SAND2017-7565C

The Center for Cyber Defenders

Expanding computer security knowledge

Artificial Network Traffic Generation

protonuke as a Tool to Support Industrial Control Systems

Mel Savich, University of Michigan
Computer Science, B.S. - Women's Studies, B.S.

Project Mentors: Derek Hart, Org. 5824 and Casey Glatter, Org. 5828

Overview

SCEPTRE uses phēnix to orchestrate creating, configuring, and launching ICS (Industrial Control System) experiments. phēnix is responsible for taking a network description and supporting configuration files and converting them to a format that can be read and deployed by a deployment service (e.g. minimega).

protonuke

protonuke is a simple, standalone, configuration-less traffic generator for IP networks. It supports four protocols:

- http
- https
- ssh
- smtp

In addition, protonuke also has servers for each of the protocols provided, and it can act as either server or client. protonuke servers do not require protonuke clients, and protonuke clients do not require protonuke servers.

Objective

Integrate protonuke into phēnix as an additional application that can be used in experiments.

Approach

Integrating protonuke required two tasks:

- creating a protonuke topology
- creating the protonuke application itself

topology

To build an experiment in phēnix, a network must be defined. The network definition is described in a set of files known as a topology. The following is a sample of a protonuke topology:

BPV_csv.EmulyticsServerHostBaseSpec.csv — UNREGISTERED

BPV_csv.EmulyticsServerHostBaseSpec.csv

```
1  HostName,InterfaceName,IPaddress,SubnetMask,DefaultRoute,OS_Type,ActiveDirectory,Exchange
2  protonuke_server_1,IF0,10.10.10.10,255.255.255.0,Auto Assigned,,,
3  protonuke_client_1,IF0,10.10.10.11,255.255.255.0,Auto Assigned,,,
4  protonuke_client_2,IF0,10.10.10.12,255.255.255.0,Auto Assigned,,,
5  protonuke_client_3,IF0,10.10.10.13,255.255.255.0,Auto Assigned,,,
6  protonuke_client_4,IF0,10.10.10.14,255.255.255.0,Auto Assigned,,,
7  protonuke_client_5,IF0,10.10.10.15,255.255.255.0,Auto Assigned,,,
8  protonuke_client_6,IF0,10.10.10.16,255.255.255.0,Auto Assigned,,,
9  protonuke_client_7,IF0,10.10.10.17,255.255.255.0,Auto Assigned,,,
10
```

Line 1, Column 1 | Tab Size: 4 | Plain Text

application

Creating an application for phēnix requires implementing four different modes:

Mode	Method Override	When code executes	Used for?
Configure	phenix.apps.base.configure()	During the phēnix create phase	Modify an experiment database (e.g. change a VM's operating system/number of processors/memory/base KVM image, add a configuration file for injection, add a new VM to an experiment)
Start	phenix.apps.base.start()	During the phenix start phase	Create/generate any files that need to be injected into the VMs (e.g. network interface files, start scripts, user application config files)
Post-start	phenix.apps.base.post_start()	Immediately after an experiment has been started	Execute code that requires information from a running experiment (e.g. get experiment start time or VLAN ID numbers, set up mirror ports on OVS switches)
Cleanup	phenix.apps.base.cleanup()	Immediately after an experiment has been stopped	Execute code that is required for cleanup (e.g. remove mirror-ports on OVS switches)

In regards to protonuke, only Configure and Start were necessary to implement.

Result

The protonuke application currently supports Ubuntu images. A user is able to create an experiment with the protonuke application and specify how many servers/ clients they want in their experiment.

Future Goals

The next steps for protonuke application development include:

1) support for other operating systems
2) compatibility with other phēnix applications

Sandia National Laboratories

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND2017-XXXXC.

U.S. DEPARTMENT OF ENERGY | NNSA National Nuclear Security Administration