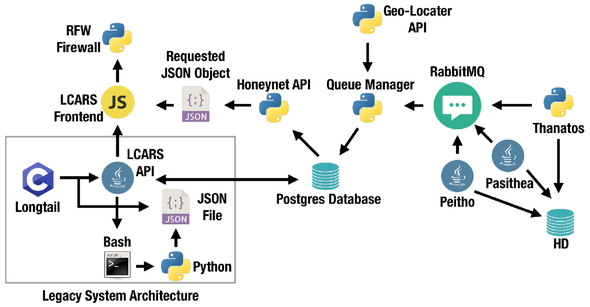
LCARS: Lightweight Cloud Application for Realtime Security

Authors Daniel N. Gisolfi and Michael Gutierrez; based on prior work by Graham Burek and Mariah Molenaer
Faculty Robert Cannnistra, Casimer DeCusatis , Matthew Johnson, Alan G. Labouseur
IBM Greg Lacey

Overview



Legacy System Architecture

LCARS is a web-based security application designed to identify, analyze, respond to, and help prevent attacks and threats targeting network infrastructure. Using this diagram as a starting point, we divided LCARS into three categories: Analysis, Threat Intelligence, and Threat Response, which we call the Reconfigurator.

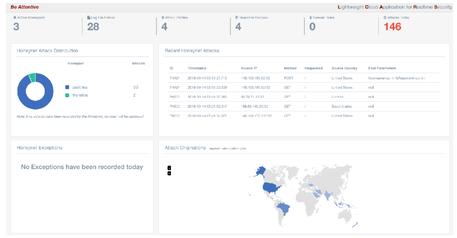
This work is sponsored in part by NSF Grant Award 1541384 — CC*DNI Integration: Application Aware Software-Defined Networks for Secure Cloud Services

Data Collection

We collect realtime data from our various honeypots within the honeynet using a message queue. Attacks data are cleansed and entered into our database for analysis. This allows for straightforward integration with our relational and graph-based analytics tools. The current infrastructure is scalable and can respond to newly added honeypots on the fly. Additionally we collect live attack data from LongTail SSH honeypots. All attack data is sent as JavaScript Object Notation (JSON) to the LCARS frontend.


```
{
  "id": "PAS02",
  "timestamp": "2018-09-14 00:00:17.934",
  "pot_name": "pasithea",
  "host_ip": "10.11.17.23/32",
  "host_PID": 1,
  "HPID": "null",
  "method": "GET",
  "requested_text": "/",
  "source_ip": "187.94.251.93/32",
  "source_port": 8080,
  "post_text": "null",
  "source_country": "Brazil",
},
{
  "id": "THA01",
  "timestamp": "2018-09-14 00:59:37.604",
  "pot_name": "thanatos",
  "host_ip": "10.11.17.23/32",
  "host_PID": 1,
  "HPID": "null",
  "method": "GET",
  "requested_text": "/",
  "source_ip": "177.99.13.19/32",
  "source_port": 4400,
  "post_text": "null",
  "source_country": "Brazil",
},
```


Attack data collected from the Honeynet



Attack data displayed in LCARS

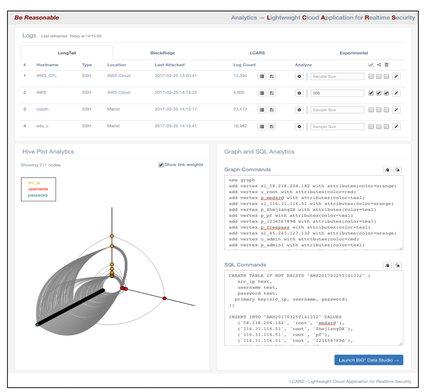
Threat Intelligence

Details for the response recipe: Fight the Power

The Response Orchestration section of the Threat Intelligence page

We built a Threat Intelligence database of *attack profiles*, *response recipes*, and *orchestrated responses*. A response recipe is a collection of firewall rules. An orchestrated response maps an attack profile to a group of response recipes. To interact with this database we built our own REST API. Our API enables us to easily create, update, and delete database items directly from our GUI.

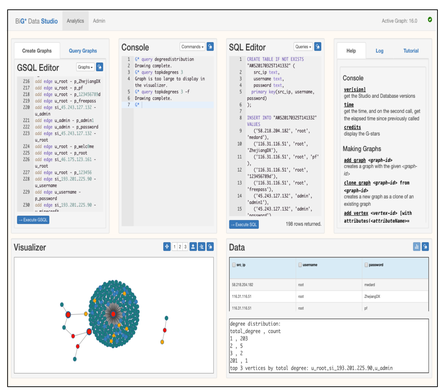
Analysis



the LCARS Analysis page showing a hive plot, graph commands, and SQL commands generated from attack data

We currently take our parsed attack data and generate hive plot visualizations, G* graph commands, and SQL commands. The graph and SQL commands are sent to BiG* Data Studio, a front end to the both the G* graph database and the PostgreSQL. relational database. This allows us to execute our graph and SQL commands and run queries against them. The hive plot pictured on the left represents the same attack data as the graph and SQL on the right.

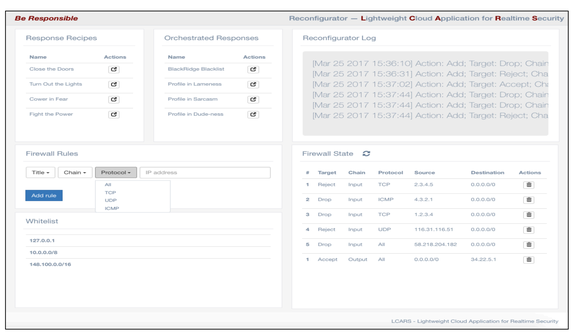
We are developing automation for process using logs from live routers and SDN controllers so LCARS can dynamically reconfigure the network when it detects an attack.



BiG Data Studio showing a graph of the LCARS-generated data running the Top-K Degrees query*

Reconfigurator

The Reconfigurator enables deployment of response recipes and orchestrated responses to our firewall. We utilize RFW (Remote Firewall), an open-source REST API for *iptables*, in order to seamlessly interact with the firewall service. Firewall rules can be deployed both in batch or on an individual basis.



The LCARS Reconfigurator page

This edition of LCARS builds on prior work by the Marist/IBM Joint Study students and faculty. The honeypot and honeynet components are based on research reported in *A HoneyNet Environment for Analyzing Malicious Actors* by the same authors. We would like to thank our fellow students as well as the faculty and staff for their support and contributions.