Foreword

Tim Wright
Security Technologies, Vodafone Research and Development

In the 10 years I have been working in the field of mobile phone security, we have seen a vast increase in the power and flexibility of the programming environment available on mobile phones, moving towards the openness of the PC and the Internet. Over that same period there have been attempts, not to close down the open environments of the PC and the Internet but, at the very least, to ‘tame’ them. This taming needed to happen and needs to continue.

Fortunately, the growth in the functionality and openness of mobile phones happened in a controlled manner, with many factors working in favor of security. Firstly, over this period most mobile phones were, and still are, bought by network operators (for sale on to their subscribers) who imposed security requirements that have kept implementation standards high. Secondly, most data coming in to and out of mobile phones involves a network operator, who has both the reason and the power to take steps on the network side to curb the effects of viruses and worms on the client side. Finally, there was the simple fact that Symbian OS phones represented a small percentage of the total mobile phone population.

Some of these factors are changing. Surely the most significant is that the percentage of mobile phones based on Symbian OS and other open operating systems is set to increase significantly. Symbian OS will become a serious and worthwhile target for writers of malware. The increasing variety of short-range and long-range wireless interfaces means that there are many ways for data and applications to get onto a phone and the proportion that operators can control will decrease. Symbian OS is entering a bigger and less controlled world and needs to be able to look after itself.

Vodafone, therefore, very much welcome Symbian’s introduction of the platform security architecture. It is Vodafone’s hope that effective
certification schemes for application developers, continued scrutiny and improvement of the most trusted parts of the Symbian OS, and complementary hardware security features for boot-time and run-time protection of the secure software will be used alongside platform security and help to ensure its long term success. Symbian OS can then be opened up to a wider range of application developers with the assurance that privileges can be allocated to code on the basis of the responsibility the developers will take, and that users and their phones can be protected from poor code and malicious intent.

This book provides background to the platform security architecture, which will be of interest to security professionals, and guidance to application developers on how best to take advantage of the improved security now available. Widespread adoption of these practices will benefit the whole mobile phone industry, including software vendors, semiconductor vendors, phone manufacturers, network operators, content providers and, not least, the phone user!