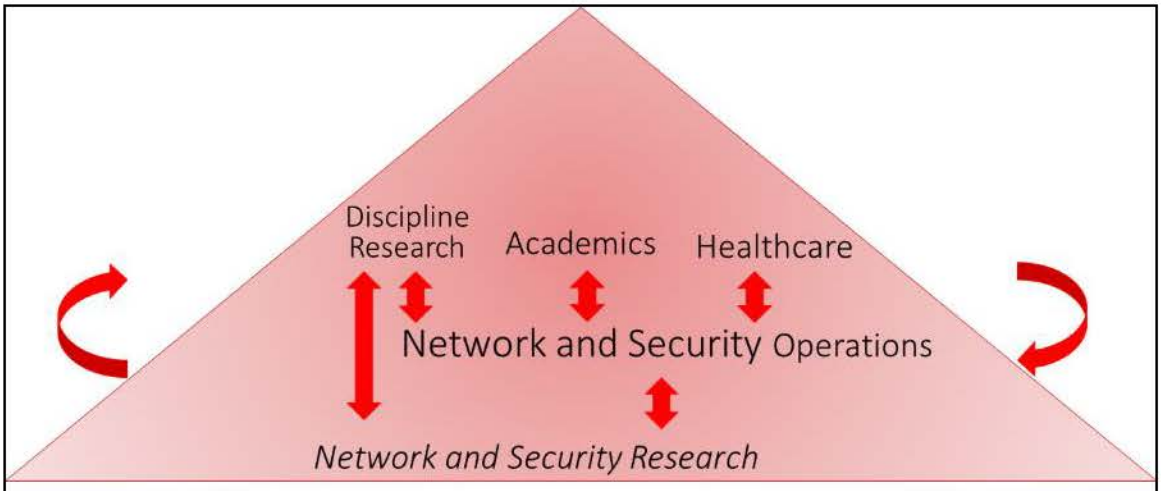


Research to Operations to University Missions

Flux Research Group
Joe Breen
University of Utah Center for High Performance Computing

What are we trying to accomplish?

- Develop network and security research ideas into operational paradigms that can enhance discipline research, academics and healthcare – the three core missions of the university.
- Create a vision of the future for network and security operations
- Create new platforms and frameworks to better support discipline research collaborations, and, network and security operations
- Enable network and security research to explore unfettered

Why are we trying to accomplish these goals?

- The three core missions of the university rely on network and security more than they ever have in the past.
- Innovative network and security research provide models and prototypes for innovative network and security operations
- Network and security operations provide interesting problems for network and security research students which provide fodder for papers and thesis projects

Flux Research Group

* Network and security are more prevalent than the past due to increasing security attacks, increased regulatory presence, i.e. PCI, HIPAA, FISMA, FERPA, etc.

How are we accomplishing these goals?

- Create infrastructure testbeds and prototype environments that can simultaneously support production work and research work.
  - Should Network research create a disruptive environment?
    - Yes, if we are to progress.
  - Should the network be a stable platform for all to use with high availability, security, integrity?
    - Yes, if we are to get work done.
  - How to use this orthogonal problem to create opportunities?
    - Opportunities to stretch the stable production world in the direction of research vision
    - Opportunities to make use of research vision to solve production issues with more efficient methods
- Create new approaches to solve difficult problems across various disciplines
  - How to use creativity in both network and security research and network and security operations to enhance other research disciplines and the academic and business missions of the university?

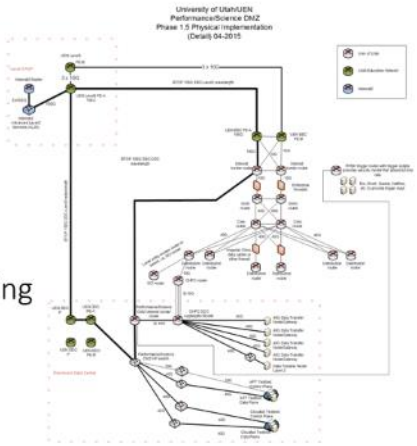
Flux Research Group

NOTE: These bullets are questions and not statements. Questions explore. Statements tell.
"The art and science of asking questions is the source of all knowledge." Thomas Berger

Flux Research Group

UTAH EDUCATION NETWORK

CC-NIE Infrastructure Investment
Part 1:
Science slices: Converting Network Research Innovation into Enhanced Capability for Computational Science and Engineering



- Science DMZ as a slice
  - Delivering Science DMZ as a Slice in the data center today
  - now in a position to deliver Science DMZ throughout campus environment over appropriate hardware through traditional MPLS and virtual routing delivery
  - one more piece of hardware needed to be able to deliver programmability to any directly connected equipment

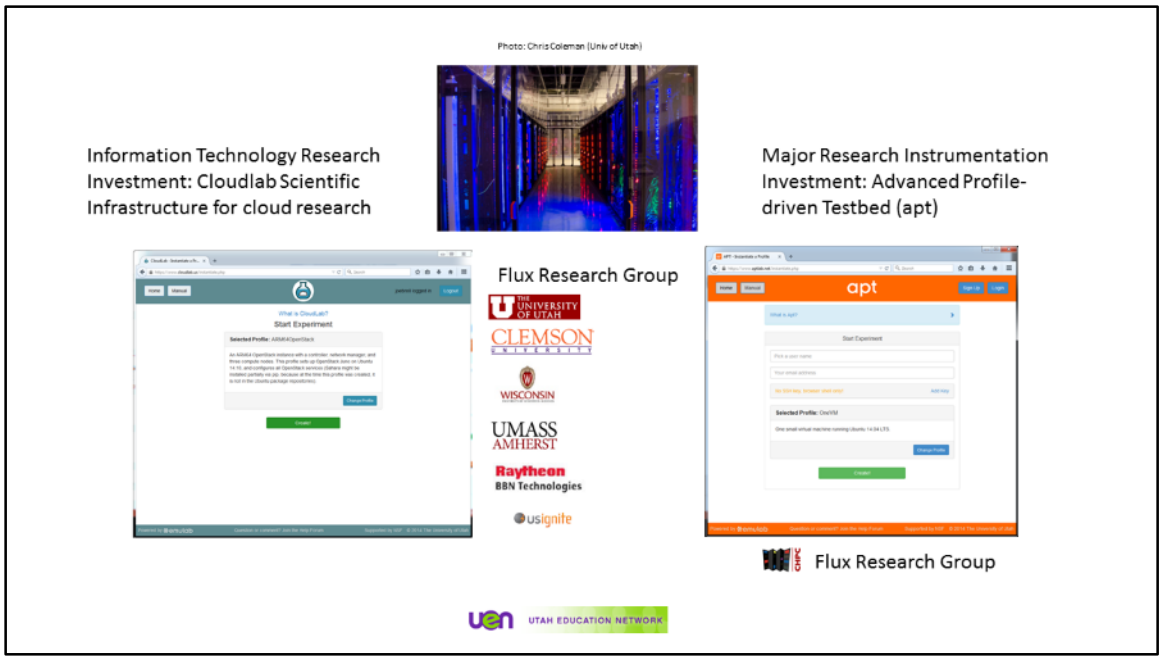


Photo: Chris Coleman (Univ of Utah)

Major Research Instrumentation (MRI): Apt: Utah internal collaboration to create a profile driven testbed for network/security experiments and HPC development

- Enabling prototypes of dynamic bare metal HPC image with ability to expand/shrink and simultaneously supporting other experiments
- Enabling multiple papers for various network and security experiments
- https://www.aptlab.net/ --
- http://www.nsf.gov/awardsearch/showAward?AWD_ID=1338155&HistoricalAwards=false
- http://aptlab.net

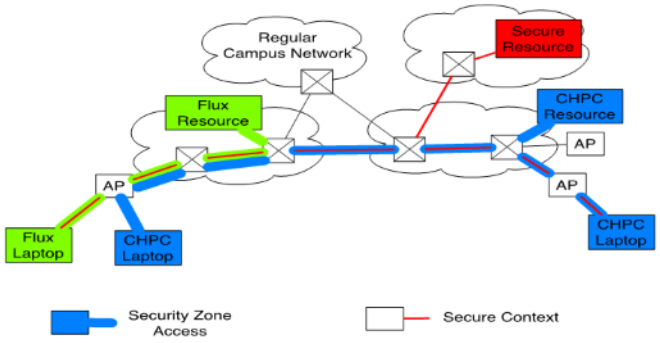
Information Technology Research: Cloudlab: Utah led collaboration to create a national profile-driven testbed supporting multiple hardware platforms and Software Defined Networking

- Enabling multiple papers for various cloud experiments
- Enabling future prototype of dynamic HPC image in multiple locations
- Enabling power investigation of low power processors in a cloud
- https://www.cloudlab.us/ --

CC-NIE Part 2: "Opt-in"

- What does "Opt-in" really mean?
  - Getting to what you really want with the right network and security characteristics
- Opt-in implies:
  - data driven
  - service driven
  - Security characteristics
  - network characteristics
- Opt-in drives the need for strong, dynamic network operations support, provisioning, management, and visibility

KnowU campus prototype



- Security contexts – Can we realize aspects of our campus data-driven security policy and manage the infrastructure seamlessly?
  - Fine grained
  - Use SSO to perform **network level access control**
  - Successful SSO authentication/authorization: dynamic user specific access to secure resource
  - Secure context after successful access to security zone

Flux Research Group

KnowU Proposal: Collaborate with the UIT Network, Security, and Identity and Access Management teams to develop a prototype platform to explore emerging network technologies, and network and security management approaches in the context of the University of Utah campus network

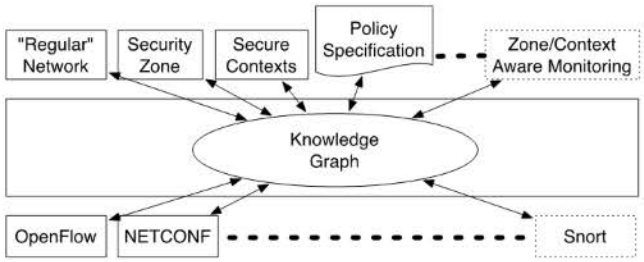
KnowU Proposal IT Goals:

- Experiment with using both "conventional" networking and software defined networking (SDN) approaches in the same network.
- Experiment with the use of "white-box" network equipment together with equipment from traditional vendors.
- Develop fine-grained security zone enforcement and monitoring mechanisms using SDN for both wired and wireless networks.
- Move towards automated network and security management

KnowU Proposal Research Goals

- Apply knowledge-centric approach to perform automated network management functions in a semi-production network environment
- Develop network management application(s) to realize fine-grained security zones on both wired and wireless networks.
- Explore application specific monitoring and management.

KnowU Architecture



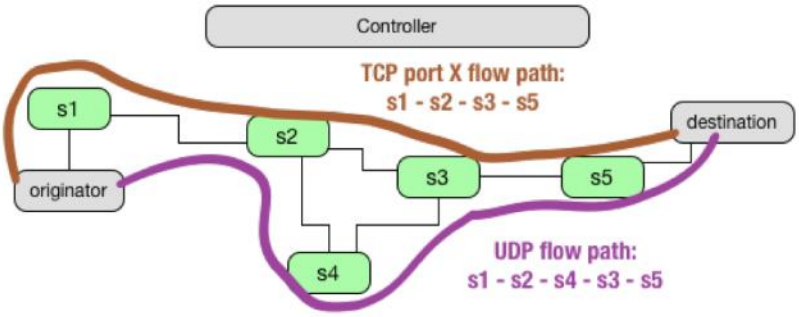
- Knowledge-centric approach
  - All data/knowledge/information about network stored in a knowledge graph (KG)
  - Network management:
    - applications interacting via KG
    - use, add, modify data in KG
    - result in network configuration changes (OpenFlow/NETCONF)

Need for tools operating at true flow level

- Tom Lehman (MAX): "I don't want to control every flow on the network, I want to control ANY flow on the network"
- How to look at flows regardless of protocol?
- How to look at flows across dynamic topologies?
- How to actively measure dynamic topologies to provide baselines of network characteristics?

SDNTrace

- Implemented as Northbound application/process on each hop with defined protocol
- Carries all path information in reply message
- Uses existing path state
- Specific to individual flow path
- Agnostic of higher layer protocols
- http://sdntraceprotocol.readthedocs.org/en/latest/



Research and prototype implementation: Deniz Gurkan, Nicholas Bastin, Ali Kouhi Kamali, Long Tran

Original operations problem description: Michael Van Norman, Dan Schmiedt, Chris Konger, Dale Carder, Kevin Mayeshiro, Joe Breen, Anita Nikolich - Internet2 SDN Working Group 2014; refinements by Internet2 SDN Working Group as a whole

Documentation:

- http://sdntraceprotocol.readthedocs.org/en/latest/
- https://media.readthedocs.org/pdf/sdntraceprotocol/latest/sdntraceprotocol.pdf
- https://bitbucket.org/dgurkan/sdntrace_protocol/overview

Original problem charter:
https://spaces.internet2.edu/display/sdn/Project+Charter+Draft

Active Measurement in network sliced world/network virtual world

- Measuring a base network substrate yields a baseline for all virtual networks crossing that portion of topology
  - What visibility exists when the virtual environment goes over another portion of topology that does not have measurement?
  - What visibility exists when the virtual environment crosses administrative domains?
  - What happens when the topology changes?
- How does one actively measure particular virtual environments?
- How does one actively measure multiple environments without causing more measurement than production traffic?
- How does one inject measurement into a "virtual network of interest"?
- Exploring a framework based on BLIPP, UNIS, HELM

Research and prototype implementation: Miao Zhang, Bruce Mah, Joe Breen, Ezra Kissel, Brian Tierney, Eric Pouyoul
Other collaborators: Eric Boyd, Martin Swany, Luke Fowler, Ed Balas

Research Projects and Papers

- DeidTect – Towards a Distributed Elastic Intrusion Detection
  - https://www.flux.utah.edu/paper/shanmugam-dcc14
- SeaCat – End to End application containment
  - http://www.flux.utah.edu/project/SeaCat
- FlowOps – FlowOps: Open Access Network Management and Operation
  - https://www.flux.utah.edu/paper/strum-thesis
- KnowOps – Network Management, Software Defined
  - https://www.flux.utah.edu/project/KnowOps
- TCloud – Self-defending, self-evolving, and self-accounting trustworthy cloud platform
  - https://www.flux.utah.edu/project/tcloud

Examples of other research that look at the network based on flows and how to automate network management, visibility, operations, etc.

Challenges and shortcomings of today's technologies (a.k.a. opportunities)

- Challenges
  - Researcher expectations vs how IT operations go...
  - Hooks into Federated Identity and Access Management
- How to better obtain clarity and transparency of what each vendor truly supports?
  - Clear datasheets regarding SDN offerings
  - Clear descriptions of exactly what OpenFlow features supported, how these features map in memory
  - Test results to be provided with time, message, and state diagrams, etc. (These may be NDA but have them available for customers.)
  - Clear descriptions of what controllers supported well
- Truly flow based toolsets, visibility into the flows, collections of statistics per flows, standard flow-based APIs
- Ability for hardware to fully support features such as multi-table, meter table supporting full rate limiting of traffic, more flexible match capabilities,
- Easy consistent access to topology information
- Security, i.e. rate limits on control plane, additional visibility for the data plane, etc.

Summary

- Research <-> Operations <-> Missions of the University of Utah
  - Develop network and security research ideas into operational paradigms that can enhance discipline research, academics and healthcare – the three core missions of the university.
  - Bring back harder questions to feed into research
- What do you really want?
  - Data-driven
  - Services driven
  - Specific network and security characteristics
- These drivers require flow based tools and frameworks to provide the management, operations, visibility, provisioning, etc. at the granularity, performance, and security level desired.