A Multifaceted Approach to Botnet Detection, Mitigation and Visualization (Framework Subproject)

iscx Information Security Centre *of* Excellence

Ehsan Mokhtari, Jonathan Miller, Ali A. Ghorbani
Information Security Center of Excellence, Faculty of Computer Science, University of New Brunswick

Description

A multifaceted Approach to Botnet Detection, Mitigation and Visualization is a strategic project funded by NSERC in collaboration with Q1Labs Inc, RCMP, and CRC. The project has three main aspects including botnet detection, mitigation and visualization. Each of these aspects is being researched and developed by a research and development group. These teams comprise researchers from the University of New Brunswick, University of Victoria, CRC, RCMP, Alabama University, and University of New Hampshire. The Framework subproject is responsible for interconnecting different components of this distributed project. Also the Framework subproject enables end-users to access the system capabilities via interactive and dynamic web interfaces.

Features

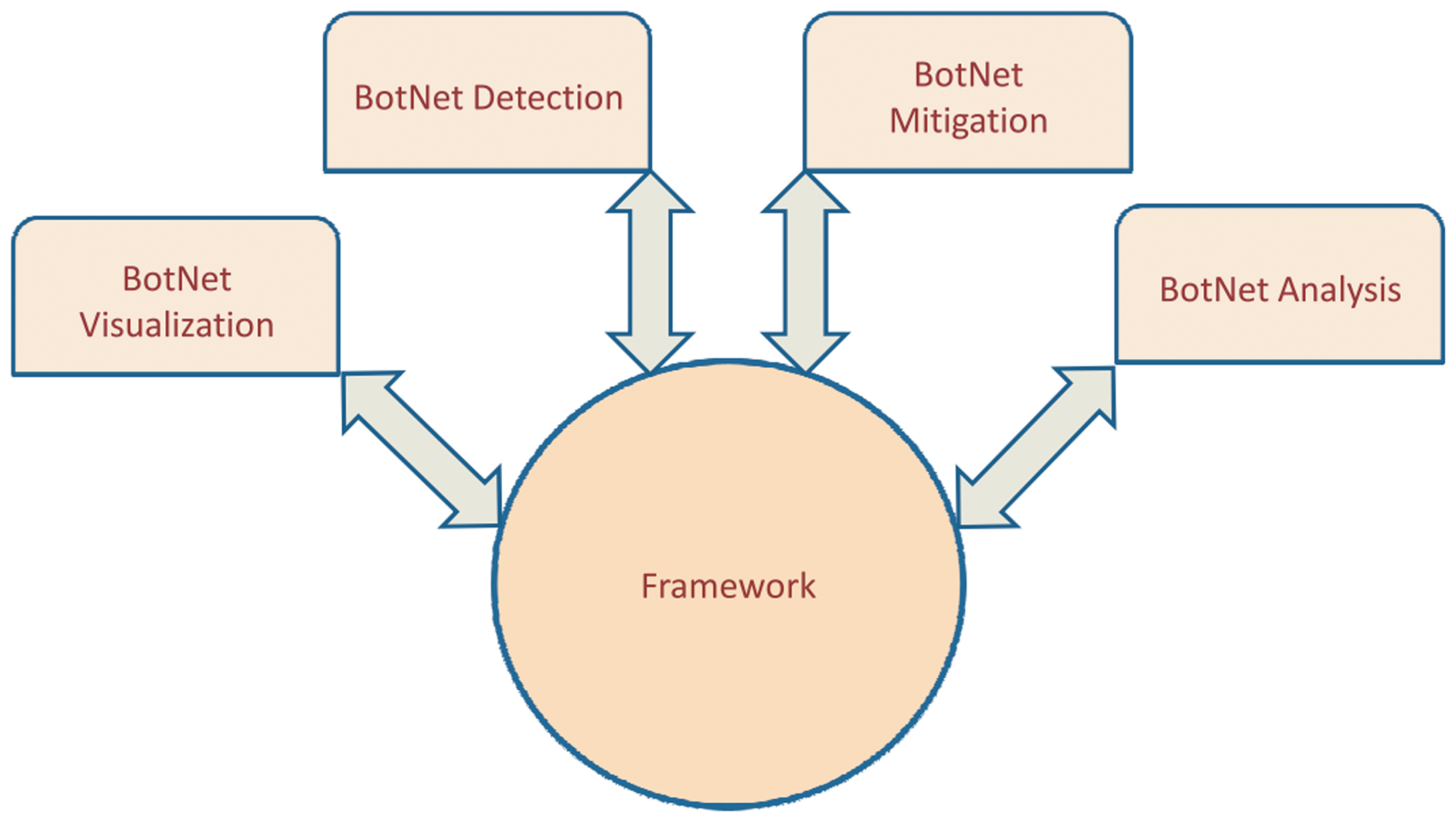
- Provides data contributors with an Alert Plugin Framework to develop customized plugins for security devices.

- Collects alerts from several distributed sources via Alert Plugin Framework.

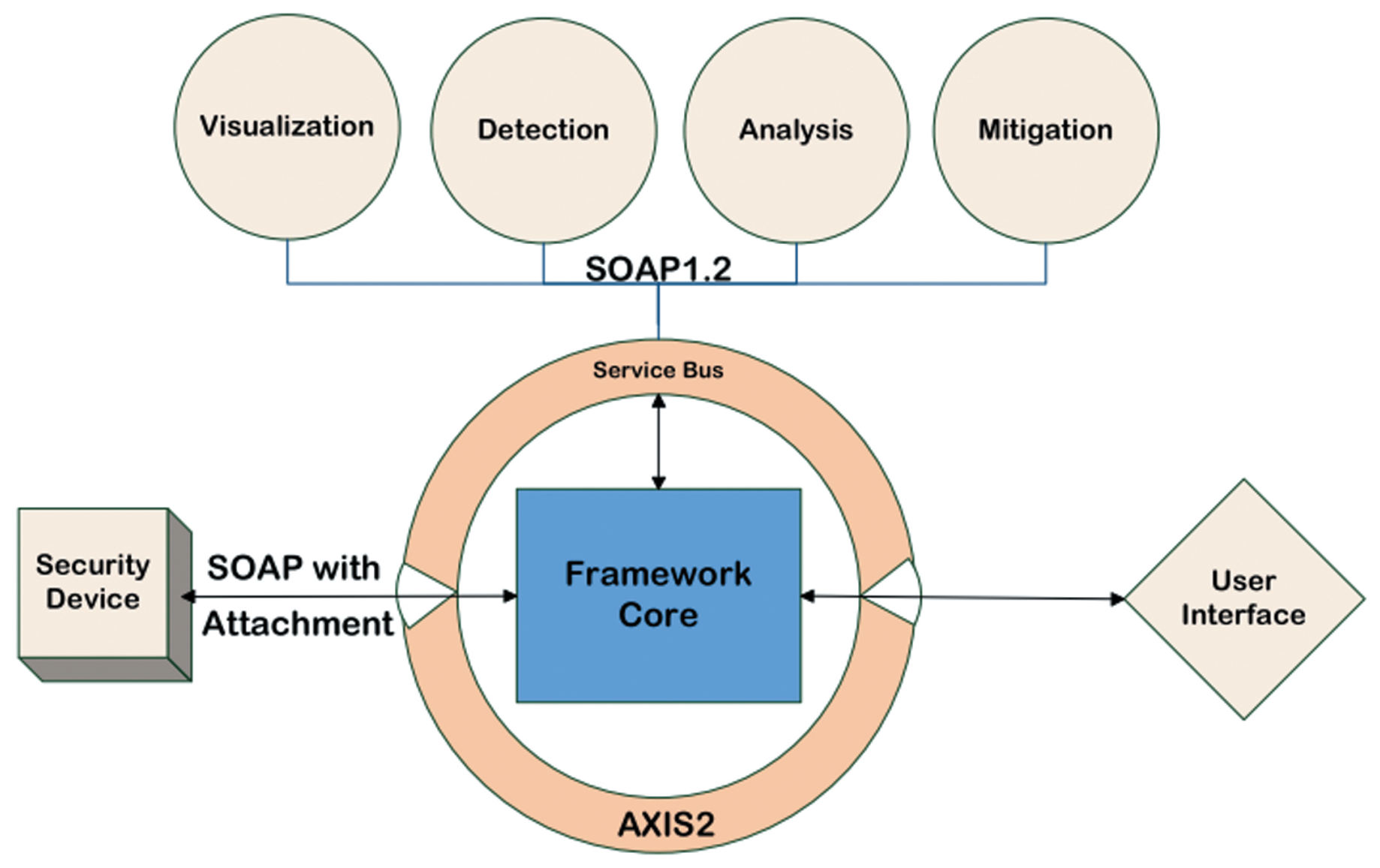
- Provides web services via Axis2 to other subprojects.

- Provides end-users with dynamic search and report facilities to query and filter the collected data.

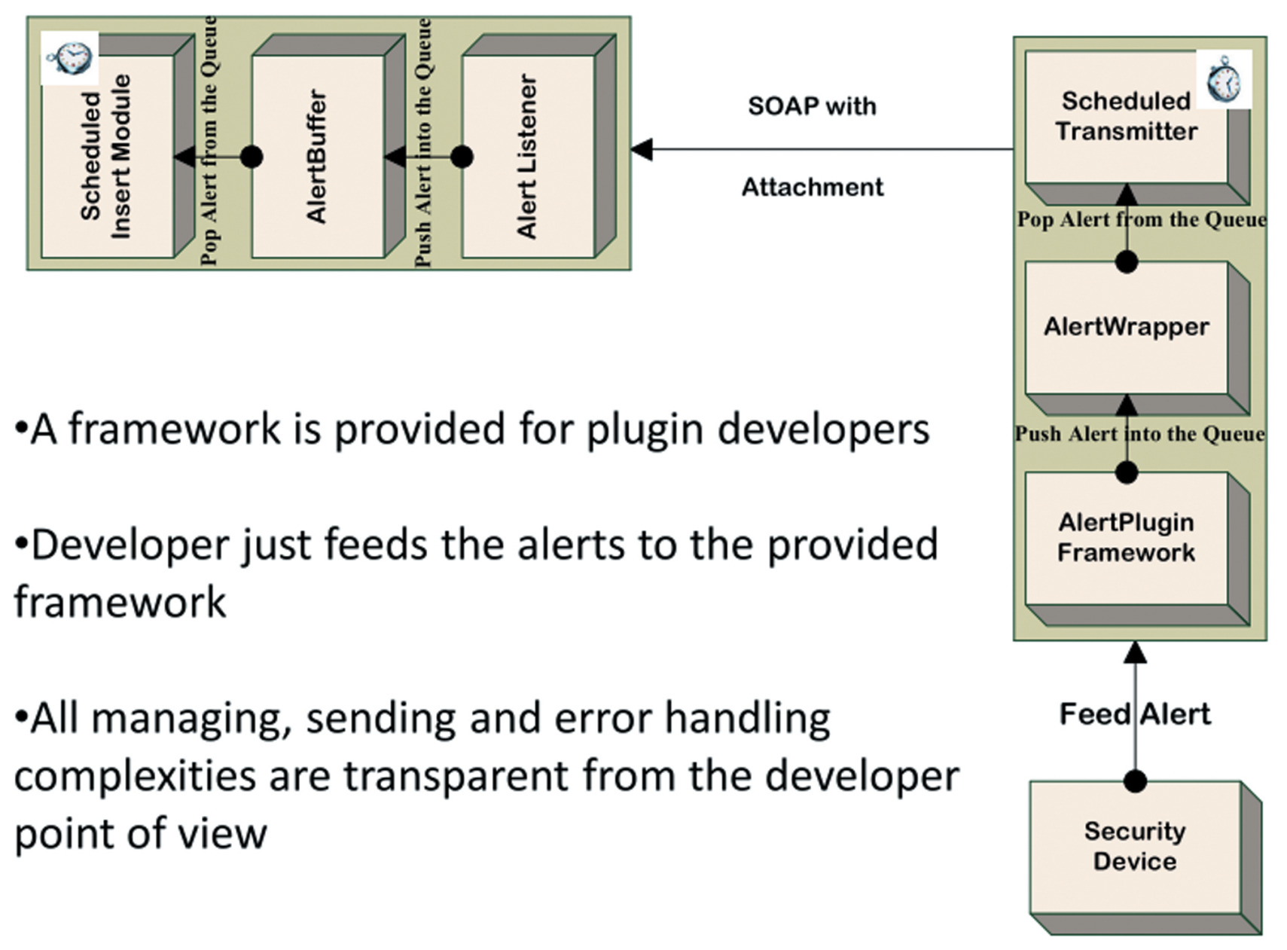
System Architecture



System Components



System Overview



- A framework is provided for plugin developers

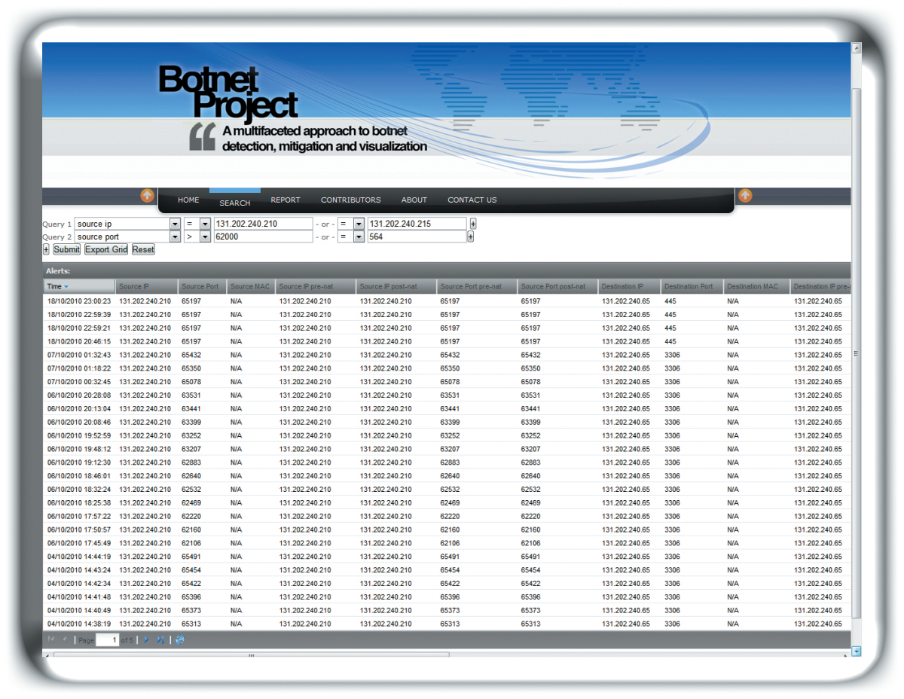
- Developer just feeds the alerts to the provided framework

- All managing, sending and error handling complexities are transparent from the developer point of view

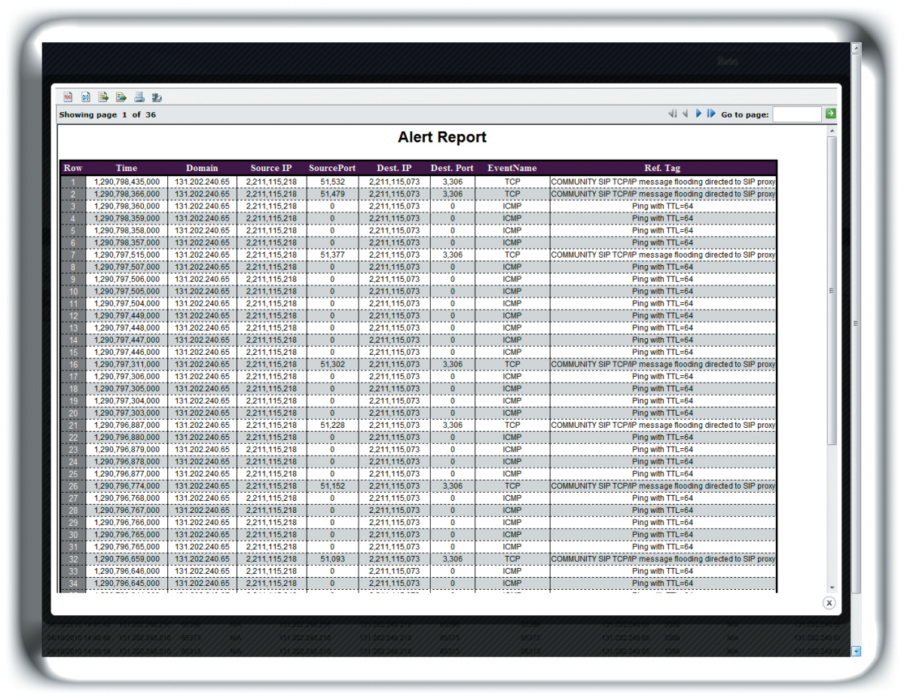
Alert Plugin

Screen Shots

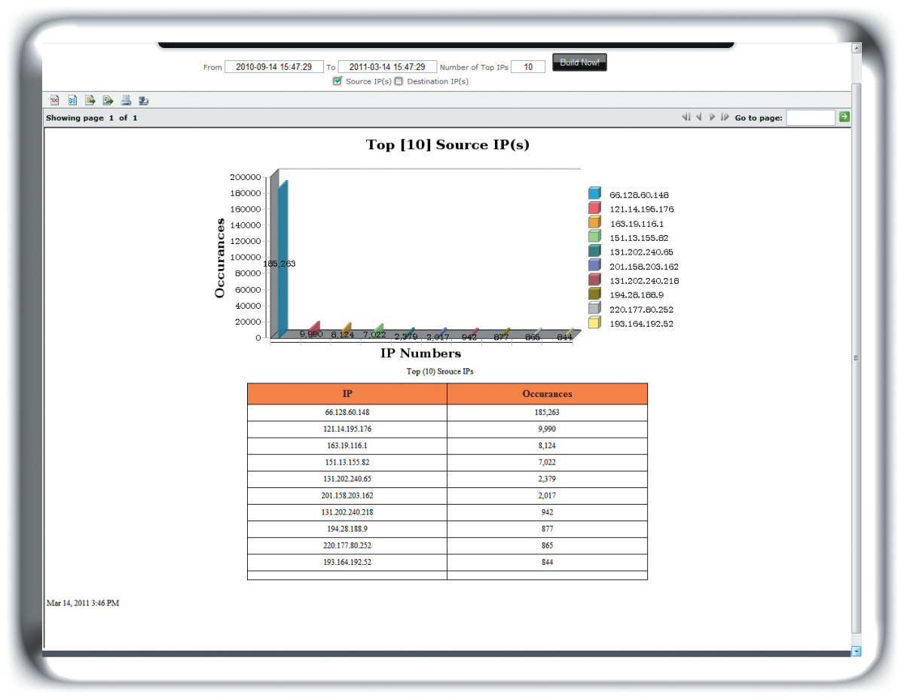
Entry View



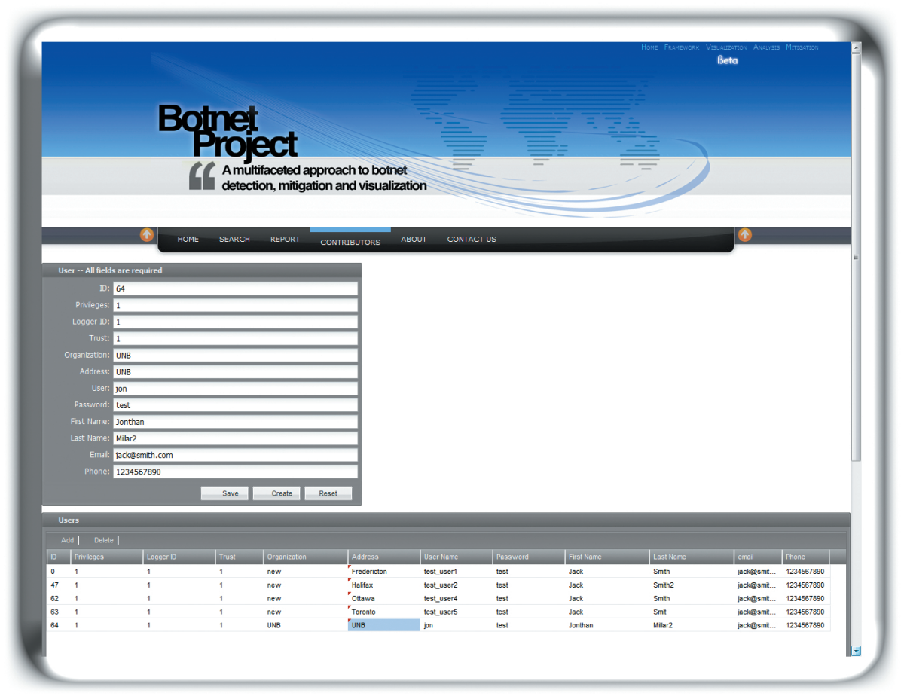
Search View



Search Export View



Report View



User Management View