Cpr/SE 491 Weekly Report **MAY15-06 Week 9 (10/25/14-10/30/14)**

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

Finished revising design document for version 1
Worked on revising project plan for version 2
Installed and experimented with jnetcap library

Individual Contributions (this week)

Names	Time Spent	Date Finished	Details of Task	How it got Completed	Why is it Important
Altay Ozen	2	10/27	Wrote Pusher script prototype	Wrote sample script in Bash	Pusher is one of our project's major components
Altay Ozen	9	10/30	Experiment with jnetpcap library	Installed it, read documentation, and created install instructions	Jnetpcap library will be used for the new Java collector
Andrew Heintz	8	10/27	Revised Design Document and Project Plan	Reviewed each document and corrected errors and discrepancies	Both documents documenting the project's progress and design
Abe Devine	4	10/30	Experiment with jnetpcap library	Installed it and wrote some code	Jnetpcap library will be used for the new Java collector
Abe Devine	3.5	10/30	Look into Ber file formats	Researched converting Ber files to Pcaps	Ber files may be the output from DeepSweep

- Jnetpcap library notes
    - Library accepts raw traffic, but not ASN.1 format
    - Therefore, Java collector not necessary unless we use ASN.1
    - Setting network filters done by strings with tcpdump syntax

- Design Document changes
    - Added system requirements (based on functional requirements in Project Plan)
    - Added software design (based on system diagram/description in Project Plan)
    - Expanded testing section a bit and added an image of reports

- Project Plan changes
    - Updated project schedule and added more detail for 2nd semester
    - Updated a number of sections to match design specified in the design document
    - Added risks specific to our project (per Zambreno's recommendation)

Total contributions for the project

Andrew Heintz (74 hrs)

Altay Ozen(71 hrs)

Abraham Devine (33 hrs)

Meeting Notes:

10/31 Client Meeting

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

- Client would like to eliminate step of creating pcaps
    - Determine when streams end and cut off pcaps at that point
    - Current collector creates pcaps when finished collecting
    - ASN.1 contains start/stop indicators for streams

- Reasons client wants Java collector instead of Go collector
    - Java collector moves closer to real-time processing
    - Go collector requires extra modules; Java collector won't

- Provisioning DeepSweep remotely isn't problem
    - Feeding it data from mail client in real-time is more difficult
    - Could use TCP replay on pcaps = Simulate sending of traffic

- Need to make sure we import the entire file
    - Collector creates files and adds data in real-time
    - Collector arbitrarily cuts off files every 100 MB
    - Xplico may not be able to piece data together

10/31 Group Meeting

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

- Discussed how to test Pusher scripts
  - Will test all 3 prototypes if we have time
  - Priority will be on testing Perl Pusher
  - Made minor fixes to regex and scripts

- Discussed tasks to be done by Thanksgiving
  - Goal is connect and test entire system
  - May modify Xplico to start system if time

- Discussed next steps after meeting with client
  - Priority is testing Pusher scripts with pcaps
  - Next priority is testing system with raw traffic
  - Will investigate how hard modifying Xplico is

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
    - Investigate how Xplico imports things (Andy, 4 hours)
    - Request repository from source.ece.iastate.edu (Andy, negligible time)
    - Work on extending Xplico to add button (Andy, 4 hours)

- Tasks for Altay
    - Look into filtering in jNetPcap libraries (Altay, 2 hours)
    - Install and experiment with TCP replay (Altay, 2 hours)
    - Write code for finding start/end of stream (Altay, 4 hours)

- Tasks for Abe
    - Upload web site to designated space and update it (Abe, 2 hours)
    - Test all Pusher scripts with pcaps from client (Abe, 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)