Networking and Security Research (NSR) Group Overview (Sept 2022)

Eric Keller

eric.keller@colorado.edu

https://eric-keller.github.io/

My mission is to make even the most complex network infrastructures dead simple to manage…

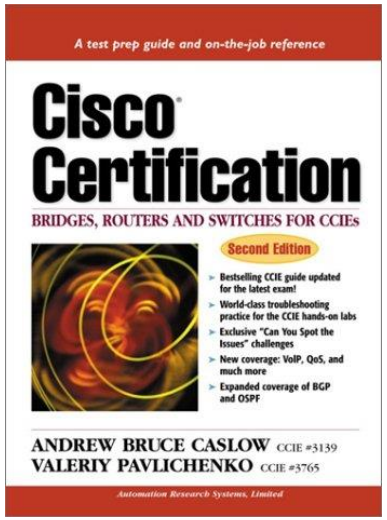
… through programmability

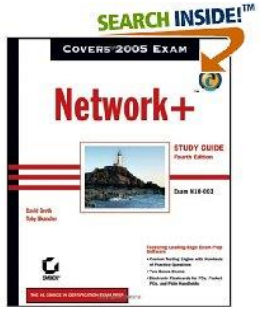
It is my belief that many of the issues we are having are people problems. We need automation, we need holistic, programmatic management where computers can define and verify.

Networking (perceived) vs Networking (our research)

How Practitioners Learn Networking

1. Certification courses on how to configure specific pieces of equipment

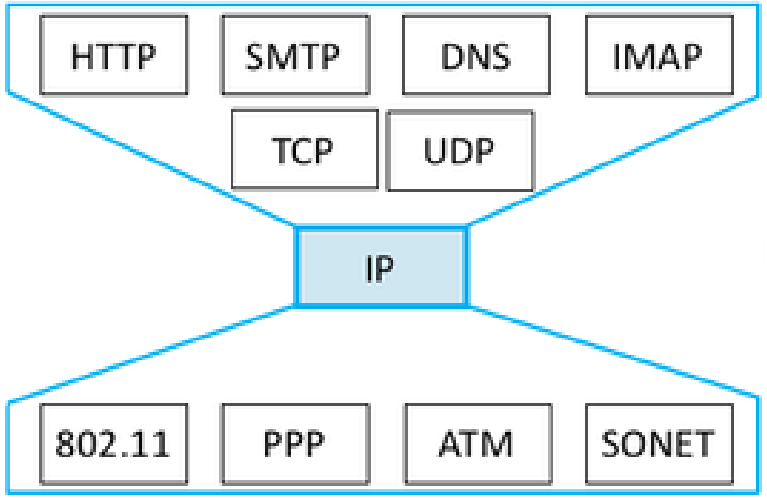




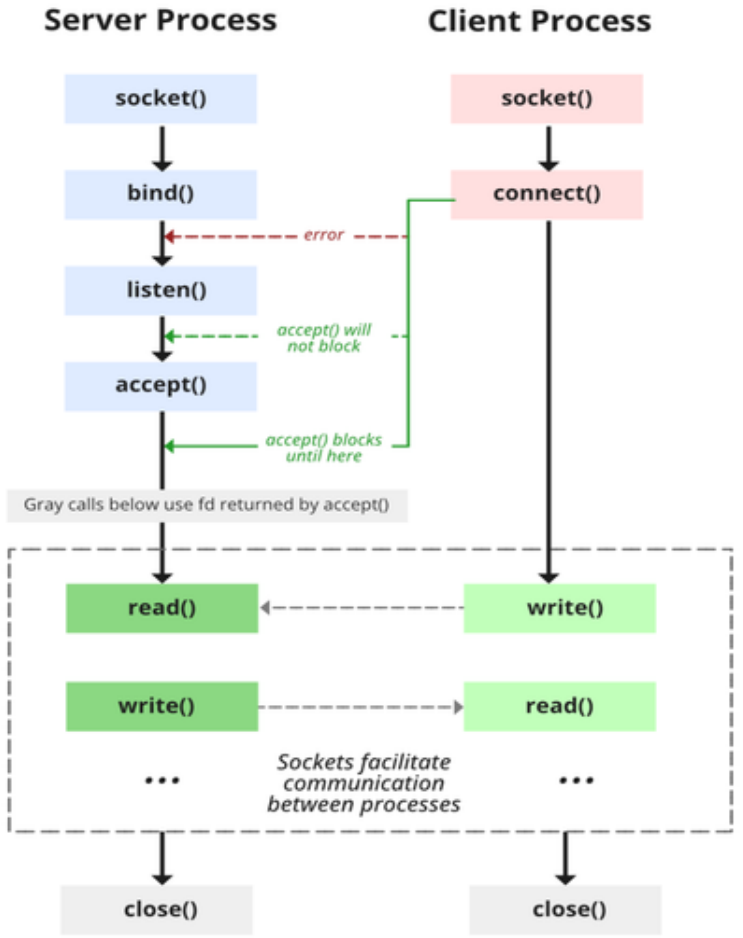
2. "On the job" training

How Colleges Teach Networking

OSI Layers



Sockets programming



My Research

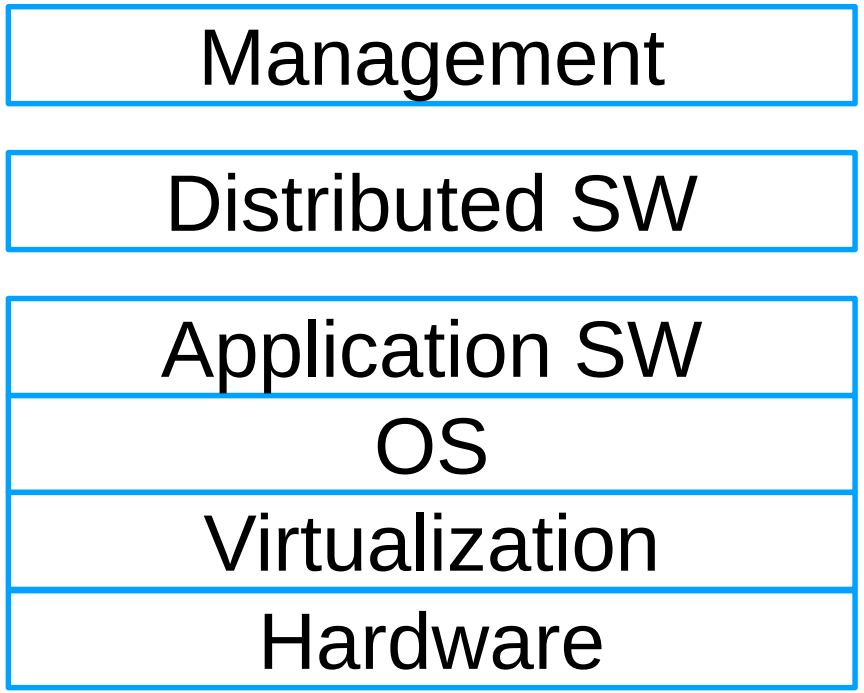
- Exploring the computer systems issues
- in enabling programmability (of traditionally non-programmable systems)
- and leveraging that programmability
- for a secure, reliable, efficient, easy to manage network infrastructure.

Networks everywhere, systems are complex

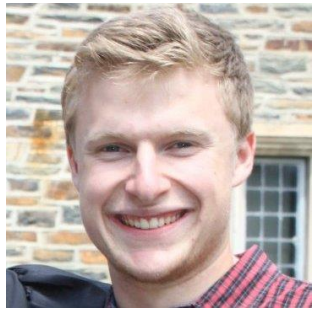
- Internet
- Data centers
- Virtual/container Infrastructure
- Data infrastructure
- Embedded infrastructure

=> 3 main pillars: Compute, Storage, Network all work together

At all layers of the computing stack

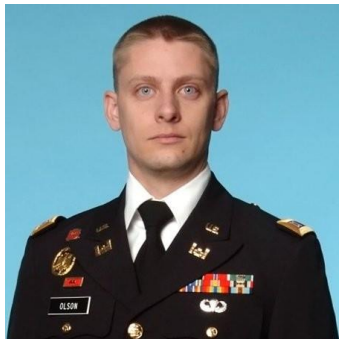


The Current Team



Greg Cusack

Marcelo Abranches



Karl Olson

Maziyar Nazari

Dwight Browne

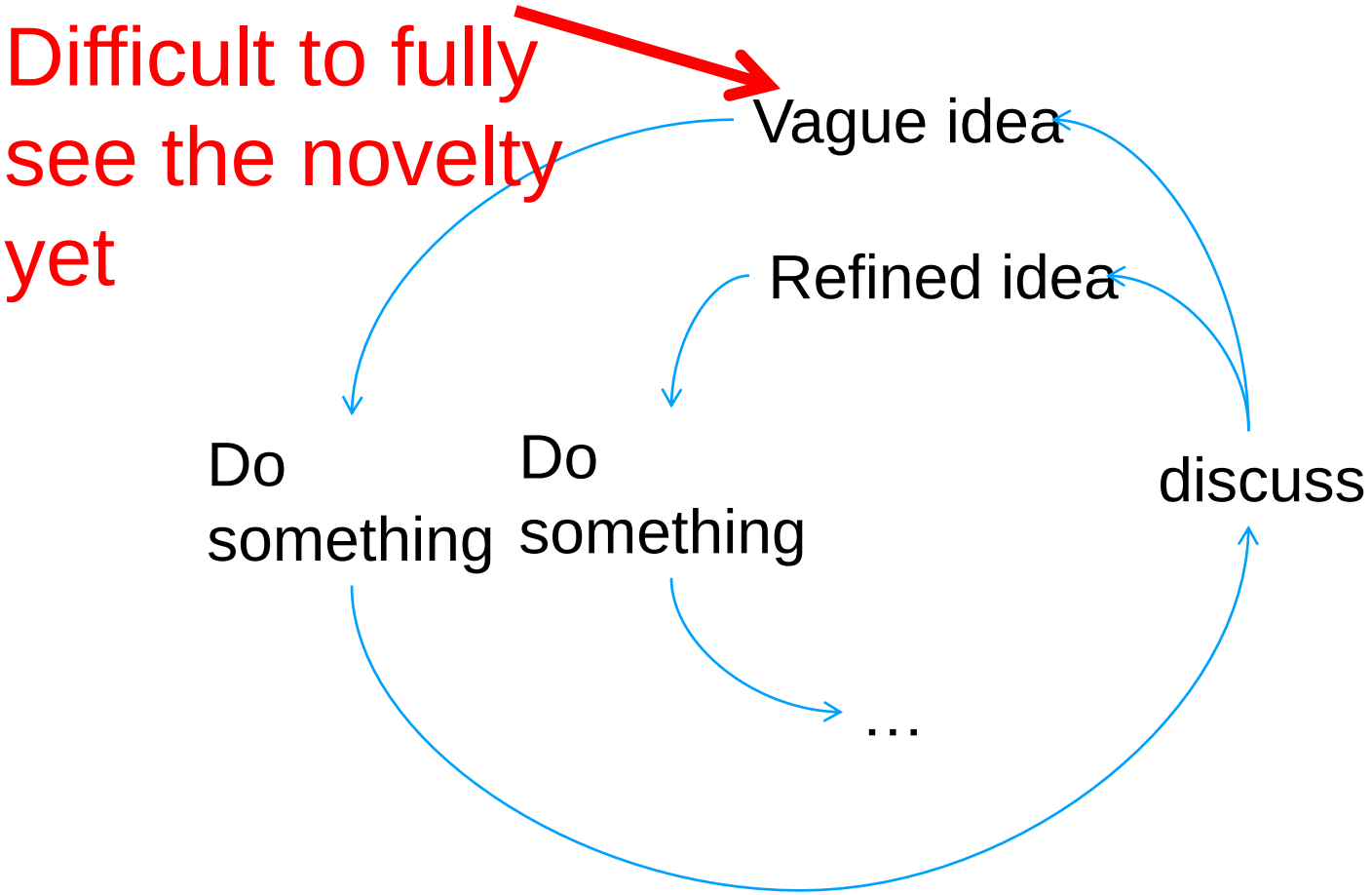
Erika Hunhoff

Bashayer Alharbi

MS Students doing Indep. Study:

- Swaminathan Sriram
- Sreeram Ganesan
- Akshay Abhyankar
- Sachin Sharma

Research is iterative



Sample of Current Projects

Transparent Network Acceleration

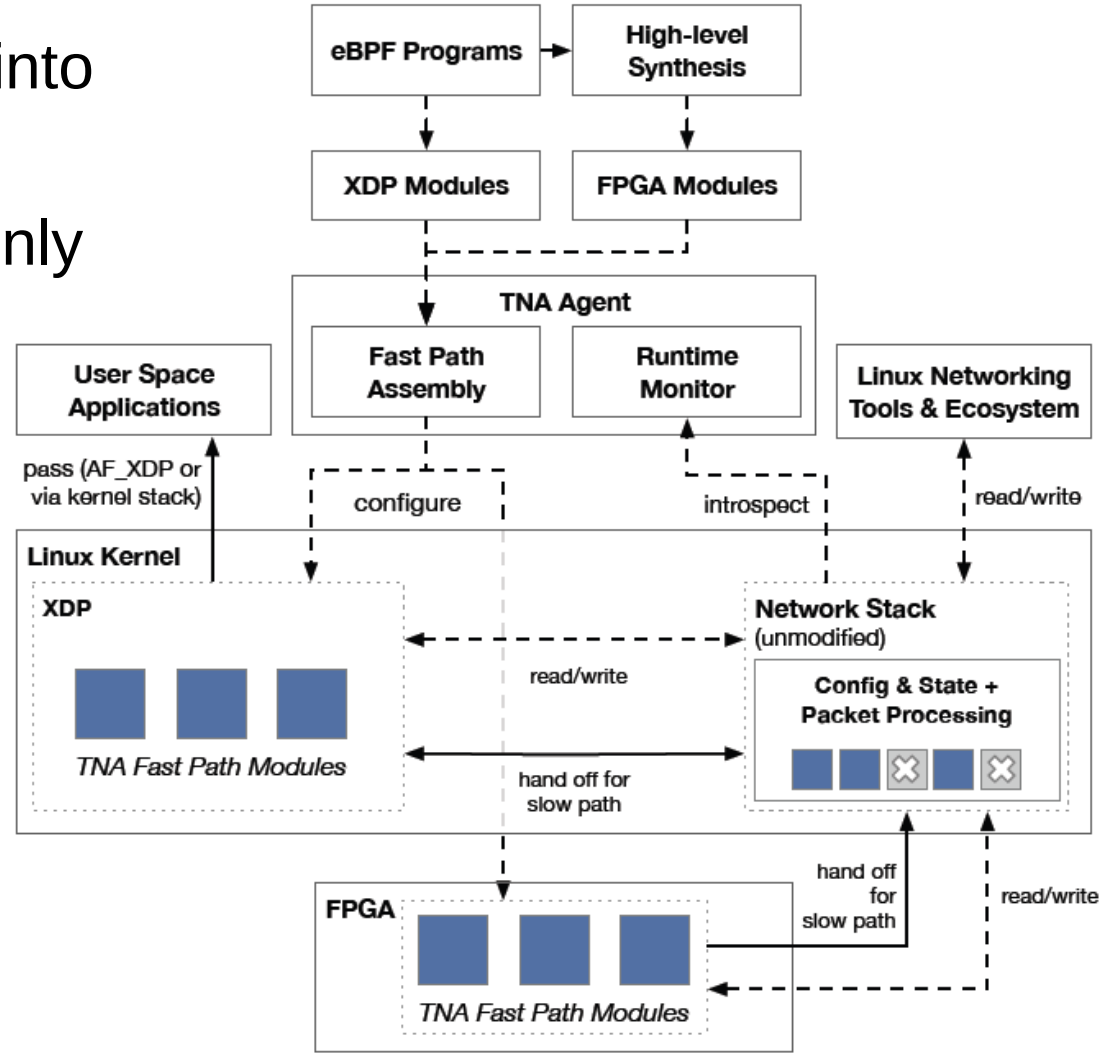
- Software-based packet processing is being widely adopted
- Linux has wide ecosystem and lots of functionality, but is too slow
- Custom is fast, but requires re-implementing everything (e.g., DPDK)

Transparent Network Acceleration

Re-imagine the Linux network stack:

(1) decomposes Linux networking functionality into fast-path and slow-path functionality

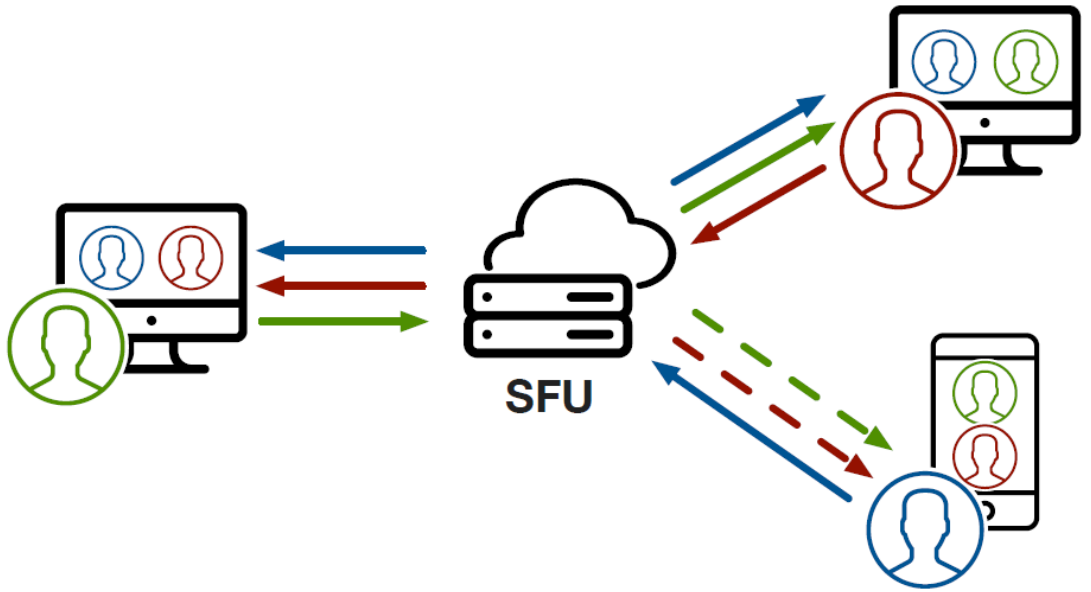
(2) automatically and dynamically instantiates only the part of the network stack that is used



Transparent Network Acceleration

Example projects:

- Example: Hardware offload - compile eBPF to FPGA
- Example: Decompose selective forwarding units (video conferencing software)



GHOST

5G Hidden Operations through Securing Traffic

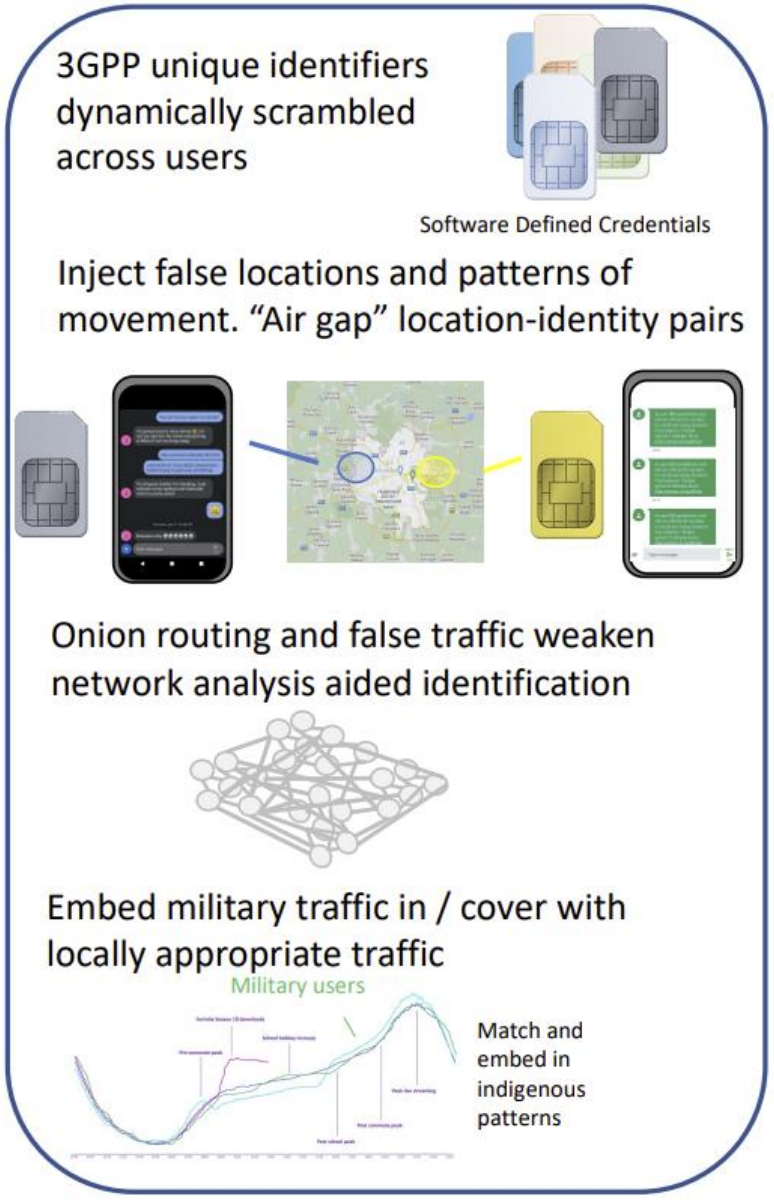
- Idea is to be able to ensure secure and anonymous communication over untrusted infrastructure
- e.g., for a military use case, being able to use 5G networks that in many areas of the world, the 5G networks are deployed and operated by organizations that are untrusted and potentially hostile to the U.S.

GHOST

GHOST prohibits traffic analysis through two mechanisms:

1. The use of Software Defined Credentials
2. anonymization techniques to obfuscate communications connections

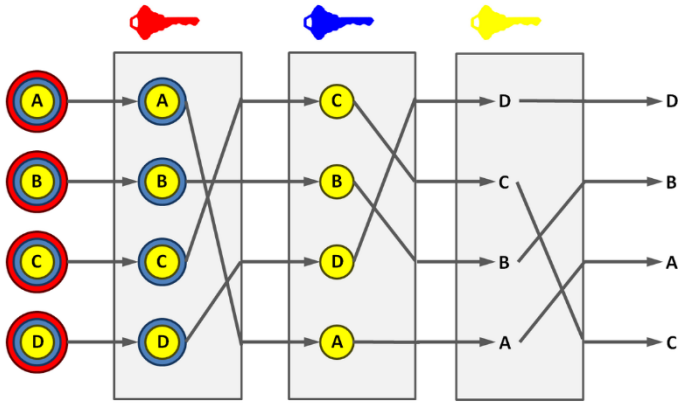
* Leverage secure hardware and needing fast packet processing



GHOST

Example projects:

- Example: help implement packet processing to obfuscate traffic
- Example: library to target SGX, Trust Zone, others



BGP Chain

- The Internet… the center of our lives
- But, the core protocol (BGP) is insecure
  (just last month, I saw at least 2 IP prefix hijacks)
- Attempts to fix that (RPKI) has issues:
  - Centralized
  - Doesn’t really work
  - Little to no incentive to deploy (still <30%)

BGP Chain

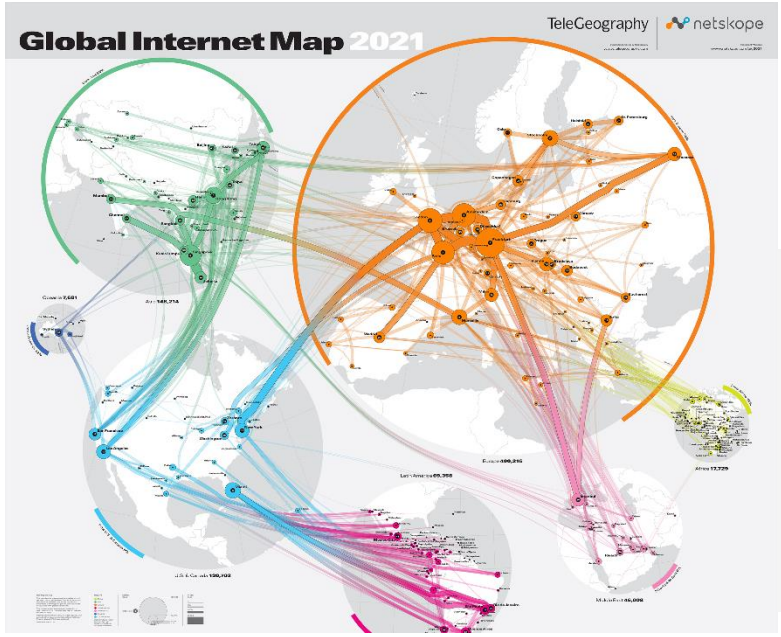
Leverage block chain as a data base of IP ownership and paths

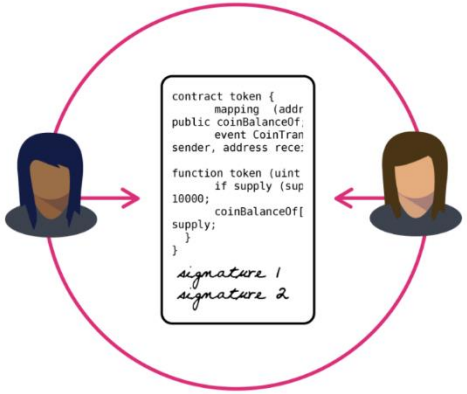
1. Decentralized
2. Smart contracts can secure route origin and paths and works with partial deployment
3. Smart contracts can solve internal network management challenges

BGP Chain

Example projects:

- Example: System to emulate the Internet
- Example: Smart contracts for network management applications





Stateless Inspired

Murad Kablan

Eric Keller

Spinoff of research from CU.

~25 employees, ~20M in VC funding, ~1M in NSF funding, deployments in large data centers / network providers

Stateless Inspired

Example projects:

- Example: Hardware offload - leverage RTE_FLOW to offload to NIC or Switch
- Make RAMCloud open source - XDP support, improved client library, usability, etc.
- Explore overlay (Aviatrix) vs. cloud-based Service Provider models

Current Independent Studies

- RDMA in serverless frameworks
- Serverless framework for ML
- Transparent acceleration of kubernetes networking
- Cost optimization among various cloud deployment models

Thanks

eric.keller@colorado.edu

https://eric-keller.github.io/

Backup

Random ideas

1. Horizontally scalable, natively fault tolerant BGP router
    1. Make stateless (store RIB in data base)
    2. Use QUIC instead of TCP (since TCP is tied to a specific instance)
2. Distributed SEED (with kubernetes)… can we emulate the entire Internet for a reasonable cost?
3. Create/extend a CNI (kubernetes related)
4. Troubleshooting (e.g., in Kubernetes)
5. Create something in P4 (caches DB request responses or proactively fetches from DB)
6. Pulumi for Network devices (e.g., run EVE-NG with some Cisco switches)
7. Avalanche (block chain)… e.g., integrate as example into SEED, recreate bitcoin hijacking attack

More Random ideas

1. Build something like DriveNets
2. Hardware offload to Switch (for something like Stateless' arch)
3. Reverse Traceroute in SEED
4. Create an application/cloud service that uses mptcp or QUIC (can you make a mpQUIC)? Look into https://pquic.org/
5. Reproduce research
6. Re-imagine RON for today's world
7. https://slack.engineering/introducing-nebula-the-open-source-global-overlay-network-from-slack/
8. https://www.syntropynet.com/
9. Bluefield DPU - https://medium.com/codex/getting-your-hands-dirty-with-mellanox-bluefield-2-dpus-deployed-in-cloudlabs-clemson-facility-bcb4e689c7e6

More random ideas

1. Build a web plug-in to measure something
2. use XDP or DPDK to define some new protocol

   * and create a wireshark plugin for that protocol.
3. Cloud based home gateway - better ability to VPN (use cloud transit), add security features (watch for bad clicks), etc.
4. Crowdsourced / Federated security
5. Something with tor
6. decentralized service

   * way to monetize without raiding privacy (see Privad)
7. Phone IDS – voice to speech + NLP + IDS
8. *Natural Language interface to network management
9. Spam – set up a SMTP server, measure lots of stuff (SNARE paper)
10. DPDK version of D-ITG
11. Study/measure/critique the cloud networking primitives (possibly include Aviatrix)
12. Cloud network monitoring + analytics platform (cloudwatch is very basic)