CS 290/190G Project Proposal

Mike Soennichsen - Brian Younan

30 April 2014

Random number generation is a key component of cryptography and obtaining highly randomized numbers is essential to good cryptographic algorithms. Random algorithms that can be predicted can be exploited to break certain cryptographic systems which is why using random and unpredictable number seeds can be essential.

Our project will use a UDOO board to implement a random number generator. We will be using a UDOO specific release of Ubuntu linux to develop. This random number generator will utilize various external inputs (microphone noise, external temperature change, etc.) to seed a random number generator. The RNG implementation will pursue high efficiency as well as an optimally random distribution of generated values.

This project will be written in C++ and use no other random number generating libraries. Using external inputs as “random” data for seeding a random number generator should help to emulate truly random numbers. By doing this, it should be easy for one to obtain pseudo-random values that do not follow any specific predictable pattern which can be used to enhance cryptographic systems.