Truly Random

Subject: IT-Security / Mobile Computing
Thesis advisor: Prof. Dr. Reto Koenig
Expert: Dr. Federico Flueckiger (Federal Departement of Finance (FDF)

Random numbers are a fundamental part of cryptography. Since the provision of random bits on a computer is rather difficult, external random number generators are rising in interest. Yet most contemporary hardware random number generators are not verifiable by nature since they claim to gather entropy on quantum level. The goal of this thesis was to introduce a concept of a comprehensible and verifiable generator, and to prove its feasibility with a corresponding prototype.

Introduction

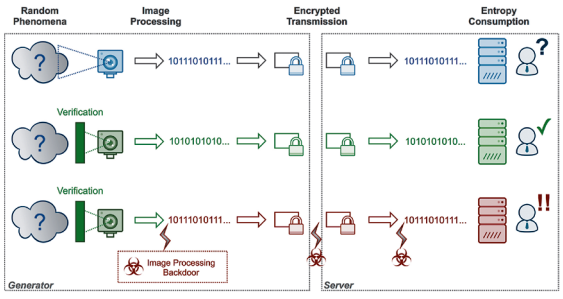
Almost every security mechanism is based on an initial random secret. If an attacker is able to reproduce this secret, even the strongest algorithms become worthless. Up to this day, computers rely on internal system states (e.g. CPU, RAM usage) to derive random numbers for cryptographic use. But with the increase of strong encryption and the advance of virtualization, it has become more and more difficult to provide enough entropy solely from system states.

Verifiability of Random Number Generators

Some companies have become aware of this need for random numbers. There are various hardware based solutions that provide random numbers. Most of them are based on quantum level phenomena such as measurement of photons or electrons. However, these phenomena are not observable by the end user. The user is unable to verify whether the result really is derived from a random phenomenon and not produced by a pseudo random number generator (PRNG) incorporated by an attacker and hence has to trust in a manufacturer, rather than in a system.

Our Approach of Verifiability

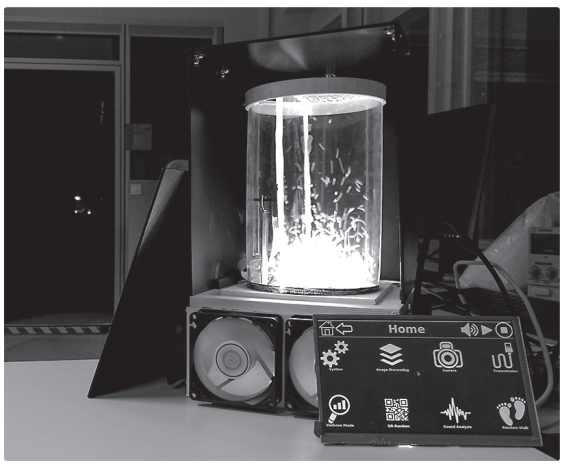
Our goal was to create a concept, that enables entropy accumulation from a comprehensible random phenomenon. By deriving random data using a camera we also enable the end user to verify the random output. By inserting a test module, the user can verify if the output on the generator or on the server corresponds to the expected values. Any changes to soft- or hardware can therefore immediately be discovered.



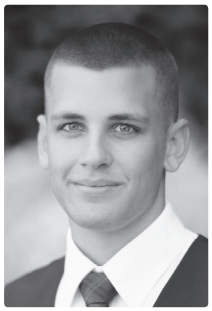
Verifiability of a camera based generator

To put our concept into practice we implemented a prototype.
We used a Raspberry Pi single-board computer to take and process pictures of styrofoam beads in a tube with intense air turbulence. The gained data is then encrypted and transmitted to a server via a USB cable. The server application decrypts the data, checks its validity and uses it to (re-)seed a PRNG of choice, in our case the /dev/random device.

Since we quickly realized that our first prototype relied too much on a specific phenomenon, we decided to open it up for a more general use with any other random phenomena observable by camera. To enable a convenient handling and to provide a safe channel for the initialization, we implemented a graphical user interface.
Functions such as a verbose view, sound output and a random walk enable an easily understandable verification of the produced random data.



Prototype based on styrofoam beads



Matteo Alain Morandi

Tobias Rothen