Homeland Security
Science and Technology

Netbrane: A Software-Defined DDoS Protection Platform for Internet Services

Colorado State University

Christos Papadopoulos

Cybersecurity Research Acceleration Workshop - Oct 18, 2017 – San Francisco CA
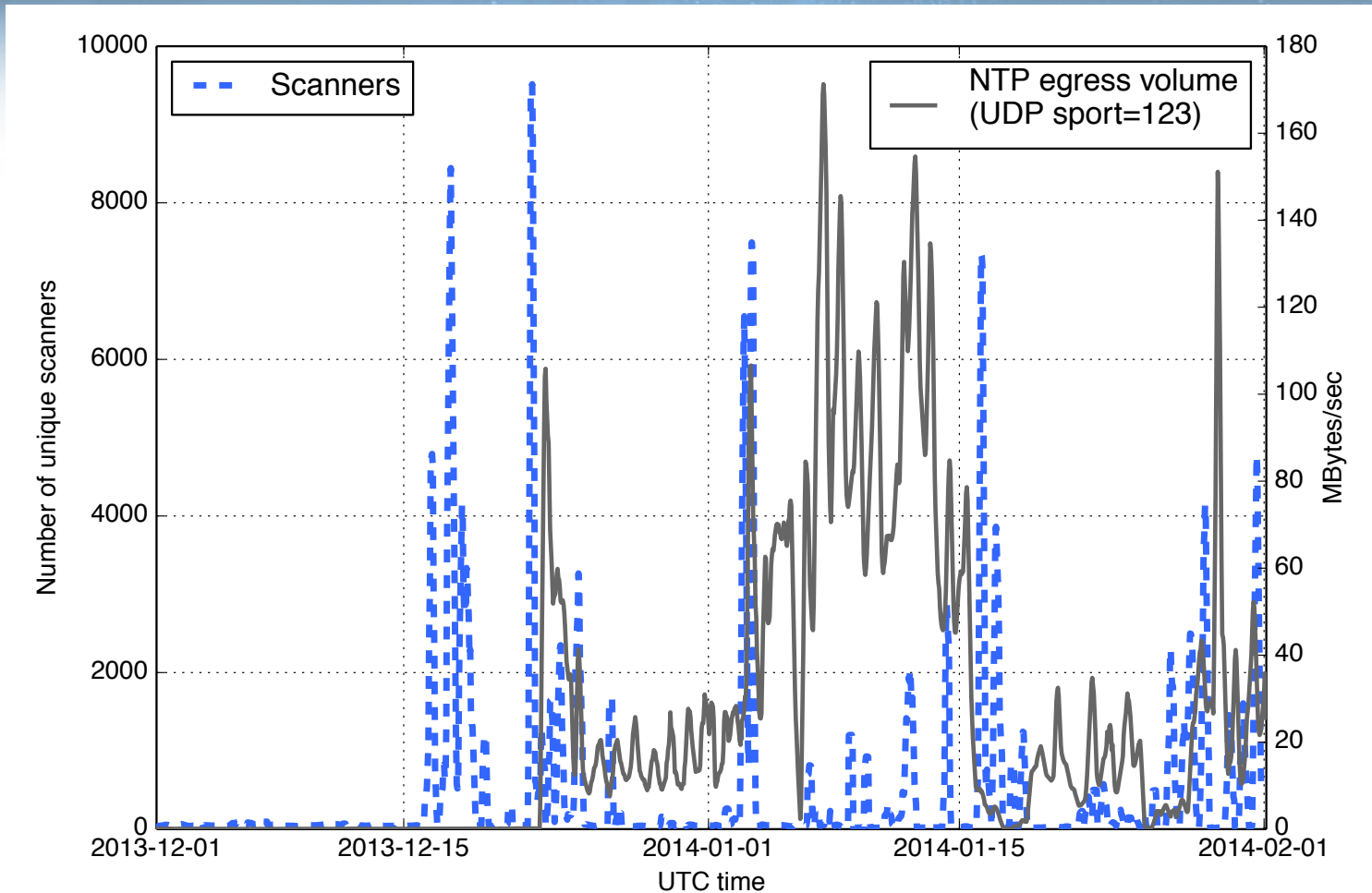
Team Profile

The Team:

- Colorado State University:
  - **Stephen Hayne**, Dimitris Kounalakis, Robert McAndrew, **Christos Papadopoulos**, Ela Sienkiewics, Spiros Thanasoulas, **Haonan Wang**

- University of California, Riverside:
  - Ahmad Darki, **Michalis Faloutsos**, Joobin Gharibshah, Mike Li
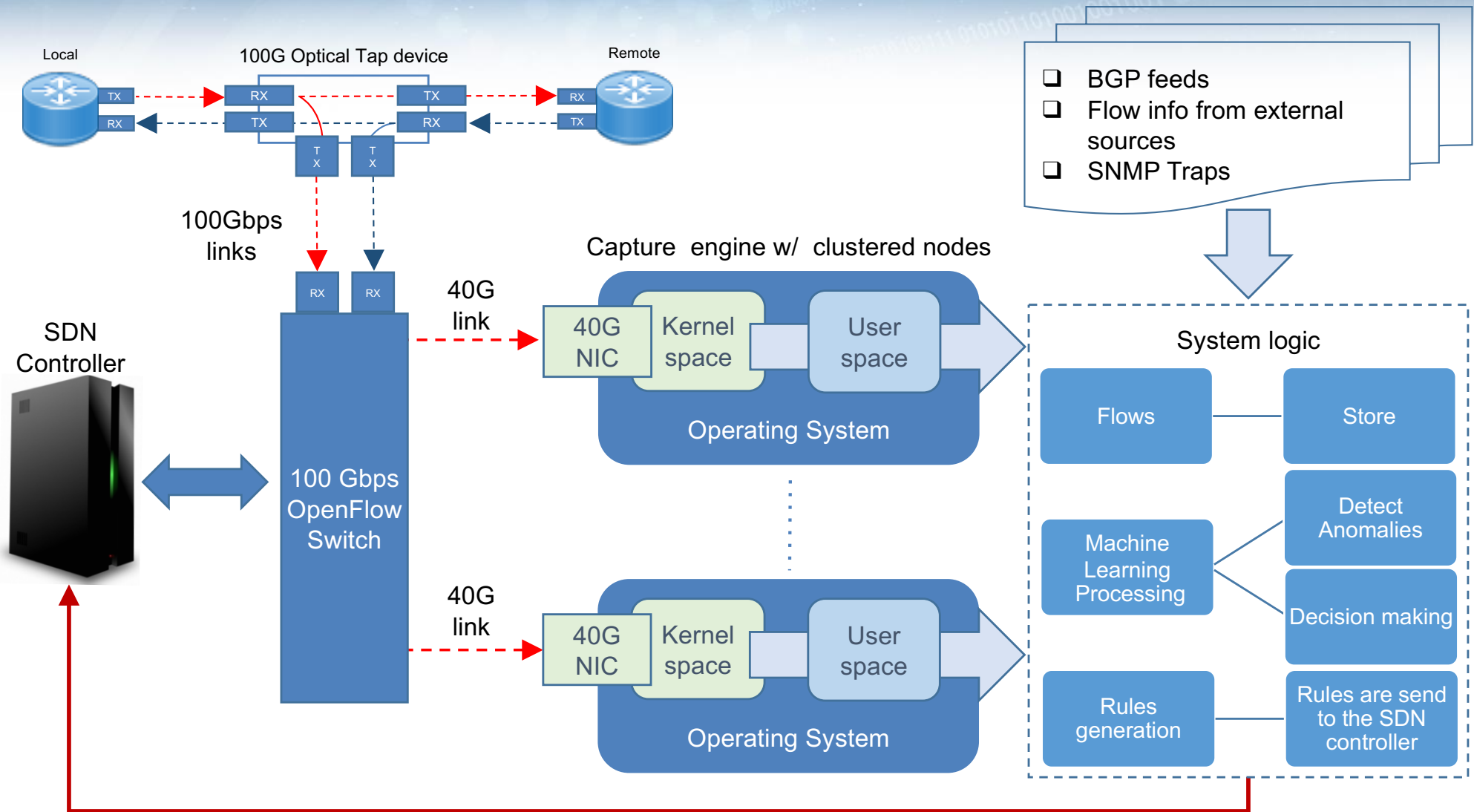
Value Proposition

- Distributed Denial of Service (DDoS) attacks will be at the top of security threats for the foreseeable future

- State of the Art DDoS defense today:
  - Intentionally hijack traffic, redirect to scrubbing centers, tunnel back to customer
  - Expensive, small clean pipe, susceptible to collateral damage

- Need to be distributed, effective and proactive:
  - Reliably detect the attack using machine learning, create filtering rules
  - Communicate filters to your upstreams immediately
  - High-capacity SDN switches to block attack
  - Defense readiness via network structural information and hints from hacker forums
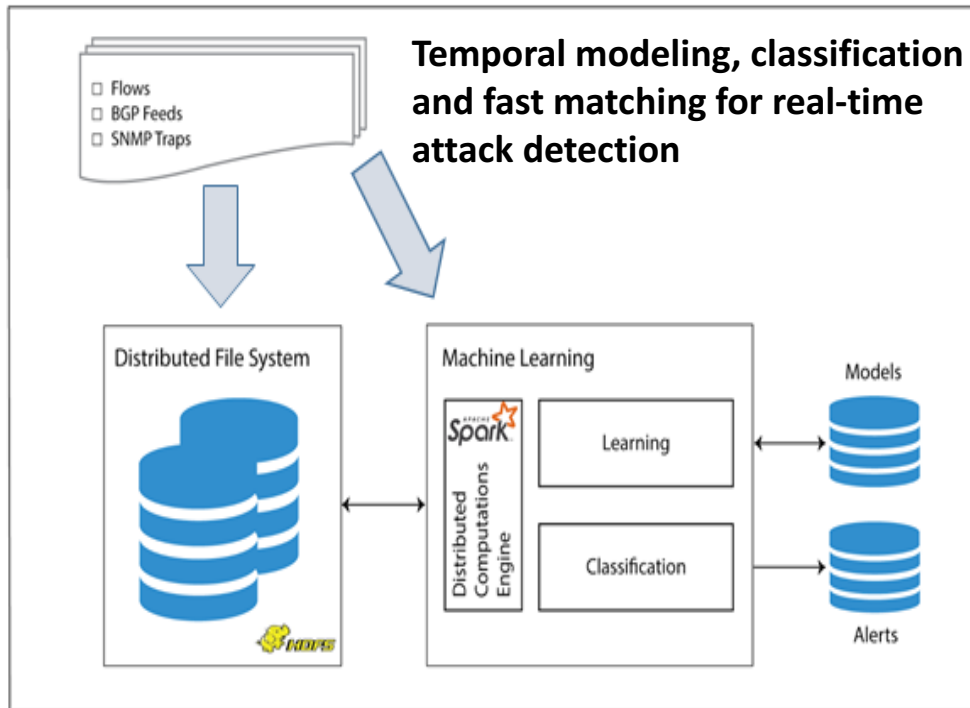
Can Attacks Be Predicted?

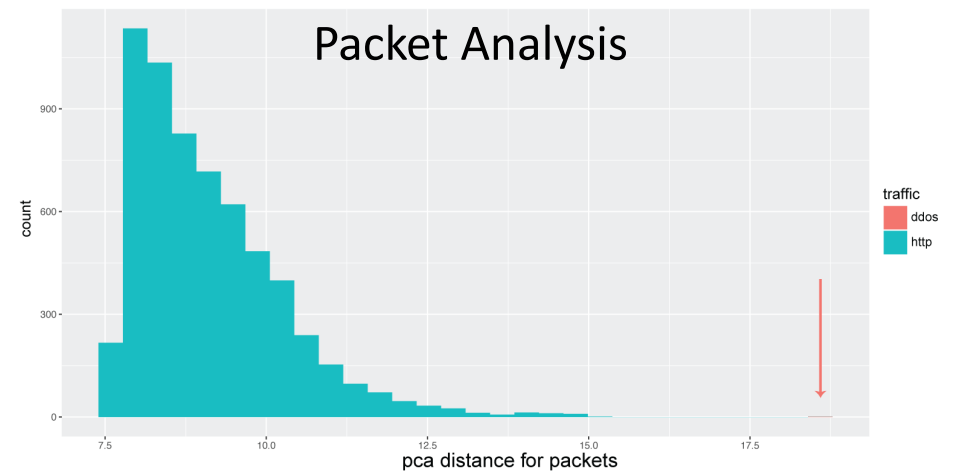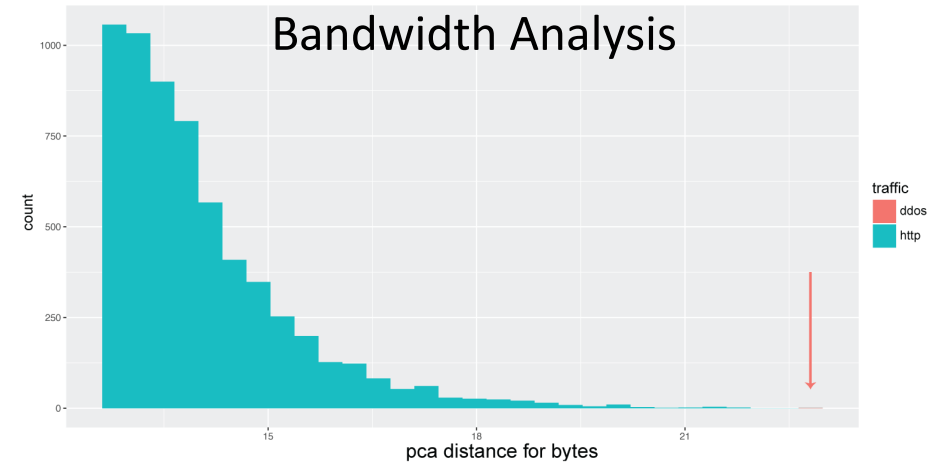Scanning activity before 2014 NTP attacks offered clues

System Architecture

Local

100G Optical Tap device

Remote

TX RX RX TX
RX TX RX TX
T X T X

100Gbps links

RX RX

SDN Controller

100 Gbps OpenFlow Switch

40G link

40G NIC | Kernel space | User space

Capture engine w/ clustered nodes

Operating System

40G link

40G NIC | Kernel space | User space

Operating System

- ❑ BGP feeds
- ❑ Flow info from external sources
- ❑ SNMP Traps

System logic

Flows | Store

Machine Learning Processing | Detect Anomalies

Decision making

Rules generation | Rules are send to the SDN controller

5

Machine Learning Component

Temporal modeling, classification and fast matching for real-time attack detection

With Machine Learning attacks that were not Visible before, easily stand out

Bandwidth Analysis

Packet Analysis

Deployment

- Pilot at CSU (ongoing)
- Larger deployment at our regional ISP (FRGP) within a year
- Expanded deployment with other upstreams immediately after that
- Requirements:
  - Optical taps for attack detection
  - 2-4U for local compute (packet->flow conversion)
  - Access to a cloud provider for ML processing
  - SDN switch for mitigation
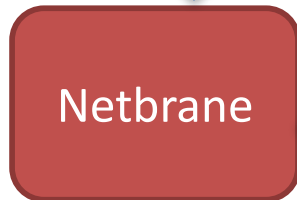
Current Prototype Deployment

Internet

4x10G

1G

SDN Switch

Traffic Monitoring

Netbrane

SDN Rules

Deploying Netbrane prototype to protect a CSU customer (in progress)
Netbrane on our regional ISP (planned)

Contact Information

Christos Papadopoulos
Colorado State University
christos@colostate.edu
+1-970-491-3267

Stephen Hayne
Colorado State University
Stephen.Hayne@ColoState.EDU
+1-970-491-7511

Michalis Faloutsos
University of California Riverside
michalis@cs.ucr.edu
+1-951-907-1501