Analyzing Secure Random Number Generators

Brian Carrier
Prof. Samuel Wagstaff

• 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.