1. Final Title

SECURITY of MOBILE COMMUNICATIONS

By Noureddine Boudriga

Professor at the University of Carthage, Tunisia

2. Summary

Mobile communications offer wireless connectivity that enables mobility and computing in many different communication environments. The huge demands from social markets are driving the growing development of mobile communications more rapidly than ever before. Consequently, a large set of new advanced techniques have emerged brought up by a larger bandwidth, more powerful processing capability, and advances in computing technology. Many new services are provided, or will be provided to potential users, and delivered with high level quality by the usage of GSM, 3G networks and wireless mesh networks in public, home, and corporate scenarios.

The exceptional growth in mobile and wireless communications gives rise to serious problems of security at the level of the subscriber, network operator, and service provider. The causes of such rise, typically due to the fragility of the wireless link nature, the mobility features, and the variety of the provided services, can be classified into the following six categories: a) the physical weaknesses and limitations of mobile and communications; b) the architecture limitations; c) the user requirements; d) the contents of provided services; and e) the evolution of hacking techniques.

Many studies have addressed carefully the mobile subscriber authentication, radio-path encryption, and secure mobility, but the so-called "*security of mobile communications*" does no involve only these relative independent domains. It indeed needs a more systematic approach to build up a framework layout capable of allowing: 1) the risk analysis of threats and vulnerabilities of a mobile communication system; 2) the assessment of a mobile communication systems in terms of provided security; 3) the protection of a service provided via mobile communication systems; and 4) the engineering and management of mobile communication security.

Five major goals are considered in this tutorial: 1) analyzing and discussing the security proposals made available by the mobile communications systems; 2) highlighting the importance of security attacks and hacking techniques; 3) discussing security policies and security practices to help better addressing the security problems and limits; 4) discussing the role the network operator, the service provider, and customer in the securing mobile communications; and 5) analyzing the promises, requirements, and limits of service provision in terms of security needs.

3. Outline of Topics

The Tutorial contains four major parts:

The first part discusses the main foundations of the techniques used for hacking systems via mobile communications. Threats and risk analysis are discussed in this part, along with the major techniques used to provide access control, authentication, and authorization in mobile communications.

The second part discusses and analysis the mechanisms and standards implemented by the GSM, third generation, mesh networks. These networks constitute the major components of what should be called wireless open architecture. The protection mechanisms involved in these networks are assessed. The security of SIM-like cards is also addressed.

The third part of this tutorial discusses the security issues related to the provision of services using mobile communications. Particularly, this part contains issues related to the security of wireless sensor networks, mobile e-services, and inter-system roaming.

The forth part analyzes the features of the security provided for applications using IP mobility. A special interest is given the security of mobile payments.

4. Bio of instructor

Noureddine Boudriga

Noureddine A. Boudriga is an internationally known academic, researcher, and scientist,. He received his Ph.D. in Algebraic topology from University Paris XI (France) and his Ph.D. in Computer science from University of Tunis (Tunisia). He is currently a full Professor of Telecommunications at the University of Carthage, Tunisia and the Director of the Communication Networks and Security Research Laboratory (CNAS, University of Carthage). He is the recipient of the Tunisian Presidential award in Science and Research (2004). He has served as the General Director and founder of the Tunisian National Digital Certification Agency (2000-2004). He was involved in very active research in communication networks and system security. He authored or coauthored many chapters and books on information security, security of mobiles networks, and communication networks. He published over 200 refereed journal and conference papers. Prof. Boudriga is currently the President of the Tunisia Scientific telecommunications Society

5. Target audience

Target audience includes:

- Computer science or telecommunications engineers in charge of the protection and management of networked systems within an enterprise.
- Information service providers involved in the development and offer of services through communication networks
- Graduate students preparing a PhD or a Master degree in network communication or information systems.
- Researchers in information security or communication networks and needing to be introduced to the issues of mobiles security.

6. Sample of viewgraphs

A sample will follow very soon