May 15-06:
Network Forensic UI

Andy Heintz, Altay Ozen, Abe Devine
Dr. Joseph Zambreno (Adviser)
Curt Schwaderer (Client)

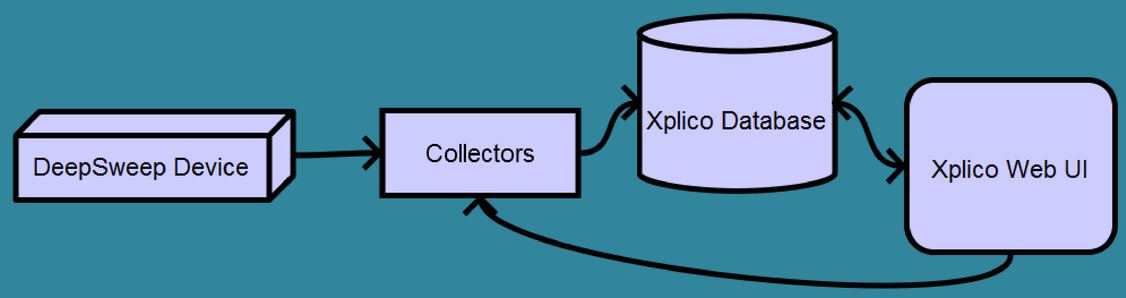
Introduction

Background
- Deepsweep is a device for monitoring network traffic
- Outputs stream of traffic for analysis

Problem
- DeepSweep is an existing device
- Does not have GUI for displaying this traffic

Solution
- Xplico is an existing web UI for displaying traffic
- Collect traffic from DeepSweep and display in Xplico

Concept Sketch



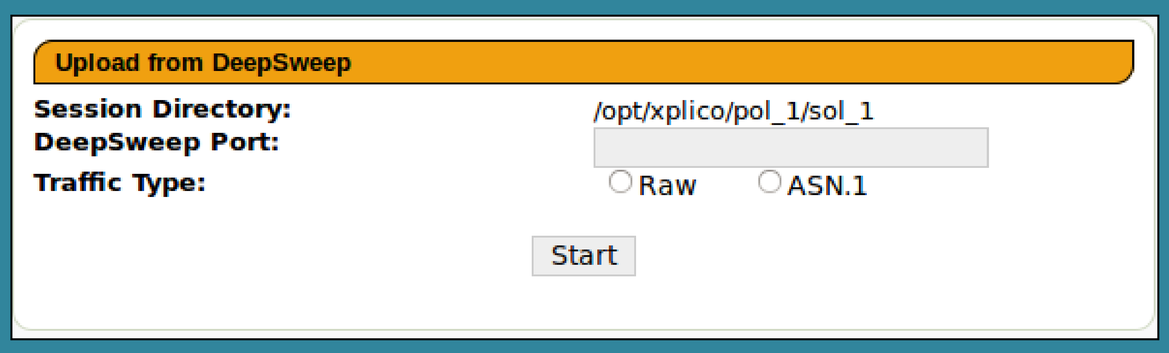
Operating Environment: Any version of Linux
Intended Uses: Displaying network traffic from Deepsweep
Intended Users: Any users of DeepSweep hardware

Functional Requirements

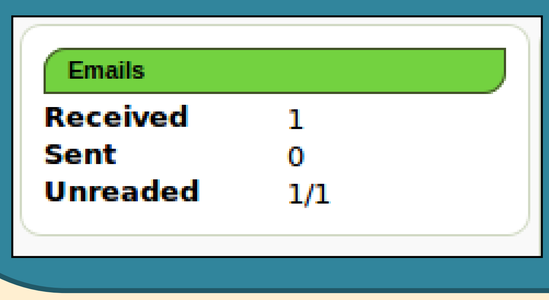
1. Xplico: Start Pusher and the Collectors
2. Raw Collector: Create pcaps from raw traffic
3. ASN Collector: Create pcaps from ASN.1 traffic
4. Xplico Pusher: Upload new pcaps to Xplico
5. Xplico: Display uploaded traffic in web GUI
6. Xplico: Generate reports for traffic

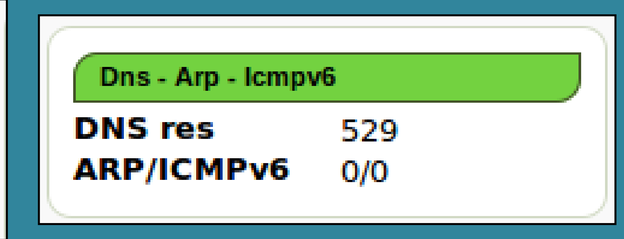
GUI Screenshots

Starting Collectors



Example Result Summary





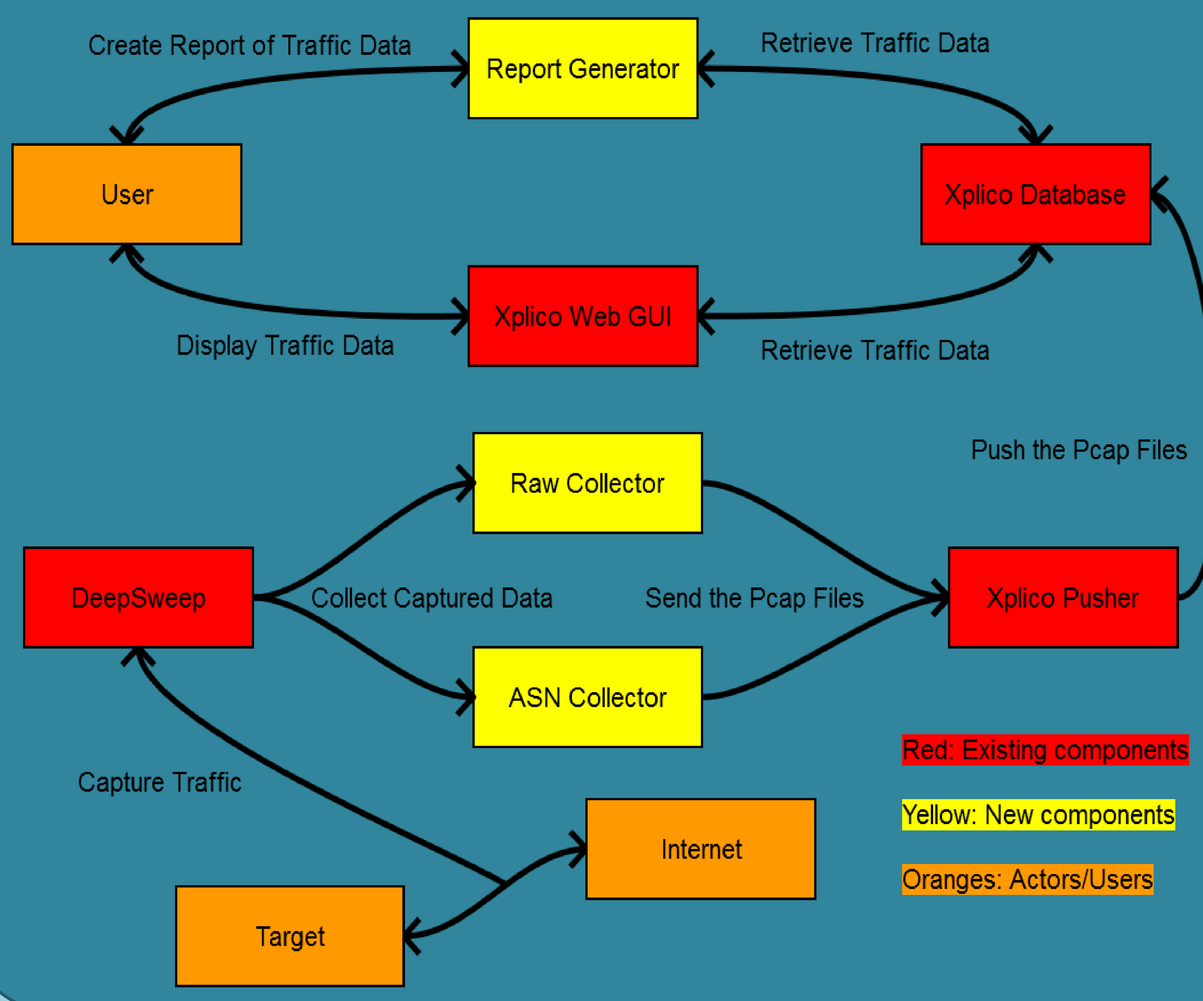
Non-Functional Requirements

Reliability: Performs consistently and recovers from errors

Maintainability: Documentation is up-to-date and accurate

Extensibility: Easy to add and upgrade additional features

Block Diagram



Technical Details

ASN & Raw Collectors (Java) : Listens for traffic on a port, and converts traffic to pcap (packet capture) files

Xplico Pusher (C) : Copies pcap data into Xplico's database

Xplico Database (SQL) : Stores data from uploaded pcaps

Xplico Web GUI (PHP) : Displays data from uploaded pcaps, and provides options for starting collectors

Report Generator (PHP) : Creates PDFs of the data

Test Plan

Component Tests: Test each module once it was written

Integration Tests: Connect and test modules together

Stress Tests: Test entire system by sending multiple pcaps continuously over a period of time

Benchmark Tests: Test entire system by sending multiple pcaps and timing how long it to decode them