Computer Science Seminar

The Sad History of Random Bits

Dr. George Markowsky, Missouri S&T

April 1, 2019
10:00 - 10:50 am
209 Computer Science Building



In this talk, we examine the history of using random numbers in computer programs. Unfortunately, this history is sad because it is replete with disasters ranging from one of the first pseudo-random number generators, RANDU, being very bad to the most recent efforts by the NSA to undermine the pseudo-random number generator in RSA's BSAFE cryptographic library. Failures in this area have been both intentional and unintentional, but unfortunately, the same sorts of mistakes are repeated. The repeated failures in getting our "random numbers" correct suggest that there might be some systemic reasons for these failures. In this talk, we review some of these failures in more detail and the 2006 Debian OpenSSL Debacle in great detail. This last event left users of Debian and its derivatives with seriously compromised cryptographic capabilities for two years. We also illustrate how this failure can be exploited in an attack. We also modify the concept of a system accident developed in the work of Charles Perrow . We identify some system failures in building pseudo-random number generators and offer some suggestions to help develop PRNGs and other code more securely.

Bio: Dr. George Markowsky is currently Professor of Computer Science at Missouri S&T. He holds an M.A. and Ph.D. in Mathematics from Harvard University and a B. A. in Mathematics from Columbia University. He was Chair and Professor of Computer Science at the University of Maine, a Visiting Scholar at the Rochester Institute of Technology, a Visiting Professor at the Lally School of Management and Technology at RPI, and Manager of Special Projects in the Computer Science Department at the IBM Watson Research Center in NY.

MISSOURI S&T