# “Security and IP-Based 3G Wireless Networks”

**Thomas F. La Porta**
**The Pennsylvania State University**

Abstract:

Telecommunication networks are evolving from closed systems with limited, standardized services, to open systems which will allow great creativity in building and deploying new services. These systems will heavily leverage Internet technology in an effort to create this open environment. This evolution is being aggressively pursued by Wireless Service Providers (WSPs). Along with the benefits of these networks come increasingly high risks of a variety of attacks that may compromise security. Current, so called second generation (2G) wireless telecommunication networks are implemented using standardized control protocols for user and device authentication, mobility management, session control and services control. These networks are closed in the sense that control messages are exchanged on a private packet-switched network based on the Signaling System No. 7 standards. Because of their closed nature, there are few successful attacks on these networks. The next, so called third generation (3G) wireless telecommunication networks are migrating towards IP technology, with the ultimate goal being an all-IP network. Standards for these systems, called the IP Multimedia Subsystem (IMS) are being defined by the Third Generation Partnership Projects (3GPP and 3GPP2). These networks will use IP for transport of information, and Internet protocols such as the Session Initiation Protocol (SIP) and Mobile IP, for session control and mobility management. These networks open the possibility for IP-based services and must interwork with 2G networks. Because new services will be introduced in the IP-domain of these networks, new attacks on 3G networks are possible. Because IP networks are more accessible than SS7 networks, the control portion of the 3G networks is now more vulnerable to attack. These attacks may be remote denial of service attacks, or attacks that target the integrity of specific services. The means of the attack may vary depending on the interworking model used and the service being offered. In this talk we discuss the different security risks in IP-based 3G networks, different attack types, and the trade-offs of high performance, open network architectures versus secure network infrastructure.

BIO:

Thomas F. La Porta received his Ph.D. degree in Electrical Engineering from Columbia University, New York, NY. He joined the Computer Science and Engineering Department at Penn State in 2002 as a Full Professor. He is the Director of the Network Research Center at Penn State. Prior to joining Penn State, Dr. La Porta was with Bell Laboratories since 1986. He was the Director of the Mobile Networking Research Department in Bell Laboratories, Lucent Technologies where he led various projects in wireless and mobile networking. He is an IEEE Fellow and Bell Labs Fellow. Dr. La Porta was the founding Editor-in-Chief of the IEEE Transactions on Mobile Computing, and previously served as Editor-in-Chief of IEEE Personal

Communications Magazine. He is the General Co-Chair of ACM Mobicom 2005. His research interests include mobility management, signaling and control for wireless networks, mobile data systems, and protocol design.