Detecting and Characterizing Internet Traffic Interception based on BGP Hijacking

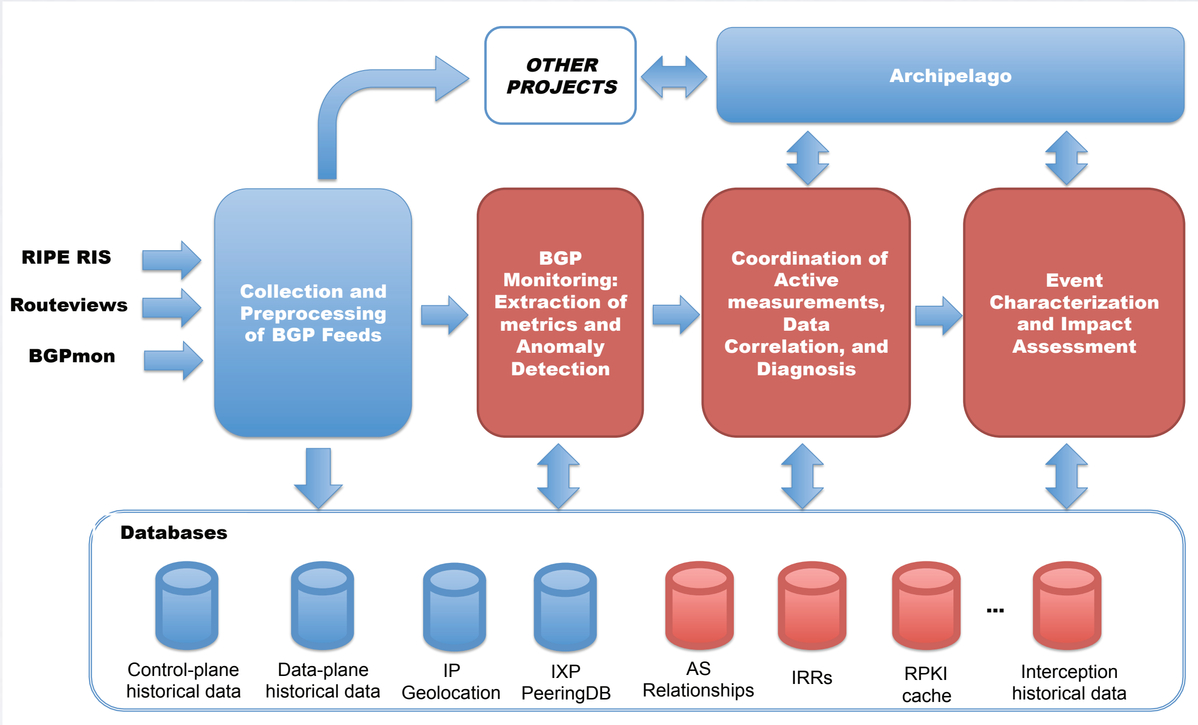
Center for Applied Internet Data Analysis
University of California San Diego

Challenge

- Near-realtime detection of traffic interception attacks based on BGP prefix hijacking
- Global view

Solution

- Detect suspicious events on the control plane; trigger data-plane active measurements.
- Auxiliary datasets (e.g., AS relationships) to assist with classification of events
- Modular system



OTHER PROJECTS

Archipelago

RIPE RIS

Routeviews

BGPmon

Collection and Preprocessing of BGP Feeds

BGP Monitoring: Extraction of metrics and Anomaly Detection

Coordination of Active measurements, Data Correlation, and Diagnosis

Event Characterization and Impact Assessment

Databases

Control-plane historical data

Data-plane historical data

IP Geolocation

IXP PeeringDB

AS Relationships

IRRs

RPKI cache

...

Interception historical data

High-level view of the components of the detection and classification system

Scientific Impact

- Methodology for near-realtime detection of BGP-based traffic interception attacks
- Reference datasets of anomalies

Broader Impact

- Publications and presentations at conferences
- Open source, re-usable software (BGPStream)
- BGP Hackathon 2016

NSF CNS-1423659, University of California San Diego
PI: Alberto Dainotti