

Priorities for Future Research in Privacy and Security for Mobile Applications

***Dr N. H. Edwards, Security Research Group Leader,
BTexact Technologies, 9th August 2002***

Privacy and security are paramount to the success of applications on mobile systems. In this short positioning paper, the need for privacy and security in mobile systems is discussed, along with technological trends which highlight that this issue is of growing concern. The paper ends with a discussion of potential areas for further research.

Current mobile systems can access a large amount of information about their users. This ranges from

- geographic position information determined by the communications network,
- personal information, e.g. calendars and address books stored on mobile devices and network servers,
- textual messages received and sent,
- communications information, e.g. calls made and received,
- financial information, e.g. low value purchases where mobile systems are used for payments, and
- audio signals (and video from terminals containing a camera).

The volume and extent of this information is increasing rapidly, driven by improvements in the processing, storage capacity and display capabilities of mobile devices. Technological advancements in networks, positioning algorithms and global positioning systems are increasing the accuracy to which a terminal's position can be calculated. Furthermore, the available mechanisms for communicating with mobile terminals are expanding with the inclusion of local wireless network components enabling connections between neighbouring devices and sensors. 'Always on' data connections now allow application data to be updated in real-time, extending the ways in which data can be used. Thus the security of data in mobile systems is a growing concern.

Maintaining the fundamental security requirements of confidentiality, integrity and availability is particularly challenging in mobile systems, as wireless signals can be readily intercepted, and the physical location and environment of the terminal is variable. At the same time, the potential market for mobile applications is huge, with end-users often willing to pay a high premium for additional services. The need for further research in this area is thus imperative.

In the light of these developments, a number of questions exist for mobile applications:

- Who owns the data – the end user or the service provider?
- How can applications which access personal data be easy to use and yet secure?
- How can the user easily control and monitor access to personal data?
- How can data held on a mobile device be backed up and retrieved without compromising the security of the data?
- How can the differing opinions of individuals regarding attitudes to data and privacy be accounted for?
- How much data should be stored for billing and legal purposes?
- How can users best be protected from malicious code such as viruses?

The area of security and privacy for mobile applications is undoubtedly complex, and there are many potential areas for future research. Outlined below are four high-priority areas to be considered.

Firstly, there is a need to develop and validate a coherent framework for security and trust for mobile applications. The traditional approach to security is to adopt a layered architecture to solve specific aspects of an overall problem. However, what is needed is a holistic approach to security on mobile systems, as the security of a system is only as strong as the weakest element. Key elements of the framework are a suitable architecture for mobile applications and a methodology guiding the use of the framework.

Secondly, there are emerging XML-based standards for the exchange of data between applications such as Web Services. These are likely to be fundamental in the next generation of mobile applications. The requirement for information security in many areas such as e-business has led to the development of many different security standards. There is a need to evaluate the use of such standards in the environment of mobile applications.

Thirdly, there are emerging biometric techniques which increase the accuracy with which users can be identified. Costs of sensors, for example for fingerprint and iris recognition, are falling and now represent only a small incremental cost on a mobile device, thus making the deployment of such sensors economically feasible. However,

the application of biometrics is a highly specialist area because of the complexity of the technologies and the practical human factor issues surrounding their use. Research is required to investigate whether biometrics may be applied usefully in the area of mobile applications.

Finally, another method of protecting information is to store information on SIM cards. These offer a secure location for data and applications, and can contain dedicated encryption hardware to maximise security of the stored data. For greater protection, the user can also remove the card completely from a mobile device. Further research is required to understand how applications can exploit the increasing memory and processing capacities of these cards to the full.

In summary, the issues of privacy and security are fundamental to the success of future mobile systems, and will grow in significance as mobile devices, networks and applications continue to advance. Further research in areas such as the development of a holistic security framework, exploiting emerging XML standards, biometrics and smart cards will help in understanding these problems and potential solutions, so that users can safely enjoy the benefit of new mobile applications.