Cpr/SE 491 Weekly Report **MAY15-06 Week 8 (10/18/14-10/24/14)**

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

Weekly Summary

Wrote prototypes of Pusher script in Perl and Python
Wrote 1st draft of design document
Revised and proofread the design document

Individual Contributions (this week)

Names	Time Spent	Date Finished	Details of Task	How it got Completed	Why is it Important
Altay Ozen	7	10/23	Wrote assigned sections of design document	Typed parts of design document in Word	Design document is necessary to determine our project' s design
Andy Heintz	3.5	10/20	Wrote Pusher script prototypes	Wrote sample scripts in Perl and in Python	Pusher is one of our project's major components
Andy Heintz	6.5	10/23	Wrote assigned sections of design document	Typed parts of design document in Word	Design document is necessary to determine our project's design
Andy Heintz	4	10/23	Revised and Proofread the design document	Reworked testing / prototype sections; Created diagram for functional decomposition	Design document is necessary to determine our project's design

Abe Devine	2	10/23	Wrote assigned sections of design document	Typed parts of design document in Word	Design document is necessary to determine our project' s design
Abe Devine	2	10/23	Created diagram of DeepSweep's functionality	Created diagram using Pencil	Part of previous week's task for examining DeepSweep code

Outline of Pusher Script

- Starts Xplico, so data can be uploaded to its database
- Starts Collector, which will listens to a port and sends data to a pcap
- Searches directory for all pcaps and uploads to Xplico

Total contributions for the project

Andrew Heintz (66 hrs)

Altay Ozen(60 hrs)

Abraham Devine (25.5 hrs)

Meeting Notes:

10/24 Adviser Meeting

Duration: 60 min **Members Present:** All

- Discussed details of Pusher
  - Explained what the Pusher script does (see above)
  - Xplico will start Pusher script via a button
- Discussed why Go Collector needs replacing
- Discussed the format of the ber file
  - Look for ASCII character sequences in file
  - DeepSweep manual might contain more information
- Discussed scheduling meeting with client and forms
- Asked Zambreno for a mid-semester assessment
  - Project is difficult to understand
  - Should work more on communication

10/24 Group Meeting

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

- Discussed whether to split Pusher into separate Handler script
  - Pro: Easier to maintain if Pusher arguments change
  - Con: Extra unnecessary script; Script may be phased out in Phase Two
  - Solution: Postponed to decide at a later point

- Discussed whether to replace Pusher script with Java module (Phase Two)
  - Pro: Less separate components, since it will be built with Collector and Convertor
  - Con: Extra work needed to rewrite and retest existing script
  - Solution: Will rewrite it – Advantage of fewer components outweighs extra work

- Discussed which language to use for Pusher script (Phase One)
  - Perl: Easy to call command line and use regex
  - Perl: May not run on every system and limited OOP
  - Python: More modern / OOP language
  - Python: May not run on every system
  - Bash: Runs on all systems and easy to call command line
  - Bash: Not OOP and limited libraries
  - Solution: Scripts are short, so we can write prototypes in all three
  - Solution: Will probably settle on Perl for immediate testing

Pending Issues

- Issue 1: Testing Uploading Pcaps
  - Limited ability to test uploading of pcap files created by Go Collector
  - Sample .ber file only has IP packets, so Xplico can't display anything
  - To test that our system works properly, we will need more .ber files

- Issue 2: Testing Complete System
  - No ability to test complete system from start to finish
  - Need a DeepSweep device – Could be running out in Oregon
  - Immediate access isn't needed, but ideally by mid-November

- Issue 3: Running System On Other Platforms
  - Xplico and/or Pusher may run different on other Linux distributions
  - Check with client which distributions it needs to run on
  - Test it on major distributions (e.g. Ubuntu, Red Hat, etc.)

Plans for Next Week

- Tasks for Andy
    - Revise design document and project plan (Andy, 4 hours)
    - Request repository from source.ece.iastate.edu (Andy, negligible time)
    - Try extending Xplico to add button (Andy, 4 hours)

- Tasks for Altay
    - Convert Perl script to bash script (more general option) (Altay, 2 hours)
    - Look DeepSweep manual and ber file using sequence (Altay, 2 hour)
    - Schedule meeting with client for next week (Altay, negligible time)
    - Install/Use jNetPcap libraries from http://jnetpcap.com (Altay, 4 hours)

- Tasks for Abe
    - Upload web site to designated space and update it (Abe, 2 hours)
    - Install/Use jNetPcap libraries from http://jnetpcap.com (Abe, 4 hours)
    - Test importing of new ber files from client (Abe, 2 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)