INTRINSIC ID

Intrinsic-ID B.V.
High Tech Campus 9
5656 AE Eindhoven
The Netherlands

T +31 40 851 90 20
E info@intrinsic-id.com
www.intrinsic-id.com

KvK CoC: 17233801
BTW VAT: NL8199.42.777.B01
Bank: ABN AMRO 62.54.16.007
IBAN: NL92ABNA0625416007

Master of Science Internship

Location: **Eindhoven, The Netherlands**
Start Date: **March 2013**

Project description

Within a research project at Intrinsic-ID we are looking for a motivated student (Electrical Engineering, Mathematics, or Computer Science), who is ready to start his/her graduation project for the MSc degree. The goal of the project is to develop a demonstration platform for a “Secure Boot” solution, based on Intrinsic-ID’s patented Hardware Intrinsic Security™. This technology is based on Physical Unclonable Functions (PUFs), which can be seen as “biometrics of a device” or a device specific fingerprint.

The first step of the Secure Boot implementation is extracting uninitialized SRAM data (Level 1 Cache) from a processor, which is running the Android 4.0 operating system. This SRAM data will be used as a PUF, in order to extract a unique cryptographic key for the hardware (tablet/mobile phone) on which the demonstration is running. This key will be the basis for the security during the rest of the boot process, allowing for a secure environment to be created on the processor. Without the key (which cannot be copied to other devices) there will be no secure environment and all applications depending on this security will therefore not be operational. The demonstration setup should provide its’ audience with a clear view of the steps being taken in the Secure Boot process and how the resulting secure environment can be used to run applications with high security requirements, even on a standard mobile device.

Responsibilities include, but are not limited to

- Making modifications on an Android boot loader in order to extract uninitialized SRAM from an ARM Cortex-A9 processor (OMAP4460 processor).
- Designing (in collaboration with experienced security architects and engineers) the architecture for a Secure Boot demonstrator on an Android tablet (PandaBoard, Android 4.0).
- Implementing the low-level building blocks for the Secure Boot demonstrator (in the ARM/OMAP/Linux/Android boot process).
- Implementing an Android application for demonstrating the Secure Boot functionality.

Required experience and appreciated qualities

- Student (Electrical Engineering, Mathematics, or Computer Science), ready to start working on final thesis project for MSc degree;
- Experience with Linux and Java programming languages;
- Experience with software development tools such as: Visual Studio, Eclipse;
- Knowledge of Cryptography primitives and experience with secure software implementation;
- Experience with Android development (preferable, not mandatory);
- Knowledge of Linux kernel is a pre;
- Knowledge of ARM Cortex A9 core is a pre (registers, ARM assembly language);
- Able to think outside of the box: find unexpected ways to solve problems or meet requirements;
- Good organizational skills and excellent problem solving abilities.

INTRINSIC ID

About Intrinsic-ID

Intrinsic-ID is the world-wide leader in security IP cores and applications based on patented *Hardware Intrinsic Security*™ technology (HIS), also referred to as 'Physical Unclonable Function'.

In HIS secret keys are extracted from the properties of chips like an 'electronic fingerprint' and used to offer a total protection of sensitive private and corporate data on mobile devices, embedded systems and in the cloud.

Intrinsic-ID is headquartered in Eindhoven, The Netherlands and has sales offices in San Jose, Tokyo and Seoul. www.intrinsic-id.com

For additional information you can contact

Vincent van der Leest
Intrinsic-ID B.V.
High Tech Campus 9
5656 AE Eindhoven
The Netherlands

vincent.van.der.leest@intrinsic-id.com
www.intrinsic-id.com