IP Fabrics: Network Forensic UI

May 15-06

Andy Heintz (Communications)

Altay Ozen (Team Lead)

Abe Devine (Webmaster)

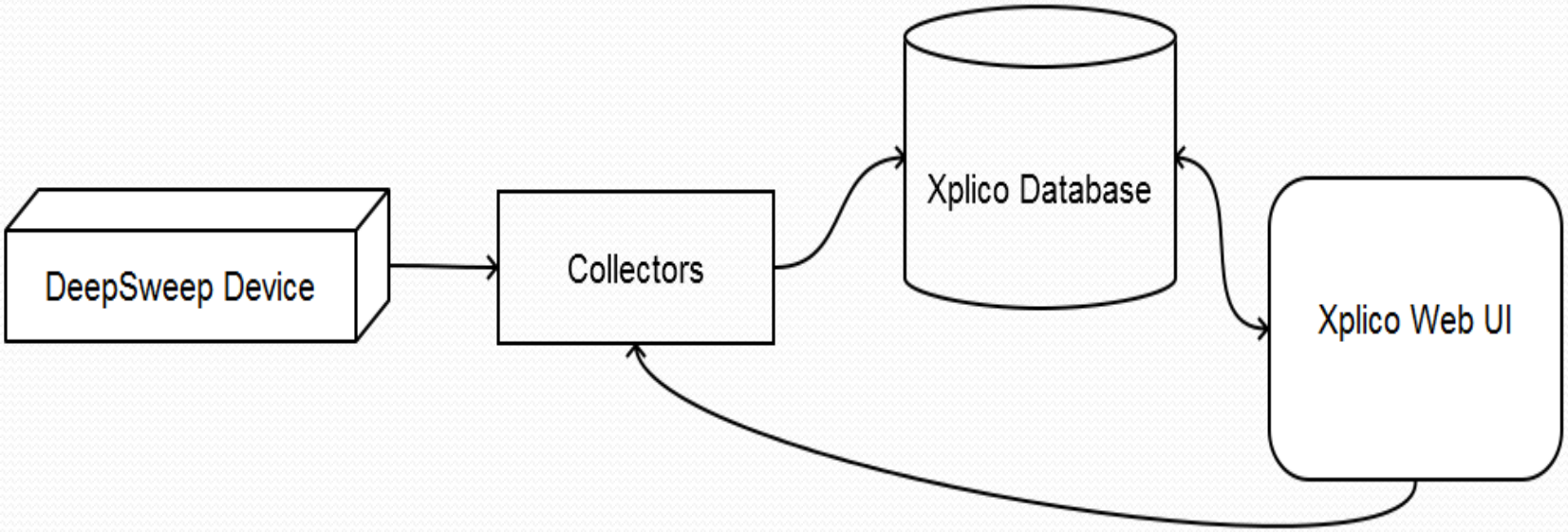
Client: Curt Schwaderer

Adviser: Dr. Joseph Zambreno

Scope of Project

- DeepSweep is an existing device for capturing traffic
- Xplico is an existing web UI for viewing traffic
- Develop an interface between Xplico and DeepSweep
- Develop functionality for generating PDF reports

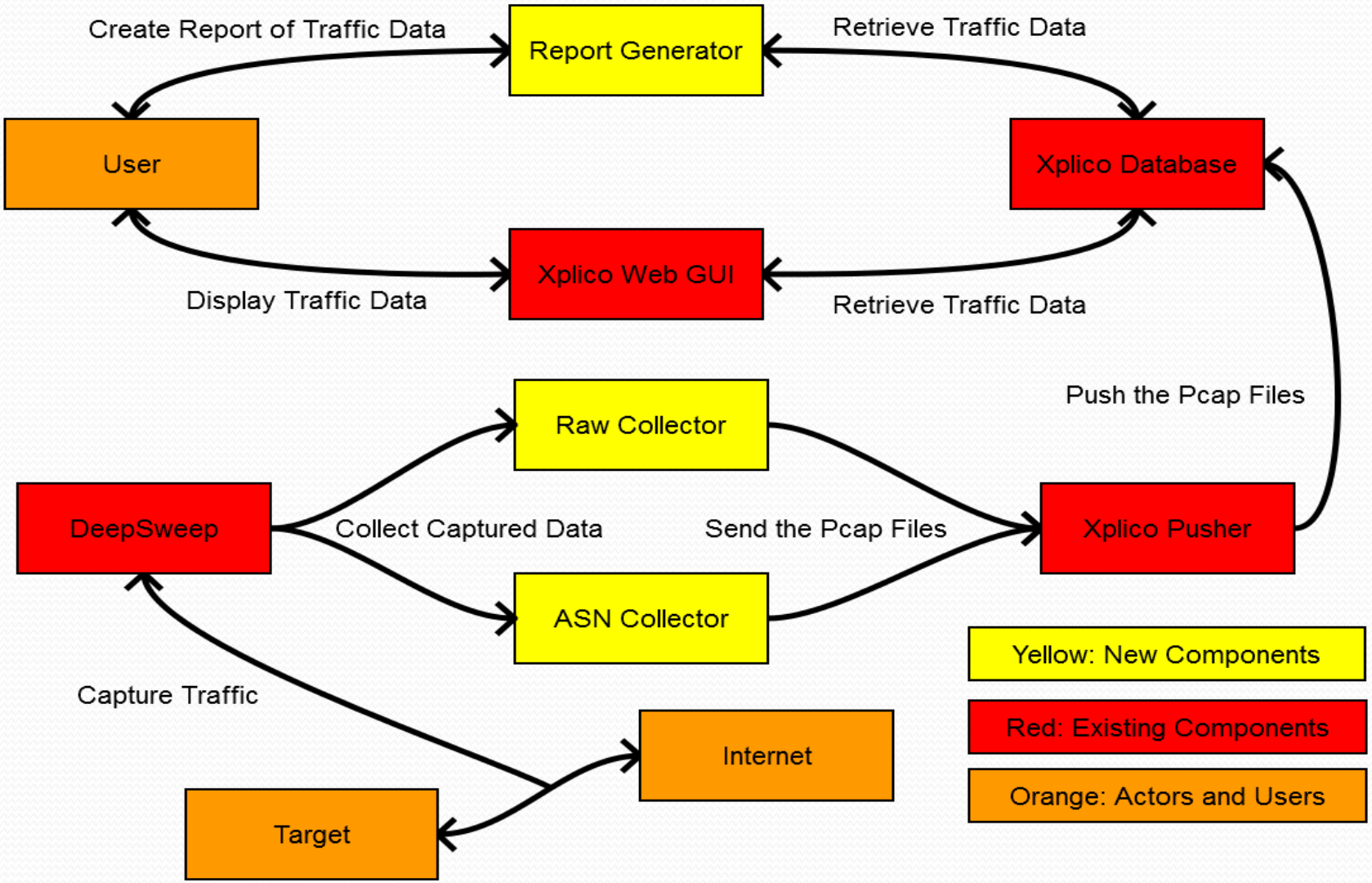
Concept Sketch



Pcap: Packet Capture
Contains captured network traffic data

ASN.1: Abstract Syntax Notation
Standard for representing data in networking

Design Diagram



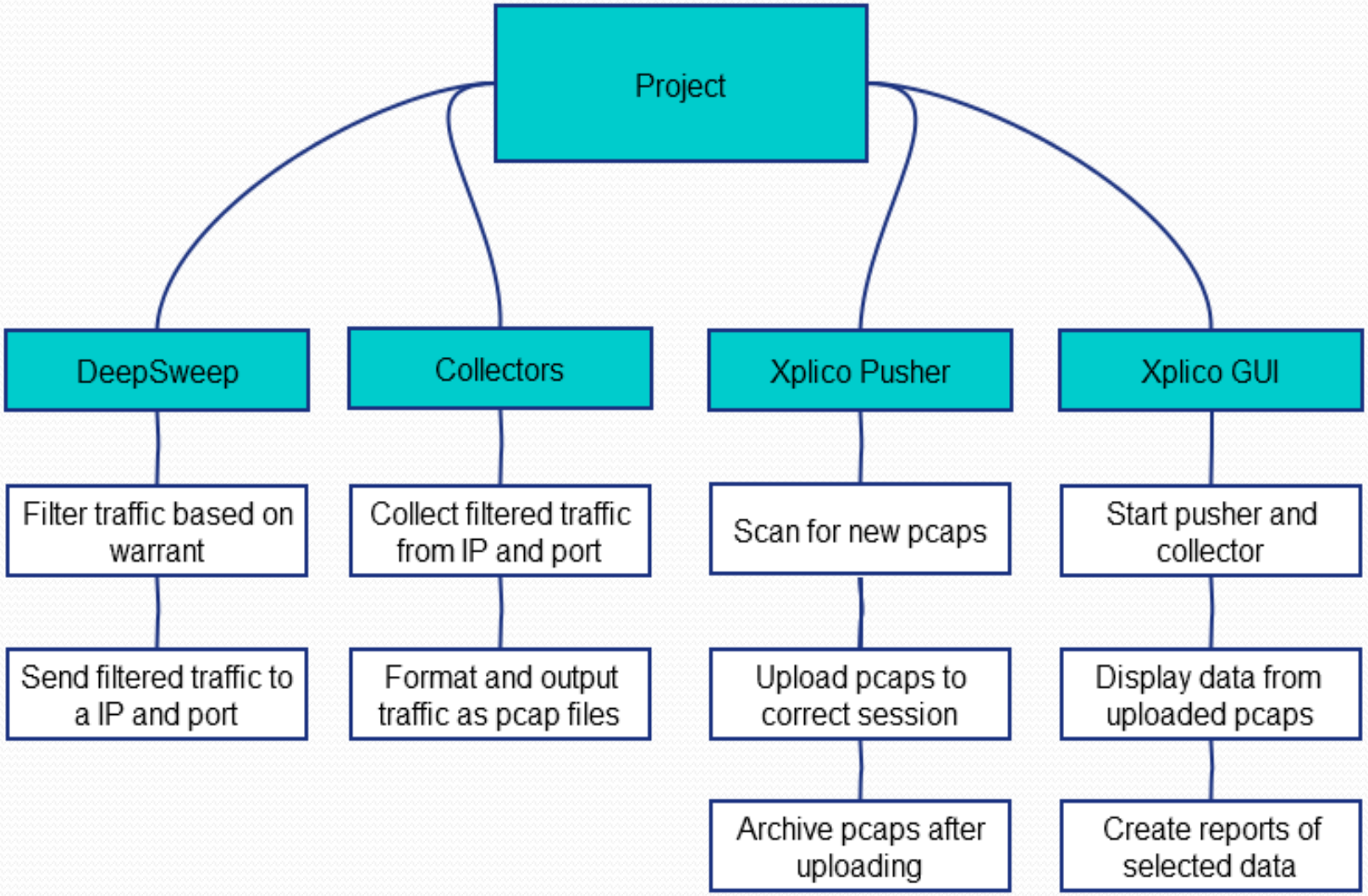
Requirements

1. Xplico (modified): Start Pusher and the Collectors
2. Raw Collector (new): Create pcaps from raw traffic
3. ASN Collector (new): Create pcaps from ASN.1 traffic
4. Xplico Pusher (existing): Upload new pcaps to Xplico
5. Xplico (existing): Display uploaded traffic in web GUI
6. Xplico (modified): Generate reports for traffic

Non-Functional Requirements

- Reliability: Application should return information consistently and recover from errors.
- Maintainability: Documentation should be up-to-date and accurate; application should be easy to upgrade.
- Extensibility: Future developers should be able to easily add additional features using the existing architecture.

Decomposition



History

- Cream Java API vs Go Collector
  - Client preferred Cream over Go
  - Decreases maintenance complexity
- C vs Java Raw Collector
  - Collector was originally written in C
  - Converted to Java since ASN Collector is Java

History

- Splitting of Pcaps
  - Less loss of data if Collector crashes
  - Increases real-time processing of Pcaps
  - Reduced buffering of pcap data
- Pcap-over-IP vs Outputting
  - Originally, sent via socket to Xplico
  - Socket needed closing for each pcap sent
  - Can output multiple pcaps to directory

Challenges

- Problem: Real-time processing of pcaps
- Time for decoding pcaps increases as pcap size increases

- Solution: Splitting pcaps into smaller pcaps
- Therefore, decoding of pcaps occurs in parallel

Challenges

- Problem: Creating pcaps from ASN output
- ASN is a flexible format – Determined by user

- Solution: Modify output from Cream
- Output is not pcap format, so Collector modifies it

Challenges

- Problem: Xplico cannot terminate Collector
- Once started, Xplico cannot access Collector’s output

- Solution: Utilize file in Xplico’s directories
- Collector runs only if file exists in Xplico’s directory

Challenges

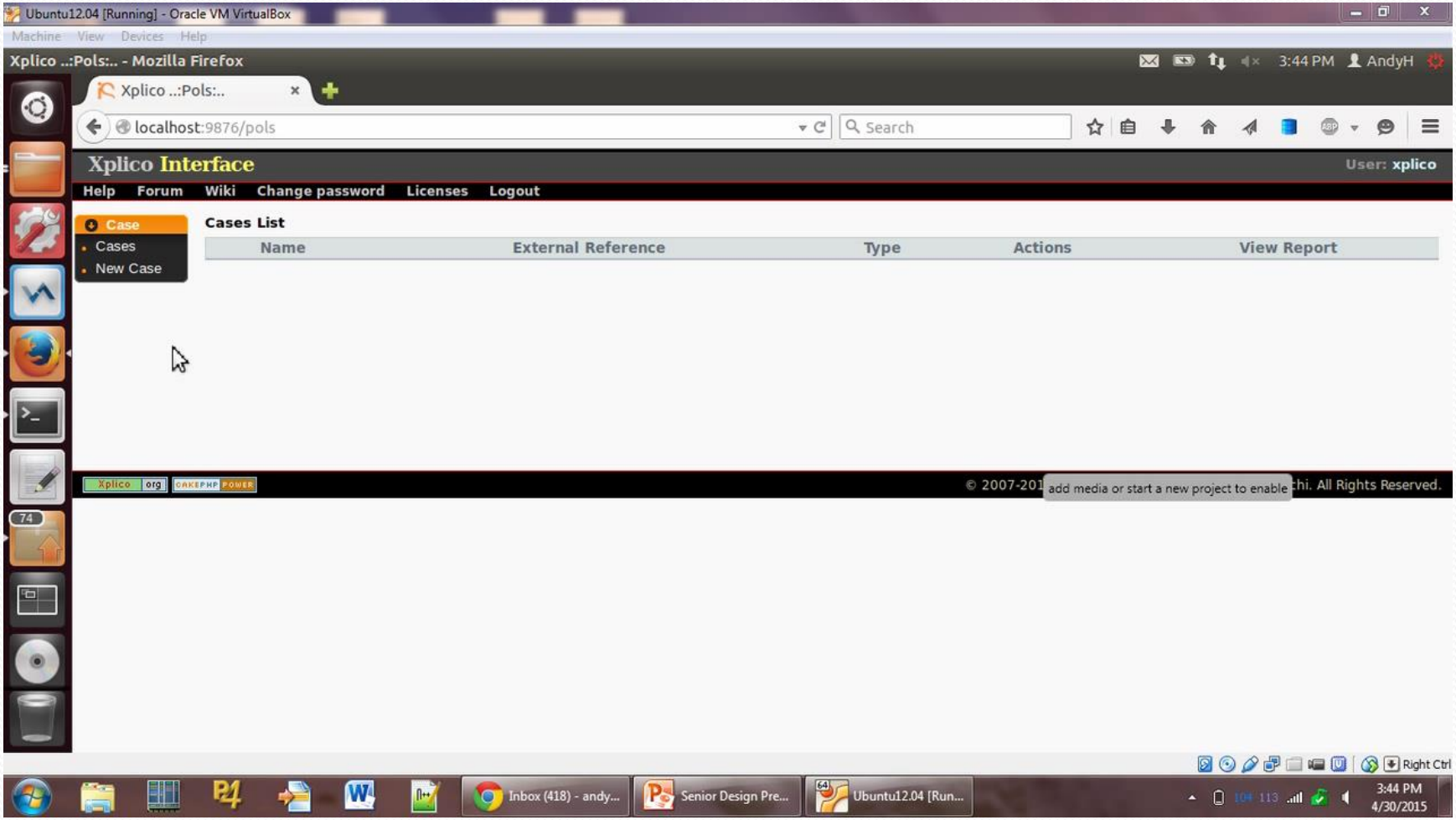
- Problem: Simulating actual traffic for testing
- Currently, we do not have access to DeepSweep device

- Solution: Create script for sending multiple pcaps at once
- Script will vary number and frequency of sending

Test Plan

1. Verify Collectors start and stop from Xplico GUI
2. Verify Collectors collect traffic and output pcaps
3. Verify pcaps created by Collectors upload to Xplico
4. Verify creating report includes selected data
5. Run regression and integration tests on system
6. Run stress and benchmark tests on system

Video


Ubuntu12.04 [Running] - Oracle VM VirtualBox
Machine View Devices Help
Xplico ..:Pols:.. - Mozilla Firefox
3:44 PM AndyH
Xplico ..:Pols:..
localhost:9876/pols
Search
Xplico Interface
User: xplico
Help Forum Wiki Change password Licenses Logout
Case
Cases
New Case
Cases List
Name External Reference Type Actions View Report
Xplico .org
CAKEPHP POWER
© 2007-201
add media or start a new project to enable
hi. All Rights Reserved.
Right Ctrl
Inbox (418) - andy...
Senior Design Pre...
Ubuntu12.04 [Run...
3:44 PM
4/30/2015

Questions?