Improving Crypto: A Novel Smartphone Based Entropy Generator

Friesen, Benjamin

Governments, businesses, financial institutions and individuals have become reliant upon cryptography and encryption to protect their information. McAfee estimates that the cost of cybercrime to the global economy is approximately $375 to $575 billion in annual losses. Much of this is due to weak cryptography. Cryptography consists of four main parts: the encryption algorithm, the implementation, random numbers, and user input. Random number generation is currently the most vulnerable element of encryption which can easily be controlled by a cryptographer. There are two types of Random Number Generators (RNGs): Pseudorandom Number Generators (PRNG), which consist of a deterministic algorithm running on a computer, and True Random Number Generators (TRNG), which rely on hardware and physical phenomena to generate true random numbers. Since TRNGs are non-deterministic, they are considerably more secure than PRNGs. Unfortunately, the lack of easily accessible and free TRNGs prevents them from being used more widely. The goal of this project is to create a free, open source TRNG which runs on an Android phone and generates random numbers by gathering entropy from the phone's sensors, and subsequently hashes it to create a 512 bit digest of the entropy. Once this is created, it can be used by any program requiring high quality random numbers. The TRNG was tested with and passed the entire DieHarder test suite. Statistical analysis performed by DieHarder indicated that the generated numbers were random. Providing this application will greatly enhance the security of personal data and help reduce cybercrime.

Awards Won:

Oracle Academy: Award of $5,000 for outstanding project in the systems software category.