Using Collaboration between an Operating System and a Virtual Machine to Prevent Keylogger Attacks

Victor Wong, Class of 2013

My research project over the summer was mainly focused on stabilizing and improving the collaboration system between an operating system and a virtual machine (OS-VM). The OS-VM collaboration detects possible keyloggers from the system by tracking bytes of information from the network, when instructions containing these bytes attempt to modify sensitive data structures, the system will stop the attempt and flag the network source.

One problem with the system previously was that it would crash at random; upon investigation, it was due to a race condition generated from using software interrupts to communicate between the OS and VM. After locking the sensitive variables during the series of OS-VM communications, the crashes ceased to appear. A stable disk image containing all the modifications for the operating system was also created for a safe state.

The second part of the project consists of researching different approaches that keyloggers use in order to infect a system. First of all, I have written a simple keylogger that intercepts key strokes from the kernel level method receive_buf in order to observe the system’s tracking process. When the keylogger module was written from scratch within the virtual machine, the system detects the “suspicious” activity but does not stop it as the module does not contain any bytes from the network. However, if the same file was sent in from an outside source, the system will flag and stop the module during the installation.

One of the findings during this fellowship is a keylogging method that has not been covered by the OS-VM collaboration; attackers can insert a new keyboard handler which acts in parallel to the existing handler through system calls that are not “suspicious”, such that the current security system does not detect these types of intrusions. After this discovery, the kernel function used for this exploit (the request_irq() method) is also added to the list of “suspicious” activities.

Faculty Mentor: Daniela Olivera

Funded by the Maine Space Grant Consortium Fellowship