Cyber-training, Research, and Education Opportunities at the University of South Carolina

Jorge Crichigno
Department of Integrated Information Technology (IIT)
University of South Carolina
jcrichigno@cec.sc.edu
http://ce.sc.edu/cyberinfra

SC Cyber-Security Webinar Series
October 8, 2020

Agenda

- Department of Integrated Information Technology at UofSC
- Academic programs
- Virtual platform
- Industry collaboration
- Research

IIT Department

- The Department of Integrated Information Technology (IIT) is within the College of Engineering and Computing (CEC) at the University of South Carolina (UofSC)
- IIT offers undergraduate and graduate degree programs
- Its research focuses on the areas of cyber infrastructure, database systems, data analytics, health information technology, and human-computer interaction
- It is more practical than theoretical; IIT emphasizes operations, applications
- Partnership with industry for internships, materials

Academic Programs

- BSc In Integrated Information Technology
- ABET accredited
- 120 credit hours
- 400-hour internship
- Curriculum includes
  - Cybersecurity
  - IT Business Operations
  - Databases
  - Networking
  - Project Management
  - Web Development
- The department is developing a fully online BSc

Academic Programs

- Minor in Integrated Information Technology
- 18 credit hours
- Several concentrations
  - **Cybersecurity Operations**
  - IT Business Operations
  - Databases
  - Networking
  - Project Management
  - Web Development

Minor Requirements

Course	Title	Credits
Cybersecurity Operations		18
ITEC 101	Thriving in the Tech Age	
ITEC 233	Introduction to Computer Hardware and Software	
ITEC 245	Introduction to Networking	
ITEC 293	Cybersecurity Operations	
ITEC 445	Advanced Networking	
ITEC 493	Information Technology Security for Managers	

Courses map learning objectives to the U.S. NICE framework (ITEC 293, ITEC 445, ITEC 493)

The National Initiative for Cybersecurity Education (NICE) Framework is a national-focused resource that categorizes and describes cybersecurity work

Academic Programs

- Minor in Integrated Information Technology
- 18 credit hours
- Several concentrations
  - Cybersecurity Operations
  - **IT Business Operations**
  - Databases
  - Networking
  - Project Management
  - Web Development

Minor Requirements

Course	Title	Credits
IT Business Operations		18
ITEC 101	Thriving in the Tech Age	
ITEC 233	Introduction to Computer Hardware and Software	
Select four of the following:		
ITEC 245	Introduction to Networking	
ITEC 564	Capstone Project for Information Technology	
ITEC 265	Introduction to Databases	
ITEC 293	Cybersecurity Operations	
ITEC 447	Management of Information Technology	

Academic Programs

- Minor in Integrated Information Technology
- 18 credit hours
- Several concentrations
  - Cybersecurity Operations
  - IT Business Operations
  - **Databases**
  - Networking
  - Project Management
  - Web Development

Minor Requirements

Course	Title	Credits
Databases		18
ITEC 101	Thriving in the Tech Age	
ITEC 233	Introduction to Computer Hardware and Software	
ITEC 264	Computer Applications in Business I	
ITEC 265	Introduction to Databases	
ITEC 370	Database Systems in Information Technology	
ITEC 570	Database Management and Administration	

Academic Programs

- Minor in Integrated Information Technology
- 18 credit hours
- Several concentrations
  - Cybersecurity Operations
  - IT Business Operations
  - Databases
  - **Networking**
  - Project Management
  - Web Development

Minor Requirements

Course	Title	Credits
Networking		18
ITEC 101	Thriving in the Tech Age	
ITEC 233	Introduction to Computer Hardware and Software	
ITEC 245	Introduction to Networking	
ITEC 445	Advanced Networking	
Select two of the following:		
ITEC 293	Cybersecurity Operations	
ITEC 493	Information Technology Security for Managers	
ITEC 545	Telecommunications	

Academic Programs

- Minor in Integrated Information Technology
- 18 credit hours
- Several concentrations
  - Cybersecurity Operations
  - IT Business Operations
  - Databases
  - Networking
  - **Project Management**
  - Web Development

Minor Requirements

Course	Title	Credits
Project Management		18
ITEC 101	Thriving in the Tech Age	
ITEC 233	Introduction to Computer Hardware and Software	
ITEC 264	Computer Applications in Business I	
ITEC 362	Introduction to Web Systems	
ITEC 560	Project Management Methods	
ITEC 564	Capstone Project for Information Technology	

Academic Programs

- Minor in Integrated Information Technology
- 18 credit hours
- Several concentrations
  - Cybersecurity Operations
  - IT Business Operations
  - Databases
  - Networking
  - Project Management
  - **Web Development**

Minor Requirements

Course	Title	Credits
Web Development		18
ITEC 101	Thriving in the Tech Age	
ITEC 233	Introduction to Computer Hardware and Software	
ITEC 362	Introduction to Web Systems	
ITEC 562	Advanced Web Support Systems	
Select one of the following:		
ITEC 245	Introduction to Networking	
ITEC 264	Computer Applications in Business I	
ITEC 265	Introduction to Databases	
Select one ITEC elective		

Academic Programs

- The Department is developing
  - A PhD in Informatics (approval expectation in 2021)
  - Undergraduate and graduate certificates
- More practical than theoretical
- Partnership with industry
  - Cisco Network Academy
  - Palo Alto Networks Cybersecurity Academy
  - VMware IT Academy
  - Intel's Barefoot Academy
  - Juniper Networks
- Flexible program

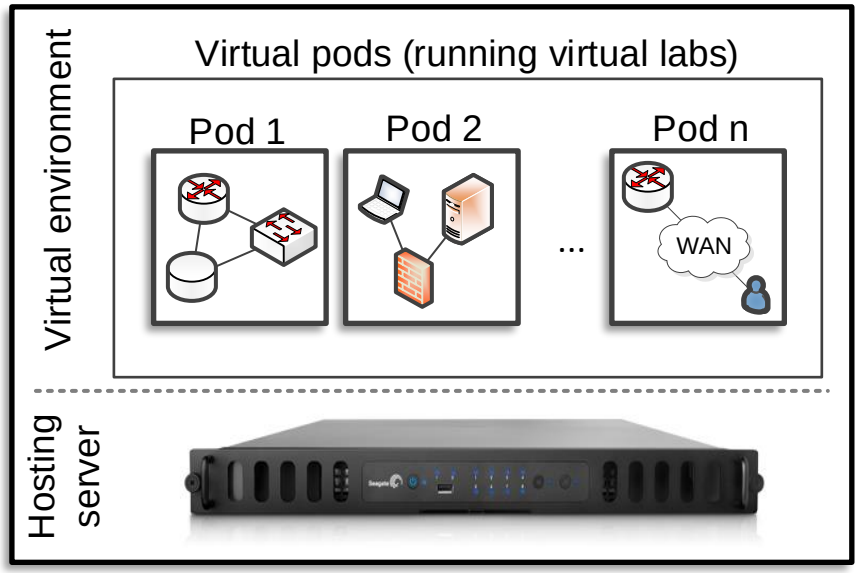
Virtual Platform

- IIT programs incorporate much hands-on activities
- The IEEE and ACM are the main societies which guide IT education
  - IT curriculum should emphasize “learning IT core concepts combined with authentic practice” and “use of professional tools and platforms” [1]
- Physical labs are typically used to teach and train IT students
- COVID exacerbated the needs of efficient technologies for hands-on education in IT
- UofSC works with the Network Development Group (NDG)[2], VMware, Palo Alto Cybersecurity Academy, Cisco, and others to virtualize labs
- A virtual platform enables an institution to move traditional curriculum relying on physical labs into an online format

1. “Information Technology Curricula Guideline 2017 (IT2017),” report by the ACM / IEEE Task Force on Information Technology Curricula, Dec. 2017. Online: https://tinyurl.com/yxauot8w
2. Network Development Group (NDG). Online: https://netdevgroup.com

Virtual Platform

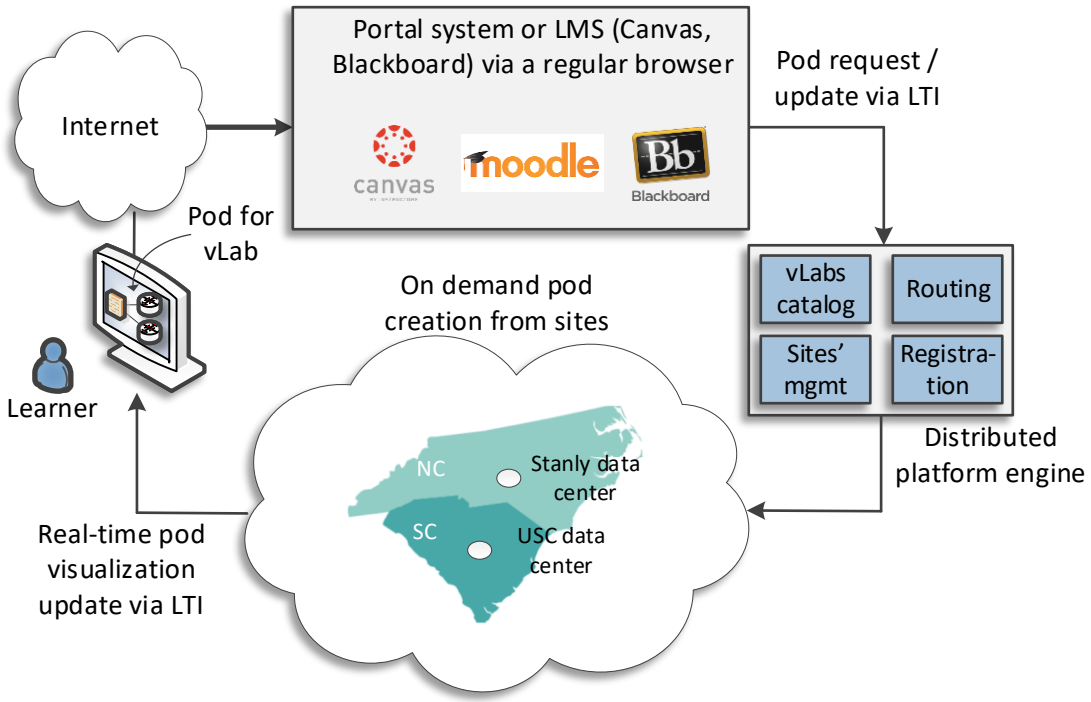
- Virtualization is a technology by which the software portion of a device (e.g., PC, routers, etc.) can execute on a general-purpose physical server as a virtual machine
- A pod is a set of virtual machines needed for the completion of a virtual lab exercise
- The pod can be as simple as a single isolated virtual machine, or as complex as autonomous systems with live traffic flowing to/from the Internet



Server hosting pods for virtual labs

Virtual Platform

- USC (SC), SCC (NC), and NDG are building a distributed virtual platform
- The goal is scalability, using the resources available on campus networks
- Since January 2020, the distributed platform has served more than 7,000 learners



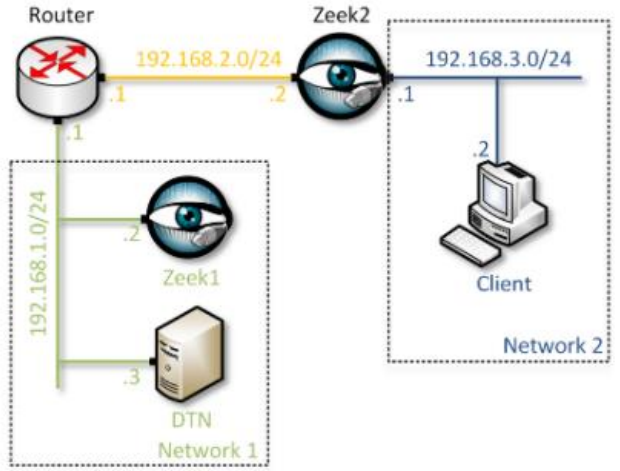
Virtual Platform

- There are multiple types of pods
  - Pods to learn concepts traditionally covered by academic programs
  - Pods to learn skills and techniques covered by certificate programs
  - Pods to perform research
- Industry partners are essential

Virtual Labs – Zeek Intrusion Detection

- The Zeek labs provide hands-on experience on Intrusion Detection System (IDS)
- Zeek is a passive, open-source network traffic analyzer
- It is primarily used as a security monitor in national labs, campus networks, enterprises, research labs

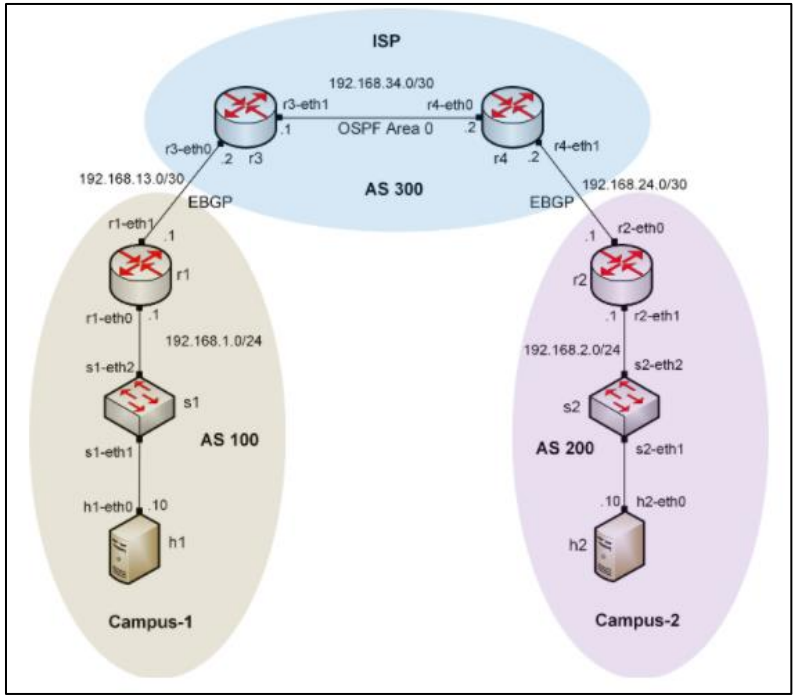
Lab 1	Introduction to the Capabilities of Zeek
Lab 2	An Overview of Zeek Logs
Lab 3	Parsing, Reading and Organizing Zeek Log Files
Lab 4	Generating, Capturing and Analyzing Network Scanner Traffic
Lab 5	Generating, Capturing and Analyzing DoS and DDoS-centric Network Traffic
Lab 6	Introduction to Zeek Scripting
Lab 7	Introduction to Zeek Signatures
Lab 8	Advanced Zeek Scripting for Anomaly and Malicious Event Detection
Lab 9	Profiling and Performance Metrics of Zeek
Lab 10	Application of the Zeek IDS for Real-Time Network Protection
Lab 11	Preprocessing of Zeek Output Logs for Machine Learning
Lab 12	Developing Machine Learning Classifiers for Anomaly Inference and Classification
Lab Manuals	



Virtual Labs – BGP

- These labs provide a detailed, hands-on experience to understand the Border Gateway Protocol (BGP), adjust its attributes, and control traffic on the Internet
- Routers use Free Range Routing (FRR) routing stack
- FRR is an open-source protocol stack that provides IP-based routing services

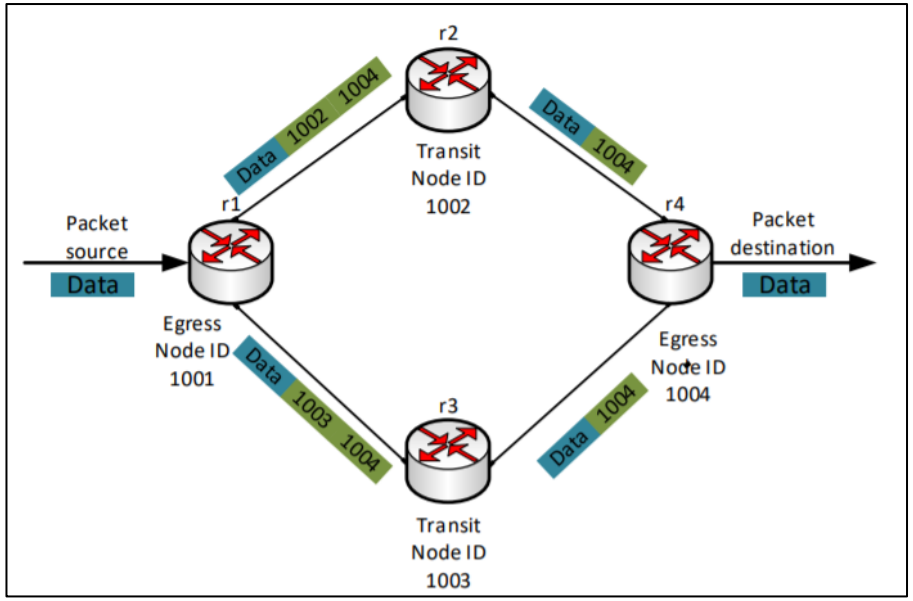
Lab 1	Introduction to Mininet
Lab 2	Introduction to Free Range Routing (FRR)
Lab 3	Introduction to BGP
Lab 4	Configure and Verify EBGP
Lab 5	BGP Authentication
Lab 6	Configure BGP with Default Route
Lab 7	Using AS_PATH BGP Attribute
Lab 8	Configuring IBGP and EBGP Sessions, Local Preference, and MED
Lab 9	IBGP, Next Hop and Full Mesh Topology
Lab 10	BGP Route Reflection
Lab Manuals	



Virtual Labs – MPLS and Advanced BGP Topics

- These labs provide a detailed, hands-on experience to understand advanced concepts and protocols
- Examples include MPLS, Multi-protocol BGP, BGP hijacking, virtual private networks (VPNs), Ethernet VPNs, and Segment Routing

Lab 1	Configuring Multiprotocol BGP
Lab 2	IP Spoofing and Mitigation Techniques
Lab 3	BGP Hijacking
Lab 4	Introduction to MPLS
Lab 5	Label Distribution Protocol (LDP)
Lab 6	Virtual Routing and Forwarding (VRF)
Lab 7	MPLS Layer 3 VPN using MP-BGP
Lab 8	Ethernet VPN (EVPN) using MP-BGP
Lab 9	Introduction to Segment Routing over IPv6 (SRv6)
Lab Manuals	



Virtual Labs – MPLS and Advanced BGP Topics

- These labs provide a detailed, hands-on experience to understand advanced concepts and protocols
- Examples include MPLS, Multi-protocol BGP, BGP hijacking, virtual private networks (VPNs), Ethernet VPNs, and Segment Routing

Lab 1	Configuring Multiprotocol BGP
Lab 2	IP Spoofing and Mitigation Techniques
Lab 3	BGP Hijacking
Lab 4	Introduction to MPLS
Lab 5	Label Distribution Protocol (LDP)
Lab 6	Virtual Routing and Forwarding (VRF)
Lab 7	MPLS Layer 3 VPN using MP-BGP
Lab 8	Ethernet VPN (EVPN) using MP-BGP
Lab 9	Introduction to Segment Routing over IPv6 (SRv6)
Lab Manuals	

Testing mistake triggered Telstra route 'hijacks'

By Juha Saarinen
Oct 5 2020
7:33AM

3 Comments

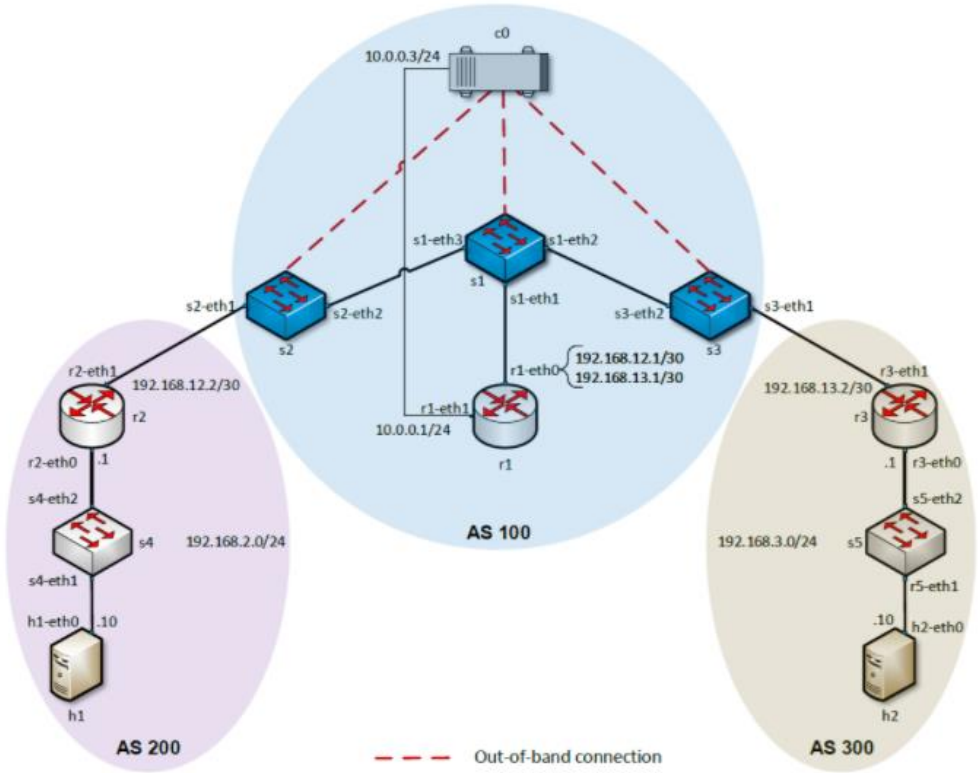
Routing mishaps difficult to prevent.

An erroneous bulk upload of static routes to a Telstra production network edge router was the cause of last Wednesday's internet-wide service disruption that saw

Virtual Labs – Software-defined Networking

- These labs provide a detailed, hands-on experience to Software-defined Networking (SDN)
- Devices and protocols include Open Virtual Switch (OVS), Open Network Operating System (ONOS) controller, VXLAN, and VPLS

Lab 1	Introduction to Mininet
Lab 2	Legacy Networks: BGP Example as a Distributed System and Autonomous Forwarding Decisions
Lab 3	Early efforts of SDN: MPLS Example of a Control Plane that Establishes Semi-static Forwarding Paths
Lab 4	Introduction to SDN
Lab 5	Configuring VXLAN to Provide Network Traffic Isolation
Lab 6	Introduction to OpenFlow
Lab 7	Routing within an SDN network
Lab 8	Interconnection between Legacy Networks and SDN Networks
Lab 9	Configuring Virtual Private LAN Service (VPLS)
Lab Manuals	



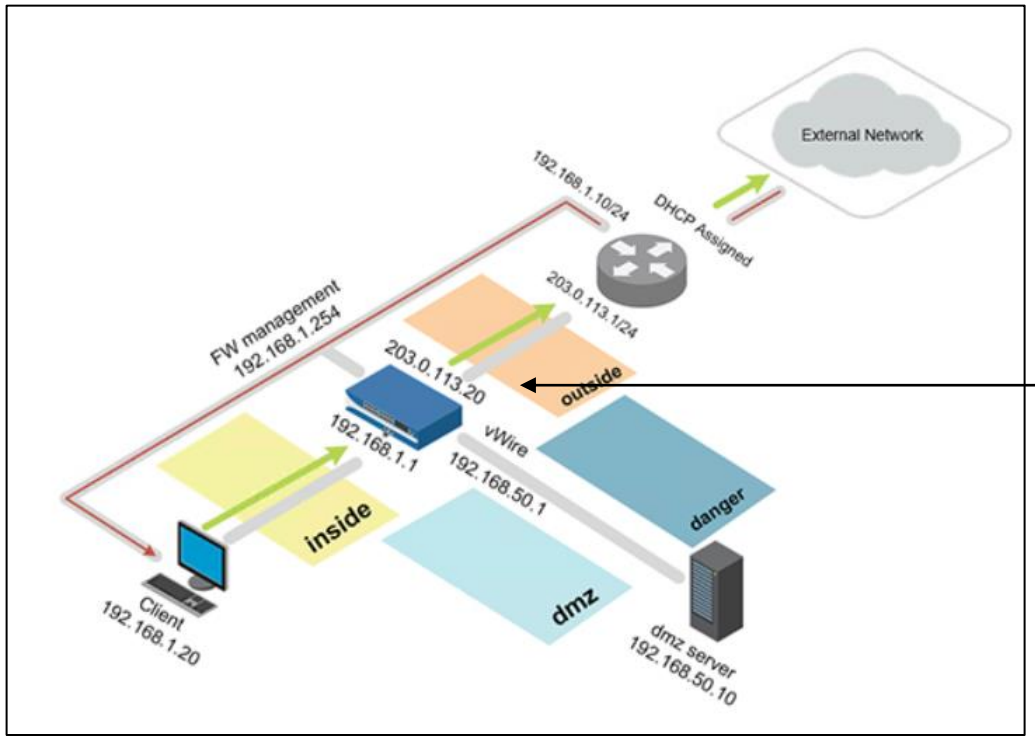
Virtual Labs – Palo Alto NG Firewall

- These labs enhance the student's understanding of how modern firewalls work, referred to as Next-generation Firewalls (NGFWs)
- Students gain hands-on experience deploying, managing, and monitoring firewalls in a (virtual) lab environment, using live traffic
- Material also prepares students for certificates
- The IEEE/ACM group "acknowledges the value of vendor and industry certifications and encourages students to pursue them as they see necessary"[1]

1. "Information Technology Curricula Guideline 2017 (IT2017)," report by the ACM / IEEE Task Force on Information Technology Curricula, Dec. 2017. Online: https://tinyurl.com/yxauot8w

Virtual Labs – Palo Alto NG Firewall

- These labs enhance the student's understanding of how modern firewalls work, referred to as Next-generation Firewalls (NGFWs)

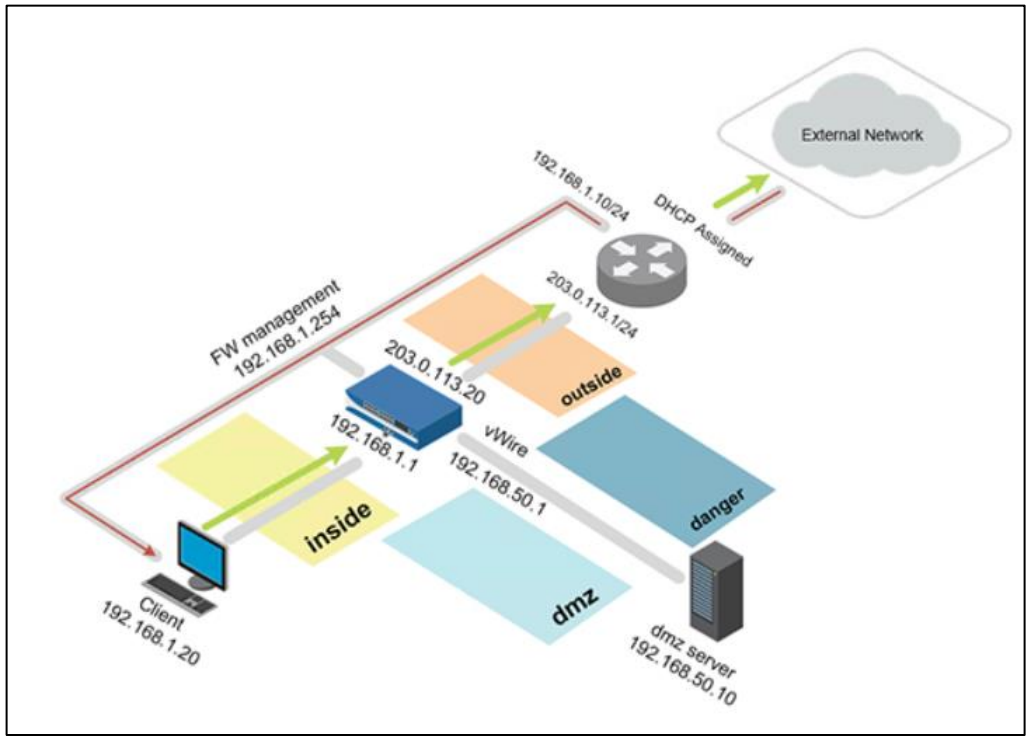


Pod deployed in private cloud

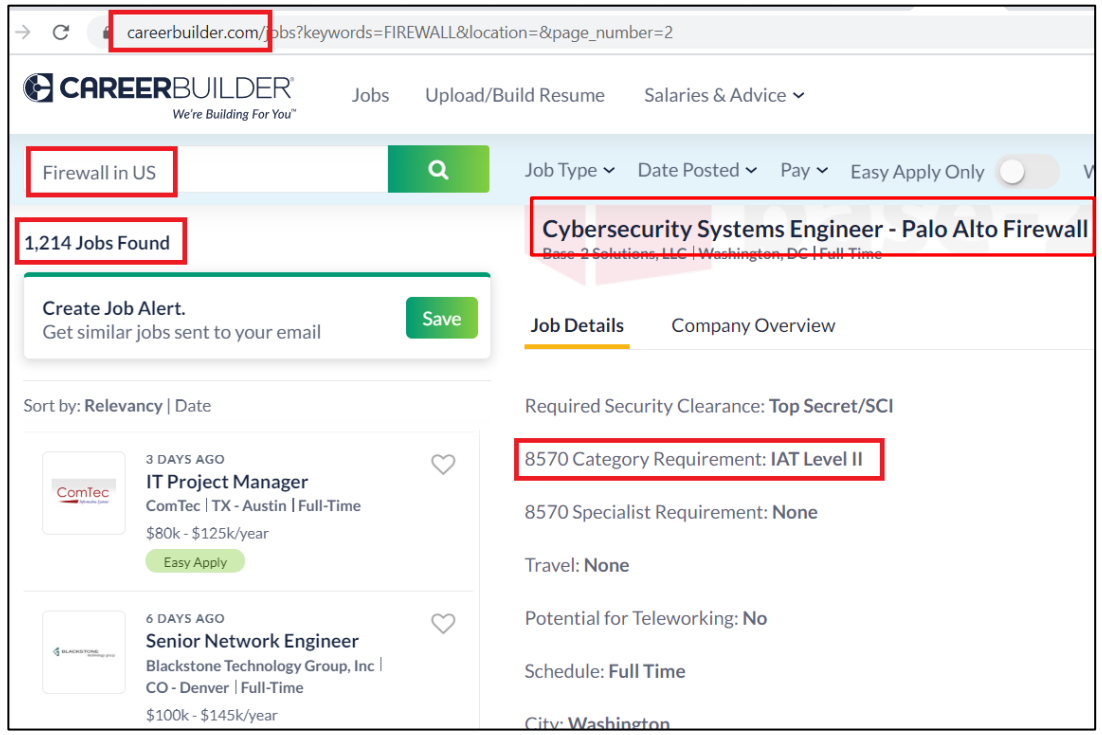
Next-generation Firewall Virtual Machine + licenses

Virtual Labs – Palo Alto NG Firewall

- These labs enhance the student's understanding of how modern firewalls work, referred to as Next-generation Firewalls (NGFWs)



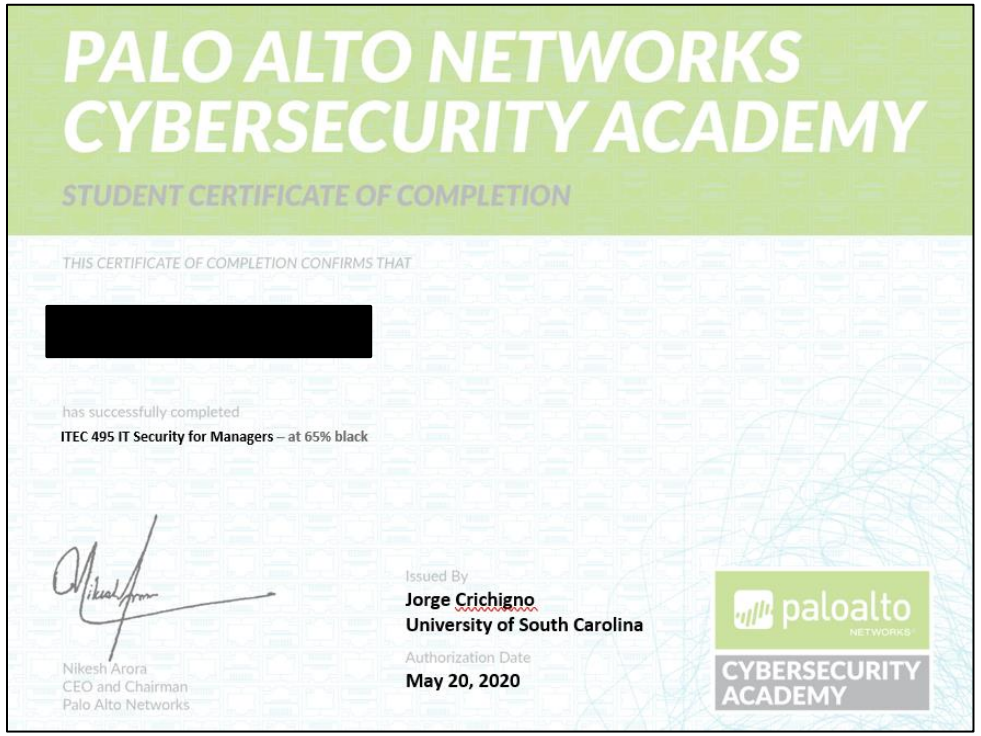
Pod deployed in private cloud



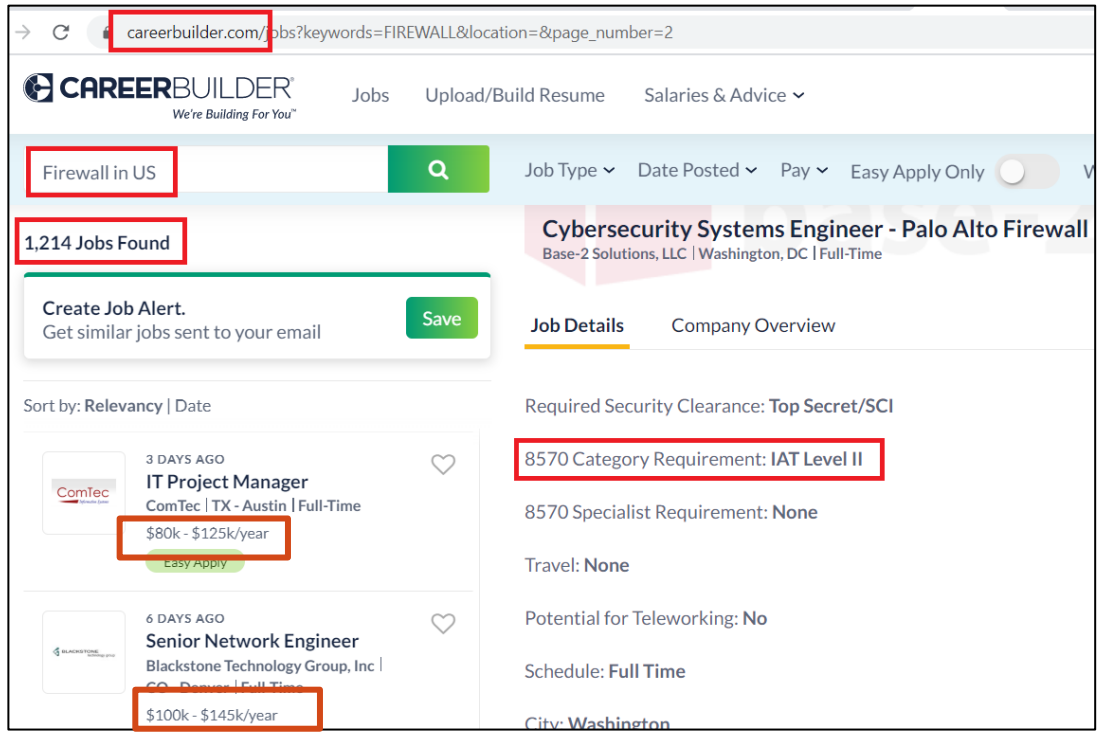
Job search

Virtual Labs – Palo Alto NG Firewall

- These labs enhance the student's understanding of how modern firewalls work, referred to as Next-generation Firewalls (NGFWs)



Additional credentials

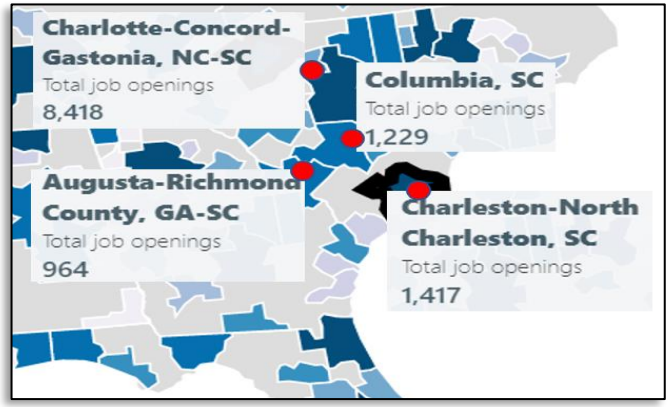


Job search

ONR's Cyber Project

- Office of Naval Research (ONR) is funding the project "Enhancing the Preparation of Next-generation Cyber Professionals"
- South Carolina cybersecurity needs
  - Naval Information Warfare Center (NIWC) Atlantic, SRNL, Fort Jackson, Shaw Air Force Base
- 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]
- The College of Engineering and Computing is addressing the workforce needs:
  - Encourage Reserve Officers' Training Corps **(ROTC)** students to obtain an IT minor
  - Undergraduate applied research

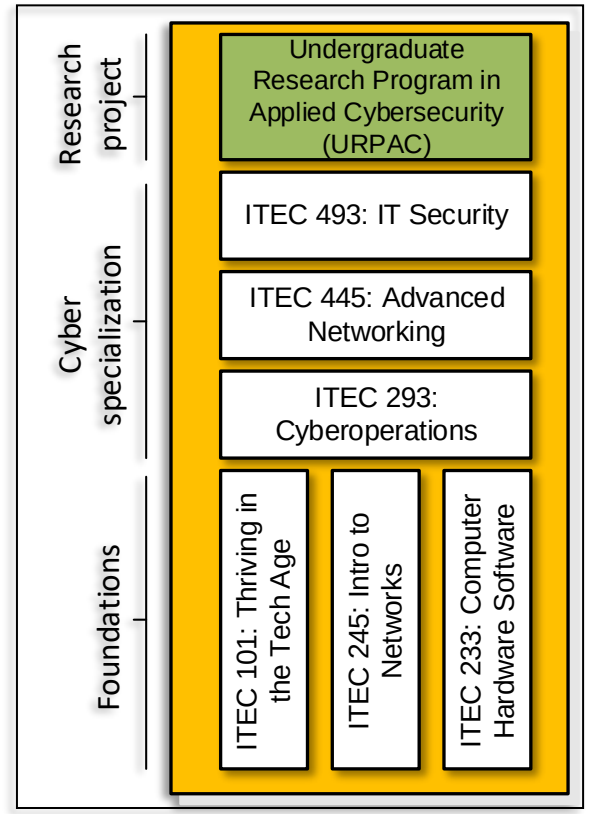
Cybersecurity job openings in four metro areas near Columbia, Feb. 2020



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

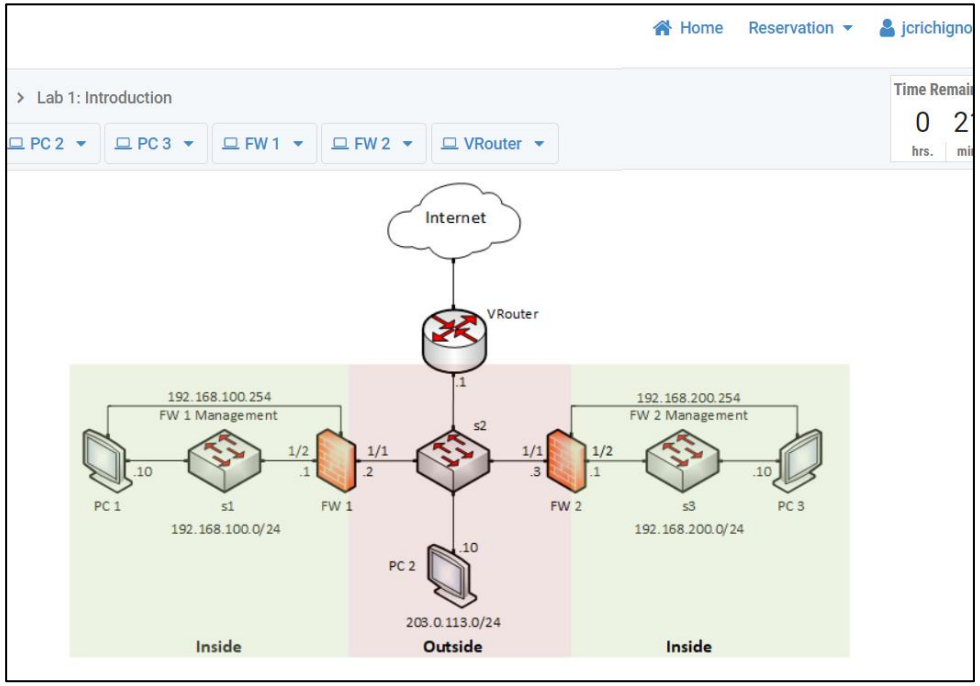
1. Minor in IT – Cyber specialization
   - Option to earn DoD's approved baseline certificates for Information Assurance Technical (IAT)
   - Self-contained specialization; no pre-reqs
2. Undergraduate applied research
3. Private cloud with professional tools and platforms
4. Collaboration with industry



Minor in IT and undergraduate research

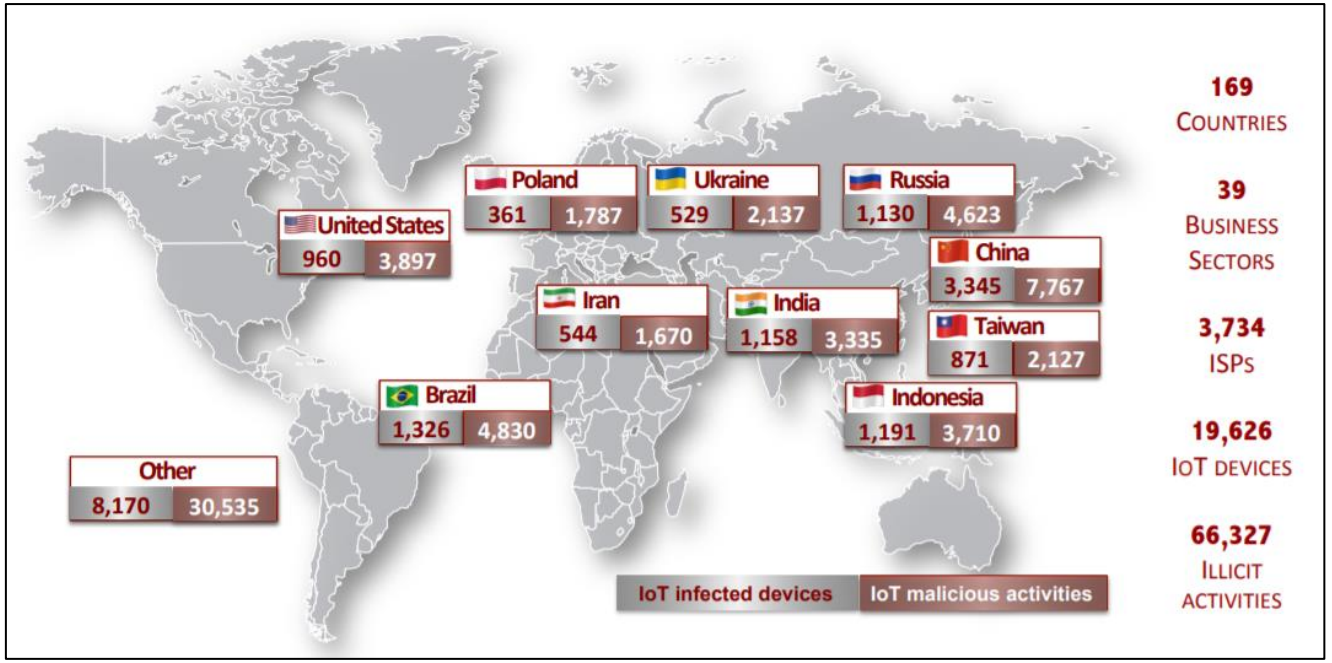
ONR's Cyber Project

- Undergraduate students work 18 hours per week, 15 weeks, $18 per hour ($4,050)
  - Applied research
  - Professional tools, platforms, market validation
  - Cisco Systems, Palo Alto Networks, VMware, Juniper, Intel
  - Focus on relevant technology, customized scenarios; e.g., IPsec-based VPNs with NGFWs

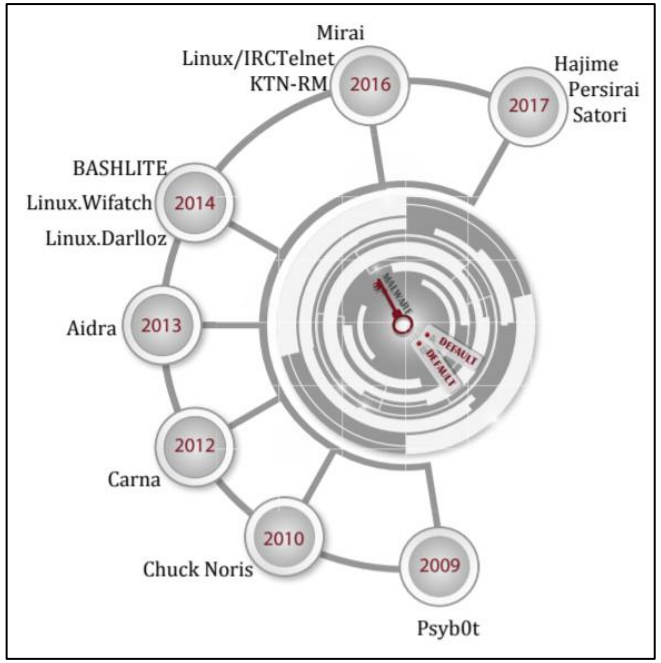


Graduate Projects

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



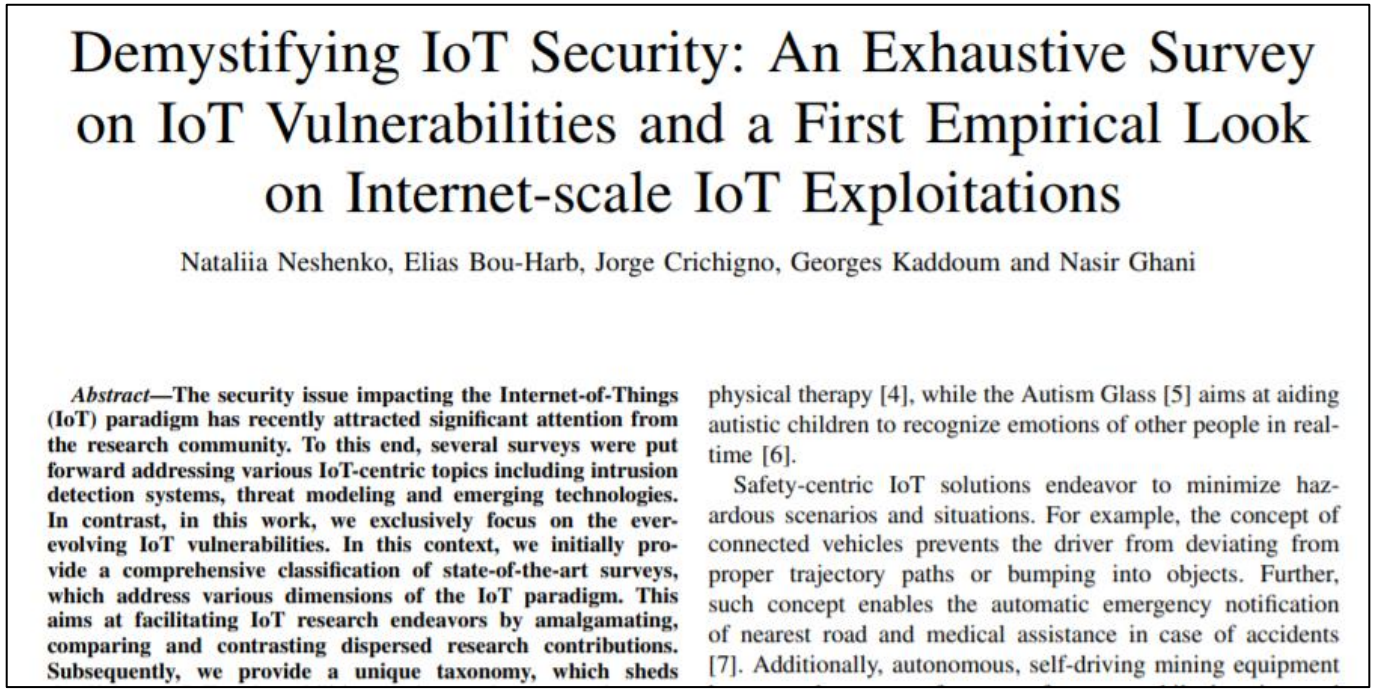
Global distribution of exploited IoT devices; results from this research project



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

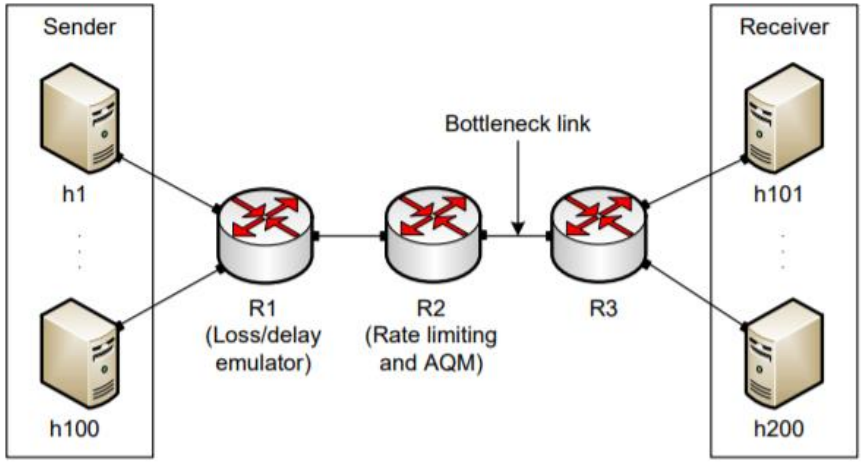
***Abstract*—The security issue impacting the Internet-of-Things (IoT) paradigm has recently attracted significant attention from the research community. To this end, several surveys were put forward addressing various IoT-centric topics including intrusion detection systems, threat modeling and emerging 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**

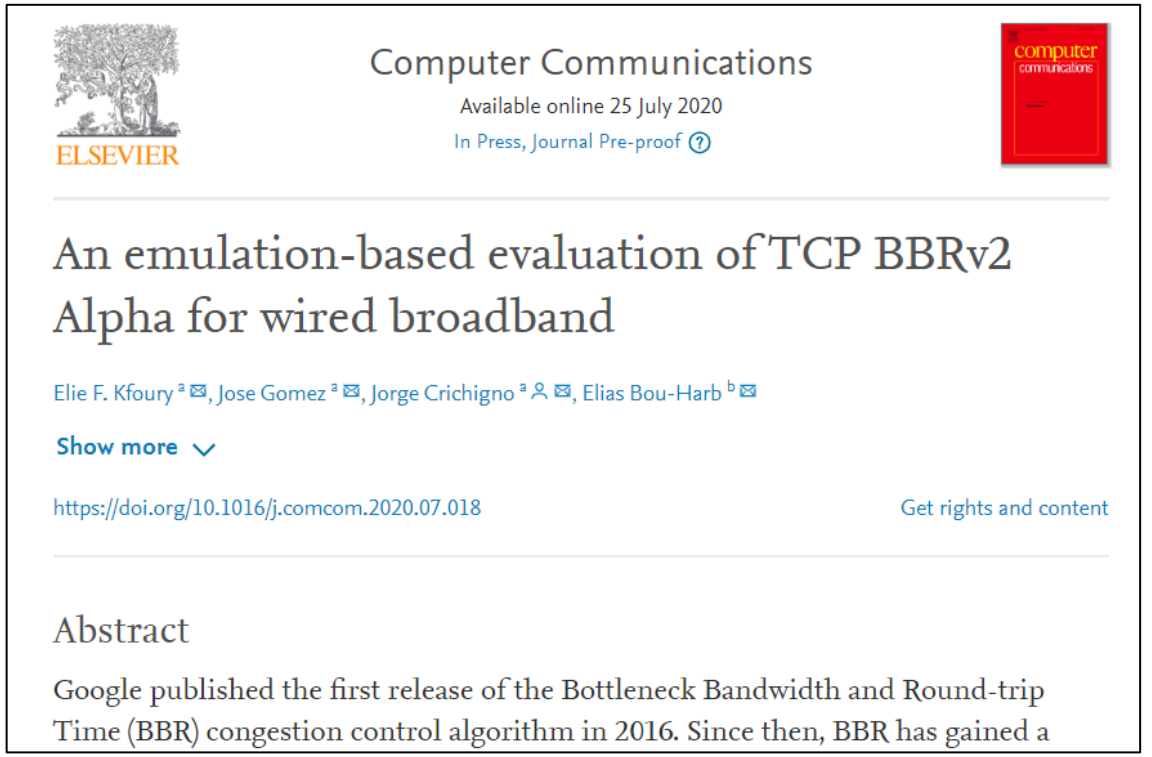
physical therapy [4], while the Autism Glass [5] aims at aiding autistic children to recognize emotions of other people in real-time [6].

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

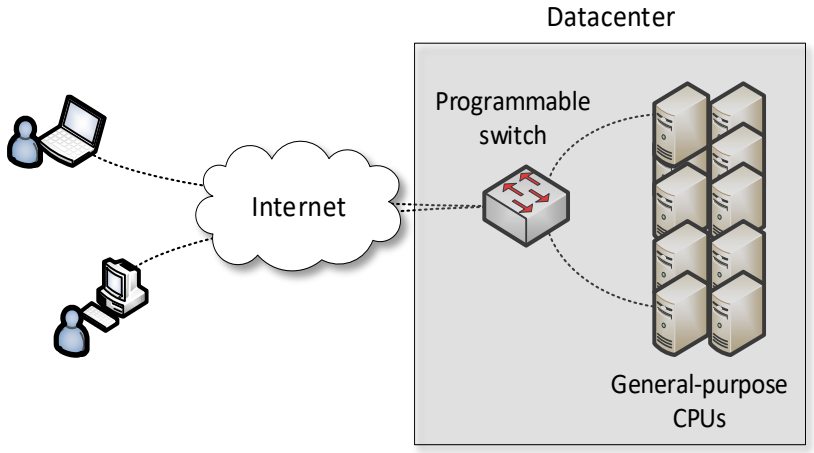
Get rights and content

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)

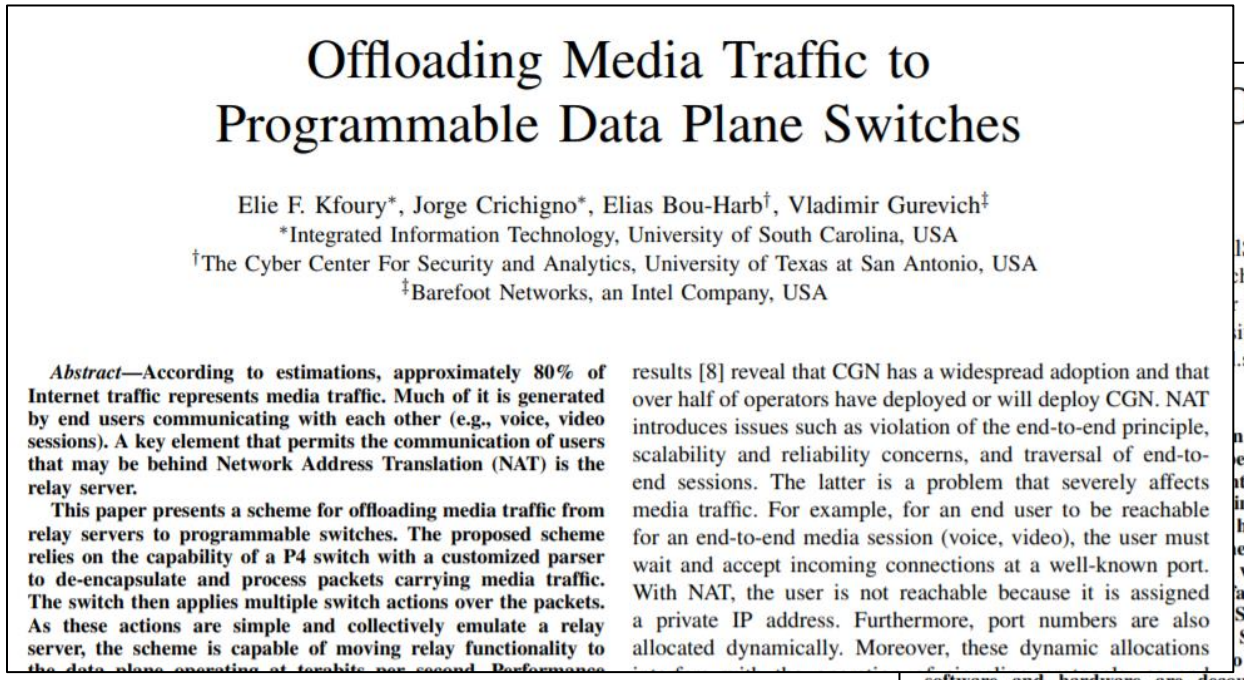


Application example: media (voice) relay server

	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)



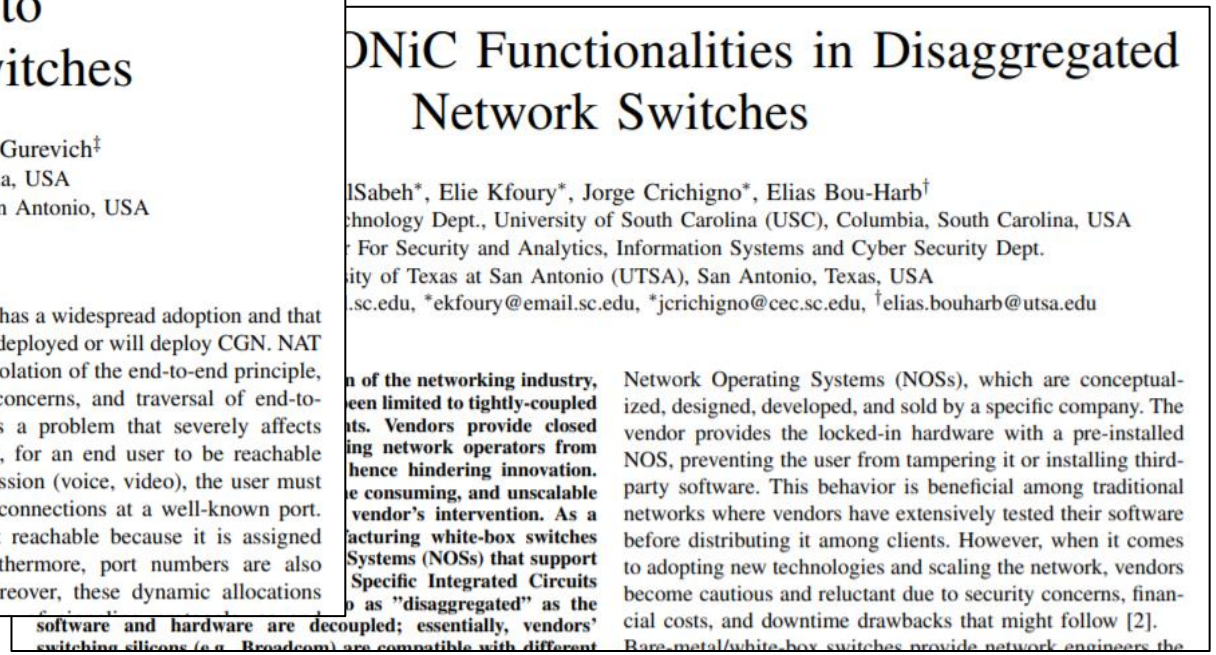
Offloading Media Traffic to Programmable Data Plane Switches

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



ONiC Functionalities in Disaggregated Network Switches

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

n of the networking industry, een limited to tightly-coupled ts. Vendors provide closed ing network operators from hence hindering innovation. e consuming, and unscalable vendor's intervention. As a facturing white-box switches Systems (NOSs) that support Specific Integrated Circuits o 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].

The END