UCF Stands For Opportunity

THE DEPARTMENT OF ELECTRICAL ENGINEERING AND COMPUTER SCIENCE, CS DIVISION

Presents the Fall 2013 EECS Seminar Series

Dr. Daniela Oliveira

Bowdoin College

“Secure and Holistic Coexistence with Kernel Extensions – A Immune System Inspired Approach”

Friday, October 18, 2013 • 11:00 a.m. • HEC 450

Abstract

Kernel extensions, especially device drivers, make up a large fraction of modern kernel code bases (approximately 70% in Linux). Most extensions are benign and represent a convenient approach for extending the kernel functionality and allowing a system to communicate with an increasing number of complex and diverse I/O devices. A small fraction of kernel extensions are malicious (rootkits) and pose a threat to kernel integrity. From a security viewpoint this situation is paradoxical: modern OSes depend and must co-live with untrustworthy extensions. Our immune system faces the exact same challenge every day: our body is made of a large number of bacteria which are mostly benign and also carry out critical functions for our physiology. However, a small fraction of them pose a threat to our body as they can cause pathologies. The immune system has evolved so that is can maintain an homeostatic relationship with our microbiota by implementing two approaches in controlling the interactions of bacteria and our organism: (i) minimizing contact between bacteria and cell surfaces and (ii) confining penetrant bacteria to certain sites. Challenging the current paradigm for OS protection that advocate leveraging only the hypervisor layer to defend the kernel for considering it vulnerable and without resources to defend itself, this talk advocates that modern OS kernels, like our immune system, should play an active role in maintaining healthy interactions with its extensions. In this talk I introduce a proof-of-concept prototype leveraging this paradigm using an x86 emulator as the hypervisor layer and Linux as the guest OS and show how the immune-system inspired approach successfully minimized kernel extensions interactions with original kernel code and data segment, preventing compromise.

Biography

Daniela Oliveira is an Assistant Professor of Computer Science at Bowdoin College in Brunswick ME. She received her PhD in Computer Science from the University of California at Davis, where she specializes in computer security and operating systems. Her current research focuses on employing virtual machine and operating systems collaboration to protect OS kernels. She is also interested in understanding the nature of software vulnerabilities. She is the recipient of the NSF CAREER Award 2012. She is on sabbatical at UCF this year being hosted by Prof. Cliff Zou.

DEPARTMENT OF ELECTRICAL ENGINEERING & COMPUTER SCIENCE