Chapter XVIII
Security in 4G

Artur Hecker
Ecole Nationale Supérieure des Télécommunications (ENST), France

Mohamad Badra
National Center for Scientific Research, France

ABSTRACT

The fourth generation (4G) of mobile networks will be a technology-opportunistic and user-centric system combining the economic and technological advantages of different transmission technologies to provide a context-aware and adaptive service access anywhere and at any time. Security turns out to be one of the major problems that arise at different interfaces when trying to realize such a heterogeneous system by integrating the existing wireless and mobile systems. Indeed, current wireless systems use very different and difficult to combine proprietary security mechanisms, typically relying on the associated user and infrastructure management means. It is generally impossible to apply a security policy to a system consisting of different heterogeneous subsystems. In this chapter, we first briefly present the security of candidate 4G access systems, such as 2/3G, wireless LAN (WLAN), WiMax, and so forth. In the next step, we discuss the arising security issues of the system interconnection. We namely define a logical access problem in heterogeneous systems and show that both the technology-bound, low-layer and the overlaid high-layer access architectures exhibit clear shortcomings. We present and discuss several proposed approaches aimed at achieving an adaptive, scalable, rapid, easy-to-manage, and secure 4G service access independently of the used operator and infrastructure. We then define general requirements on candidate systems to support such 4G security.

GENERATIONS OF PUBLIC LAND MOBILE NETWORKS

From 1G to 2G

The first generation of public land mobile networks (PLMN) is characterized by the fact that both control channels and traffic channels are analog. Voice (commonly at 3 kHz) and data (if any) are frequency-modulated on a carrier. Today, these networks are usually summarized under the common name first generation (1G) although there are different analog network standards like Nordic mobile telephony (NMT), American mobile phone system AMPS), and total access communication system (TACS).

NMT was the first commercially operated PLMN (1981). NMT uses two different frequency bands about 450 and about 900 MHz (NMT 450 and NMT 900). NMT900 was introduced in 1986 as a result of the fact that the number of channels in NMT 450 was insufficient. NMT 900 has been implemented in Europe, the Middle East, and Asia.

AMPS was specified by the U.S. consortium TIA/EIA/ANSI. The first AMPS network became operational in 1984. In 1988, an extension providing additional frequency bands was added (E-AMPS). AMPS networks are found in the Americas, Australia, and in Asia.

TACS is a modification of AMPS aiming at the British market, where the standard was operational in 1985. TACS also received a wider frequency band in 1988, E-TACS. Since that time, TACS has spread to many countries around the world.

In 1982, at the time of the commercialization of the first 1G networks, the Groupe Spécial Mobile was formed at CEPT (*Conférence européenne des Administrations des Postes et des Tèlécommunications*, the creator and standard-body predecessor of today's *European Telecommunications Standard Institute, ETSI*), with the task of developing a Europe-wide standard for cellular communication. In other words, the scope here was to provide the same service (voice) by a new, universal system.

In 1987 the CEPT working group decided to build a digital, narrowband time division multiple access (TDMA) system. In 1990, ETSI published Phase I of the GSM system specifications. Three frequency bands have been defined for global system for mobile communications (GSM) usage: 900MHz, 1800 MHz, and 1900 MHz. The corresponding standards are similar, aiming at

Table 1. Ten years cycles in the mobile networks (from a European view)

Year	Milestone	Cycles		
1981	*Commercial deployment of NMT:* ***1G start***	1G to 2G: 10 years		
1982	Creation of Groupe Spécial Mobile at CEPT			
1984	Commercial deployment of AMPS networks in the US			
1986	Big number of users leads to NMT extensions			
1988	Big number of users leads to AMPS extensions			
1989	European Union RACE Project "invents" UMTS		3G conception: 10 years	
1992	World Administrative Radio Conference (today: WRC) allocates 230 MHz to Future Public Land Mobile Telecommunication System (FPLMTS).			
1992	*Commercial deployment of GSM:* ***2G start***			2G to 3G: 10 years
1994	Second wave of UMTS research projects			
1995	RACE vision of UMTS			
1996	Creation of UMTS task force			
1996	*Digital overcomes analog*			
1997	Establishment of the UMTS Forum			
1999	UMTS decision			
2000	WRC designates IMT-2000 extension bands			
2002	*Commercial deployment of UMTS:* ***3G start***			