1-1-2015

"The Objectives of this RCEU are to Explore and Analyze the Various Entropic Methods Available on Mobile Devices (Smartphones) and to Analyze the Randomness of the Selected Sources Mixed Together"

Wai Yin Mok
University of Alabama in Huntsville

Proposal: 2015 RCEU Program

Faculty Mentor
Dr. Wai Yin Mok
Associate Professor of Information Systems
308 BAB
256-824-6980
mokw@uah.edu

Project Summary

The objectives of this RCEU are to explore and analyze the various entropic methods available on mobile devices (smartphones) and to analyze the randomness of the selected sources mixed together.

In computing, entropy is the randomness generated by the normal operations of various hardware and software components. It is then collected and often used in cryptographic systems as a source of randomness. While the potential attacker may know how the cryptographic system works, the attacker will not be aware of the specific key that is being used. Thus, entropy from various sources is collected to generate a pseudo-random key. These can then be mixed together to increase randomness. If just one source of entropy was used, the key would be easier to predict. For instance, if the key was only based on the system clock, the range of possible keys would be greatly reduced if the attacker knew approximately when the seed was generated.

Smartphones have many sources of entropy that are readily available such as the GPS, accelerometer etc. The first part of this project would be focused around exploring and searching for other potential sources of entropy. Once several have been selected, these sources will then be analyzed and compared by their measured randomness.

Student Duties

A list of tasks for the prospective student.

- Analysis of hardware and software
- Review of relevant literature
- Implementation of cryptographic protocols
- Mobile programming
- Comparison of random number generators

The student will gain exposure to many of the fundamental concepts of cryptography, information security, and mobile programming. He will get hands on experience learning to program with mobile devices. The student will gain experience using references to solve problems. He will search for and utilize potential sources of entropy. The student will gain experience working on an open-ended project, solving problems as they arise, and in presenting a final product.

Faculty Supervision and Mentoring

The chosen RCEU student will be mentored by Dr. Wai Mok for the duration of the project. The student will meet with Dr. Mok several times a week to discuss questions and progress.

Schedule:

Selection of android device that will be used for testing. This should be done before the research begins.

Exploration of possible sources of entropy to be used. Late May/early June.

Decide which sources will be used. These will be decided based on predicted entropy levels and feasibility of gaining access to these sources. Late May/early June.

Run tests to generate and obtain entropy from these sources. Early June/ late June.

Combine various entropy sources using mixing functions. Late June/ early July.

Compare randomness from singular and mixed sources of entropy. Early July/ late July.

Demonstrate possible use in a cryptographic protocol. Late July/ early August.

Present report on findings.