Usable Mobile Security

Prof. N. Asokan
University of Helsinki
Lead Principal Investigator

Dr. Matthias Schunter
Intel Labs
Principal Investigator
and Chief Technologist

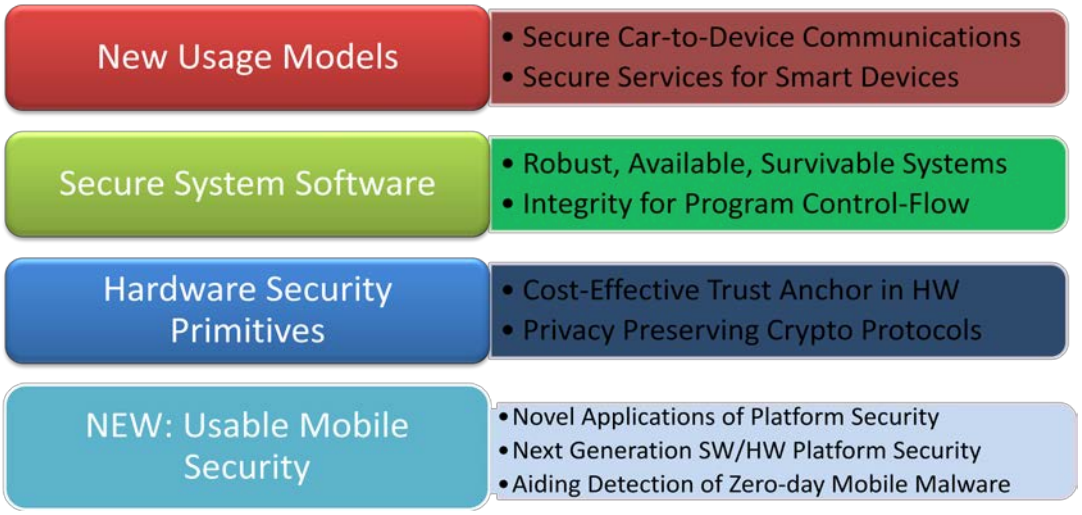
Abstract
The Intel Collaborative Research Institute for Secure Computing (Intel CRI-SC) established on May 23, 2012 as a public-private partnership between Intel Labs and Technische Universität Darmstadt, Germany including the Center for Advanced Security Research (CASED) was extended to the University of Helsinki in Finland on August 1, 2013. This addendum to the original white paper on ICRI-SC outlines the initial key research themes that focus on secure computing for interconnected mobility.

Executive Summary

The new extension to the Intel Collaborative Research Institute for Secure Computing (Intel CRI-SC) is jointly operated by Intel Labs and the University of Helsinki, Finland. The Institute conducts research in **usable mobile security**. It sponsors industry and scientific research to improve security and privacy for mobile devices and users while emphasizing the usability and deployability of these mechanisms. The new Institute will initially focus its research along three different strands. In *open access to trusted execution environments,* we will investigate how to safely open up hardware-based trusted execution environments to application developers in a controlled manner. In *novel applications of mobile platform security,* we explore whether widely deployed platform security techniques can be used to address the security and privacy needs of emerging usage scenarios like in-vehicle infotainment. In *malware insights,* we attempt to gauge the extent of mobile malware infection in the wild, and see if indicators that can be gathered inexpensively from mobile devices can help in the search of previously unknown malware by identifying a pool of devices potentially vulnerable to mobile malware.

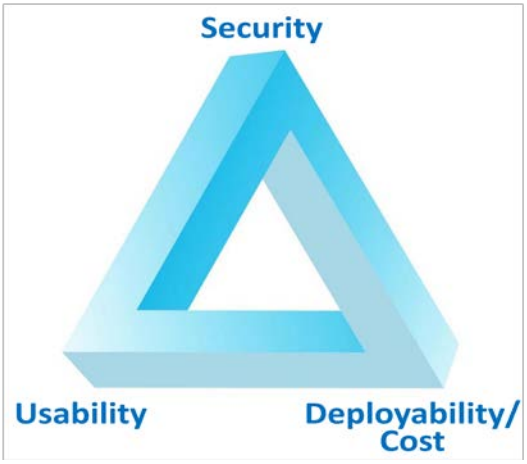
Strategy and Vision

The new institute in Finland continues the emphasis on the user-centric research strategy by focussing on a new strategic theme of **usable mobile security**. This means that our aim is to develop novel security and privacy technologies for mobile devices and users, informed by usability considerations in the mobile setting.



Usable Mobile Security: The new Research Thrust introduce by the Finnish Intel CRI-SC

The popularity of mobile devices is exploding. For the majority of users, a mobile devices constitutes their first exposure to the Internet and the first personal computing device. Security and privacy solutions intended for mobile users and devices must therefore *simultaneously* satisfy three criteria: they need to provide sufficient protection, while being easy to use and inexpensive to deploy.



Initial Research Themes

The overall goal of the new Institute is to develop techniques for improving security guarantees for mobile users without sacrificing usability. We will begin with explorations in three strands.

Strand 1: Open Access to Trusted Execution Environments

Strand 2: Novel Applications of Platform Security

Strand 3: Mobile Malware Insights

Motivation and background:

Strand 1: Open Access to Trusted Execution Environments

Hardware-based Trusted Execution Environments (TEEs) are widely deployed on mobile devices. But their use has been limited. Application developers have not had any standard, widely available interfaces to be able to make use of TEE functionality. There have been some recent research efforts to safely open up TEEs for developer use. But these have been proprietary. Our goal in this strand is to investigate how to safely open up TEE functionality for use by application developers using standard interfaces where possible, and proposing extensions to standards otherwise?

Strand 2: Novel Applications of Platform Security

Different Platform security solutions are widely used in various mobile operating systems such as Android, iOS, Windows Phone, Blackberry and others. The number of security mechanisms in Linux kernel is also growing: kernel namespaces attempt to provide isolation to a set of running processes, control groups allow limiting resources (CPU usage, memory etc.) that a group of processes should have access to, Linux Security Modules (Smack, SELinux, AppArmor, SEAndroid) provide necessary mandatory access controls. Our goal in this strand is twofold: (a) can these existing platform security mechanisms be used to address the security needs in emerging usage scenarios, such as In Vehicle Infotainment (IVI) and usages that require secure interaction between mobile & embedded devices? and (b) how can we improve the usability of these platform security mechanisms, which has been widely recognized as a problem?

Strand 3: Mobile Malware Insights

Mobile Malware is reportedly on the rise. Actual infection rates are still low compared to malware on PCs, but they are not negligible: recent estimates suggest this to be somewhere between 0.0009% (by independent academic researchers) and over 5% (reported by an anti-virus vendor in a recent press release). Our goal in this strand is to explore lightweight on-device instrumentation techniques to estimate as well as predict malware infection.

Approach

Strand 1: Open Access to Trusted Execution Environments

We posit that safely exposing TEE functionality in a controlled manner to application developers and other third parties is possible. We will begin by building/adapting the necessary tools (such as an open source TEE emulator) needed for further research and using them to realize selected usage scenarios, such as application-specific secure storage.

Strand 2: Novel Applications of Platform Security

We will approach each sub-goal by focusing on a specific example.

For the “new usage scenario” subgoal, we choose “application migration” as the scenario: we will build a threat model, analyze existing kernel-based lightweight virtualization techniques, designing an application migration solution and prototyping it on Tizen OS.

For the “improving usability of platform security” subgoal, we will investigate if group sourcing (i.e., gathering and aggregating feedback from one’s social circles) is an effective way of providing sufficient information for ordinary users to make informed decisions about using apps and content. To this end, we are building the backend infrastructure for group sourcing and will apply it first in the specific case of Facebook applications/content by prototyping a Facebook application, called Friend Application Rating (FAR) and browser plugin. We choose Facebook first because it will allow us to get enough users that can help us conduct a user study to evaluate the effectiveness of the approach. If promising, UH will investigate how apply this approach to the application installer on a smartphone platform (e.g Tizen or Android).

Strand 3: Mobile Malware Insights

We posit that extremely lightweight instrumentation techniques can gather sufficient information from a device to be able to predict if the device is likely to be (a) infected in the future or (b) infected with a previously unknown malware. We will collect data from mobile devices by introducing lightweight instrumentation on a widely deployed smartphone app. We will complement this dataset with malware datasets and experiment with applying various statistical techniques to evaluate if we can construct prediction techniques anticipated by our hypotheses.

The big picture

Our focus on deployability and usability underlies all three strands: opening up TEEs to app developers can pave the way for improving security and usability of individual applications by giving app developers the ability to benefit from hardware-based security. If widely deployed platform security mechanisms can be used in innovative ways to meet the security needs of new usage scenarios, the chances of success for such usage scenarios will be improved. On the other hand, a negative result will justify the need for developing new platform security mechanisms. Exploiting lightweight instrumentation to narrow down the pool of devices potentially vulnerable to mobile malware can constitute an effective aid in the search of previously unknown malware.

Acknowledgements

We thank Prof. Sadeghi of the ICRI-SC in Darmstadt for support in establishing this Institute. This addendum is based on contributions and feedback from the extended Intel CRI-SC Team. Contributors include Jian Liu, Petteri Nurmi, Thomas Nyman and Sini Ruohomaa from the University of Helsinki and Bryan McGillion and Elena Reshetova from Intel.