile Subscriber Identity (IMSI)**
  It is a unique and confidential identity for the mobile subscriber (MS) and is the same in GSM, GPRS, and UMTS. The structure of IMSI is shown below (Pandya, 1997):

  IMSI = MCC + MNC + MSIN,

  where
  MCC = mobile country code (3 digits),
  MNC = mobile network code (2 digits),
  and
  MSIN = mobile subscriber identity number (normally 10 digits).
- **Mobile Subscriber International ISDN (Integrated Services Digital Network) Number (MSISDN)**
  The MSISDN is used for service separation. A subscriber may have several services provisioned and

Figure 1. GSM, GPRS, and UMTS network architectures (Lin & Chlamtac, 2001)