Contribution ID: **47** Type: **Presentation**

Grid Network Accounting for Incident Response

Description of the work

It would be useful to better log the network flows and connections through our firewall for, amongst other reasons, to be able to respond more confidently to CSIRT advisories, that often ask to check for connections to/from a given IP address.

Grid service administrators may not have administrative access to switch or router equipment in their hosting environment that can record such information (using netflow or sflow).

A solution should be installable by grid site administrators on the hosts / vms / firewalls they control.

For logging / probe solutions that run on firewalls it is important that the monitoring does not significantly degrade the throughput or latency of the system.

A key requirement is that logs should be relatively compact. For instance, full iptables plain-text logging of all packets would require significant storage.

In general, grid sites may not have funding to purchase commercial network traffic logging and analysis hardware or software, and as mentioned above the grid site administrators may not have administrative access. If it is available at a site it can of course be used, but we assume that a site
wishes to implement a low-cost software-based solution.

Probes, repeaters, and tunnels should be configured securely to avoid tampering.

There are a variety of options
* iptables rules with rate limiting
* traffic analysis software such as ntop
* software based probes such as fprobe, nprobe, softflow, argus.

The approach is to install network probes on firewalls or vm hosts controlled by grid site administrators and to feed the output to collectors which store the flow data. Various tools can be used to visualise and search the stored data.

For NGI-wide deployment, probes need to send flow data through secure tunnels to a central collector.

Issues include simplifying deployment of probes and collectors and evaluation of the performance impact.

Wider impact of this work

The aim of this work is to describe a usable method of network logging to better equip grid sites and NGIs of all sizes (and sites in similar distributed infrastructures) to respond to network security incidents.

Printable Summary

Grid infrastructure providers and research communities run distributed Computer Security Incident Response Team functions, which coordinate incident response on a global scale. Unfortunately, international research collaborations can provide a path for security incidents to propagate easily.

To make use of network information from investigations grid sites must record network activity in sufficient detail. Firewall logs provide partial records of network activity. Network administrators can make use of logging facilities provided by routers. However, grid sites may not have direct access to such facilities and so need a solution that can record traffic efficiently in terms of network performance, storage space, and search.

We describe the use cases for network logging in the grid CSIRT context; we explore several approaches and related work in this area; we describe a deployment of our chosen solution at NGI scale; we evaluate the solution in practice; and provide recommendations.

Primary author: O'CALLAGHAN, David (TCD)

Co-author: KENNY, Stuart (Trinity College Dublin)

Presenter: O'CALLAGHAN, David (TCD)

Track Classification: EGI Operations (Tiziana Ferrari: track leader)