2014 Inter fd8fe

2014 Internet2 Global Summit

2014 Internet2 Global Summit

- Notes:
- Fortinet Fortigate 3810D (100gb capable firewall)
- 19% of this year’s participants are women. 30% of speaker are women. I2 and ESNet working to improve diversity.

27 Oct Keynote Harper Reed

- Obama Campaign 2012
- hired engineers rather than interns, about 40 engineers
- narwhal was a consistent API that then got used by various tools like dashboard, mobile apps, contribute, calling, etc.
- big data is a misnomer, but did lots of data analytics
- why celebrate storage? celebrate questions and answers
- used modeling to not only track your most likely donation, but also who you influence
- moved the campaign from just micro-targeting to 2-way conversation
- we use ubuntu because we’re adults
- building a great team
- not easy
- pruning - don’t be afraid to fire people
- always be creative
- hire people who are smarter than you
- trust
- measure everything
- don’t be afraid to hire people that look different from you (diverse team makes better products)
- practicing failure
- failing is hard, but important to understand, improves success
- difference between functional and usable
- A/B testing

- allowed us to understand where we we were wrong
- fail safely — when it fails, it should cause no harm
- practice! (game day)
- similar to chaos monkey approach
- created runbacks from the failure tests
- facilitating community
- community is #1 external asset
- focus on authenticity
- purpose
- empowerment
- most important:
- safety
- normal person + anonymity + audience = troll
- create an environment worth trusting!

27 Oct Tech TalK: Stacy Morrone “Pushing the Boundaries of Traditional Classrooms”

- tell me and I forget. teach me and I remember. involve me and I learn. Benjamin Franklin

27 Oct Dave Meyer, CTO at Brocade: On the Hidden Nature of Complex Systems:

- Initial start: if IP networks are simpler (than ATM, FR, TDM, etc) why is OPEX and CAPEX so much higher?
- he was at Sprint and working under the IP division, got re-orged under ATM and Kansas City
- Initial investigation:
- Simplicity Principle: too much complexity = too much cost
- but what IS complexity? no explanatory power, confused symptoms and root cause
- What is complexity?
- hidden structure that arises in systems
- purpose is to create robustness to environmental and component uncertainty
- lots of stuff under the hood that you don’t notice until something breaks
- why hidden?
- fundamental property of complexity
- universal architecture principles (layering, constraints that deconstrain) acts as an abstraction layer

- Pmax - on the left side of graph, domain of robust, once you pass the tipping point, enter the domain of the fragile
- Robustness
- scalabiity - robustness to changes in size and complexity
- reliability - robustness to component failures
- efficiency — resource scarcity
- modularity — component re-arrangements
- robustness — preservation of a certain property in the presence of uncertainty in components or the environment
- Fragility = opposite of robustness
- you are fragile if you are dependent on 2nd order effects
- Complexity/Robustness spirals (Robust yet Fragile)
- make some changes to add robustness, what you change, has its own fragility and bugs,
- if you create robustness somewhere, you will create fragility somewhere else
- Tradeoffs
- tradeoff frontier on complexity curve
- Understanding “Robust Yet Fragile” is THE challenge
- understanding universal architectural principles
- how do you manage spiraling complexity/fragility
- don’t focus on what is likely or typical, but what is catastrophic

27 Oct James Donn on Splunk/Cloud Mgmt: Security and IT analytics

- Splunk and NetPlus
- Overview of Splunk functionality and architecture
- some examples from Harvard
- Cloud
- Splunk > cloud
- hosted solution at AWS that splunk runs for a single tenant
- splunk > storm
- bad initial start at initial cloud offering
- splunk > enterprise
- traditional on-prem
- splunk > running on AWS AMI’s

- Splunk Hybrid Search
- datacenter, private, public cloud
- 1 search head to different on prem and cloud solutions
- Splunk Stream
- picks up network data via tcpdump

28 Oct Opening up Innovation

- Overview of AL2S by Rob Vietzske
- University of Utah Campus Network Requirements by Steve Corbato
- segmentation drivers
- Science DMZ's
- vulnerable devices
- protected information
- high reliability (bio-specimens, research)
- close tie to campus IAM
- centralized and scalable device mgmt
- IPv4/IPv6
- lower total cost of ownership
- Partnership
- campus partners
- network research, emulate, protein
- computational science
- production network
- advanced regional network
- external partners
- internet2, GENI, NSF, NOAA, UDOT, UTA
- ACI-REF
- Looking to build a Science DMZ on top of SDN, rather than plugging SDN into it
- APT (advanced profile driven testbed)
- CloudLab (Utah, Clemson, Wisconsin, UMass Amherst)
- Need to look into EmuLab and GENI
- Bill Snow of On.Lab
- On.Lab is a non-profit development organization
- focus on Internet and Cloud Service Providers

- ONOS SDN Use Cases
- multilayer SDN control of IP and optical
- peering of SDN islands with rest of internet
- NF as a service in central office
- SDN based WAN control w/ segment routing
- SDN-IP for external networks
- peers via BGP with Internet routers, presents itself as another AS
- Larry Peterson also from On.Lab
- Open Cloud: value add cloud on Internet2
- set of large clusters in Internet2 POP's and regional networks to start providing cloud infrastructure
- services instantiated o a set of VM's connected by a set virtual networks (VN's)
- cloud = datacenter + backbone + edge
- building a 4th tier on top of commodity stuff
- leverage internet2 infrastructure for performance
- key enablers for Open Cloud
- XOS - Service Orchestration
- Network Hypervisor (OpenVirtX)
- Service composition
- Syndicate - a CDN
- Moving into OpenCloud pilot shortly
- Observation:
- Insist on vendor-neutral northbound interfaces in your SDN capable products
- networks shouldn't be about plumbing but service provisioning

28 Oct Securing Science DMZ

- relatively open networks, border noise reduction
- science DMZ is essentially an enclave on the network w/ 100gb
- lots of collaboration on funding, network planning, security, customer requirements
- common components:
- enclave firewall
- IDS or IPS
- host-based protection

- Bro, an open source network security analysis tool, is heavily used in cluster mode for 100gb science DMZ's by multiple institutions
- Bro is apparently much more awesome than many existing IPS systems
- GridFTP and perfSonar are common tools in Science DMZ's as well
- most of the Science DMZ's being deployed today are single-tenant, not a lot of multi-tenant infrastructure planning being done

28 Oct Grover Browning, AL2S and production support of research

- gcbrowni@iu.edu
- basically building layer 2 VLANs on Internet2
- about 80 workgroups using AL2S today on I2
- about 250 people authorized to build VLAN's today
- in last 4 months, about 9000 calls using API to create or teardown VLAN's
- about 600 VLAN's across AL2S infrastructure
- used for both research and operations, I2 has no visibility into what's going across these VLAN's though
- XSEDE is the poster child for AL2S use cases. They built a multi-point layer2 network for research purposes
- University of MO — simulation as a service, remote sensor beacon network for elder care
- Clemson is also using AL2S for their stuff
- much easier and cheaper than an MPLS VPN service. You just have your own private VLAN service.

28 Oct ACI-REF Panel "Condo of Condo's" w/ James Cuff and co.

- allows institutions to collectively compete for grants, rather than individually
- really need to get Nick plugged in w/ Clemson and their network team and their service model for working w/ RC

29 Oct Pushing the Boundaries of Traditional Classrooms

- first iteration of improvements
- group-based desks, mix of regular and bar height, portable white boards
- teachers stuck on wanting to still use projectors and standard whiteboards
- interactive whiteboards were too fussy to use
- teachers had to apply to use the room, not great for traditional lecture, but good for collaboration

- “it felt like I was in a big living room”
- Steelcase Learn Lab
- long rows of collaborative tables
- projection screens at weird angles
- not terribly popular
- other designs working better
- a design from Steel Case
- Video Conference class rooms
- issues: can’t move anything, can’t touch anything
- space should be reconfigurable
- eagle eye cameras from polycom, moves to who is talking
- see presentation. This wasn’t that interesting to pay attention to.

29 Oct Keynote:

- Privacy and Cyber-Security
- Lee Hamilton — have we lost the battle on privacy already?
- Organizations can likely already find out what they want to find out.
- we’ve found out a lot of stuff in last several months as government “confesses” to some activities post-Snowden
- checks and balances — too many of the checks are exclusively in executive branch.
- FISA courts not performing anywhere to his satisfaction
- this is the largest expansion of government power in his life time
- Fred Cate
- if an engineer were approached by DHS to disclose systems data, may not be able to even tell his supervisor
- only recently, rules have changed so that he can tell OGC and another person necessary to gather the information
- we are bargaining our privacy for access to certain services or discounts (rewards cards, EULA’s, etc.)
- need a cyber security commission
- President, NSA etc. only started talking when it was disclosed. They haven’t really said anything substantive since then.
- self-government is one of the most monumental achievements of humankind
- build in as much privacy as possible. help lawmakers. don’t lose sight of cybersecurity challenge.

- Brad Wheeler
- no negotiating when you have no power. privacy policies can be changed every day.
- too many actors, need unity of effort
- law lags behind the threat
- if its free to you, you're not the customer, you're the bait
- IU does not let schools and professors manufacture financial risk by taking their own credit cards. we also need to lock down cyber security risk more seriously
- Bottom line:
- self-government can work. Needs to be applied more to privacy and cyber-security. needs to be activated and energized to provide more conversation, balance of power, accountability
- technology can't solve it by itself. always circumvented eventually

100gb based Open flow science DMZ

- Open flow
- Perf sonar
- Bro

Various Vendor Conversations

- Aspera (owned by IBM) as 10gb/100gb cost effective network vendor, highly programmable ASIC
- Matrix Integrations as a R&E specific VAR
- strong in SDN space and optical space
- reselling Tallac SDN starter kit
- Technology Concepts Group, Intl
- single stream for vendor sourcing, negotiations
- Fortinet
- new 100gb capable firewall 8710d (?)
- got brochures on this
- Ciena
- got brochures on the 6500 (traditional optical) and the new 8700 platform (more SDN/MPLS-based)

Multi-layer SDN for flexibility in R&E networks

- based on experiences w/ SDN at GEANT
- Generation 1 test bed

- Géant Open Flow Facility
- SDN focused testbed based on Xen hypervisor w/ full mesh of open vswitches
- Gen 2 test bed
- DyNPaC
- CEOVDS

30 Oct Open Daylight

- Cisco's take on Open Daylight
- it's about applications, best quality of experience, openness, flexibility
- gaining momentum
- cisco open sourcing many components of ODL
- cisco network applications, built to work w/ ODL
- wan automation engine
- bgp-ls topology
- path manager
- netconf acl editor
- hyperglance
- wan automation engine
- openflow manager - can program and visualize flows
- nexus data broker (tap and span, monitoring, aggregation)
- cable operator apps
- supported platforms
- nexus 5, 7, 9
- catalyst 3, 4, 5
- Brocade's Take on OpenDaylight
- current network industry landscape is vendor dominated in terms of features, updates, tweaks, etc. Users have to wait for features
- w/ open source, balance can shift more to users
- lots of momentum on ODL as platform of choice, Linux Foundation behind it
- Use Cases for ODL
- custom analytics and compliance
- big data
- service configuration and policy
- research and new protocols

- security
- QoS and traffic mgmt
- WAN optimization
- One example
- bandwidth calendaring, increase bandwidth for certain users at certain times of day
- Q&A
- Brocade — competitive advantage between vendors may not continue to be on proprietary features but how well they support innovation through ODL and SDN
- Cisco — that plus hardware performance
- cisco moving more to merchant silicon
- N9k a lot cheaper as a result
- REST API
- is there, can't do everything with it.
- REST CONF (?) is a better API method for programmatic access due to data types
- ODL likely not a full-blown orchestration platform, will likely stick to networking
- ODL most used for research networks, Science DMZ type stuff, not yet much on standard campus network
- "hybrid mode" - division between campus and SDN-based enclaves

30 Oct Securing SDN

- bridge to SDN — use hybrid BGP/SDN
- goal
- build a multi-domain distributed architecture
- better inbound path declaration
- shared policy across sites
- no need for topology awareness, nor heavyweight L2
- no low-level (open flow) details exposed
- my AS, my policy
- Security Issues w/ BgP
- too many humans involved
- social issues
- existing security solutions (like BGPSec and RPKI) are too onerous
- Security issues w/ SDN
- forged traffic flows

- attacks on switches
- attacks on controllers, etc.

#learning/conferences