Editorial for the special issue of the IEE ECEJ on *Security for Mobility*

Chris Mitchell

14th September 2002

Over the last 10-15 years, mobile telecommunications has grown from being a small niche technology to a massive industry. Mobile telephones are now ubiquitous, and the divisions between PCs, PDAs, mobile phones and other mobile devices are becoming increasingly blurred. Against this background, the security of information handled by these devices, and of the mobile devices themselves, becomes ever more important, and this is the focus of this special issue of the IEE *Electronics and Communication Engineering Journal*.

In the brief history of mobile telecommunications, security has traditionally meant securing the radio path between the mobile phone and the local base station. The evolution of this security from the provisions in GSM to UMTS is covered in the first paper in this special issue, *UMTS security*, by Boman, Horn, Howard and Niemi. This paper presents a detailed description of the security facilities protecting the UMTS access network, within a context which explains the evolution from GSM. The paper also describes the security provisions for UMTS internal network security, something not covered by previous mobile standards (notably GSM). This leads into a discussion of the use of IP security facilities for multimedia session control, exemplifying the growing convergence between mobile telecommunications and the Internet.

Until now, the cryptographic techniques employed for mobile telecommunications security have primarily been of symmetric or 'secret key' type. That is, the schemes employed rely on the use of pre-established shared secret keys. However, the situation is likely to change in the future heterogeneous computing and communications environment, where UMTS and GSM technologies will be just two amongst many communications techniques. In such environments, public key cryptography is likely to be of increasing importance. To use public key cryptography requires the establishment of a Public Key Infrastructure (PKI) and issues associated with the management and use of a PKI in a mobile environment are the focus of the second paper in this issue, *PKI in mobile systems*, by Dankers, Garefalakis, Schaffelhofer and Wright.

Security for GSM and UMTS mobile devices relies on an internal smart card for the secure storage of cryptographic keys (and other security parameters). The use of such a portable and removable security token is likely to be vital in the future provision of security services for a wide range of mobile devices. The third paper in this issue, *The smartcard as a mobile security device* by Scheuermann, describes the evolving smart card technology that makes this possible, and also outlines future possible applications of these devices.

The next two papers, *Mobile agent security* by Borselius, and *Security issues for downloaded code in mobile phones* by Babb, Bishop and Dodgson, consider software security issues arising in future mobile systems. Multi-agent systems appear to be a promising technology in a variety of application domains, including middleware for mobile systems. When agents themselves are mobile, a variety of significant security

issues arise, which are the focus of the paper by Borselius. The paper by Babb et al. looks at the major security issues associated with the use of mobile code within the context of the mobile phone, including Software Defined Radio.

The final two papers, *Secure m-commerce* by Schwiderski-Grosche and Knospe and *Securing the delivery of digital content over the Internet* by Waller, Jones, Whitley, Edwards, Kaleshi, Munro, MacFarlane and Wood, are concerned with applications of mobile technology. M-commerce is one such application domain, and one with enormous practical potential. However, for this to become a practical reality, the security issues considered in the paper by Schwiderski-Grosche and Knospe need to be addressed. Another major application domain for mobile technology is the delivery of digital content. Again, for this to become a commercial reality means that security issues associated with content protection need to be addressed – this is the topic of the final paper by Waller et al.