Master project at NXP Semiconductors or Radboud Universiteit Nijmegen

Rollback protection of TEE

More and more functionality is moved from dedicated devices to apps running on a smartphone. This also holds for security sensitive functionality, like for instance payment and access control. In order to enhance the security, ARM processors, on which most mobile phones and tables are based, are equipped with TrustZone. Trustzone is a hardware feature that enables the processor to run into two worlds: a secure world and a normal world. Normally, the mobile phone is running from the normal world. Only if a security sensitive process needs to be executed, the mobile phone switches to the secure world. In order to make use of the security provided by TrustZone, it must be enabled by installing the proper software on it (e.g., the operating system that runs in the secure world). A more generic term for the secure area of the processor is Trusted Execution Environment (TEE).

The basic feature offered by TEE is process isolation: Even if the phone is rooted, a malicious app is not able to access apps running in the TEE. However, for a lot of security features it is up to the manufacturer to decide whether or not to implement them and it is also often not very clear which ones are and which ones are not implemented. One such feature is roll-back protection. In a rollback attack, it is the goal of the adversary to restore an older version of the program data. For instance, if a balance is stored on the mobile phone, an adversary may want to restore the balance to the value just before a transaction. In this way, he can buy a product (e.g., a ticket) without the money being subtracted from the balance.

The goal of this master project is to test whether the TEE of some popular smartphones are protected against rollback and investigate the reason of the outcome. The attack should be implemented in the normal world.

Your profile:
- Computer science student
- Knowledge of security
- Knowledge of Android

The project will take six months, including the writing of a final thesis report.

Contact information:
Prof. Wil Michiels
High Tech Campus 46
5656AE Eindhoven
NXP Semiconductors
Wil.Michiels@nxp.com