Analyzing Secure Random Number Generators

001011010011100110101101001010101011010100010110101101010010010101101011101100101100100011010

Brian Carrier
Prof. Samuel Wagstaff

101011010010110101010100100110101001110100101110101001010001010110101000111010101001010110101

- Analyzed 10 SSL & SSH applications.
    - Found SSL bug in Netscape 4.72 and Opera 3.62 web browsers.
- Compared estimated vs. observed entropy values in Entropy Gathering Daemon (EGD) and OpenBSD kernel.
    - Found mixing bug in EGD 0.6.
- Designed tests for estimating the entropy values of system commands
- Analyzed generator designed by Profs. Wagstaff & Atallah, based on quadratic residues. It was implemented by Anya Berdichevskaya.