“Teaming Together on Information Security and National Defense Research”

Defense Innovation Board

Georgia Cyber Center

November 20, 2019

Jorge Crichigno

Department of Integrated Information Technology

University of South Carolina

Columbia, SC

University of South Carolina

- Contact Information
  - Jorge Crichigno, Associate Professor
  - Department of Integrated Information Technology (IIT)
  - University of South Carolina (UofSC)
  - jcrichigno@cec.sc.edu
- Departmental Information
  - Bachelor of Science in IIT
  - Networks, cyber, business aspects, web, cloud, programming, HCI
  - ABET accredited
  - Minor in IIT, advisement tracks
    - ✓ Cyberoperations
    - ✓ IT Business Operations
    - ✓ Databases
    - ✓ Web
    - ✓ Project Management
    - ✓ Networks

Training

- “Cyberinfrastructure Expertise on High-throughput Networks for Big Science Data Transfers”
  - UofSC is the anchor institution of the “Cyberinfrastructure Network of Expertise”
  - UofSC, University of South Florida, University of Texas at San Antonio, Florida Atlantic University
  - Enhancing and securing cyberinfrastructure for big science data transfers
  - Technologies / collaborators / academies: Department of Energy (ESnet), Juniper Networks, Cisco Systems, Tofino’s Barefoot Networks

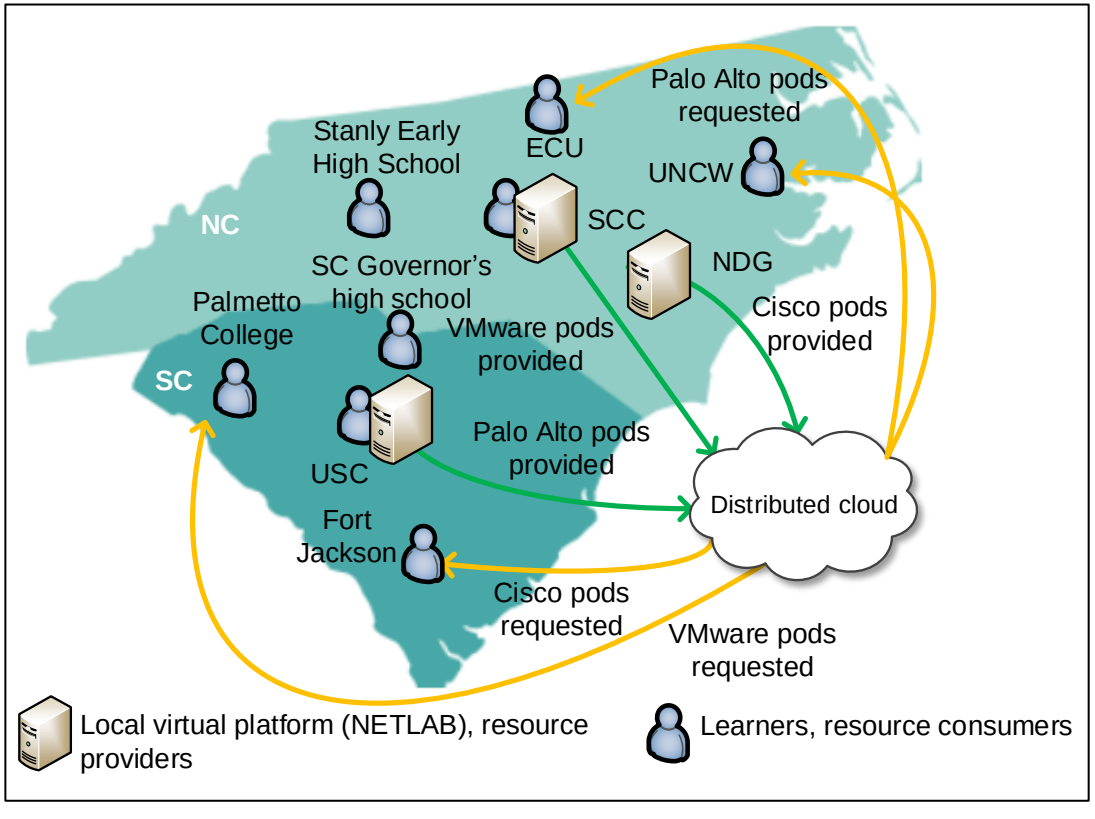
Training

- Cyber training for IT professionals
- Self-pace, summer training
  - South Carolina, Arizona, California, Florida, Texas
  - 2019 / 2020:

Dates	Workshop	Place	Attendance
July 22-23, 2019	Training Workshop SC	UofSC, Columbia, SC	77
July 25-26, 2019	Developing Workshop SC	UofSC, Columbia, SC	69
July 30-Aug. 1, 2019	Training Workshop AZ	ASU, Tempe, AZ	62
		Total:	**208**

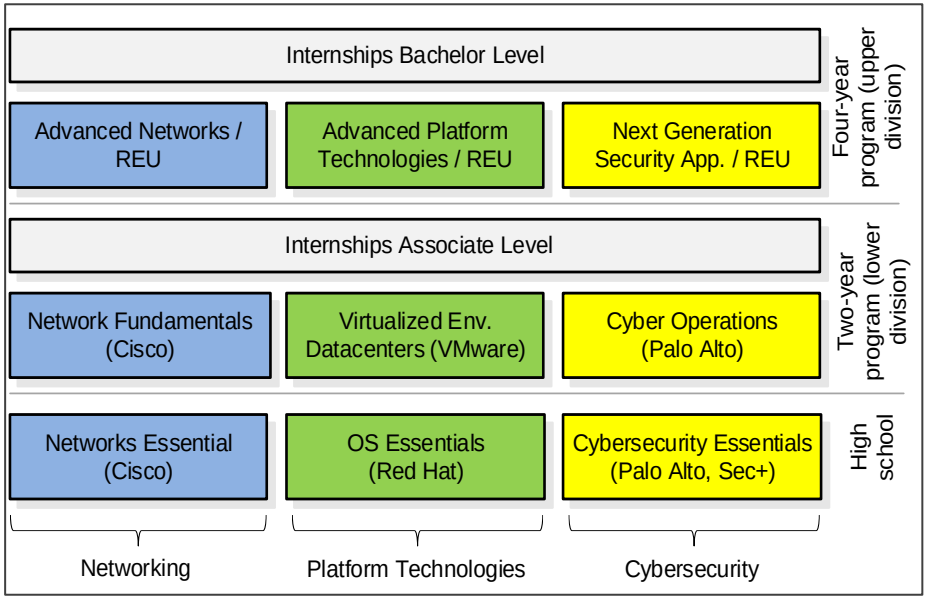
Workforce

- "Multi-state Community College, University and Industry Collaboration to Prepare Learners for 21st Century Information Technology Jobs"
  - Professional development for high-school teachers, technical college and university professors, and IT professionals
  - Focus on instruction, workforce development for IT
    - ✓ Networks
    - ✓ Cybersecurity
    - ✓ Cloud
    - ✓ Operating Systems



Workforce

- Week-long instructor trainings (Summer)
- Statewide platform
- Connection with job market
  - SC and NC Chambers of Commerce
  - Cisco, Palo Alto, VMware



- DoD 8470 Information Assurance workforce technical personnel (IAT):
  - Level 1: Computing environment information assurance
  - Level 2: Network environment information assurance
  - Level 3: Enclave, advanced network and computer information assurance

Course	IAT 1	IAT 2	NICE framework
ITEC 233 Intro to HW/SW	✓		
ITEC 245 Intro Networks	✓		
ITEC 293 Cyberoperations - SOCs			
ITEC 445 Advanced Networks		✓	
ITEC 493 IT Security / Next-gen FW			✓

NICE: National Initiative for Cybersecurity Education

Workforce

- USC ROTC, Minor in Information Technology – Cyber (1)
- Internships – Cyber (2, 3)

1

3

2

Savannah River NUCLEAR SOLUTIONS™
FLUOR • NEWPORT NEWS NUCLEAR • HONEYWELL

Savannah River National Laboratory™
OPERATED BY SAVANNAH RIVER NUCLEAR SOLUTIONS

☑ Home — ☑ Search openings — ☑ Search results — ☐ Job details

Job details

Job 1 of 1

Submit to job | Send to friend | Save to cart | View similar jobs

Auto req ID	4471BR
Job Abbreviation Title	SRNL Industrial Control Systems Security Intern
Job Description	Savannah River National Laboratory (SRNL) is a multi-program laboratory applying state of the art science and practical, high- Department of Energy's (DOE) Savannah River Site (SRS), the laboratory develops and deploys innovative technologies to ad Intern will participate in the development of a virtual network which simulates known environments to research vulnerabilities of through scanning and patching industrial controllers and generating documentation to ensure each system meets SRS cyber s environments and robotics systems.
Major	Computer Science Other
Other Major	Cyber Security, Industrial Systems, Virtual Reality, Industrial Controls/Robotics
Basic Qualifications (Quantifiable; e.g. Three Years Experience, Bachelors Degree)	Junior or Senior Knowledge and skill in basic computer applications and coding. Pursuing degree in Computer Science, Cyber Security, Industrial Systems, Virtual Reality, Industrial Controls/Robotics or relate Minimum overall GPA of 2.5 on a 4.0 GPA scale
Preferred Qualifications (e.g. Masters Degree)	Preferred courses: Introduction to Computer Networks Advanced Computer Networks IT Security
Removal Date	22-May-2019

Submit to job | Send to friend | Save to cart | View similar jobs

Research

- “Building a Science DMZ for Data-intensive Research and Computation at the University of South Carolina”
- “Small: Devising Data-driven Methodologies by Employing Large-scale Empirical Data to Fingerprint, Attribute, Remediate and Analyze Internet-scale IoT Maliciousness”

Research

- Adoption of latest technology for a variety of applications
  - In-network computation
  - In-network cache
- IT security, rapid DDoS detection using advanced switching capabilities
- 6-node 100 Gbps testbed, programmable switches and associated development kit (Barefoot agreement)

Towards a P4-Driven Unified DDoS Detection and Mitigation Strategy

Kurt Friday, Elie Kfoury, Elias Bou-Harb, Jorge Crichigno Benitez
The Cyber Center for Security & Analytics,
University of Texas at San Antonio, San Antonio, Texas, USA
Department of Integrated Information Technology,
University of South Carolina, Columbia, South Carolina, USA
kurt.friday@utsa.edu, elias.bouharb@utsa.edu,

***Abstract*—Distributed Denial of Service (DDoS) attacks have terrorized our networks for decades, and with attacks now reaching 1.7 Tbps, even the slightest latency in detection and subsequent remediation is enough to bring an entire network down. While strides in Software Defined Networking (SDN) have provided a promising means of addressing such maliciousness, all efforts to ultimately harness said capabilities have inevitably come up short. Fortunately, P4 recently came about as a platform agnostic language for programming the data plane and thus allowing for customized and sophisticated switch pipelines. To this end, in response to the sheer extent of this modern-day maliciousness coined DDoS, we propose a first-of-a-kind P4-based detection and mitigation scheme that will not only function as intended regardless of the size of the attack, but overcomes the vulnerabilities of SDN that have characteristically been exploited by DDoS. Moreover, it is geared towards the unimpeded traversal of legitimate traffic and overall functioning of the SDN network in which it resides, amid the vast array of attacks currently ex-**

Offloading Media Traffic to Programmable Data Plane Switches

Elie F. Kfoury*, Jorge Crichigno* and Elias Bou-Harb†
*Integrated Information Technology, University of South Carolina, USA
†Cyber Center For Security and Analytics, University of Texas at San Antonio, USA

(NAT). Despite being developed more than 20 years ago as a temporary solution, virtually all home and most enterprise and campus networks today still use NAT. Furthermore, recent studies show that the number of network operators deploying Carrier-grade NAT (CGN) is increasing [9]. CGN is a scheme that extends the traditional NAT (that occurs at the customer premise equipment) to a large-scale deployment inside the service provider's network. Survey results [10] reveal that CGN has a widespread adoption and that over half of operators have deployed or will deploy CGN. Although NAT mitigates the depletion of IPv4 addresses, it 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

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

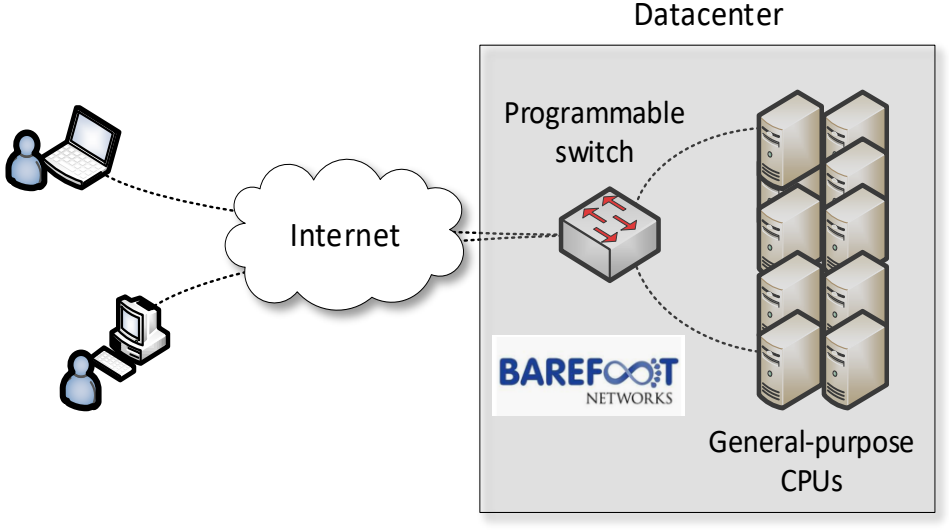
***Abstract*—The security issue impacting the Internet-of-Things (IoT) paradigm has recently attracted significant attention from the research community. To this end, several surveys were put forward addressing various IoT-centric topics including intrusion detection systems, threat modeling and emerging 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 the light on IoT vulnerabilities, their attack vectors, impacts on numerous security objectives, attacks which exploit such vulnerabilities, corresponding remediation methodologies and currently offered operational cyber security capabilities to infer and monitor such weaknesses. This aims at providing the reader with a multidimensional research perspective related to IoT**

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 keeps workers away from unsafe areas, while location and proximity IoT sensors allow miners to avoid dangerous situations [8]. Moreover, deployed IoT sensors at factories monitor environmental pollution and chemical leaks in water supply, while smoke, toxic gases and temperature sensors coupled with

Research

- Key idea
  - In today's world, most computational tasks are executed in general-purpose computers (PCs, cloud computing)
  - Some tasks may be "offloaded" (executed) in switch hardware operating at terabits per second rates
  - Speed (precise maximum latency) and volume (terabits per second)



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

Outcomes

Orders of magnitude throughput improvements
Customized network behavior