# Teaching and Research on Cybersecurity Using Next-Generation Devices

Jorge Crichigno, Neset Hikmet, Jason Porter
Department of Integrated Information Technology (IIT)
College of Engineering and Computing
University of South Carolina

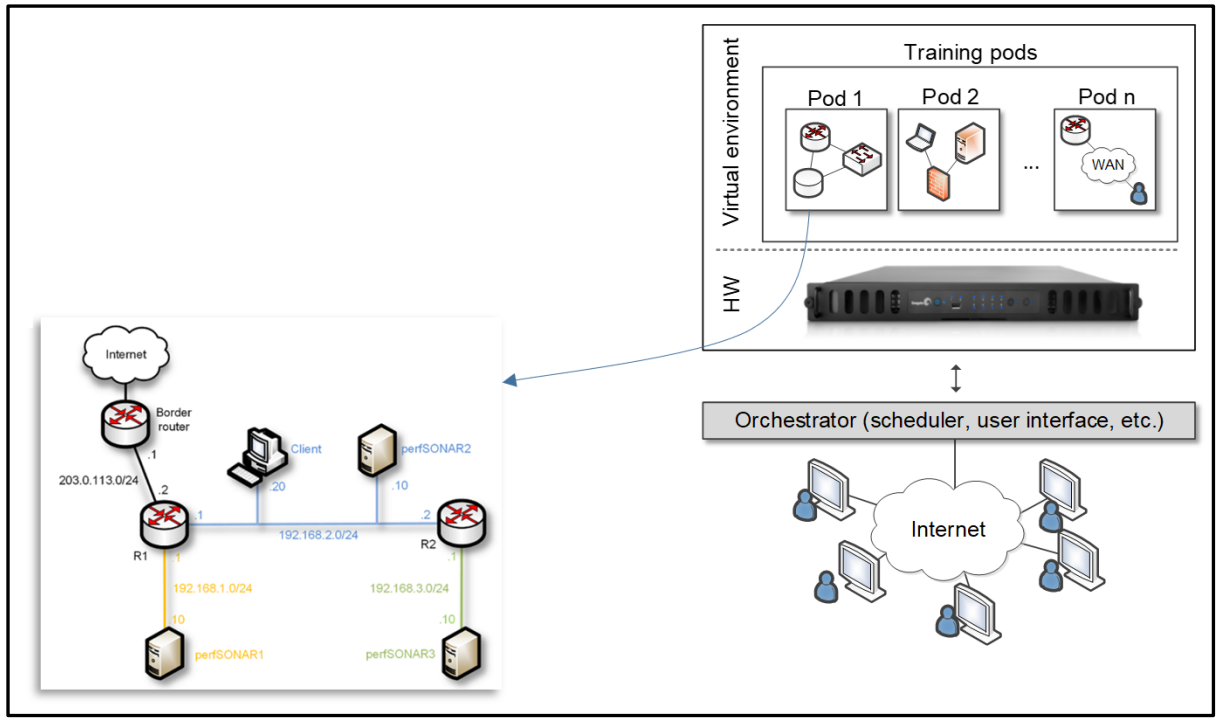
University of Minnesota – University of South Carolina Meeting
Online
March 15, 2021

# Agenda

- Projects at IIT
- Local private cloud to support virtual labs and remote-access capabilities
- Expanding local cloud to a multi-state distributed cloud
- Support for teaching and research using private cloud
- Office of the Naval Research (ONR) project
  - Enhancing the Preparation of Next-generation Cyber Professionals

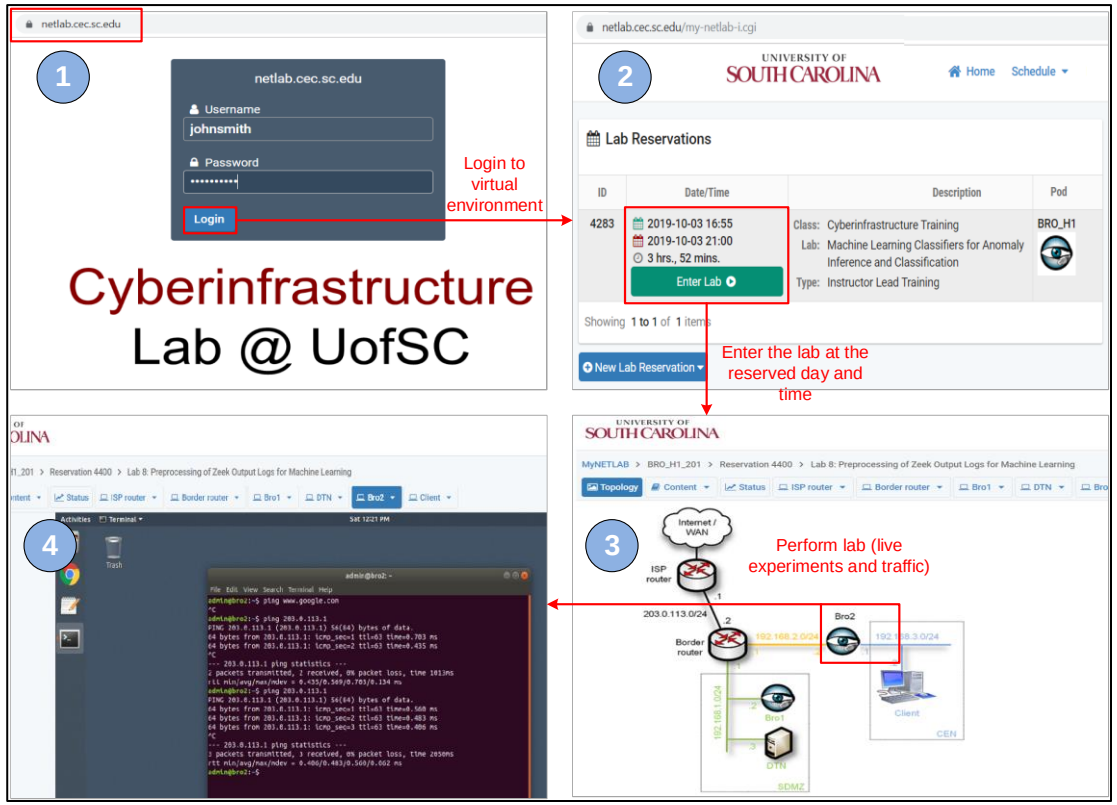
# NSF Cybersecurity

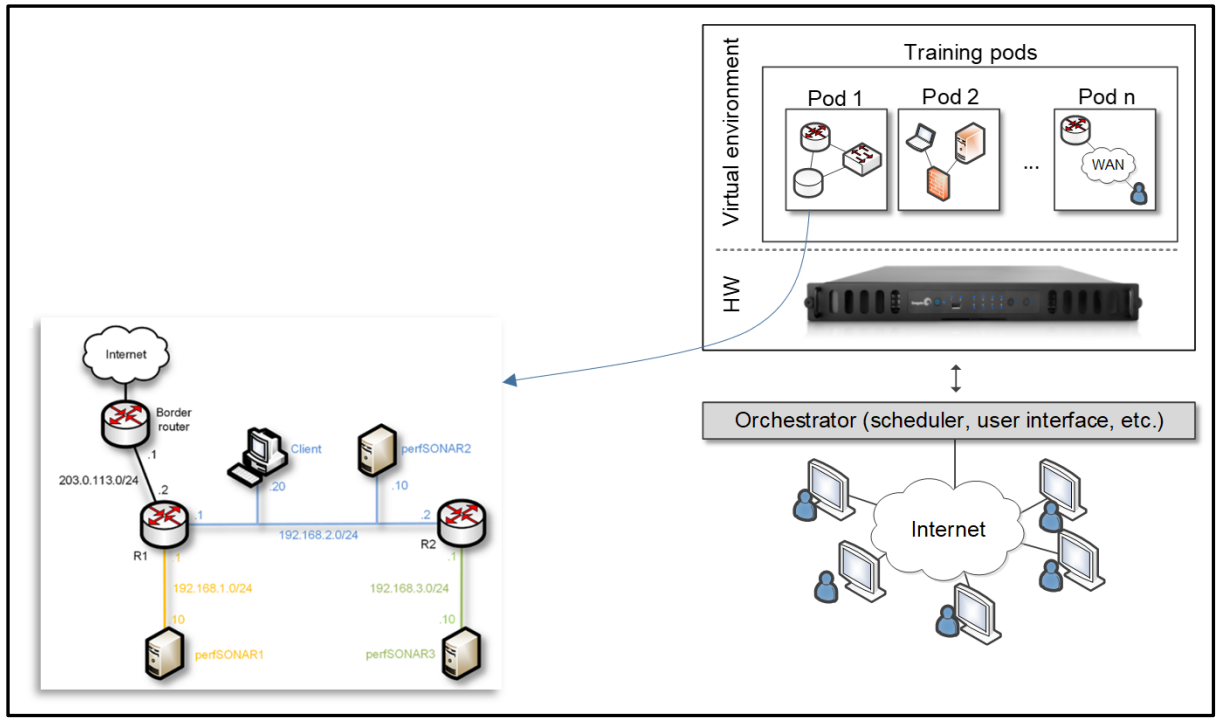
- NSF Cybersecurity (2018)
- Local private cloud for teaching and research in cyber at UofSC
- Build a private cloud
- Real protocol stacks and live traffic experimentation
- Scalable platform, hundreds of users simultaneously



# NSF Cybersecurity

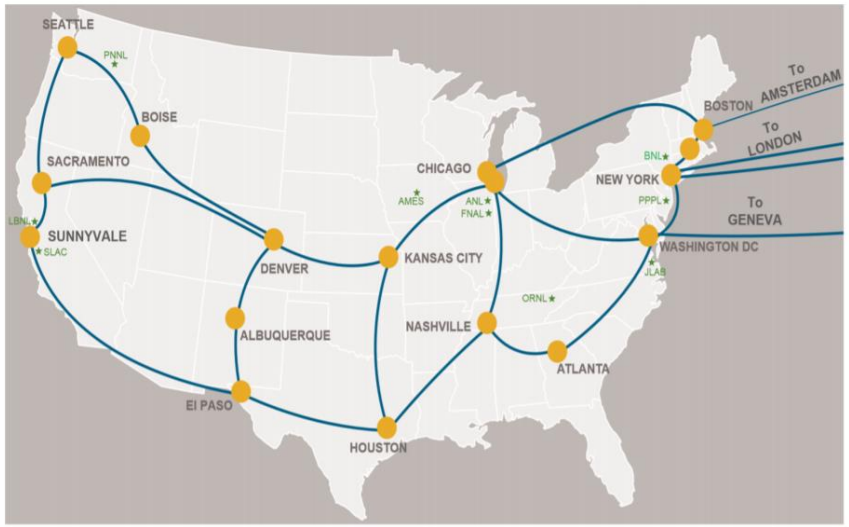
- Portal system



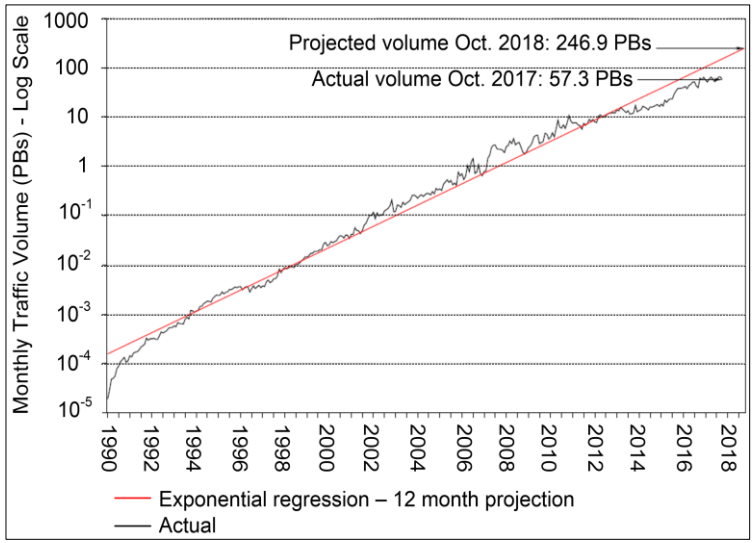



# NSF Cybertraining

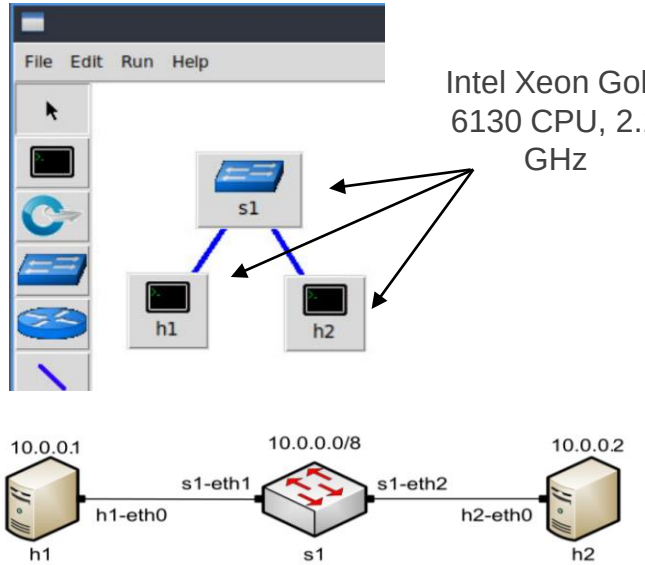
- NSF Cybertraining (2019): Cyberinfrastructure for moving big data
- There is a need for IT technical expertise country-wide
- E.g., ESnet is the network connecting national labs, research institutions
  - Managed by the Department of Energy (Berkeley National Lab)
- Rates of 50 Gbps, emulation of high-performance systems




ESnet



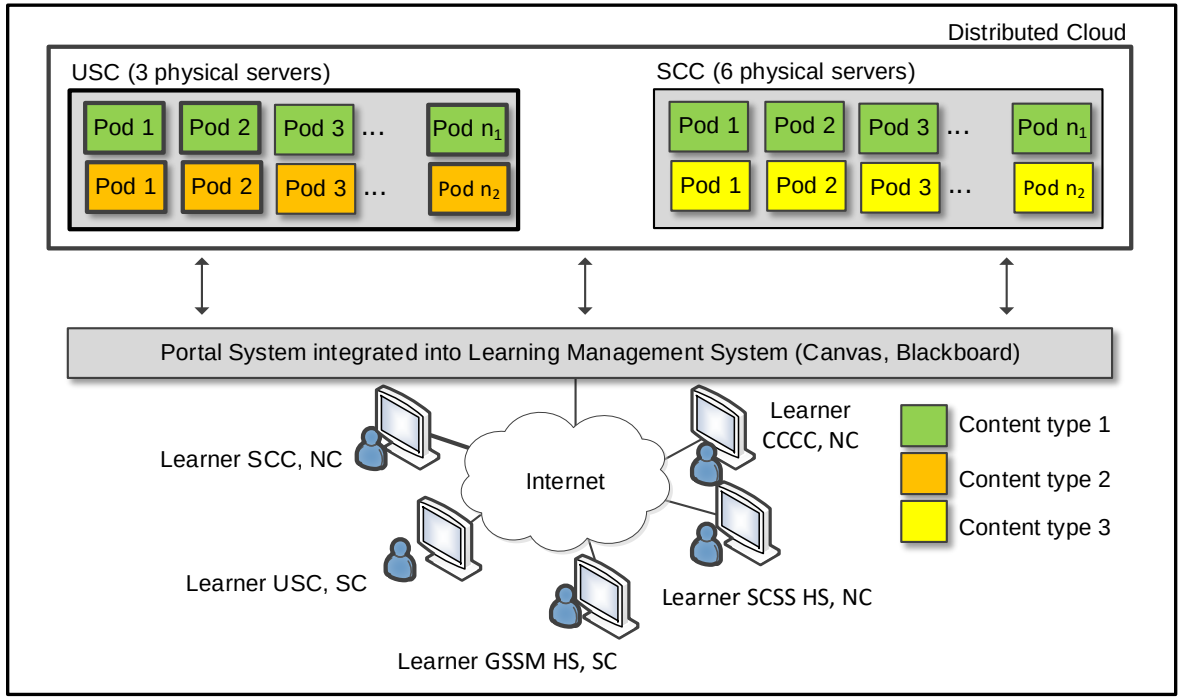

Monthly average traffic volume, ESnet




Three-node network emulation

# NSF ATE and CC

- NSF Advanced Technical Education (ATE) and NSF Campus Cyberinfrastructure (CC) (2019)
- Development of a multi-state distributed cloud to support teaching, research
- 2+2+2 program (HS + College + University)
- Distributed cloud pools resources from SC and NC, serves institutions seamlessly
- Requests to use the platform
  - Berkeley National Lab
  - SANS institute (“girlsgocyber”)
  - Multiple higher-ed institutions
  - International Networks at Indiana
  - Fort Gordon (2 cyber courses)
  - Texas’ Lonestart Education and Research



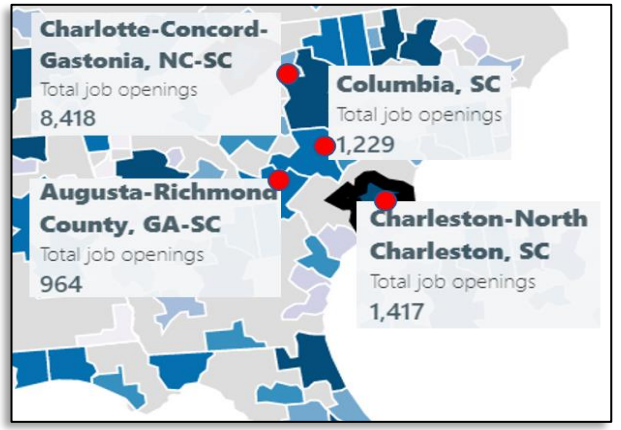
# Private Cloud Use

- Private vs public cloud

| Feature | Private Cloud | Public Cloud (e.g., AWS) |
|---|---|---|
| **Granularity to allocate physical resources** | Very granular | Not granular (access to the physical resources requires additional fees) |
| **Easy to create custom pods** | Easy | More difficult; hard to design complex topologies |
| **Cost** | Cost effective when used extensively | Cost effective for individual / small virtual machines; costly for large virtual machines over time |
| **IT Staff** | Higher cost | Lower cost |
| **Application layer for pedagogy and presentation of virtual scenarios** | Very flexible | Not flexible; limited to providers' interface, e.g., command-line interface |
| **Time-sharing compute resources** | The owner controls who can access resources. Easy to implement time-sharing policies | Cloud provider controls who can access resources (typically, a fee is required per user accessing resources) |

# ONR's Cyber Project

- "Enhancing the Preparation of Next-generation Cyber Professionals" (2020)
- South Carolina cybersecurity needs
  - NIWC Atlantic, SRNL, Fort Jackson, Shaw Air Force Base, private industry
- Recruiting the American military's cyber force is more difficult than ever
  - DoD has been struggling to hire more than 8,000 cyber positions (2018)[1]
  - Shortage of cybersecurity professionals
- The College of Engineering and Computing is addressing the workforce needs:
  - Encourage STEM, **ROTC** students to obtain a minor in IT
  - Undergraduate applied research
  - Private cloud
  - Collaboration among industry, government, education institutions

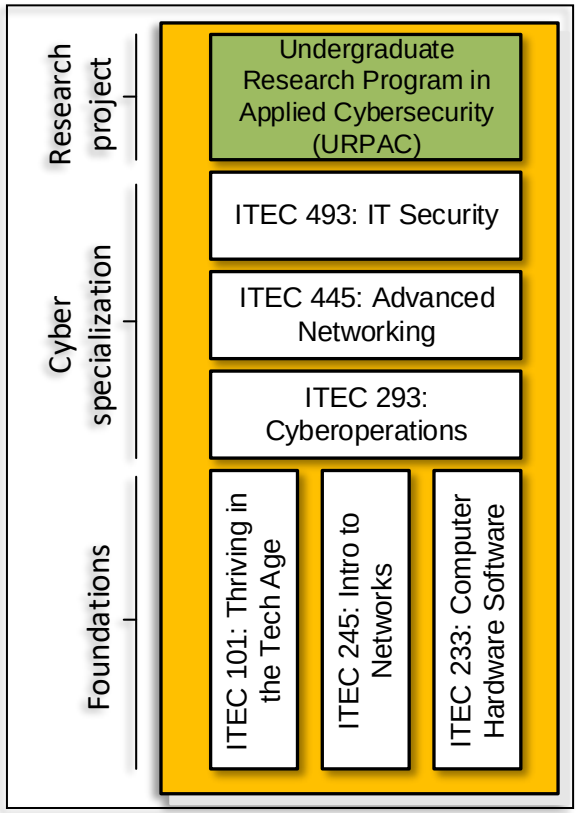



Cybersecurity job openings in four metro areas near Columbia, Feb. 2020

1. J. Lynch, "Inside the Pentagon's Struggle to Build a Cyber Force," Fifth Domain publication, October 29, 2018. Online: https://tinyurl.com/yyelqomp

# ONR's Cyber Project

1. Minor in IT – Cyber specialization
   - Option to earn DoD's approved baseline certificates for Information Assurance Technical (IAT)
   - Self-contained specialization; no pre-req for other STEM majors / **ROTC**
2. **Undergraduate applied research**
   - CEC faculty, graduate student mentors
   - Advisory entity by NIWC Atlantic, project guidelines
3. Private cloud with professional tools and platforms
   - Hands-on applied research with physical and virtual equipment
4. Collaboration
   - Partnership with Intel, Cisco Systems, Palo Alto Networks, VMware, Juniper




Minor in IT and undergraduate research

# ONR's Cyber Project

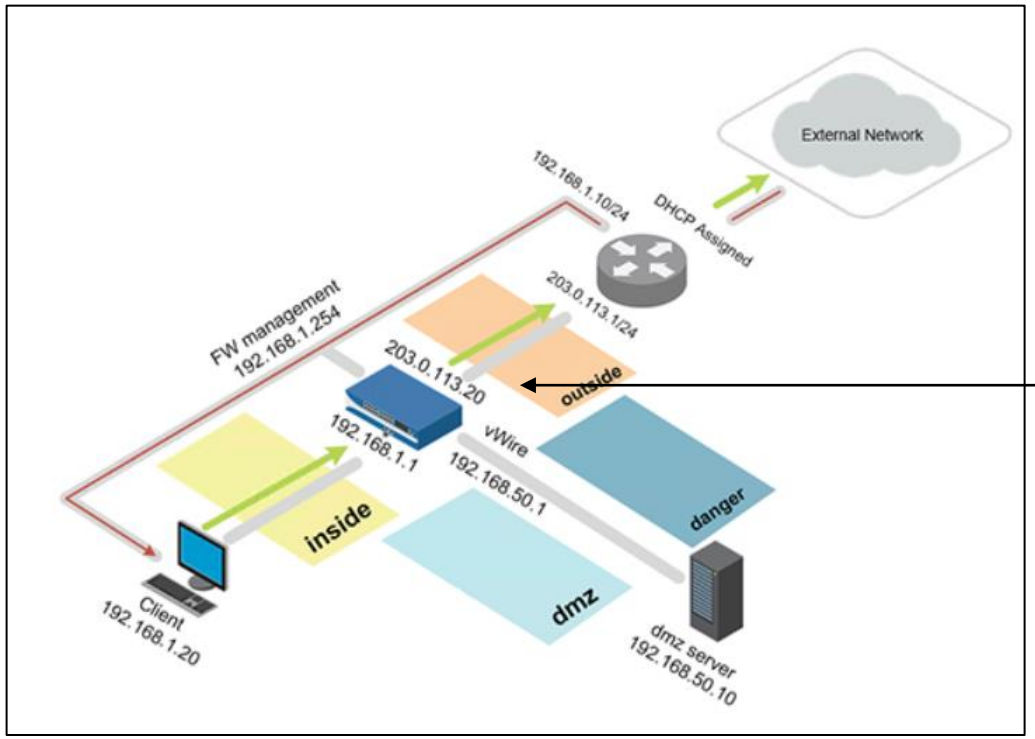
- DoD's Information Assurance (IA) workforce is classified in IA technical (IAT):
  - Level 1 (IAT 1): Computing environment information assurance
  - Level 2 (IAT 2): Network environment information assurance
  - Level 3 (IAT 3): Enclave, advanced network & computer information assurance
- It requires partnership
  - Cisco Systems, Palo Alto Networks, VMware, Juniper, Intel

| Certificate | Material Covered in | IAT 1 | IAT 2 | NICE framework | Networks cert. |
|---|---|---|---|---|---|
| A+ | ITEC 233 | ✓ | | ✓ | |
| Cyberoperations | ITEC 293 | ✓ | | ✓ | |
| Security+ | ITEC 293 | ✓ | ✓ | ✓ | |
| CCNA Security | ITEC 493 | ✓ | ✓ | ✓ | |
| CCNA Routing/Switching | ITEC 245, ITEC 445 | | | | ✓ |
| ACE | ITEC 493 | | | ✓ | |
| PCNSE | ITEC 493 | | | ✓ | |

NICE: National Initiative for Cybersecurity Education (NIST)

# ONR's Cyber Project

- Collaboration
  - Applied teaching and research -> professional tools, platforms, market validation
  - Cisco Systems, Palo Alto Networks, VMware, Juniper, Intel



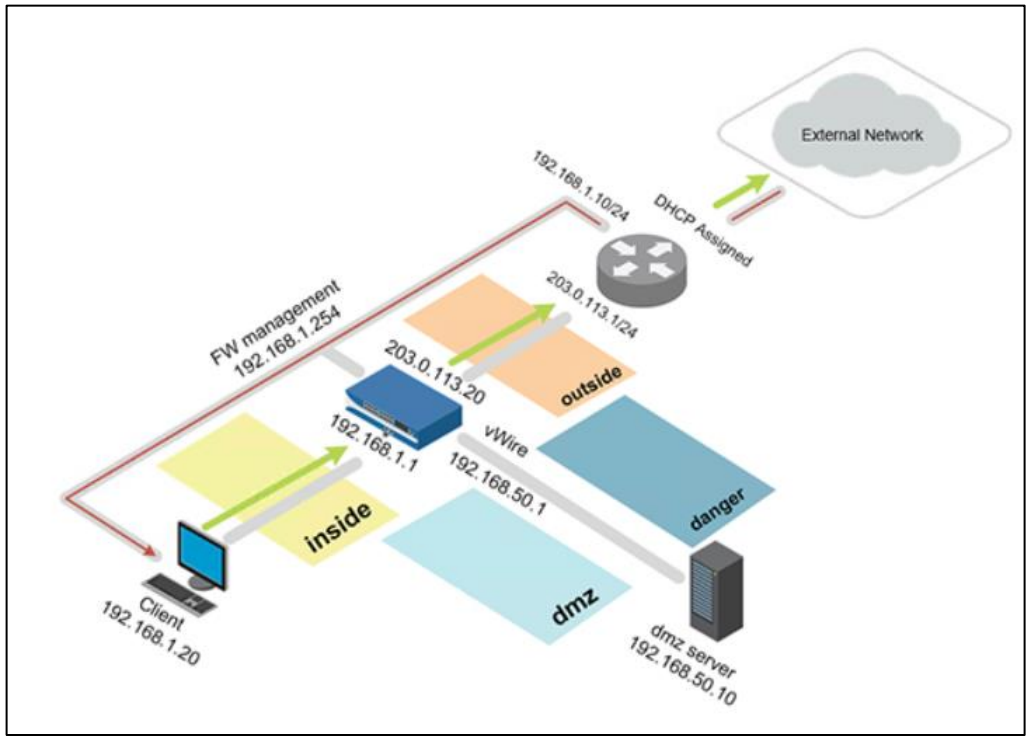

Pod deployed in private cloud

**Next-generation** Firewall Virtual Machine + licenses

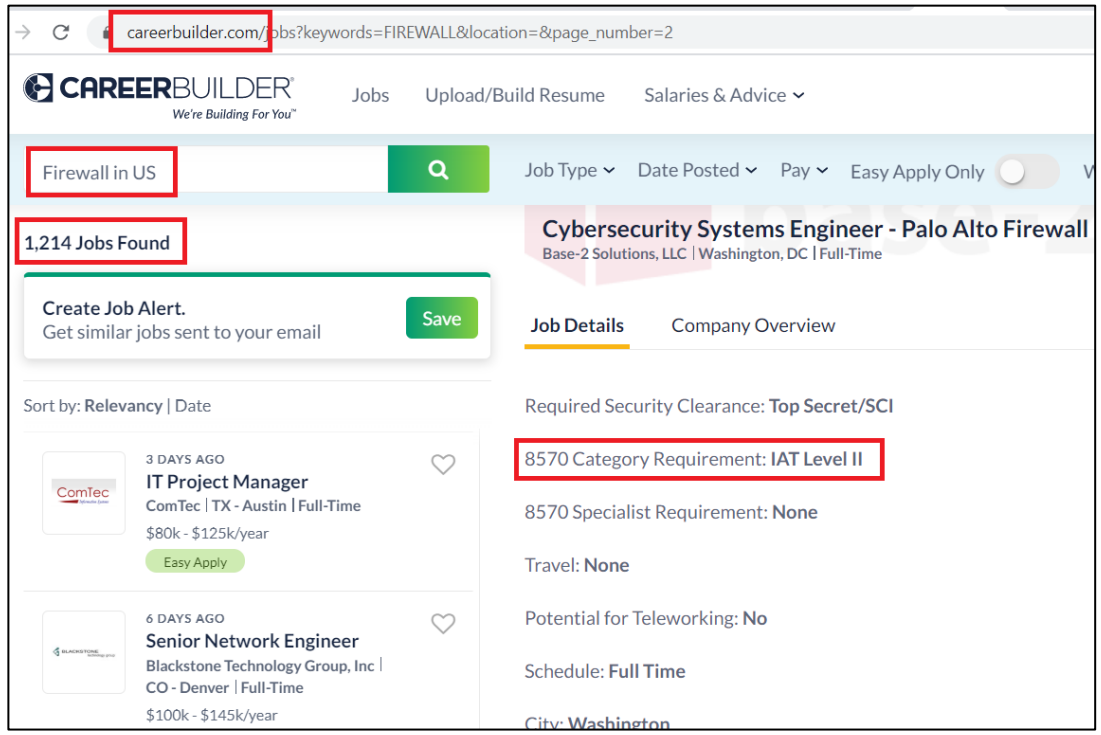
# ONR's Cyber Project

- Collaboration
  - Applied teaching and research -> professional tools, platforms, market validation
  - Cisco Systems, Palo Alto Networks, VMware, Juniper, Intel

- ✓ Bachelor's degree
- ✓ IAT
- ✓ Theory
- ✓ Hands-on expertise Palo Alto




Pod deployed in private cloud

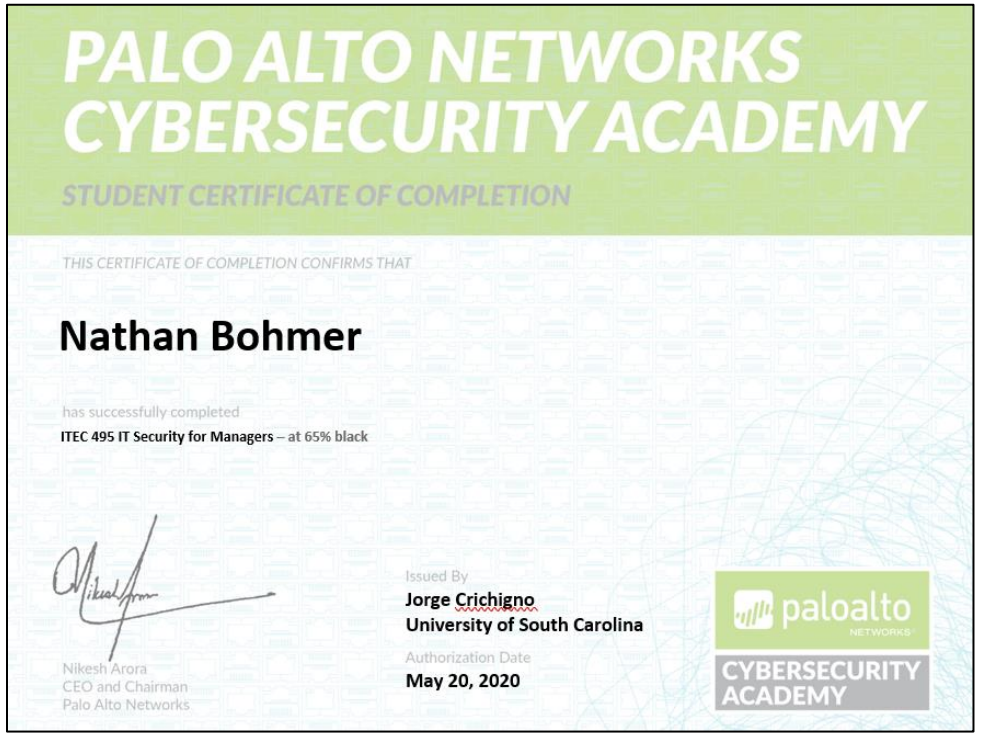



Job search

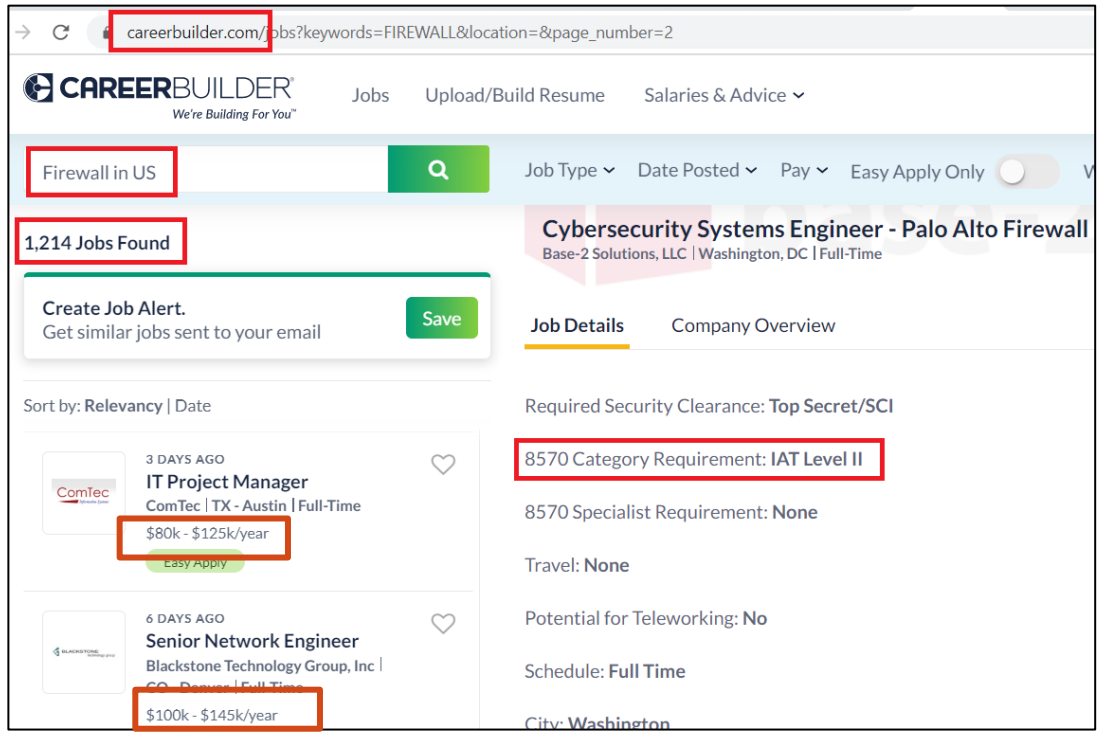
# ONR's Cyber Project

- Collaboration
  - Applied teaching and research -> professional tools, platforms, market validation
  - Cisco Systems, Palo Alto Networks, VMware, Juniper, Intel

- ✓ Bachelor's degree
- ✓ IAT
- ✓ Theory
- ✓ Hands-on expertise Palo Alto




Additional credentials

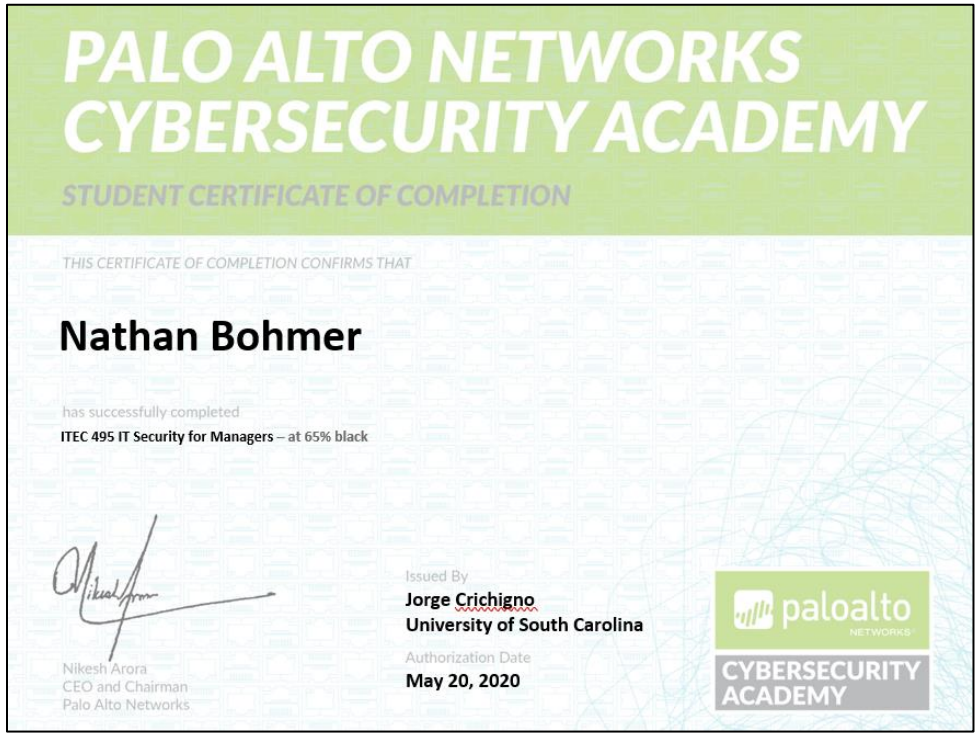



Job search

# ONR's Cyber Project

- Collaboration
  - Applied teaching and research -> professional tools, platforms, market validation
  - Cisco Systems, Palo Alto Networks, VMware, Juniper, Intel

- ✓ Bachelor's degree
- ✓ IAT
- ✓ Theory
- ✓ Hands-on expertise Palo Alto


PALO ALTO NETWORKS
CYBERSECURITY ACADEMY

STUDENT CERTIFICATE OF COMPLETION

THIS CERTIFICATE OF COMPLETION CONFIRMS THAT

**Nathan Bohmer**

has successfully completed

ITEC 495 IT Security for Managers – at 65% black

Nikesh Arora
CEO and Chairman
Palo Alto Networks

Issued By
Jorge Crichigno
University of South Carolina

Authorization Date
May 20, 2020

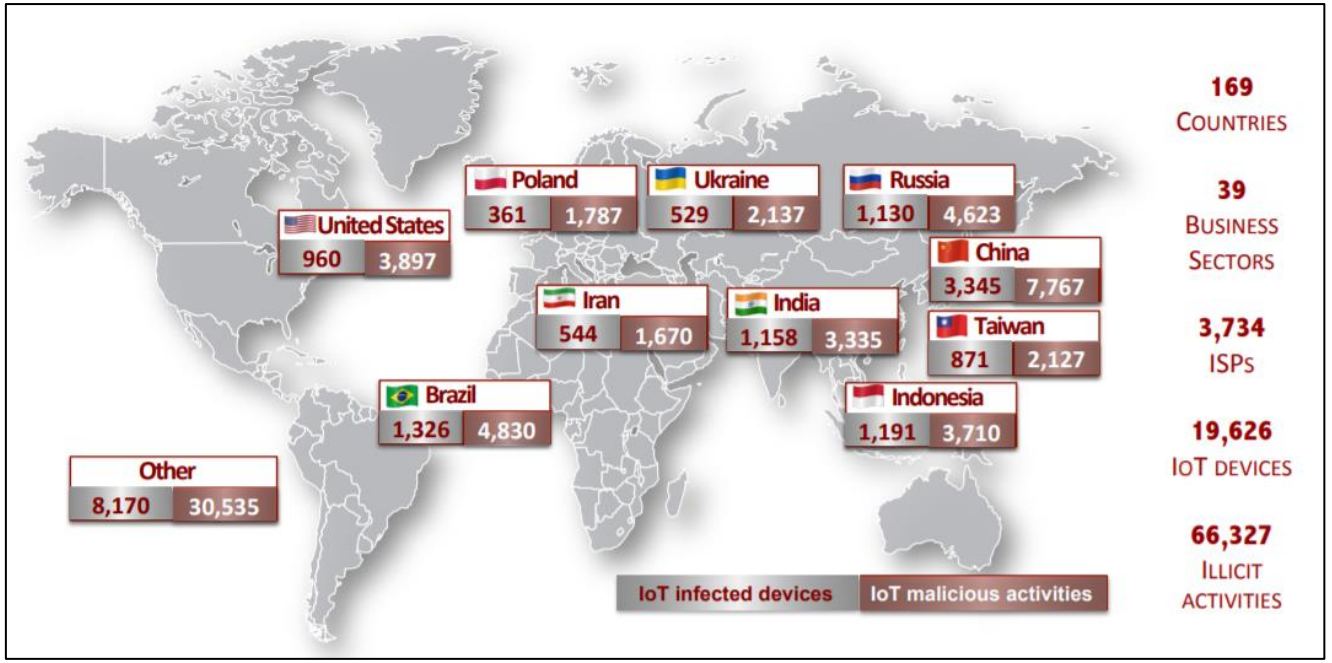
paloalto NETWORKS
CYBERSECURITY ACADEMY

Additional credentials

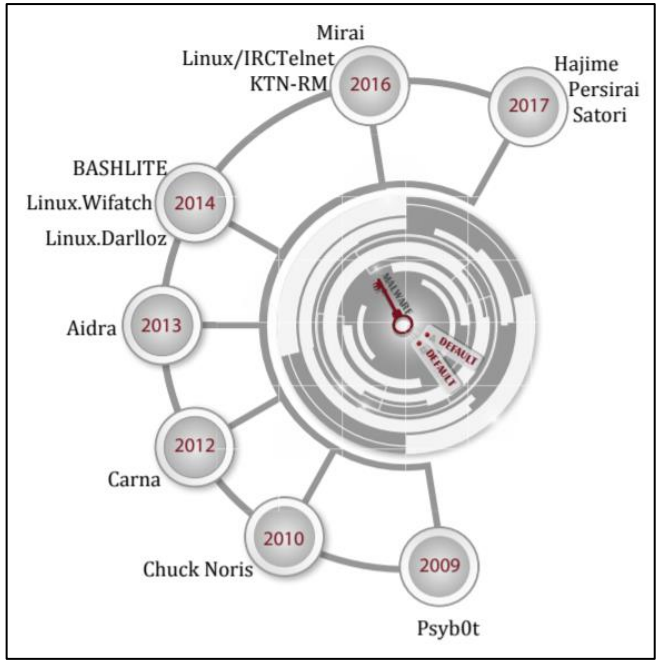

UofSC's ROTC

# Graduate Projects

- Development of new techniques against attacks targeting “Internet-of-Things” devices
- Agreement with the Center for Applied Internet Data Analysis (CAIDA) (San Diego)



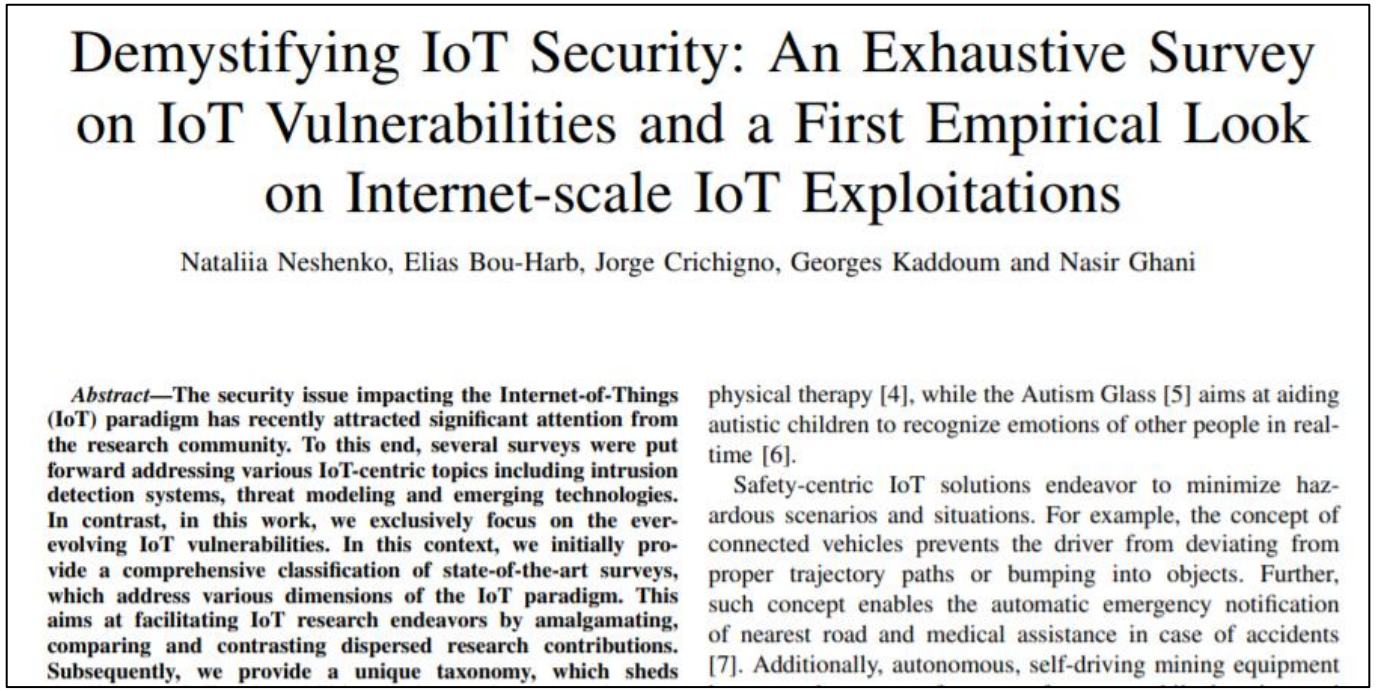

Global distribution of exploited IoT devices; results from this research project




Malware exploiting default credentials

# Graduate Projects

- Development of new techniques against attacks targeting “Internet-of-Things” devices
- Agreement with the Center for Applied Internet Data Analysis (CAIDA) (San Diego)



Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-scale IoT Exploitations

Nataliia Neshenko, Elias Bou-Harb, Jorge Crichigno, Georges Kaddoum and Nasir Ghani

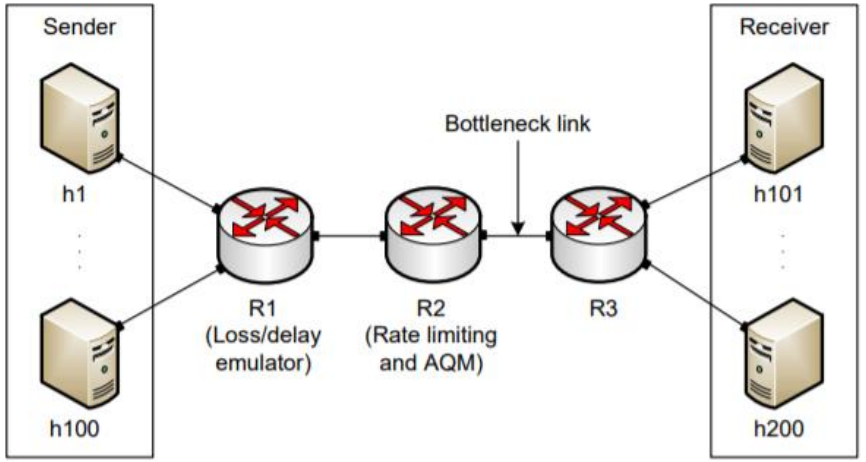
***Abstract*—The security issue impacting the Internet-of-Things (IoT) paradigm has recently attracted significant attention from the research community. To this end, several surveys were put forward addressing various IoT-centric topics including intrusion detection systems, threat modeling and emerging technologies. In contrast, in this work, we exclusively focus on the ever-evolving IoT vulnerabilities. In this context, we initially provide a comprehensive classification of state-of-the-art surveys, which address various dimensions of the IoT paradigm. This aims at facilitating IoT research endeavors by amalgamating, comparing and contrasting dispersed research contributions. Subsequently, we provide a unique taxonomy, which sheds**

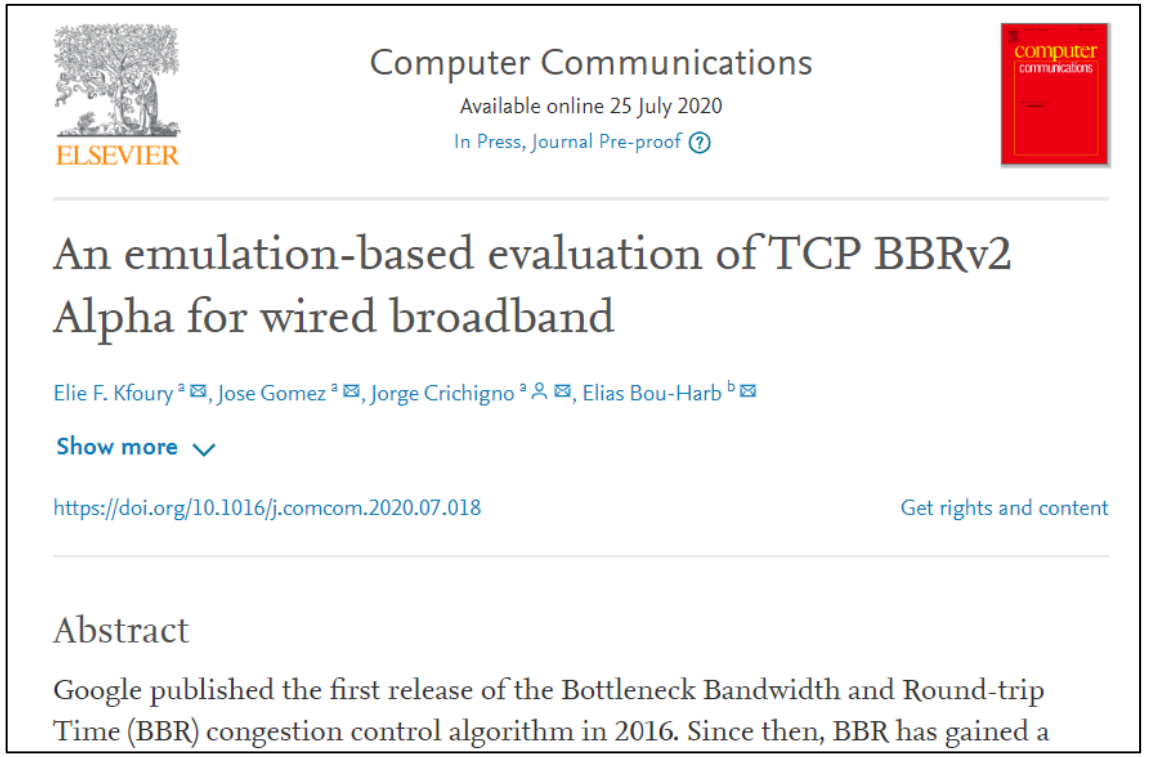
physical therapy [4], while the Autism Glass [5] aims at aiding autistic children to recognize emotions of other people in real-time [6].

Safety-centric IoT solutions endeavor to minimize hazardous scenarios and situations. For example, the concept of connected vehicles prevents the driver from deviating from proper trajectory paths or bumping into objects. Further, such concept enables the automatic emergency notification of nearest road and medical assistance in case of accidents [7]. Additionally, autonomous, self-driving mining equipment

# Graduate Projects

- Performance testing Google's new communication protocol
- Feedback to Google (used in Youtube, Chrome, and other apps)
- Emulating behavior in private cloud before Google's protocol public release



ELSEVIER

Computer Communications

Available online 25 July 2020

In Press, Journal Pre-proof

An emulation-based evaluation of TCP BBRv2 Alpha for wired broadband

Elie F. Kfoury [a], Jose Gomez [a], Jorge Crichigno [a], Elias Bou-Harb [b]

Show more

https://doi.org/10.1016/j.comcom.2020.07.018

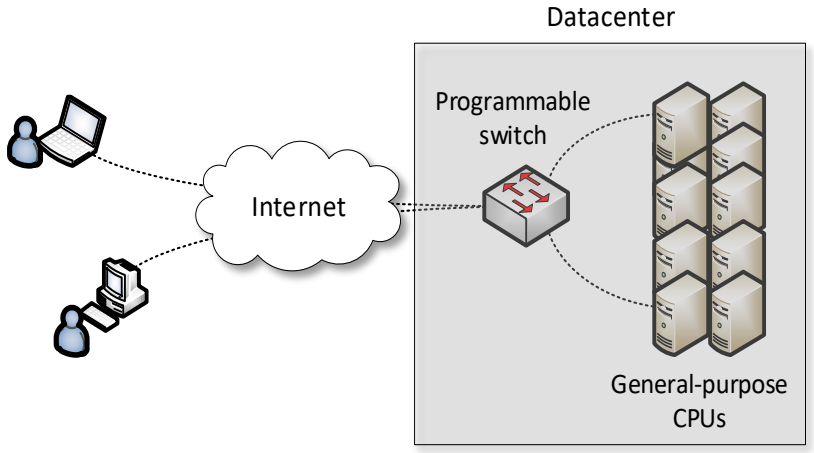
Get rights and content

Abstract

Google published the first release of the Bottleneck Bandwidth and Round-trip Time (BBR) congestion control algorithm in 2016. Since then, BBR has gained a

# Graduate Projects

- Improving system's performance using next-generation switches
- Offloading computational tasks to network switches
  - Orders of magnitude faster than general-purpose CPU
  - Very limited instructions set (e.g., no multiplication, no division, simple operations)
- Agreement with Intel (chips, software development environment)

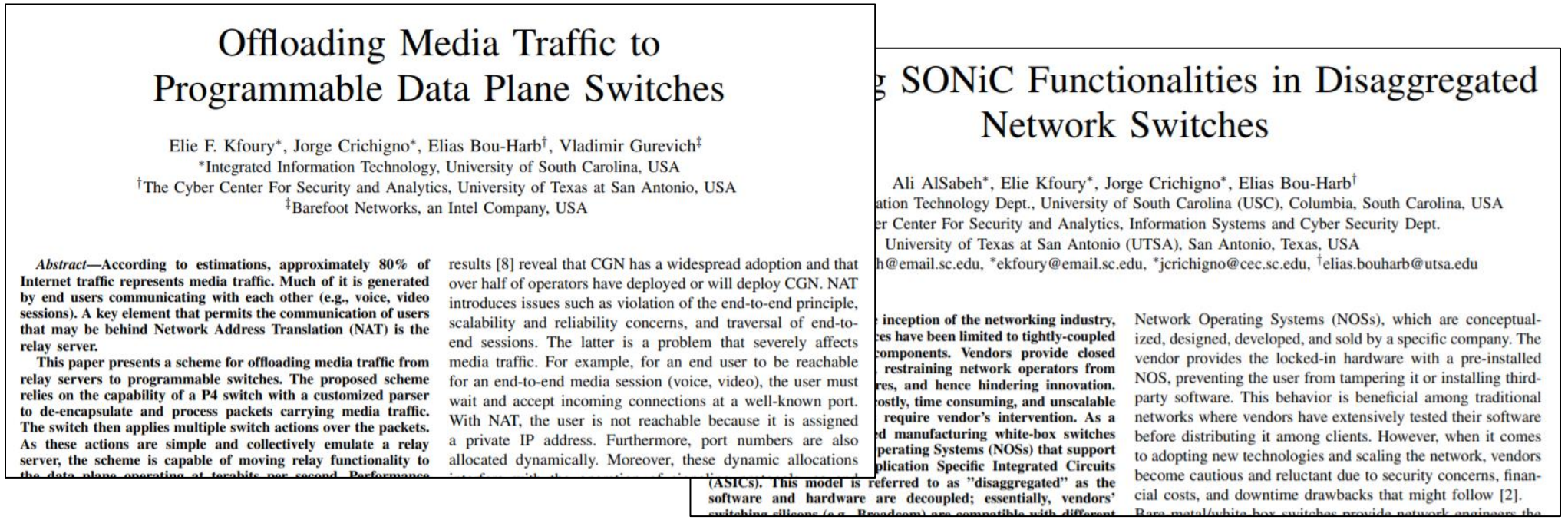



Application example: media (voice) relay server

| | Programmable Switch | General-purpose CPU |
|---|---|---|
| **Cost** | $6,000 | $ 10,000 - 25,000 |
| **Capacity** | ~35,000,000 connections per switch | ~500 connections per core |
| **Latency** | 400 nanoseconds | Tens to hundreds of milliseconds |

# Graduate Projects

- Improving system's performance using next-generation switches
- Offloading computational tasks to network switches
  - Orders of magnitude faster than general-purpose CPU
  - Very limited instructions set (e.g., no multiplication, no division, simple operations)
- Agreement with Intel (chips, software development environment)



Offloading Media Traffic to Programmable Data Plane Switches

Elie F. Kfoury*, Jorge Crichigno*, Elias Bou-Harb†, Vladimir Gurevich‡
*Integrated Information Technology, University of South Carolina, USA
†The Cyber Center For Security and Analytics, University of Texas at San Antonio, USA
‡Barefoot Networks, an Intel Company, USA

***Abstract*—According to estimations, approximately 80% of Internet traffic represents media traffic. Much of it is generated by end users communicating with each other (e.g., voice, video sessions). A key element that permits the communication of users that may be behind Network Address Translation (NAT) is the relay server.**

**This paper presents a scheme for offloading media traffic from relay servers to programmable switches. The proposed scheme relies on the capability of a P4 switch with a customized parser to de-encapsulate and process packets carrying media traffic. The switch then applies multiple switch actions over the packets. As these actions are simple and collectively emulate a relay server, the scheme is capable of moving relay functionality to**

results [8] reveal that CGN has a widespread adoption and that over half of operators have deployed or will deploy CGN. NAT introduces issues such as violation of the end-to-end principle, scalability and reliability concerns, and traversal of end-to-end sessions. The latter is a problem that severely affects media traffic. For example, for an end user to be reachable for an end-to-end media session (voice, video), the user must wait and accept incoming connections at a well-known port. With NAT, the user is not reachable because it is assigned a private IP address. Furthermore, port numbers are also allocated dynamically. Moreover, these dynamic allocations

g SONiC Functionalities in Disaggregated Network Switches

Ali AlSabeh*, Elie Kfoury*, Jorge Crichigno*, Elias Bou-Harb†
ation Technology Dept., University of South Carolina (USC), Columbia, South Carolina, USA
er Center For Security and Analytics, Information Systems and Cyber Security Dept.
University of Texas at San Antonio (UTSA), San Antonio, Texas, USA
h@email.sc.edu, *ekfoury@email.sc.edu, *jcrichigno@cec.sc.edu, †elias.bouharb@utsa.edu

**inception of the networking industry, ces have been limited to tightly-coupled components. Vendors provide closed restraining network operators from res, and hence hindering innovation. costly, time consuming, and unscalable require vendor's intervention. As a ed manufacturing white-box switches perating Systems (NOSs) that support plication Specific Integrated Circuits (ASICs). This model is referred to as "disaggregated" as the software and hardware are decoupled; essentially, vendors'**

Network Operating Systems (NOSs), which are conceptualized, designed, developed, and sold by a specific company. The vendor provides the locked-in hardware with a pre-installed NOS, preventing the user from tampering it or installing third-party software. This behavior is beneficial among traditional networks where vendors have extensively tested their software before distributing it among clients. However, when it comes to adopting new technologies and scaling the network, vendors become cautious and reluctant due to security concerns, financial costs, and downtime drawbacks that might follow [2].

# NIWC Atlantic

- Collaboration with NIWC Atlantic is essential
  - We want to acknowledge Michael Merriken and Captain Sanders
- Advisory entity to the project
- Provide input for undergraduate research projects
- Coordination with UofSC's ROTC
  - Navy
  - Army
  - Air Force