1 Trusted mobile computing: An overview of existing solutions

1.1 Introduction

Applications targeting banking, ticketing, health monitoring applications or even Digital Rights Management (DRM) for multimedia applications have to be secured so that the user confidence will increase. Therefore a need for mobile trusted computing arose as data security has not been considered as mandatory in existing mobile operating systems (OS). Many solutions have been proposed and the ones described here are

- Secure Element
- Trusted Platform Module
- Trused Execution Environment
- Virtualization

1.2 Application Provisioning Models

ICOM The most spread model is Issuer Centric Smart Card Owner (ICOM). This model is service oriented. Indeed, every service provider installs its own application(s) on the device and does not share its secure environments with other issuers or with the users. The provider has full control over the card, changes to it and communication with it. This centralized management system is the reason why this model achieves such strong security levels. The drawbacks are that the user has limited access to the card and the card cannot be used to secure third party applications. If more services or features need to be added new cards will have to be distributed.

UCOM In this model, users have the full control of their cards management. Indeed, they are able to install any applications they want on their smartphone. The ownership of the card is transferred from the issuer to the user who is responsible for the operations the card makes.

1.3 Attacker Models

Malicious app attacker: The attack is performed by a malicious installed application. Indeed, the attacker designs the application to intercept sensitive information transmission and processing. The application is able to use all the declared permission to spy on other applications.
Root attacker: This kind of attacker have root credentials and are able to run applications with root permissions. It allows them to inspect the file system. This scenario is increasingly common. Indeed, millions of Android users have rooted their phone.

• Intercepting root attacker: This kind of attacker has the same abilities of the root attacker with an access to the input/output operations and the capacity to inspect the device memory.

- Malicious App: Is performed by a malicious installed application
- Root: Attacker gets access to root credentials and is able to run applications with root permission.
- Intercepting Root: Attacker is root and has access to I/O operations.

1.4 Hardware-based Solutions

Among the existing solutions, the hardware-based ones are the most deployed by manufacturers. Indeed hardware security solutions have the advantage of greatly reducing intrusions and attacks. In addition, low engineering and manufacturing costs of silicon components allow integration in large public terminals.

1.5 Software-based Solutions

the new generation of smartphones is now able to run several virtual OSs on the same device. Each virtual OS has a new and parallel stack with all features of a regular OS. Furthermore, to prevent malicious applications installed on a Rich OS from stealing data in a Secure OS for instance, an isolation has to be set up between the different OSs.

1.6 Comparative Analysis

Trusted Execution Environments are the best solution described in the paper. Their computation and memory capacities are not limited like that of the SE or the TPM. On top of that TEEs are resistent to root attackers which the virtualization is not. The main disadvantages about TEE mentioned is the it is ICOM (not really anymore) and that it requires secure boot.