Mobile Device Security and Trusted Computing – Next Steps

The mobile industry is embracing new challenges. The coming boom in do-it-all and specialized mobile communication devices connected via the wireless Internet will soon create network end-points that number nearly two billion. While these smart-phones, cell-phones, and other communicators expand network boundaries, new services will emerge to meet growing consumer and enterprise demands.

Device theft and loss has always been an issue for mobile devices and with the inclusion of sensitive personal information such as address books, as well as high value premium a service on the devices, the risk from loss is increasing. In addition, as mobile devices become smarter and support more data functions, the industry is facing many of the same threats as personal computers from malicious software and attacks. Currently the online criminal activity targeting these new hand-helds is fairly limited. The industry now has a good opportunity to take proactive measures before mobile security issues become a more significant industry problem, by building protective mechanisms into mobile devices.

Security Must Be Standardized

Mobile manufacturers and service providers recognize a need for security solutions that function across multiple platforms, on multiple networks and can be trusted to responsibly handle multiple media types. However, the bounty of consumer products and applications geared to the Internet generation will create significant opportunities for abuse. Devices that store and move money electronically for sensitive m-banking transactions or other valuable proprietary digital content exchanges could be at risk from anywhere the signal can be detected.

Increasingly, today's fast, powerful technologies allow users to enjoy business information as well as personal content from both enterprise and home networks on the same device. Owners at home might download music for their morning commute or access the web for traffic information, and before leaving work sync that same device with their office software to upload work files and e-mails. Mobile devices must be capable of supporting strong security for a wide range of both personal and business requirements.

In the enterprise, some IT departments want to deliver equal service levels and access privileges to all clients, be they in-house clients or remote users with hand-held devices. To comply with regulatory guidelines for managed access, tools for strong identity protection and user/device authentication must be available and be virtually invisible to every user.

The cost of non-standard point solutions can be high and can result in vertical solutions that require more support and inhibit interoperability between applications. Without a common approach to handle trust, security and protection in devices, managing all this becomes too complex. The Trusted Computing Group's (TCG's) Mobile Phone Work Group (MPWG) was formed to address all these concerns.

TCG Objectives for the Mobile Phone Work Group

TCG develops and promotes open, vendor-neutral, industry standard specifications for trusted computing building blocks and software interfaces across multiple platforms. The TCG mobile security specification aims to ensure hardware and software perform as designed and mitigate attacks from any unauthorized parties. The security in mobile devices must be able to protect the

Copyright© 2005 Trusted Computing Group – other names and brands are properties of their respective owners

interests of users, including their privacy, as well as device manufacturers, network operators, and service providers.

For mobile phones and devices, this means operating systems, platforms, and application level functionalities, as well as SIM, USIM, UICC cards, etc., interact in a secure and trusted manner. This methodology enables trusted authentication (i.e., that the mobile device is what it says it is, and the user is who they say they are.) In addition, it gives assurance that the platform configuration and software running on it have not been tampered with and enables trustworthiness to be assessed.

Implementing a standard industry specification will benefit manufacturers in reducing in-house R&D costs, increasing confidence in supporting the required functionality, increasing interoperability with other vendors' products, and opening up the possibility to expand their supplier base. In turn, component manufacturers will equally be able to expand their customer base.

The design specification maximizes design efficiencies in hardware and software, requiring that solution stacks for different domains are as similar as possible. Trusted platforms are sometimes based on Trusted Platform Modules (TPM), a security chip specified by TCG which functions as the basis of trust within a device. However, due to the small size of mobile devices, TPM technology needs to be adapted for use in hand-held products. TCG's mobile specification will build on TPM security and the TCG trust model, and is subject to the TCG security specification requirements.

How MPWG Use Cases Present the Trusted Mobile Experience

To guide subsequent technical specification work within TCG's Mobile Phone Working Group, the following document presents eleven use cases. The document provides interested parties outside of the TCG with a description of the work being carried out by the MPWG.

These use cases intend to outline the types of security challenges where the TCG specifications might be used, in order to enhance value delivered through mobile devices.

The use cases are:

User Data Protection and Privacy - Enable the protection of user's personal information, such as identity and address books, from access or copying by unauthorized parties.

Platform Integrity – Ensure device operation occurs with only authorized operating system(s) and hardware.

Device Authentication – Ensure that 1) device authentication may be used to assist in end user authentication, and 2) that it may prove the identity of the device itself.

Robust DRM Implementation – Ensure any implementation of a DRM specification can be trusted to protect the data that users acquire and the content and service providers require .

SIMLock / Device Personalization – Ensure that subsidized mobile devices remain locked to the appropriate network until unlocked in an authorized manner.

Secure Software Download – Enable the secure download of application software or updates, firmware updates or patches to protect against attacks.

Secure channel between device and UICC – Provide shared functioning for security sensitive applications (e.g., an m-commerce application) that must implemented partly in the UICC and partly in the device.

Mobile Ticketing – Enable new services based on a user purchase of an electronic ticket which is downloaded to the mobile device and used for entry to an event or access to a service.

Mobile Payments – Enable the mobile device to serve as a user's wallet or purse for electronic payments to point of sale devices. Support for a variety of payment sources including credit cards, debit cards, pre-paid funds, and online accounts.

Software Usage – Assure that software applications retain their integrity against attacks, adhere to device user policies, and cannot interfere with other device functions.

Copyright© 2005 Trusted Computing Group – other names and brands are properties of their respective owners

Prove Platform/Application Integrity to End User – Provide the ability for the user to verify, either at boot time or on application start up, the trustworthiness of the device and/or application.

What's Ahead for Trusted Computing and Mobile Devices

These eleven use cases form the basis of the current technical requirements, architecture and specifications work within TCG. TCG's mobile security specification is estimated to be ready for publication in the first half of 2006.

Once the specification is available, device manufacturers will have the opportunity to embed state-of-the-art, standardized security level capabilities into their products. From then onwards, carriers, service and content providers, as well as end-users can have a higher degree of confidence in mobile devices.

For more information, please contact:

Trusted Computing Group Administration
5440 SW Westgate Drive Suite 217
Portland, OR 97221
Email: admin@trustedcomputinggroup.org
Phone: (503) 291-2562, Fax: (503) 297-1090

Copyright© 2005 Trusted Computing Group – other names and brands are properties of their respective owners