Cpr/SE 491 Weekly Report **MAY15-06 Week 3 (9/13/14-9/19/14)**

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

Figured out how live stream works (Altay, 9/14)
Figured out how to load and examine pcap files (Andy, 9/16)

Read/Looked at DeepSweep code (Altay, 9/17)
Read/Looked at Xplico code (Andy and Altay, 9/18)

Researched licensing implications (Andy and Abraham, 9/18)
Researched (Java preferred) alternatives to Xplico (Abraham, 9/17)

Contacted client to setup demo for next Friday (Altay, 9/19)

Meeting Notes:

9/12 Advisor Meeting

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

Covered progress from this past week
Determined we need to meet with client next week
Discussed results of research on licenses
Discussed possible alternative to Xplico – Network Miner
Discussed what we need to do to use DeepSweep

9/19 Group Meeting

Duration: 150 min **Members Present:** All

Discussed last week's tasks and what pending issues arose
Discussed and assigned tasks for next week
Determined what we need from the client for the next phases

Created template for project plan from old documentation
Looked at past project plans for examples
Discussed what each part of the plan should contain

Pending Issues

Problem: Need a copy of Go collector and/or API
Solution: Will contact client to obtain copy of it

Problem: Are there alternatives for Xplico?
Solution: Network Miner? Will need further research

Problem: Setup meeting to demo Xplico to client
Solution: Will contact client to setup meeting

Plans for next week

We will work on the project plan. The following parts are assigned to each person.
We estimate it will take 6 hours for each person to complete all of their parts.

Problem Statement - Altay
Resources - Abraham
Work Breakdown Structure - Andy
Project Schedule - Andy
Risks - Abraham

System Diagram - Altay
System Description - Altay
Operating Environment - Andy
User Interface Description - Andy
Functional Requirements - Altay
Non-Functional Requirements - Abraham
Deliverables - Abraham

Compile all parts into one document – Andy

Read the DeepSweep documentation and code – Everyone,* 2 hours

Research further on alternatives to Xplico – Everyone,* 2 hours

* Assuming there is time after project plan is finished

Individual Contributions (this week)

Names	Time Spent (hrs)	Date Finished	Details of Task	How it got Completed	Why is it Important
Andrew Heintz	3.5	9/16	Load and examine pcaps in xplico	Downloaded sample files from xplico web site; load into xplico; and experimented with different views	Loading pcaps is one of Xplico's basic functionalities
Andrew Heintz	4.5	9/18	Look into licensing issues for Xplico	Read GPL, Creative Commons, and LGPL licenses/FAQs	Xplico is a third-party open-source program the client wants to use with their proprietary program
Andrew Heintz	2	9/18	Look at code for Xplico	Looked at code and attempted to figure how it works	Xplico is one of the major components of our project
Altay Ozen	4	9/14	Test and examine live stream	Created internal (NAT) network and tested live stream	Live stream is one of Xplico's basic functionalities
Altay Ozen	4	9/17	Look at code for DeepSweep/Xplico	Looked at code and attempted to figure out how it works	DeepSweep is the client's program, which will produce the data for Xplico
Abraham Devine	1.5	9/18	Look into licensing issues for Xplico	Read general info on open source and copyright	Xplico is a third-party open-source program the client wants to use with their proprietary program
Abraham Devine	1.5	9/18	Look into alternatives to Xplico	Found possible alternative – Network Minor	Xplico is in C, which might pose issues with integration

Total contributions for the project

Andrew Heintz (19 hrs)

Altay Ozen (17 hrs)

Abraham Devine (8 hrs)