Cpr/SE 491 Weekly Report **MAY15-06 Week 12 (11/15/14-11/21/14)**

Advisors: Joseph Zambreno **Client:** Curtis Schwaderer (IP Fabrics, Inc)

Members (roles):

Altay Ozen (Team Leader and Team Key Concept Holder)
Andrew Heintz (Team Communication Leader)
Abraham Devine (Team Webmaster)

Project Title: Network Forensics User Interface

Individual Contributions (this week)

Names	Time Spent	Date Finished	Details of Task	How it got Completed	Why is it Important
Altay Ozen	8	11/20	Finished writing pusher and raw collector inside of Xplico	Finished writing code for listening to port, forwarding pcaps to Xplico, and writing to archive directory	Pusher is going to be part of Xplico in the long run
Andy Heintz	2	11/15	Fixed and modified Perl Pusher script	Modified to archive pcaps and fix bugs	Perl was temp solution until C Pusher is finished
Andy Heintz	5	11/20	Tried to fix problems with installing Xplico after building it	Traced through PHP and C code to find what is broken	Xplico may need modifications, and thus need to be built from its source code
Abe Devine	2.5	11/20	Tested Pusher script with new changes	Ran scripts with pcaps from client	Pusher script transfers traffic from DeepSweep to Xplico
Abe Devine	2.5	11/20	Figured out scripts for Xplico startup and session_mng scripts	Examined scripts in text editor	Necessary to start Xplico with the correct script; session_mng can push pcaps into Xplico

- Fixing Perl Pusher Script
    - Perl variables start with $ and can occur in strings, so escape $ signs
    - Output from backticks commands has new lines, so call chomp
- Modifying Perl Pusher Script
    - Pcaps are moved to $HOME/ArchivedPcaps after upload
    - If unable to connect to Xplico, the file isn't moved

- Using Xplico Pusher
    - Xplico can push pcaps into itself using session_mng.pyc
    - Requires the case and session name to import
- Using C Collector
    - Currently contains code for Pusher – Will remove this
    - Requires Deepsweep port, Xplico port, Archive directory, Interface name

- Debugging CakePHP
    - Need to change Configure::write('debug', 0); in core.php
    - Call debug function - debug($var, $showHtml, $showFrom)
- Installing Xplico After Building Source
    - Installation doesn't create pol_1, pol_2, etc. directories or install their files
    - Dema program requires these files to store data

Total contributions for the project

Andrew Heintz (97 hrs)

Altay Ozen (95.5 hrs)

Abraham Devine (51.5 hrs)

Weekly Summary

- Fixed, modified, and tested Perl Pusher script
- Finished writing Pusher/Collector in C
- Figured out session_mng.pyc and Xplico startup script
- Worked on problems with installing Xplico

Meeting Notes:

11/7 Adviser Meeting

Duration: 30 min **Members Present:** All

- Demoed latest version of programs
  - Perl script for running session_mng.pyc
  - C Collector/Pusher for collecting and pushing raw traffic
  - Difficult for GUI to obtain interfaces for Collector
- Discussed options for installing Xplico
  - Best idea is to install Xplico and then copy PHP files
  - C Collector would be separate program
- Discussed upcoming presentation
  - Good idea to have about twelve slides
  - Don't get too technical that you can't answer questions

11/7 Group Meeting

Duration: 180 min **Members Present:** All

- Discussed remaining tasks for semester
  - Need to finish final versions of document
  - Discussed changes to documentation
  - Need to put together presentation slides
  - Contact client – Invite to presentation and set up meeting
  - Will pull together demo of current scripts/programs
- Discussed revisions to design
  - Start-up script is /etc/init.d/xplico
  - C Collector will be built and run separate from Xplico
  - Replace Pusher scripts with calling session_mng.pyc
  - Changed start button location to Session page

Pending Issues

- Issue 1: Xplico Importing
  - Xplico cuts pcaps off at defined point
  - Xplico may not piece data together correctly
  - Will create tests specifically for testing this

- Issue 2: Determining Interface
  - C collector for raw traffic requires an interface
  - Eventually, this will be started from the PHP GUI
  - Not certain how to obtain list of interfaces

Plans for Next Week

- Tasks for Andy
  - Revise for final version of documentation (6 hours)
  - Work on presentation slides (4 hours)
  - Fix install and try to copy PHP files over (2 hours)

- Tasks for Altay
  - Work on presentation slides (4 hours)
  - Work on removing Pusher code from C Collector (2 hours)
  - Test session_mng.pyc with C Collector (2 hours)

- Tasks for Abe
  - Work on presentation slides (4 hours)
  - Add error checking to session_mng.pyc script (2 hours)
  - Fix paths to PDFs on web site (negligible time)
  - Work on learning basics of PHP (2 hours)

Assignments for Slides

PROJECT PLAN (~5 slides)

Problem Statement (Abe)
Functional Requirements (Altay)
Non-functional Requirements (Abe)
Potential Risks & Mitigation (Abe)
Project Milestones & Schedule (Andy)

SYSTEM DESIGN (~5 slides)

Functional Decomposition (Abe)
Detailed Design (module diagram/description) (Altay)
User Interface (Andy)
Resources/Languages/SW Specifications (Altay)
Test Plan – simulation, what tests, what metrics, hypothesis, etc. (Andy)

CONCLUSION (~3 slides)

Current Project Status with respect to milestones (Altay)
Task Responsibility/Contributions of each project member (Everyone)
Plan for Next Semester (Andy)