Concordia University
ENCS
Engineering & Computer Science

Concordia Institute for Information Systems Engineering

THE CONCORDIA INSTITUTE FOR INFORMATION SYSTEMS ENGINEERING
IS PLEASED TO PRESENT THE FOLLOWING GUEST LECTURE IN OUR CIISE DISTINGUISHED SEMINAR SERIES

Dr. José M. Fernandez
École Polytechnique, Montréal

No Calm after the Storm: A Study of Modern Botnets

In this presentation, we will survey the developments in botnet technology as they have being deployed and employed in the "real world" in the last few years. Of most notable importance and notoriety is the Storm worm that appeared in 2007 and that had all but disappeared by the end of 2008. From a technical and research point of view, it marks the departure from IRC-controlled botnets to sophisticated command and control architectures using a combination of peer-to-peer networking and a network of http servers with fast changing domain names (aka fast flux networks). This has made Storm one of most researched on malware in the last few years. We will present the results of our research on graph theory-based simulations of the P2P networks employed by such botnets and the relative efficacy of various mitigation strategies, some of which were indeed been tested "in-the-wild" against the Storm botnet. We will conclude by discussing more recent developments in botnet technology. Nature abhors a vacuum and Storm has indeed been replaced by other equally sophisticated botnets. In particular we will discuss the Waledac botnet. We will discuss its similarities and differences with the good ol' Storm, and its relative strengths. We will close by discussing the various options that are available and viable, to both researchers, industry and law enforcement, to try to mitigate and counter this threat.

Biography: José M. Fernandez is an assistant professor in the Department of Computer & Software Engineering at the École Polytechnique de Montréal. He completed his Ph.D. work in Quantum Computing in 2004 at the Université de Montréal, and obtained his M.A.Sc. on the topic of Theoretical Cryptography at the University of Toronto in 1993. In between those, he worked in industry and for the public sector as a software developer & project manager, information security analyst, and system manager. He currently directs the SecSI Research Lab at the Ecole Polytechnique, where his research interests concentrate on performance analysis of security solutions through both theoretical modeling and simulation and as-realistic-as-possible laboratory experiments. Work by members of the lab in the last few years has covered Intrusion Detection Systems, Malware reverse-engineering and performance analysis including botnets, Denial-of-Service attacks, and security in ad-hoc mobile networks and other trust management systems.

Thursday, November 26, 2009

16:00 – 17:00

EV003.309