

EXAMIN: Tools for Malware Incubation

Steve Brueckner Greg Durrett Hajime Inoue
ATC-NY
Ithaca, NY
{steve, gdurrett, hinoue}@atc-nycorp.com

September 7, 2007

Governments and other large organizations rely on enormous quantities of software. Software is primarily obtained from outside and only customized or integrated. Organizations cannot obtain or do not have the expertise to audit this software for backdoors or other malicious features.

Our goal with EXAMIN is to develop a set of tools that allows organizations to test their software by deploying it virtually before deploying it on real systems with real data. The environment appears real to the untrusted software, and allows investigators to inspect its behavior and internal state. Because our environment is hosted in virtual machines and connected to virtual networks, malicious software is unable to escape.

EXAMIN consists of a hypervisor, a tool for configuring and deploying a set of virtual machines and connecting them in virtual networks, a set of virtual machine “honey-pots” for luring malicious code to reveal itself, and introspection libraries and applications for monitoring the untrusted application.

Using a hypervisor allows us to short-circuit the “lowest hook” arms race involved in putting malware detection in the OS. It also allows us to inspect the internal state of the guests’ OS and even their applications without modifying their internal state.

We have completed portions of the virtual machine and network design tool, and have some proof-of-concept tools for introspection. The introspection library allows us to extract the process and module lists for guest Linux kernels. We have also written a utility that notifies us when portions of memory have changed. We can therefore detect when the system call table or other sensitive data structures have been modified.

Although others have demonstrated prototypes for paravirtualized guests, ours is the first effort aimed at hardware-assisted VMs and the first for production use.