IRNC: AMI The InSight Advanced Performance Measurement System

Jens Gregor, UTK
Carter Bullard, QoSient
Buseung Cho, KISTI
Joe Gipson, Cisco









Project Summary

- Develop and study tools for advanced flow-level network measurement using enriched Argus data
- Network performance + cyber security analytics
 - Better understanding of network utilization
 - Identification of network performance issues
 - Shine light on threats and anomalous behaviors
- Angel Kodituwakku: Comp. Engr. MS at UTK
- Greg Cole: Original PI retired January 2016
- Gloriad: Equipment decommissioned April 2016

InSight System Architecture

Data Acquisition Visualization **Data Processing Argus Flow** Kibana/Shield **Data Enrichment** Global Science Registry / GeoIP Node • Bad actors, Botnets Node • IP/Port scanners, spammers Node **Data Analytics** · Graph models: raw data, inferred Markov chains: event likelihoods 2012-2015 Elastic Search Gloriad **Database** Repository (14TB)

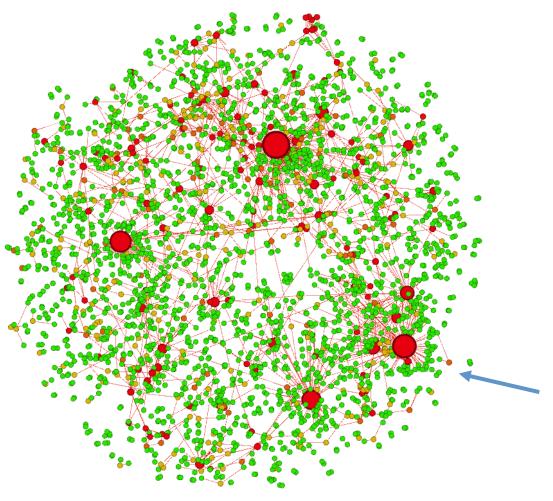
Completed Tasks

- 1. Migration to new multi-core servers
- 2. Argus data repository restore / backup
- 3. Kibana and Elastic Search upgrade

On-Going Tasks

- 1. Data processing: Pearl 6 implementation
- 2. Graph model and Markov chain building
- 3. Kibana dashboards with D3 visualization

Gloriad Traffic Snapshot Dec 1, 2015



Time: 12:00:00-12:05:00

Vertex: IP address

Edge: Flow (send/receive)

Mapping: Force Atlas

