Master project at NXP Semiconductors
Vulnerability assessment HCE applications

Mobile devices are increasingly being equipped with NXP's Near-Field Communication (NFC) technology. This enables several interesting applications, such paying with your mobile phone. Traditionally, the NFC communication in a mobile phone was directly forwarded to a secure element, which is a strongly protected, closed platform. On this platform the security-sensitive cryptographic algorithms can securely be executed.

Recently, Android added Host-Card Emulation (HCE) in order to make NFC accessible to the application processor. The advantage of this is that any app running under Android can make use of the NFC functionality. The downside, however, is that the apps run in an unprotected environment, where the most realistic attack model is the so-called white-box attack model. In this attack model the attacker is assumed to have full access to and full control over the execution environment.

To still offer a certain security level when running within the white-box context, one can apply software protection techniques to the software. Important is to assess the security level of these solutions. Two very relevant type of attacks we know from protecting secure elements are power analysis and fault injection attacks. In the former type of attack, one tries to extract a cryptographic key by studying power traces. In the latter type of attack, one tries to inject faults into an execution. Next, by comparing the outcome of the faulty execution with the outcome of a normal execution, one tries to find the implemented cryptographic key.

Within NXP we have developed tools, based on dynamic binary instrumentation (DBI), for generating execution traces within the white-box attack model. On these traces we can next apply analyses that we also use in power analysis attacks.

The end-result of this master project is to extend the DBI-tooling such that it can be used to easily introduce faults in a software execution. Next, this should be used to extract keys from software implementations of cryptographic algorithms analogously as this is done for hardware solutions

Your profile:

- Computer science student
- Knowledge of security
- Good C-programming skills

The project will take six months, including the writing of a final thesis report. It will be carried out onsite at the High Tech Campus in Eindhoven, The Netherlands, due to the required high-intensity knowledge transfer and supervision, as well as the availability of specific hardware and software tools. Working in this project at NXP Semiconductors in Eindhoven implies working in a stimulating, multidisciplinary environment at the forefront of technology, with knowledgeable colleagues, and an excellent infrastructure.

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