May 30th, 2014

Federal Trade Commission
Office of the Secretary, Room H-113 (Annex X)
600 Pennsylvania Avenue NW
Washington, DC 20580

RE: Mobile Security Project, Project No. P145408

Dear Commission,

Infineon welcomes the opportunity to offer comments to the Federal Trade Commission's inquiry on the State of Mobile Security. Mobile devices like smart phones have become critical enabling tools for consumers to access information and services that support communication, health, employment, commerce and myriad additional entertainment applications. More and more personal information is stored on these mobile devices, making them a significant risk for identity theft if not properly secured.

Infineon is a global semiconductor company with core competencies in the fields of security, wireless communication and embedded control. Our microcontrollers and ICs are facilitating security in an increasingly networked and mobile world. For example, secure chips enable mobile payment systems security, local network security, cloud security, and electronic ID documents. As the market leader in hardware-based security, Infineon believes a hardware root of trust (HRoT) is fundamental to securing sensitive information, transactions and devices.

Consumer privacy is rooted in a foundation of secure design practices, and cemented by the use of a hardware root of trust to protect the security of a device and its many varied applications. Convenience has driven broad adoption of mobile devices, but the vulnerabilities of inadequately secured devices and applications will drive more theft of data, and theft of identity if security is not designed in to devices and applications. In response to your call for comments, we offer Infineon's perspective on secure platform design and security lifecycle updates, two elements critical to protecting consumer data used on mobile devices.

Secure Platform Design: How can platforms create robust development environments while limiting the potential for abuse by privacy-infringing or malicious third-party applications? Have particular design approaches proven more or less effective than others in protecting consumer privacy and security? What, if any, are the trade-offs between different approaches to providing developers with access to consumers' personal information or device resources?

Infineon Technologies North America Corp.
Office Address 640 N. McCarthy Blvd., Milpitas California 95035 USA
Tel 866-951-9519 Internet www.infineon.com

Adding security functionality to a mobile device through software is inefficient and ineffective. Devices must be secure by design, anchored by a hardware root of trust containing a separate execution environment that can monitor and enforce the security and integrity of the device. The device security functions must be made available to the mobile operating system to ensure applications and services, such as mobile device management (MDM), can use these functions. The mobile device management solution will be required to manage device provisioning, integrity, configuration profiles, interfaces, applications, and services

The use of a separate execution environment as a secure root of trust is required. Trying to reuse the host processor execution environment leaves the secure environment at risk from the complexities of the host processor. In particular, the host processor is an extremely complex hardware implementation running large, complex and rapidly changing software. These factors make securing a host-based secure environment extremely difficult and prone to vulnerabilities.

Infineon therefore believes that a dedicated, tested and stable environment is necessary as the root of trust for any secure platform. Only a platform that builds on such an environment as a root of trust can provide secure platform features such as integrity measurement and trusted boot which are required to enable true application security.

The federal CIO Council has established mobile security baseline requirements in its May 2013 document, Government Mobile and Wireless Security Baseline (https://cio.gov/creating-a-foundation-for-mobile-security/). These baseline requirements are specifically directed to government devices and applications, and Infineon fully supports the baseline reference to NIST SP800-53R4 . Together with the Mobile Security Reference Architecture, these guidelines incorporate privacy by design. The device security requirements call for secure FIPS 140-2 encryption and storage for authentication credentials and other sensitive data at rest, as well as securing communication through a VPN service.

Security Lifecycle and Updates: What is the security lifecycle of a mobile device? What are consumer expectations with respect to the security lifecycle of their mobile devices? What are the challenges in creating, testing, and distributing security updates to end-user devices? What, if any, are the implications of slow update cycles? Are there steps that platforms, manufacturers, telecommunications carriers, and other players can take to streamline this process?

Innovation and change are a constant in the market for mobile devices. Size, shape, speed, features, applications, and security updates are evolving with each new smart phone, tablet, or wearable device. As these devices become more nimble for a wide range of uses – entertainment to financial transactions to identity credentials to health measurement to critical communication – the importance of protecting sensitive data and transactions increases.

There are two distinct security lifecycles with mobile devices to consider when evaluating whether a device is secure enough to protect its user.

- The lifecycle of the mobile device itself
- The lifecycle of any user credential that may reside on the mobile device

It is important to distinguish between these two when considering the lifecycle management of mobile devices.

The security lifecycle of a mobile device should be initiated as early as possible in the production and provisioning/user personalization process. Establishing an early security foundational trust anchor to support subsequent manufacturing, logistics, issuance, and final ownership provides the assurance for the security audit trail of a device (is this a genuine xphone? running genuine network? with valid software and updates?). Having this security audit trail credentialing for the device allows for automation in both attestation of the platform trustworthiness and revocation methods if the device trustworthiness has been compromised (i.e. lost stolen phone, or hack).

Due to the diffused production and distribution of mobile devices, initiation of lifecycle controls on a mobile device can be challenging even up to the provisioning-personalization-issuance step. Where does the trust point start in time/location, and how can this trust point be managed over the entire lifecycle of the mobile device?

The employment of a separate execution environment as a secure root of trust on the device can alleviate the complexity of enforcing the device security policy over the lifetime of the device. A hardware root of trust technology has the capability to trace the trust model as far back as the chip production. Once the hardware root of trust is logically bound to the mobile device, at or before the point of sale, there is the capability to enforce security policies for both the mobile device itself and any issued digital certificates/credentials.

The lifecycles of user identity credentials (personal digital certificates, for example online banking) are more persistent over time and typically "outlive" any given mobile device on which they may reside. This would imply that a secure mechanism for transferring user identities between mobile devices is required in any lifecycle protocol.

As an example, in some U.S. states it is being seriously discussed to have the personal driver's license as a credential on the mobile phone. While current mobile and credentialing technology is more than capable of making this work, there are remaining policy questions such as:

- What are the trust anchors in the process to be loading a government issued credential onto a mobile device of unknown trustworthiness?
- A personal smartphone is typically replaced by the owner every 2-4 years while the driver's license is typically issued for 10 years. How to securely transfer a driver's license credential from the old to new phone without unintentionally opening the method to malicious behavior?
- How to efficiently revoke the driver's license on the old phone as it moves into the aftermarket?

In this example, once the hardware root of trust is logically bound to the mobile device there is the capability to enforce security policy for both the mobile device itself, and for the transference of any user identities stored on the device in a secure manner.

Security by design is fundamental to protecting devices and applications of mobile devices. Infineon firmly supports the establishment of a trust anchor from the beginning of platform production

that can validate the device, its operations, software updates, and user credentials. A hardware root of trust protects mobile devices and their users.

Sincerely,

Joerg Borchert, Phd
Vice President
Chip Card and Security ICs