Chapter 3

Mobile Trusted Computing
Based on MTM

Jan-Erik Ekberg
Nokia Research Center, Finland

ABSTRACT

Trusted computing (TC) denotes a set of security-related hardware and software mechanisms that make a computing device work in a consistent manner, even in the presence of external attacks. For personal computers, TC typically is interpreted to be a software architecture designed around the trusted platform module (TPM), a hardware chip residing on the motherboard and implemented according to the specifications of the Trusted Computing Group (Trusted Computing Group, 2008A). In embedded devices, the state-of-the-art in terms of hardware security and operating systems is significantly different from what is present on personal computers. So to stimulate the take-up of TCG technology on handsets as well, the recently approved mobile trusted module (MTM) specification (Trusted Computing Group, 2008B) defines new interfaces and adaptation options that match the requirements of the handset business ecosystem, as well as the hardware in use in the embedded domain. This chapter provides an overview of a few hardware security architectures (in handsets) to introduce the reader to the problem domain. The main focus of the text is in introducing the MTM specification – by first presenting its main functional concepts, and then by adapting it to one of the hardware architectures first described, essentially presenting a plausible practical deployment. The author also presents a brief security analysis of the MTM component, and a few novel ideas regarding how the (mobile) trusted module can be extended, and be made more versatile.

INTRODUCTION

In recent years, mobile phones have left the era of being closed embedded communication devices, increasingly turning into “hand-held multimedia computers”. In addition to providing reliable, basic communication services (voice calls, SMS), contemporary handsets often provide the integrated services of music players, digital cameras, GPS
navigators and gaming devices. The possibility to
download and execute 3rd-party applications on
the mobile platform makes handsets remarkably
similar to personal computers in terms of open-
ness and configurability.

A little-recognized fact is that this service
convergence has stimulated device manufactur-
ers to include advanced hardware- and operating
system security features in their devices – this
has been needed to balance user expectation and
the strict regulatory requirements on the reliabil-
ity of communication devices against virus and
mal-ware threats that follow from introducing
device openness.

Thus, there are hundreds of millions of de-
ployed handset devices in the world today that
are e.g. capable of protecting keys, assuring
code integrity or making digital signatures using
hardware-based features. Although these features
today primarily are used to provide the necessary
assurance that the handset in all possible scenarios
will handle incoming and outgoing calls in an
uninterruptible and reliable way, the mechanisms
can as well in parallel be used for the benefit of
3rd party applications. As this happens, the role
of trust modeling and trust management will play
the crucial role of linking the security mechanisms
to user perception and/or activity.

The traditional driver for platform security on
handsets is the regulatory environment. Devices
that participate in radio communication typically
undergo testing to determine that the device keeps
within the bandwidth allocated for the commu-
nication and that the transmission power does
not exceed what is deemed safe for the user. For
licensed bands also the conformance to protocol
is a regulated activity. In practice this implies that
both hardware and software are tested, and the
approved license also includes the expectation
that no (application) software installed at a later
time can modify the tested and approved device
features. This situation clearly motivates the need
for software integrity as well as some degree of
isolation or integrity guarantees for configuration
data that affects the communication.

Another important driver for handset security
features is the business ecosystem in which
phones often are sold. Communication service
providers (operators) may sell below cost / sub-
sidize end-user devices as a part of a long-term
communication contract, where the assumption is
that the monetary loss at the time of device sale
is recaptured as communication revenue. In this
setup the operator clearly requires some technical
assurance that the device actually is used for
communication, using the service provided by
the operator in question. Constraints and enforce-
ments related to this so called SIM Lock need to
be properly rooted in hardware-assisted platform
security services, since the breaking of the device
lock feature by definition is a lucrative business
opportunity. Digital rights management (DRM)
for music and video is by nature a very similar
security service.

Unfortunately the state of the art in handset
trust mechanisms is that they are widely deployed,
but manufacturer- or even product-specific. This
is not acceptable for 3rd-party solution providers.
Given a consistent, cross-platform secure trust
infrastructure for handsets, at least the following
services could bring clear benefits to users:

- Payment- and banking services is a specific-
  ic field that has high security requirements,
  both in terms of protecting / isolating se-
  crets (or value), and in terms of trusted in-
  terfacing. Payment services also resonate
  well with the mobility and the personal
  aspect of a handset.
- Authentication and access control of all
  sorts, whether to get access to web pages,
  company networks, one’s car or one’s apart-
  ment could be made both more convenient
  and more secure, if credential handling in
  the device is founded on a well-established
  trust infrastructure.
Related Content

Technology: A Bane or Boon for Cross-National Levels of Generalized Trust?
Blaine G. Robbins and Maria S. Grigoryeva (2010). Trust and Technology in a Ubiquitous Modern Environment: Theoretical and Methodological Perspectives (pp. 123-144).
www.irma-international.org/chapter/technology-bane-boon-cross-national/42904/

Technology Related Trust Issues
www.irma-international.org/chapter/technology-related-trust-issues/60586/

Trust Related Technology Practices
www.irma-international.org/chapter/trust-related-technology-practices/60585/

Research Design
www.irma-international.org/chapter/research-design/60584/

Analyzing the Ethical Dilemma between Protecting Consumer Privacy and Marketing Customer Data
www.irma-international.org/article/analyzing-ethical-dilemma-between-protecting/78292/