Computer Science Colloquium

No Secrets: A Brief History of TrueCrypt and the Open Crypto Audit Project

Kenn White

The Open Crypto Audit Project

Wednesday, April 23, 2014
5:30pm – 6:45pm
Petty Building, Room 224

Abstract: In the wake of extraordinary revelations of government mass surveillance, subverting encryption standards, and the widespread compromise of global Internet infrastructure, serious questions arise, in many cases demanding revisiting long-standing assumptions about trust and the very foundations of information security.

In this talk, we will discuss the events which led to a global community-driven public review of one of the most popular open source privacy software packages in use today — TrueCrypt. This is the story of how nearly $70,000 was crowd-funded in just over 2 weeks, and what we are hoping to learn through a formal cryptanalysis and security audit. Finally, what lessons learned can we apply to other critical security infrastructure, including OpenSSL, Linux, and other code that powers the Internet? Please join us for a lively conversation on secrets, trust, and privacy in the digital age.

Speaker Bio: Kenneth White is a principal scientist and senior security research & development engineer at Social & Scientific Systems (SSS), a technical consultancy in clinical research and global health. His work focuses on cloud security, machine learning, and distributed database architecture. At SSS, White led the Biomedical Informatics team that designed and runs the operations center for the largest clinical trial network in the world, with research centers in over 100 countries. Together with Matthew Green, White co-founded the TrueCrypt audit project, a community-driven initiative to conduct the first comprehensive cryptanalysis and public security audit of the widely used TrueCrypt encryption software.

White holds a MEd from Harvard and is a PhD candidate in neuroscience and cognitive science, with research focusing on expert systems, real-time classification and machine learning. He is a technical reviewer for the Software Engineering Institute, and publishes and speaks frequently on computational neuroscience, signal processing, and security engineering. He tweets @kennwhite.