Introduction

A problem in cyber-security today is the lack of widespread random numbers. Although random number generating algorithms are built into most computer programming languages, these random numbers are not actually random, they are pseudo-random (Haahr n.d.). Random numbers are used often for encryption, for instance two random numbers are used to generate a public encryption key for RSA encryption (Cruise 2014). RSA encryption is the most popular method of encryption in the world and is used to store everything from credit-card numbers to social security numbers. The more random the encryption key is the safer the data is from the malintentioned hackers and criminals looking to sell credit card numbers or commit identity theft. Unfortunately smaller websites that store data may be using sub-par random numbers to protect data (if it is even protected at all)! In order for data to be really safe, every website that stores data should encrypt it using real random numbers. In order to make random numbers it is necessary to have some kind of source of random data that can be converted into numbers in some way or another. In the case of Random.Org that data is atmospheric noise (Haahr n.d.). In some research the random source was cell phone pictures (Zhao 2009).

This should be important to banks, web developers, server administrators, SQL administrators, Government agencies, lawyers or anybody else who keeps confidential data on a computer, doctors, and anybody who has a bank account, an account on a website, a lawyer, one who has been in the hospital, a doctor's office, or a dentist that uses a computer that is connected to the internet. Without encryption an expert hacker could get copies of all kinds of records or credit card numbers from a store’s computer or server system (many examples in the last year i.e. Home Depot, Target, Sony Pictures). In the US there is an average of 28,765 data breaches a year, costing $194 per capita (Ponemon, 2013). That is a total of $5,580,410 a year because of lost data. It is an obvious problem that needs more than one solution, but random numbers are the first step.