"3G Wireless Security- A Government Perspective"
Doug Rahikka, NSA

Abstract -

The National Security Agency (NSA) has been working several years now on developing end-to-end secure voice and data wireless solutions. In the world of 1G analog cellular, the solution was just to transmit the standard STU-III or third generation secure telephone unit 2400 bps wireline voiceband modulated waveform directly through the traditional FM-modulated analog cellular transmission format. Unfortunately, the digitized vocoders present in both 2G and 3G digital cellular systems are designed to compress voice-like signals and are unfriendly to or incompatible with compression of modem signals. Thus, in order to achieve end-to-end voice security in the context of 2G and 3G cellular technologies, the NSA has developed a signaling protocol known as FNBDT or Future Narrow Band Digital Terminal. The FNBDT protocol specifies a minimum essential operation mode which uses the MilStd3005 MELP or Mixed Excitation Linear Prediction vocoder at 2400 bps. The use of MELP for secure voice will ensure end-to-end secure digital interoperability across domains of narrowband satellite channels, moderate bandwidth 2G systems, and future higher bandwidth 3G systems. Indeed, with the advent of '2.5G' (such as GSM GPRS) and 3G systems, bit rates will start to push over 100kbps per user (even up to 1Mbps per user), thus enabling true multimedia applications such as video-conferencing. The solutions that NSA will be developing for 3G systems will maintain a baseline interoperable FNBDT mode so that backwards interoperability will be possible with 2G systems that will still be prevalent and coexisting during the technology rollover.

One of the themes of the ongoing evolution from 2G to 3G cellular is the transition from the circuit-switched paradigm to the packet-switched paradigm, or the convergence of wireless with the Internet and its packetized IP protocols. The security constructs and demands of packet switching are more complicated than of circuit switching, requiring continuous packet authentication versus the one-time authentication done on 2G systems. Strives are being made in 3G security evolution to require 2-way authentication schemes which will both authenticate the user to the system (as is done in 2G) and the system to the user (to defeat base station impersonation and other adversarial attacks). Strives likewise are being made in 3G security evolution to enhance the performance and strength of voice encryption applied to the air interfaces. The NSA Information Assurance mission supports the development of robust security features in commercial 3G systems, especially for future government SBU (Sensitive But Unclassified) users who may not have high-grade end-to-end FNBDT-interoperable wireless security devices.

This talk will review the NSA's 1G, 2G, and 3G wireless security products, plans, experiments, feasibility demos, and prospective needs and requirements. This will be done from the perspective of a government researcher who has lived and seen much of the NSA's past notable accomplishments (and discouraging business case and standards influencing failures) in the 1G and 2G arenas, and who looks with hope and eager anticipation at the promise of 3G. Of course, '4G wireless' is beginning to be spoken of at the industry technical conferences ! Since the government is often caught in the situation of being "a day late and a dollar short" (or in the case of the fast moving wireless field "a generation late and a billion dollars short"), and secure end-to-end interoperability must be enabled and maintained across many domains, a continuous vigilance must be devoted to developing protocols and architectures that work across the multiple digital wireless generations (without making any special accommodative demands on the commercial infrastructures).