Electrical & Computer Engineering Seminar

"System Support for Rapid Recovery and Attack Resistance"

Abstract

We propose a system to provide resistance to attack and rapid recovery from viruses, worms, problematic system updates, and other negative system changes. Our system uses two key techniques: isolation and intrusion detection. First, for isolation, we collect user data in a file system virtual machine (FS-VM) so that system corruption does not automatically compromise it. We also isolate groups of applications from each other by placing them into virtual machines, called virtual machine appliances (VMAs), so that we can place stronger limits on their behavior. User data is exported to the VMAs by the FS-VM as needed. Second, for intrusion detection, we incorporate a standard network intrusion detection system (NIDS) and firewall into a special network virtual machine (NET-VM) as well as integrate file system access controls into the FS-VM. To support both isolation and intrusion detection, we design a VMA contract system that is used to define the acceptable behavior of each VMA in terms of network and file system access requirements as well as any device access or system resource limits. The NET-VM enforces the network-based VMA contract rules and the FS-VM enforces the file system-based VMA contract rules. We add support for our system into a modern, low overhead, open source virtual machine monitor (VMM), namely the Xen hypervisor. We discuss the design, implementation, and evaluation of our proposed system. Evaluation of our system will be both in terms of performance costs and effectiveness against various real world attacks.

Todd Deshane
PhD Candidate, Engineering Science
Clarkson University

Thursday, September 27, 2007
CAMP, Room 177
4:00 P.M.