Kindsicher: Safe-Browsing for Children at Home

Project Status

Chaitanya Achan, Philip Lundrigan, and Christian Schreiner

November 7, 2014

Infrastructure Setup (Christian)

The physical network wiring along with the routers and switches necessary to support the project has been completed. The server hardware is running and has passed initial reliability tests.

Upcoming tasks
Complete server software installation and the design of the SNISR extensions.

IDS setup and evaluation (Phil)

I am working on the filtering portion of this project. This has involved configuring Snort and getting familiar with it. I have been reading through the Snort manual so that I can understanding the necessary Snort configuration settings. The idea is to use Snort as a way of blocking TCP connections to unauthorized IP addresses. From my initial testing, Snort seems to be too slow to block all connections. For long TCP connections (such as downloading a picture), Snort works. For short TCP connections (such as downloading HTML for a website), Snort is too slow to react to block the connection.

My goal for last week was to have Snort figured out and blocking connections to IP addresses, which I have not completed yet. I was not expecting Snort to have problems with blocking the connection. I have had to do some digging around to see what is going on, such as looking at Wireshark traces.

Upcoming tasks
For next week, I plan on figuring out why Snort is not responding quick enough. It might be a configuration error on my part, the computer I am running Snort on might not be fast enough, or it could be that Snort is not able to do what we need it to do. If that is the case, I will look into other options for blocking TCP connections.

Reporting setup and evaluation (Chaitu)

I have been looking at understanding BASE, which is a graphical interface to display the logs generated by the Snort IDS. I installed Snort, BASE and other related software on my Linux VM and have got these to work together. I had to make some adjustments to the Snort alert rules so that HTTP transactions show up in the BASE reports.

Upcoming tasks

As a next step, I will be looking at getting domain names from the IP addresses of the visited websites in the BASE reports. Going forward, we need to use Snort and BASE to build our whitelist of websites.