UNIVERSIDAD
COMPLUTENSE
MADRID

Facultad de Informática

ANUNCIO DE CONFERENCIA
POSGRADO

Great Expectations: A Critique of Current Approaches to Random Number Generation Testing & Certification

Julio César Hernández Castro
University of Kent

Facultad de Informática
Sala de Grados - viernes 26 de abril de 2019 - 18:00
Entrada libre hasta completar el aforo

Resumen:

Random number generators are a critical component of security systems. They also find use in a variety of other applications from lotteries to scientific simulations. Randomness tests seek to find whether a generator exhibits any signs of non-random behaviour. However, many statistical test batteries are unable to reliably detect certain issues present in poor generators. Severe mistakes when determining whether a given generator passes the tests are common. Irregularities in sample size selection and a lack of granularity in test result interpretation contribute to this. This work provides evidence of these and other issues in several statistical test batteries. We identify problems with current practices and recommend improvements. The novel concept of suitable randomness is presented, precisely defining two bias bounds for a TRNG, instead of a simple binary pass/fail outcome. Randomness naivety is also introduced, outlining how binary pass/fail analysis cannot express the complexities of RNG output in a manner that is useful to determine whether a generator is suitable for a given range of applications.

Sobre Julio César Hernández Castro:

Prof. Hernandez-Castro works at the School of Computing at the University of Kent in Canterbury, UK. He has worked on a variety of topics in Computer Security, but recently has focused on randomness generation and testing, and in particular in certification. He has published more than 200 papers in peer-reviewed conferences and journals, has an h-index of 26 and around 3,700 citations (according to Google Scholar).