

Future Cryptographic Requirements from Mobile Applications

Chris J. Mitchell, Kenneth G. Paterson and Vaia Sdralia,
Information Security Group, Royal Holloway, University of London,
Egham, Surrey, TW20 0EX, UK.
e-mail: {c.mitchell,kenny.paterson,vaia.sdralia}@rhul.ac.uk

7 November 2002

1 Introduction

The main motivations behind this contribution are the current major trends in mobile systems beyond 3G: the miniaturisation and distribution of terminal functions across Personal Area Networks (PANs) and Body Area Networks (BANs) made up of limited chip area, low power consumption, processing power, and code size versus high bandwidth applications; ad hoc wireless networking; context aware services and associated user privacy issues.

In this position paper, we outline several areas where we believe new cryptographic research will be required in order to meet the needs of future mobile systems. We focus on cryptographic algorithms, protocols, and privacy technologies.

2 Lightweight and Secure Stream Ciphers

Link-level confidentiality will be as important in future mobile systems as it has been in GSM and 3G systems. Today, mobile terminals are powerful enough that implementation aspects of encryption algorithms are no longer such a major concern. However, with the likely advent of ultra-portable devices, personal area networks and wearable computing, all networked via wireless links, the implementation complexity of encryption algorithms (in terms of gate count, current consumption and speed of operation) may once again become a live issue. There will be a consequent need to develop lightweight algorithms, particularly stream ciphers, whose security level is properly understood. Crypto-algorithm implementation issues may also become important because of the encryption requirements of high-bandwidth applications, even for normal handsets.

3 Lightweight Public-key Cryptography and Protocols

3G standards do not make use of public-key cryptographic algorithms. It is likely that systems beyond 3G will, to enable a host of functions including payment, digital rights management, mobile code management, and (possibly) eventually handset and network authentication. Some form of public-key infrastructure (PKI) will then also be required in mobile systems, so as to allow verification of authenticity of public keys. In many situations, it will be desirable to implement some or all of these functions in the handset SIM, or equivalent tamper-resistant token, in which private keys will be embedded. This will still present a rather limited computational environment for some time to come.

Therefore, along with these developments will come a continued need to research lightweight public-key algorithms and protocols. For example, elliptic curve cryptographic techniques are

already well established and offer computational and bandwidth advantages over more conventional algorithms in some situations. Recently, there has been much academic interest in identity-based systems, which offer PKI-like functionality, but without the need to handle certificates. Fully understanding how these technologies can be adapted to the mobile environment will be important. An important related issue will be to understand how the complexities of these security mechanisms can be made comprehensible or invisible to end users. This may necessitate new cryptographic research.

4 Privacy Control Management

Context aware services which might include calendar data, user location data, social context, personal preferences, type and status of the communication network infrastructure have been much talked about in the mobile world. As these are widely perceived to conflict with users' privacy rights and requirements, new techniques are needed to allow users to conveniently shield their contextual information, but still to allow calls to be appropriately billed, and services delivered to mobile devices. Therefore, new cryptographic techniques will have an important role to play here.

Additionally, there is a need to understand how privacy protection for end users can be balanced against the legitimate requirements of law enforcement. Developing cryptographic techniques (such as extended escrow capabilities) which help to strike this balance seems necessary.

5 Delegation protocols and distribution of security functions

Networks of low power devices may be obliged to share access to physically secure subsystems storing secret and private keys and implementing complex cryptographic functions. For this to be done in a satisfactory way, delegation of responsibility will need to be managed securely, and with appropriate protocols. Novel cryptographic solutions are likely to be required to enable low power devices to securely delegate the computation of a security sensitive function (e.g. a digital signature) to another device in the same PAN/BAN. This issue becomes even more problematic if delegation of functions needs to take place to devices which are not fully trusted, e.g. if a device wishes another device to help with a cryptographic computation without revealing its secret or private key.

6 Multicast key management

There is a clear trend towards integrating broadcast and mobile wireless technologies. Secure communication requires that the content and context is authenticated, encrypted and integrity checked. The group members and the service providers want to be sure that their communication is not eavesdropped and that members leaving the group cannot read the messages. This brings a range of issues, many of which relate to DRM, given that broadcast channels are largely used for distributing proprietary content. Supporting the secure distribution of content to a future mixture of mobile and broadcast enabled devices will require careful design and optimisation of techniques for distribution of keys to multiple recipients of proprietary digital content.