Cpr/SE 491 Weekly Report **MAY15-06 Week 11 (11/8/14-11/14/14)**

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

Tested Pushers scripts with pcaps provided by client
Figured out how to build and install Xplico
Worked on modifying Xplico's PHP part to start Xplico C modules
Worked on modifying Xplico's C parts to push pcaps into Xplico

Individual Contributions (this week)

Names	Time Spent	Date Finished	Details of Task	How it got Completed	Why is it Important
Altay Ozen	1	11/12	Tested TCPreplay with jnetpcap	Used lo interface of TCPreplay to test jnetpcap	TCPreplay may be a way to test our code without a DeepSweep device
Altay Ozen	5	11/13	Looked into pcap-over-ip	Examined C modules of Xplico	Pcap-over-ip is how Xplico imports pcap files
Altay Ozen	3	11/13	Began writing part of pusher inside of Xplico	Wrote code for opening sockets	Pusher is going to be part of Xplico in the long run
Andy Heintz	3.5	11/10	Built Xplico from source	Began with instructions, and modified as needed	Xplico will need to be rebuilt to include modifications
Andy Heintz	2.5	11/13	Set up access to SVN repository	Requested repository, set up access, and attempted to connect	Need SVN repository to store project code

Andy Heintz	2	11/13	Worked on modifying Xplico to start itself	Tried modifying start page so it starts the Xplico C modules	Client wants Xplico to start automatically
Abe Devine	1	11/13	Updated web site to include new documents	Modified HTML and uploaded updated page and documents	Need documents on web site instead of Blackboard
Abe Devine	7	11/13	Tested Perl and Bash scripts	Ran scripts with pcaps from client	Pusher script transfers traffic from DeepSweep to Xplico

- Figured out how to build Xplico from source
  - Xplico's instructions didn't include what programs you need for building it
  - Xplico's instructions used the development version of nDPI
  - Not surprisingly, in a year, there's been file renames and major changes to nDPI
- Set up SVN access and tried to get SVN client to work
  - Was able to commit files via command line
  - SmartSVN isn't working properly (did work for 309)
  - All of us have admin access; Dr. Zambreno has read access
- Modifications to PHP to start Xplico
  - Need modify user_controller.php to change the start page
  - Couldn't add button because not possible to add a button handler
  - Looking at how to start Xplico automatically when web page is loaded
  - Not clear which script actually starts Xplico properly

- Modifications to C to push pcaps into Xplico
  - Code opens sockets for DeepSweep and Xplico currently
  - Code will listen to DeepSweep socket until certain amount of data recorded
  - Code writes all this data to Xplico's socket once it reaches this cap
- Xplico's Pcap-over-IP
  - Xplico's port numbers start at 30000 and increment by 1
  - When a session is created, Xplico assigns the next available port number
  - Xplico reads pcaps over IP in chunks of 1024*1024 bytes

Total contributions for the project

Andrew Heintz (90 hrs)

Altay Ozen(87.5 hrs)

Abraham Devine (46.5 hrs)

Meeting Notes:

11/7 Adviser Meeting

Duration: 0 min **Members Present:** All

(None – Adviser was busy this week)

11/7 Group Meeting

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

- Need to test complete system ASAP
- Raw traffic is read directly by Xplico
- Go Collector doesn't seem to be needed for raw traffic

- Raw data does not have a marker for starting or ending
- Xplico's default cap is 1014 * 1024
- For testing, if this is too large, add a flag to set the cap

- Groups of packets may be split between files
- Xplico will just discard these packets
- DeepSweep may group packets before sending

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: Start-up Script
    - Xplico appears to have 2 scripts for starting
    - Script 1: /etc/init.d/xplico
    - Script 2: /opt/xplico/script/sqlite_demo.sh
    - Unclear which script starts it properly

- Issue 3: Starting Pusher
    - Xplico can start C module and Pusher script
    - Xplico can start script, which will start Pusher
    - Xplcio can start C module, which will start Pusher

Plans for Next Week

- Tasks for Andy
  - Modify Pusher scripts to move imported pcaps (2 hours)
  - Modify PHP to start Xplico's C module (6 hours)

- Tasks for Altay
  - Finished C code for pushing pcaps into Xplico (4 hours)
  - Test C code for pushing pcaps into Xplico (4 hours)

- Tasks for Abe
  - Test modified Pusher scripts (4 hours)
  - Fix paths to PDFs on web site (negligible time)
  - Figure out what the two scripts do (4 hours)

Long Term Plans

Modify Xplico PHP code to start Pusher automatically
Modify Xplico C code to incorporate Pusher code
Test entire system (DeepSweep Hardware, Collector, Pusher, Xplico)
Demo entire system to client (after Thanksgiving, possibly)