Cory Bryan

SE4930

December 13, 2011

Article Summary 1

Summary of “Sandboxing and Virtualization: Modern Tools for Combating Malware”

“Sandboxing and Virtualization: Modern Tools for Combating Malware”, written by Chris Greamo and Anup Ghosh, discusses current methods used in software to protect the system from malware infections. According to the article, only 19% of new malware is detected by antivirus software on the first day after the malware is discovered, and only 61.7% is detected after 30 days. This clearly shows that antivirus software alone isn’t enough to protect a system from malware, and other techniques are needed. The techniques described in this article are sandboxing, partial virtualization, full virtualization, and secure virtualization.

Sandboxing is a technique that is increasing in popularity for applications that have been historically known to have many security flaws, such as web browsers and Adobe Reader. In this article, the authors use Chrome as their primary sandboxing example. Sandboxes are usually applied to program components that are heavily targeted by malware writers, and can require significant architectural changes to existing software. Chrome’s sandbox encapsulates the browser’s rendering engine, where most browser exploits are targeted. All other parts of Chrome exist within a browser kernel process, which the rendering engine communicates with to write outside the sandbox. Sandboxes are vulnerable to kernel vulnerabilities and attacks which trick the user into installing software.

Partial virtualization is only briefly described. It encapsulates an entire process in a sandbox. The process is limited in what permissions it has, and is provided with a virtual file system. This technique is also vulnerable to kernel exploits.

Full virtualization virtualizes hardware and resources to run an operating system under a virtual machine. This technique can either run directly on the hardware in a bare metal configuration, or can run as a process on a host OS. Malware that infects a guest OS is contained within the VM, and even kernel exploits are contained, unlike in sandboxing and partial virtualization. Secure virtualization is an extension to full virtualization which adds network isolation, real-time attack detection, fast recovery, forensic data collection, and hypervisor integrity checks.

From this article I learned about various techniques to protect an operating system from malware and application exploits. I learned the most from their section on sandboxing, especially the fact that it would be easier to design an application with sandboxing in mind, rather than add it later. This is good to know for my own software development, and is something that should be researched better when the opportunity to use it comes.

Source:

Greamo, Chris, and Anup Ghosh, "Sandboxing and Virtualization: Modern Tools for Combating Malware," IEEE Security and Privacy Magazine, March/April 2011; http://www.computer.org/csdl/mags/sp/2011/02/msp2011020079.html.