Security for mobility

by Chris Mitchell

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, personal digital assistants (PDAs), mobile phones and other mobile devices are becoming increasingly blurred. Against this background, the security of the information handled by these devices, and of the mobile devices themselves, becomes ever more important, and this is the focus of this issue of *Electronics & 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 the second-generation digital GSM (Global System for Mobile) standard to the third-generation UMTS (Universal Mobile Telecommunications System) standard is covered in the paper on 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 (Internet Protocol) 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 the 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 communication 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 paper on 'Public key infrastructure in mobile systems', by Dankers, Garefalakis, Schaffelhofer and Wright.

Security for GSM and UMTS mobile devices relies on an internal smartcard 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. Our third paper, 'The smartcard as a mobile security device' by Scheuermann, describes the evolving smartcard 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 mobile 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.*

Professor Chris Mitchell is with the Information Security Group at Royal Holloway, University of London.