Processing Network Traffic at Line Rate

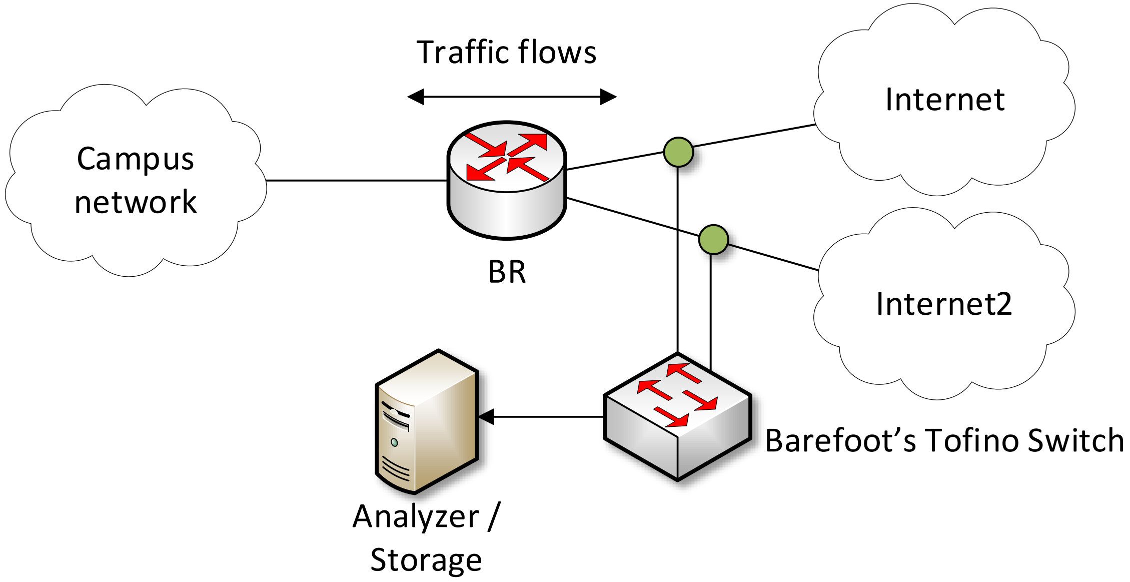
Jorge Crichigno

Presentation to the Department of Information Technology
at University of South Carolina

Online
October 21, 2020

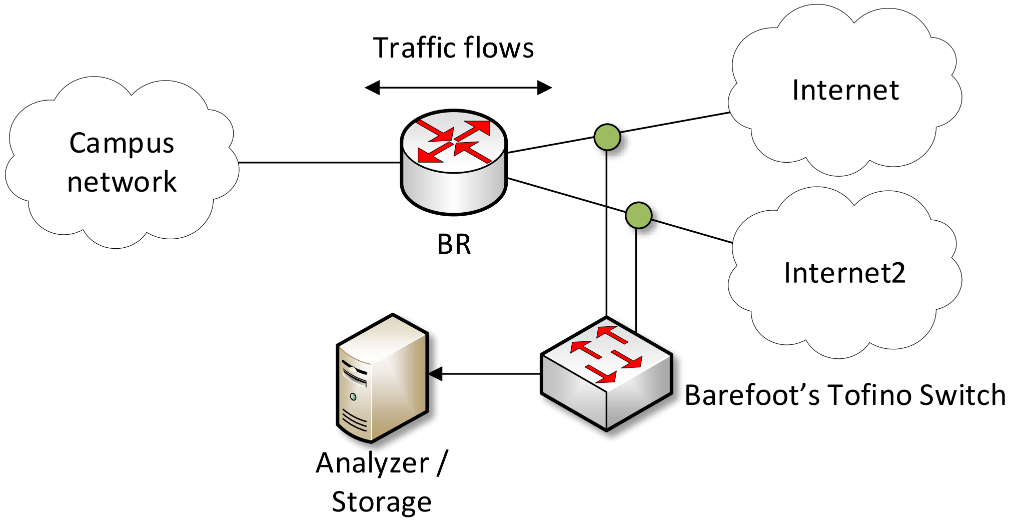
Streaming Analytics

- Streaming analytics of a campus network at line rate (100 Gbps)
- The topology consists of a Barefoot's Tofino switch that receives traffic from two taps reading traffic to/from Internet and Internet2
- An analyzer and storage server are also attached to the Tofino switch to collect the data processed by the switch



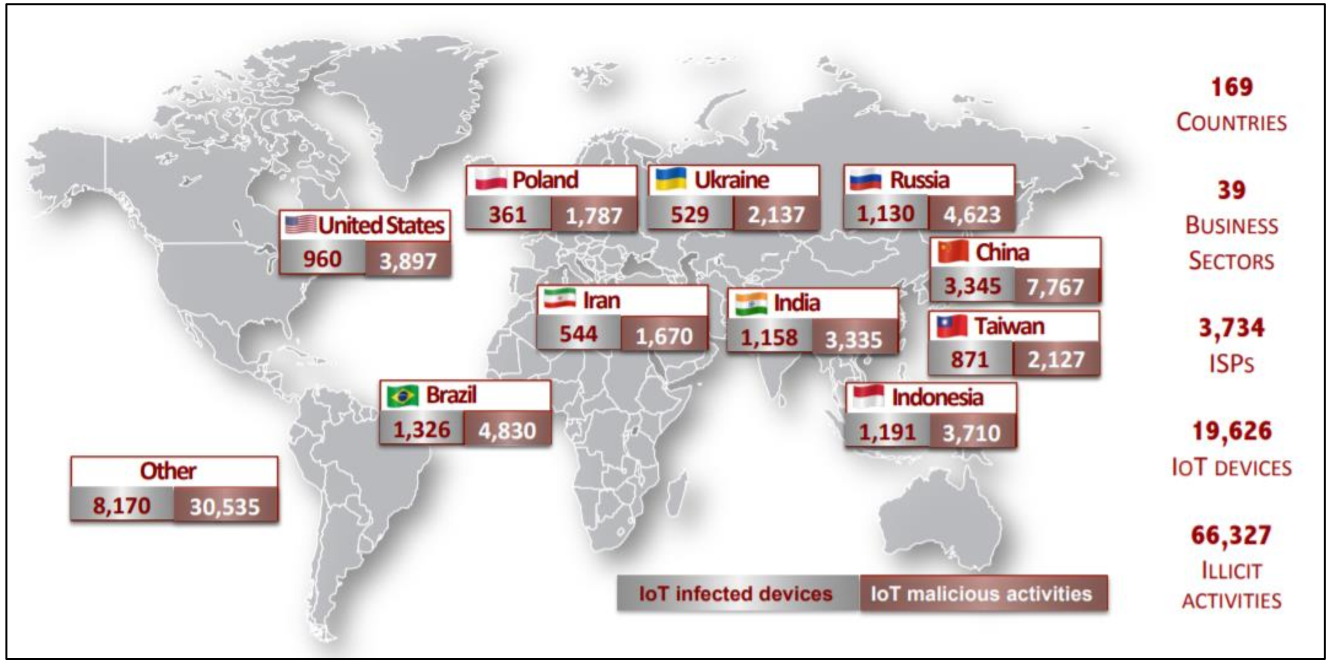
Streaming Analytics

- The Barefoot’s Tofino switch will process packet headers only; payload is discarded
- The switch will track and store flow information only (for example, src-dst IPs, src-dst ports, application layer protocol, TCP flags, number of bytes, inter-packet arrival time, flow duration, latency between src-dst pair)
- The system can anonymize traffic to feed to streaming analytics (analyzer), if needed (for example, anonymizing src / dst IP or portions of them)
- Switch can remove all Personally Identifiable Information (PII) at line rate

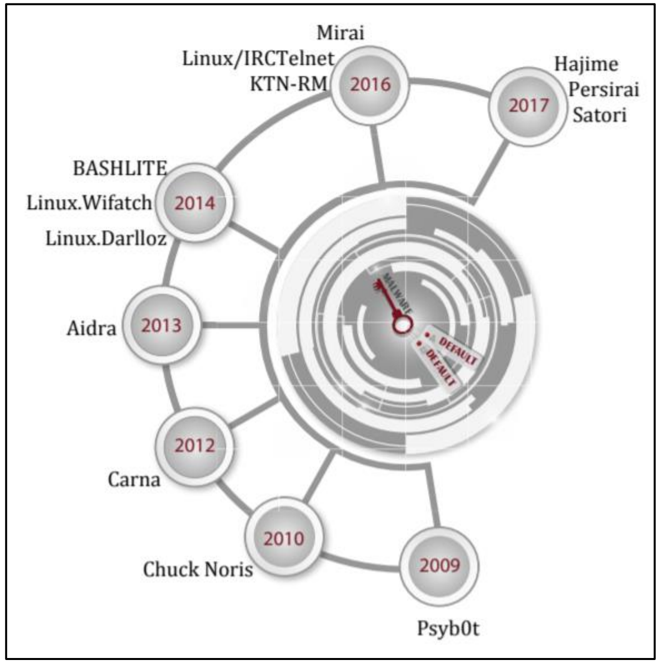


Streaming Analytics

- There is no campus network doing data analytics at line rate
- The following is an example of the type of work that can be executed
  - Detect compromised devices on campus at line rate, using passive data
  - Similar work has been conducted on non-real time, using traffic from the Center and Center for Applied Internet Data Analysis (CAIDA, www.caida.org) (University of California San Diego)



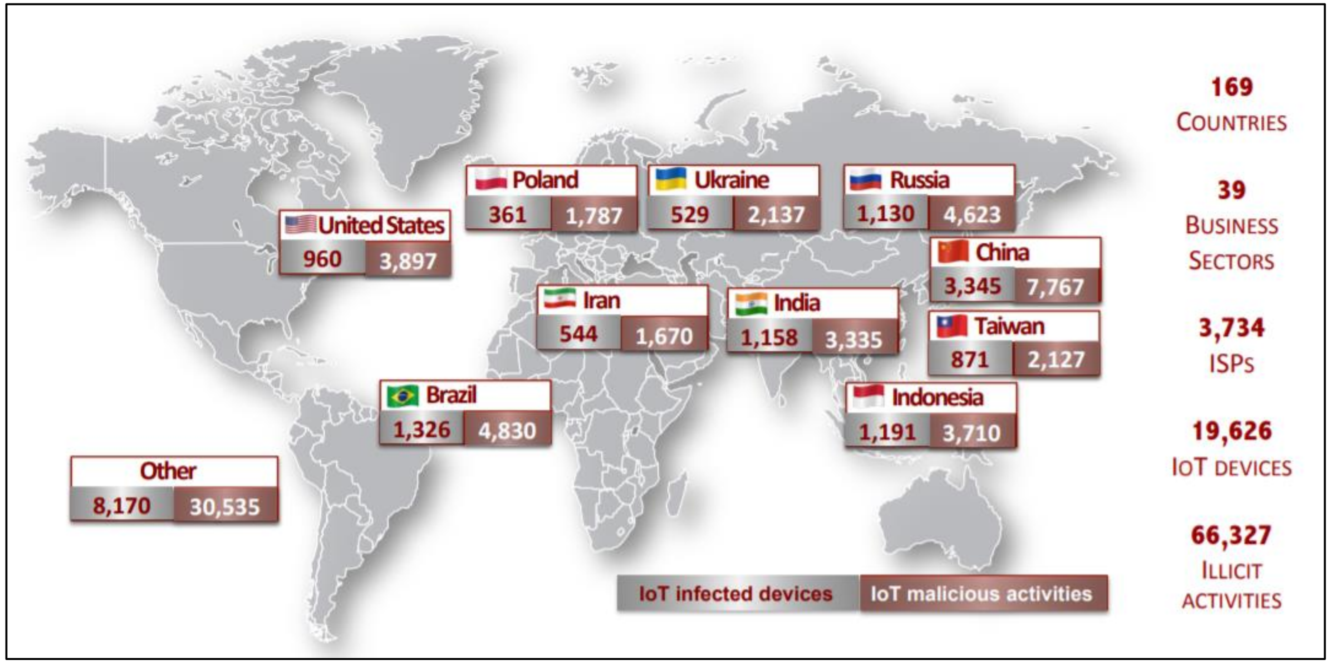
Global distribution of exploited IoT devices; results from UofSC research



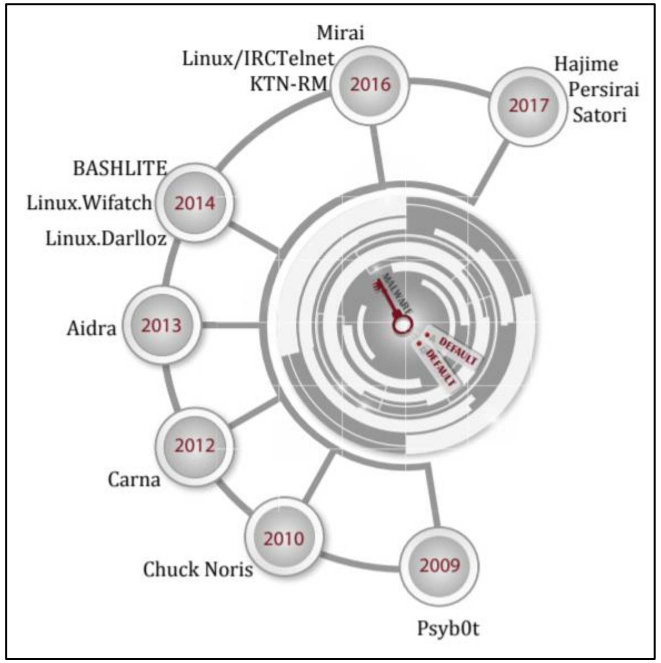
Malware exploiting default credentials

Streaming Analytics

- Global distribution of exploited IoT devices by passively analyzing packet headers from CAIDA
  - Exploited IoT devices: these devices are contacting ‘unavailable’ IP addresses (this IP block is referred to as ‘Darknet.’ No healthy device would contact this IP block)



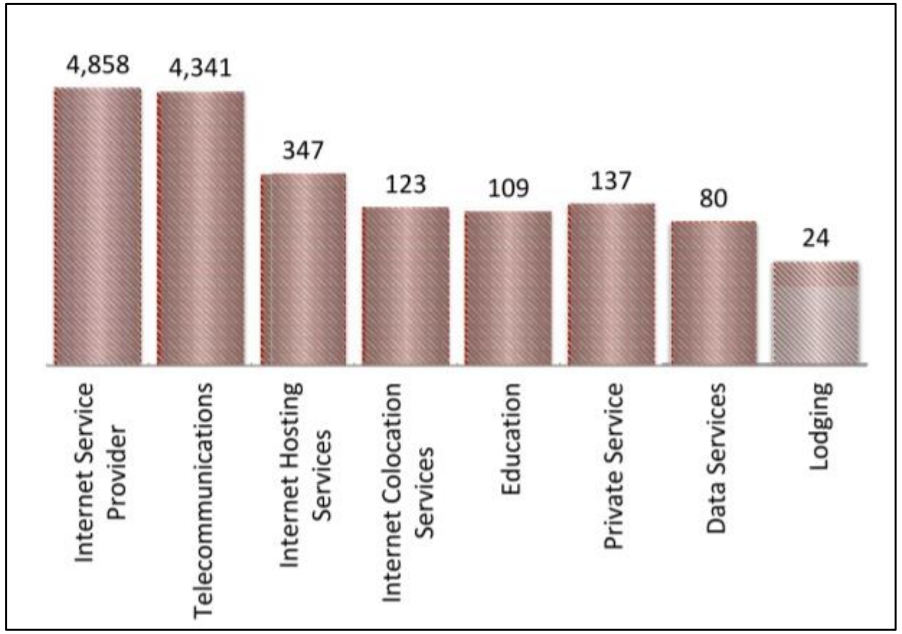
Global distribution of exploited IoT devices; results from UofSC research



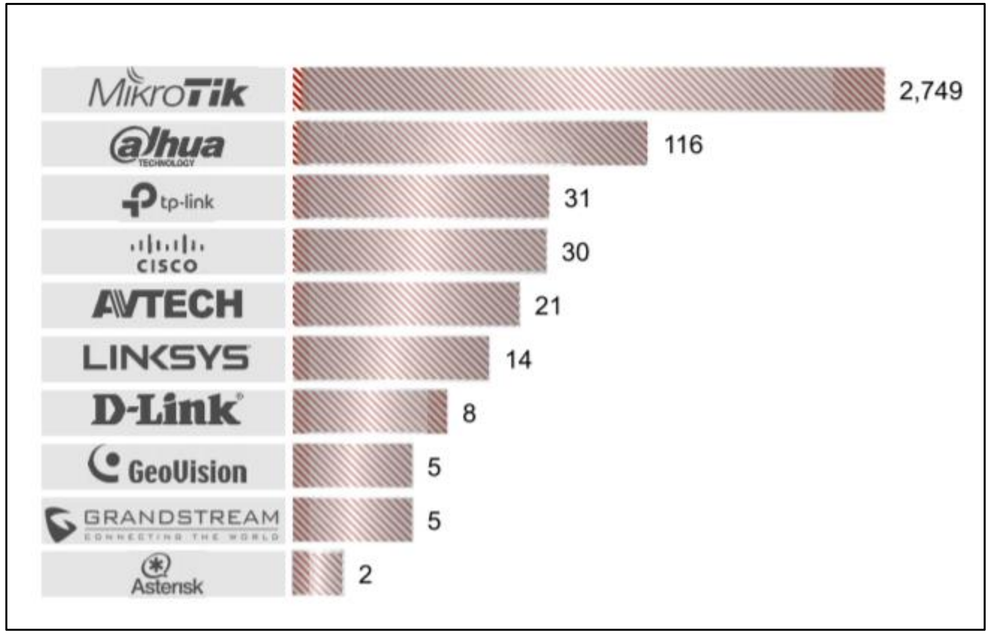
Malware exploiting default credentials

Streaming Analytics

- Global distribution of exploited IoT devices by passively analyzing packet headers from CAIDA
  - Exploited IoT devices: these devices are contacting ‘unavailable’ IP addresses (this IP block is referred to as ‘Darknet.’ No healthy device would contact this IP block)



Top sectors hosting exploited IoT devices



Top ten manufacturers of exploited IoT devices

Streaming Analytics

- This data will enable undergraduate and graduate research work
- Novel results regarding the type of threats faced by a large campus network
- Processing and detection at line rate or near line rate
- Strengthen the results of current funded project
- Funding opportunities

Streaming Analytics

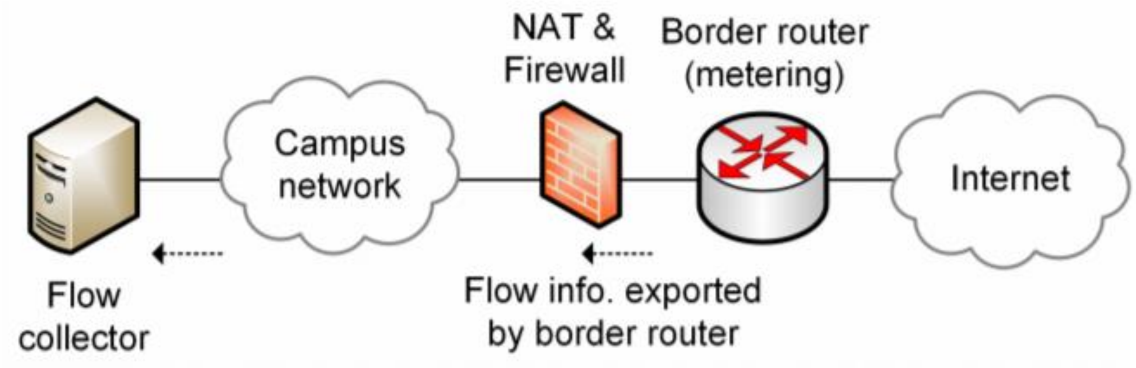
- This data will enable undergraduate and graduate research work
- Novel results regarding the type of threats faced by a large campus network
- Processing and detection at line rate or near line rate
- Strengthen the results of current funded project
- Funding opportunities

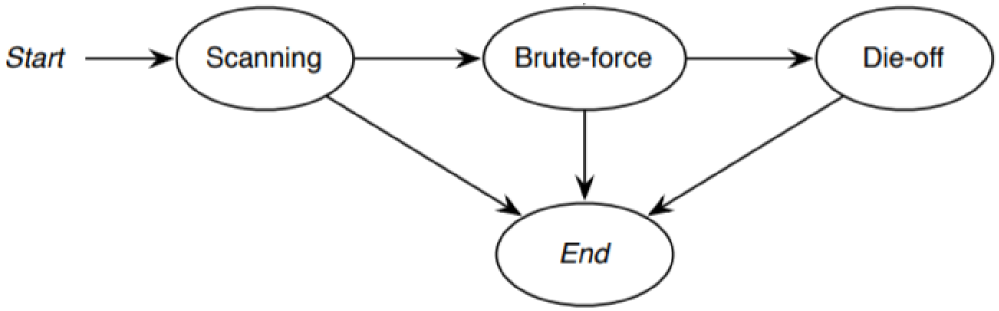
Office of Advanced Cyberinfrastructure

Cybersecurity Innovation for Cyberinfrastructure (CICI)

Honeypot

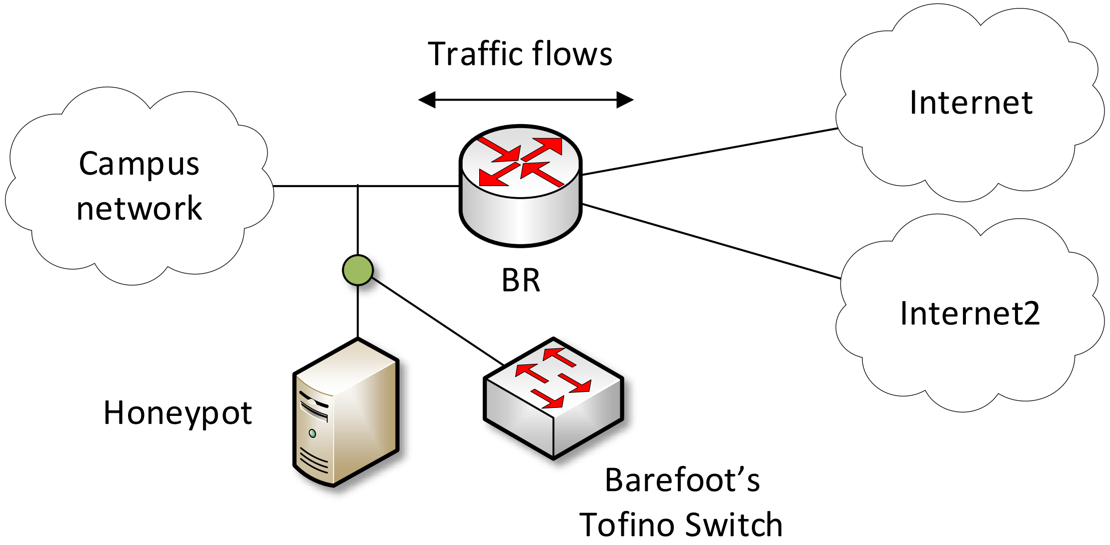
- Flow-based intrusion detection uses flow information to detect malicious activities
- Payload is not used
- Some legacy networks use Netflow to collect flow statistics; for example, SSH compromise detection





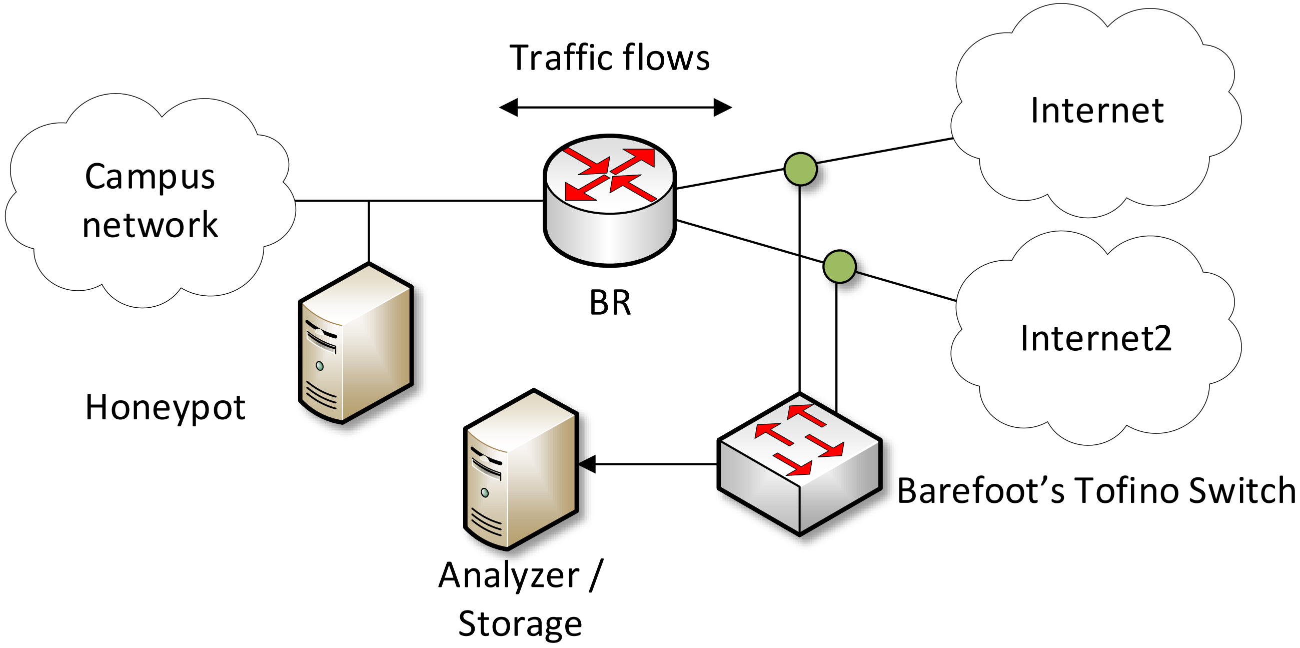
Honeypot

- The main idea is to use the programmable switch as an instrument to detect malicious activities in real time or near real time
- Customized processing (no dependency on Netflow implementations)
- Granular time resolution



Honeypot + Streaming Analytics

- Network topology


Traffic flows
Campus network
Internet
Internet2
BR
Honeypot
Analyzer / Storage
Barefoot's Tofino Switch