Cpr/SE 491 Weekly Report **MAY15-06 Week 10 (11/1/14-11/7/14)**

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	4	11/5	Figured out filtering in jnetpcap	Wrote example code and tested it	Jnetpcap library will be used for the new Java collector
Altay Ozen	3.5	11/6	Experimented with TCP replay	Ran it with pcaps from client using various options	TCP replay allows us to get raw traffic for testing from pcap files
Andrew Heintz	8	11/6	Studied Xplico's PHP code	Browsed code and used grep / find to locate specific terms and files	Xplico will be extended to add new functionality for the client
Abe Devine	2	11/6	Uploaded web site to server	Used SFTP with Filezilla to transfer files	Web site is a required part of this course
Abe Devine	3.5	1/6	Tried to setup complete system for testing	Attempted to install Virtualbox and Kali OS	Need to setup OS for testing project

- Xplico General Notes
  - PHP uses CakePHP libraries (www.cakephp.org)
  - CakePHP is structured based on MVC
  - Netbeans has plugin for CakePHP
  - Database for Xplico is DboSqlite3
- Xplico Directories
  - PHP code is located in system/xi2
  - CakePHP libraries are in system/xi2/cake
  - Xplico code is in system/xi2/app
- Changing Xplico
  - Need modify user_controllers.php and maybe login.ctp
  - Will need rebuild Xplico - http://wiki.xplico.org/doku.php?id=building
  - Need figure out PHP's system library - http://php.net/exec
  - Could put Pusher into Xplico - Wouldn't have to rewrite it for Java

- jNetPcap Filtering Notes
  - Library listens to all ports and interfaces by default
  - Filtering limits what the library listens to
  - Uses TCPdump syntax for filtering expressions
- TCP Replay Notes
  - Replays traffic by sending them to the original destination
  - Can loop replay – Sends it specified number of times
  - Don't want to send it to original destination
- Redirecting TCP Replay
  - Solution 1: Listen to entire lo (local loopback) interface instead
  - Solution 2: Use encapsulated traffic – Forces it to specified port
  - Solution 3: Use netcat instead – Can specify IP and port

Total contributions for the project

Andrew Heintz (82 hrs)

Altay Ozen(78.5 hrs)

Abraham Devine (38.5 hrs)

Weekly Summary

Worked on jNetPcap examples
Experimented with TCP replay for testing
Studied Xplico's PHP code
Uploaded the web site to ISU server

Meeting Notes:

11/7 Adviser Meeting

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

- Summarized last week's client meeting
  - Discussed why client wants Java collector
  - Discussed solutions for testing
  - See last week's report for more info
- Summarized what Altay worked on
  - Discussed how filtering works for jNetPcap
  - Discussed how we will use TCP Replay
- Summarized what Andy worked on
  - Discussed structure of Xplico's web GUI
  - Discussed implementing Pusher as part of Xplico
- Summarized what Abe worked on
  - Discussed status of web site
  - Discussed issues with getting Kali setup

11/7 Group Meeting

Duration: 120 min **Members Present:** All

- Discussed how to redirect TCP replay
  - Solution 1: Listen to entire lo (local loopback) interface instead
  - Solution 2: Use encapsulated traffic – Forces it to specified port
  - Solution 3: Use netcat instead – Can specify IP and port
  - Will test both solution 1 and solution 3 this next week

- Reviewed our web site
  - Uploaded weekly reports from last couple weeks
  - Will update with project plan and design document this week

- Discussed CakePHP and Xplico
  - PHP uses CakePHP libraries (www.cakephp.org)
  - CakePHP is structured based on MVC (model-view-controller)
  - Pusher could be implemented in PHP as part of Xplico
  - Instructions for rebuilding Xplico aren't clear

- Reviewed progress on this semesters' tasks
  - Need some further testing on collecting traffic
  - Modifying Xplico appears to be feasible for this semester

Pending Issues

- Issue 1: Testing Complete System
  - Client will be providing pcaps for testing
  - Will use TCP replay to get raw traffic from pcaps
  - Allows us to simulate system without hardware

- Issue 2: Xplico Importing
  - Collector cuts pcaps off at arbitrary point
  - Xplico may not piece data together correctly
  - Will create tests specifically for testing this

- Issue 3: Check if File is Finished
  - Collector may write to file in real-time
  - Pusher script needs to check if Collector is writing
  - Will create tests specifically for testing this

Plans for Next Week

- Tasks for Andy
  - Modify Xplico to call Pusher script (6 hour)
  - Request repository from source.ece.iastate.edu (negligible time)
  - Build Xplico with changes and test if time (2 hours)

- Tasks for Altay
  - Figure out how Xplico handles importing pcaps-over-ip (4 hours)
  - Testing TCP replay with jNetPcap library (2 hours)
  - Reroute raw data directly to Xplico via netcat (2 hours)

- Tasks for Abe
  - Upload design document and project plan (2 hours)
  - Test all Pusher scripts with pcaps from client (6 hours)

Long Term Plans

Test Pusher script together with Go Collector and Xplico
Modify Pusher script to handle error conditions
Test entire system (DeepSweep Hardware, Collector, Pusher, Xplico)
Demo entire system to client (before Thanksgiving, possibly)