2014/2015 Seminar Series

www.cs.unb.ca/ seminarseries

UNB Faculty of COMPUTER SCIENCE

Fredericton · New Brunswick · Canada

Clinical trials in Computer Security: A first proof-of-concept experiment.

By: José M. Fernandez

Abstract:

The success of malicious software (malware) attacks often depend upon both technical and human factors. Most mass-market and targeted attacks depend on user actions such as clicking on drive-by-download web sites or opening email attachments. In addition, even the most security conscious users are vulnerable to zero-day exploits and even the best security mechanisms can be circumvented by poor user choices. While there has been significant research addressing the technical aspects of malware attack and defense, there has been much less research reporting on how human behavior interacts with both malware and current malware defenses.

To try to shed some light on this issue, we performed at Polytechnique Montreal a 4 month-long field study, conducted in a fashion similar to the clinical trials used to evaluate medical interventions and pharmaceutial drugs. This study involved 50 subjects whose laptops were instrumented to monitor possible infections and gather data on user behavior. Although the population size was limited, this initial study produced some intriguing, non-intuitive insights into the efficacy of current defenses, particularly with regards to the technical sophistication of end users. In this presentation, we will describe the methodology employed, present some of the results obtained and discuss lessons learned from the design and worldwide-first conduct of an experiment of this type in computer security.

Joint work with Fanny Lalonde Levesque, Carlton Davis, Jude Nsiempba (Polytechnique) and Anil Somayaji & Sonia Chiasson (Carleton University)

Bio:

Dr. Fernandez is an associate professor in the Department of Computer & Software Engineering at Polytechnique Montreal. He heads the Laboratory for Information Security Research (SecSI) and his main area of research is computer security. His current research interests include malware, cybercrime, cyber warfare, security of SCADA systems, security product testing methodologies, and security and integration of logical and physical access control systems. He has several years of professional experience as a practitioner of Information Security in both industry and government. He holds Bachelor's degrees in Mathematics and Computer Science and Engineering from MIT, a Master's in Cryptology from the University of Toronto, and a Ph.D. in Quantum Computing from the Université de Montréal.

Wednesday, October 15 @ 4:30 PM

Information Tech. Centre (550 Windsor St.) , ITC 317