Cybersecurity Research Acceleration Workshop and Showcase

October 18, 2017 | San Francisco, CA
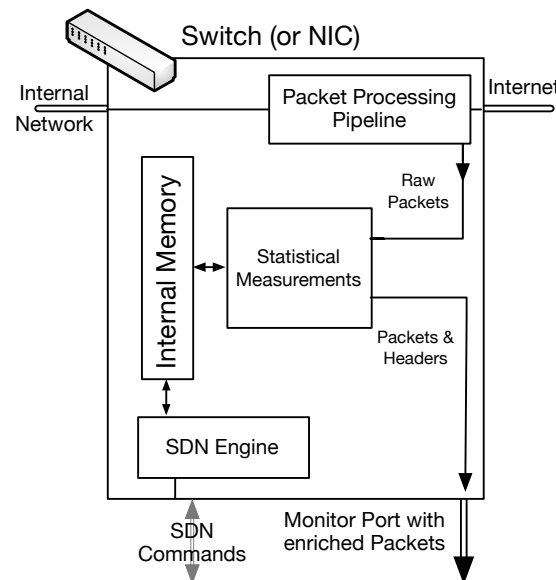
Quad Chart for: Effective and Economical Protection for High-Performance Research and Education Networks

Challenge:

- Increase performance of network monitoring for high-speed scientific environments.
- Expand visibility into research and education networks.

Solution:

- Hardware/Software co-design with:
  - Accelerated statistics
  - Connection establishment offloading
  - TCP stream reassembly
  - Hardware pattern matching
- Advance visibility for R&E networks:
  - Support domain-specific protocols
  - Enable network profiling
  - Enable better active response
  - Enforce security policies

Switch (or NIC)

Internal Network — Packet Processing Pipeline — Internet

Internal Memory

Statistical Measurements

Raw Packets

Packets & Headers

SDN Engine

SDN Commands

Monitor Port with enriched Packets

Impact:

- Enable better protection of high-speed research and education networks, specifically DMZ environments.
- Integrates with Bro network monitor already widely used in R&E community.

What we need:

- Your feedback on
  - Network visibility issues
  - Protocols used in environments
  - Current monitoring performance pain points

Contact:

- johanna@icir.org
- robin@icir.org
- dopheide@es.net