Overview Cybersecurity
College of Engineering and Computing
University of South Carolina

Jorge Crichigno
Department of Integrated Information Technology
jcrichigno@cec.sc.edu

SRNL Deputy/Associate Lab Directors Visit - Meeting
Swearingen 3A75
College of Engineering and Computing – University of South Carolina
January 25, 2023

UNIVERSITY OF
South Carolina

College of Engineering and Computing

- The University of South Carolina is a National Center of Academic Excellence (CAE) for Cyber Defense Education (CAE-CDE), and a CAE for Research (CAE-R)
  - Designation made by the National Security Agency (NSA)
  - Computer Science and Engineering (CSE) is the primary unit
  - IIT is the main department supporting CSE
- The College of Engineering and Computing offers ABET Accredited Programs
  - B. Sc. Computer Science (CSE)
  - B. Sc. Information Technology (IIT)
  - Multiple minors; e.g., Cybersecurity Operations, Networks (IIT)

Enhance the Preparation of Cybersecurity Professionals
Support: Office of Naval Research (ONR)

Purpose: cybersecurity - workforce development (undergraduates)

2020 – 2022

Preparing Cyber Warfare Professionals by Integration of Curriculum, Experiences, and Internships

- Supported by ONR, 2020 – 2022 ($250,000)
- Goals:
  1. Develop a cybersecurity concentration within an academic minor in Information Technology.
  2. Establish an Undergraduate Research Program in Applied Cybersecurity.
  3. Deploy virtual equipment pods on a virtual platform, accessible over the Internet, to support and facilitate the research and teaching activities from anywhere, without compromising hands-on experiences.
  4. Establish meetings among industry, government, high schools, and higher-education institutions to enhance cybersecurity preparation.

Project Overview

- **Goals:**

1. Develop a cybersecurity concentration within an academic minor in Information Technology.
   Minor in Cybersecurity Operations is now offered, starting Fall 2021.
   Learners can obtain DoD's 8570 approved certs (cyber, networks skills, 8/16-week course).

Cybersecurity Operations, Minor

Degree Requirements (18 Hours)

Course	Title	Credits
Select one of the following:		3
ITEC 101	Thriving in the Tech Age	
ITEC 204	Program Design and Development	
ITEC 552	Linux Programming and Administration	
ITEC 233	Introduction to Computer Hardware and Software	3
ITEC 245	Introduction to Networking	3
ITEC 293	Cybersecurity Operations	3
ITEC 445	Advanced Networking	3
ITEC 493	Information Technology Security for Managers	3
Total Credit Hours		**18**

https://tinyurl.com/4mbj3z4k

Project Overview

- **Goals:**

2. Establish an Undergraduate Research Program in Applied Cybersecurity (14 weeks).

   The program has been established and supports between 10-12 students per semester.

Cadet	Branch	Name	Semester	Project
1	Navy	Christian S	Spring 2021	Application ID
2	Army	Brendan C	Fall 2020	Protection against Bruteforce Attacks with NGFW
3	Army	Jack S	Fall 2020	Mitigating Routing Hijacking Attacks
4	Army	Matthew D	Fall 2020	Mitigating Routing Hijacking Attacks
5	Army	Chris N	Fall 2020	Protection against Reconnaissance and Scan Attacks
6	Army	Jack S	Spring 2021	Policy-based Forwarding
7	Army	Matthew D	Spring 2021	Policy-based Forwarding
8	Civilian	Keegan S	Fall 2020	An open-source library for computer networks and cybersecurity
9	Civilian	Dakota M	Fall 2020	Distributed Denial of Service (DDoS) Protection with Next Generation Firewalls (NGFWs)
10	Civilian	Lauren W	Fall 2020	Protection against Bruteforce Attacks with NGFW
11	Civilian	Josue H	Fall 2020	Site to site VPN with NGFWs
12	Civilian	Brian N	Fall 2020	Distributed Denial of Service (DDoS) Protection with Next Generation Firewalls (NGFWs)

⋮

Project Overview

- **Goals:**

2. Establish an Undergraduate Research Program in Applied Cybersecurity (14 weeks).

   The program has been established and supports between 10-12 students per semester.

Chris Ngo

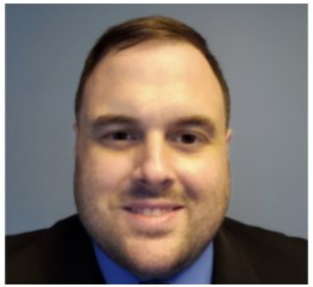
Jack Sadle

David Williams

Matt Driver

Christian Tsirlis

Ryan Tallent



Project Overview

- **Goals:**

2. Establish an Undergraduate Research Program in Applied Cybersecurity (14 weeks).

   The program has been established and supports between 10-12 students per semester.

Brad Wilson, IT student

"The skills I learned during my ONR project were very similar to those skills needed to become part of the Networking/Perimeter team at Savannah River National Laboratory (SRNL) … My managers [at SRNL internship] were very pleased with my knowledge and experience with next generation firewalls. I was offered a full-time position contingent upon my graduation in May 2022".

Name	Position
Ty Love-Baker	2nd Lt. at United States Marine Corps, DC
Dakota McDaniel	Security Analyst at Lowe's – COO Pluto (Los Angeles, CA)
Lauren Waddell	IT Specialist, SC Department of Insurance (Columbia, SC)
Josue Hernandez	Security Service Specialist at IBM (Chicago, IL)
Kyle Radzak	Info. Security Specialist at Lowe's (Charlotte, NC)
Nathan Bohmer	Project Coordinator at Black Box Networks (Southport, NC)
Brad Wilson	IT Intern at SRNL – Now FT at SRNL (Aiken, SC)
Zach Fowler	IT at Blue Cross Blue Shield (Columbia, SC)
Nathan Long	Technology Analyst at AIG (Charlotte, NC)
Sam Kelley	IT Infrastructure Engineering (Wells Fargo, Chandler, AZ)

⋮

Project Overview

- **Goals:**

2. Establish an Undergraduate Research Program in Applied Cybersecurity (14 weeks).

   The program has been established and supports between 10-12 students per semester.

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

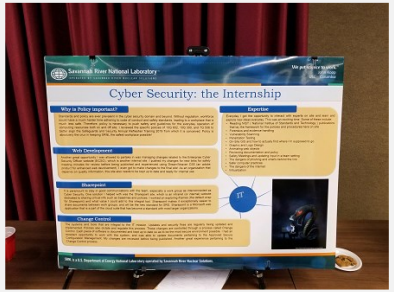
Job details

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

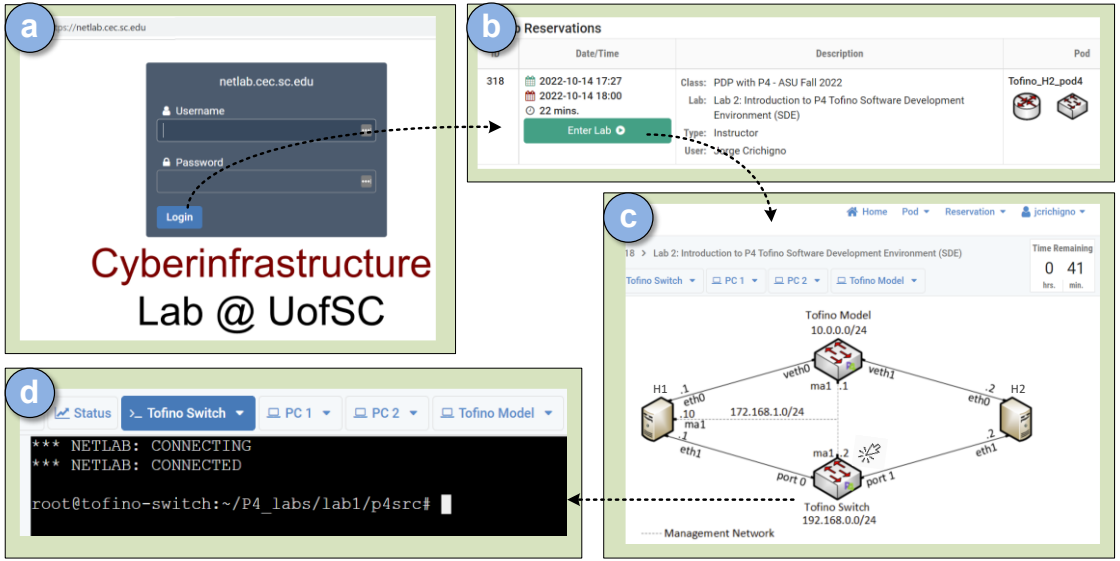
Submit to job | Send to friend | Save to cart | View similar jobs



Project Overview

- **Goals:**

3. Deploy virtual equipment pods on a virtual platform, accessible over the Internet, to support and facilitate the research and teaching activities from anywhere, without compromising hands-on.
   - The cloud system supports education and research
   - It was established by USC, Stanly Community College, and the Network Development Group (NDG) in 2019
   - It is currently used by colleges, universities, the National Guard, and multiple agencies



Project Overview

- **Goals:**

4. Establish meetings among industry, government, high schools, and higher-education institutions to enhance cybersecurity preparation.
   - Lawrence Berkeley National Lab (LBNL)
   - National Guard – Cyber & Information Advantage Battalion (CIAB)
   - SANS institute (“girlsgocyber”)
   - Multiple higher-ed institutions
   - International Networks at Indiana
   - Texas’ Lonestart Education and Research (TX)
   - Florida Lambda Rail Research and Education Network (FL)
   - Front Range GigaPop (CO)
   - Great Plains Network (Midwest States)
   - Internet2 (National)
   - U.S. Army Cyber Center of Excellence (CCoE) (Signal School)

Project Overview

- **Goals:**

4. Establish meetings among industry, government, high schools, and higher-education institutions to enhance cybersecurity preparation.
   - Intel
   - VMware
   - Palo Alto Networks
   - Juniper Networks
   - Cisco Systems

Project Overview

- **Goals:**

4. Establish meetings among industry, government, high schools, and higher-education institutions to enhance cybersecurity preparation.

UNIVERSITY OF South Carolina SoX Southern Crossroads

SoX Virtual Training Workshop

Wednesday March 22, 2023, 01:00PM – 05:00PM ET

Wednesday March 29, 2023, 01:00PM – 05:00PM ET

Click Here to Register

Organizers	Venue
Southern Crossroads / Southern Light Rail (SOX / SLR)	Online
The Engagement and Performance Operations Center (EPOC)	Link will be published soon
The Research Computing (RC) Group at University of South Carolina	

Project Overview

- **Goals:**

4. Establish meetings among industry, government, high schools, and higher-education institutions to enhance cybersecurity preparation.

UCF / FLR Workshop on Networking Topics

Thursday February 16, 2023, 08:00AM – 04:00PM ET

Friday February 17, 2023, 08:00AM – 01:00PM ET

Click Here to Register

Organizers	Venue
University of Central Florida (UCF)	University of Central Florida (UCF)
Florida LambdaRail (FLR)	12351 Research Pkwy, Orlando, FL 32826
The Engagement and Performance Operations Center (EPOC)	
Energy Sciences Network (ESnet)	
University of South Carolina (USC)	

Project Overview

- **Goals:**

4. Establish meetings among industry, government, high schools, and higher-education institutions to enhance cybersecurity preparation.

UNIVERSITY OF South Carolina

A Hands-on Tutorial on P4 Programmable Data Planes

NSF ESnet ENERGY SCIENCES NETWORK

Internet2 Technology Exchange

Monday December 5, 01:30-04:30pm

Organizers	**Venue**
The Cyberinfrastructure Lab at UofSC	Sheraton Denver Downtown Hotel
Energy Sciences Network (ESnet)	Denver, Colorado

Project Overview

- **Goals:**

4. Establish meetings among industry, government, high schools, and higher-education institutions to enhance cybersecurity preparation.

A Hands-on Workshop on P4 Programmable Data Planes

UNIVERSITY OF South Carolina

CENIC 2022 Annual Conference

Wednesday September 28, 01:30-03:00pm, Pacific Time

Organizers	**Venue**
The Cyberinfrastructure Lab at UofSC	Hyatt Regency
	Monterey, California

Project Overview

- **Goals:**

4. Establish meetings among industry, government, high schools, and higher-education institutions to enhance cybersecurity preparation.

Tutorial on Science DMZ

NSF CC* PI Workshop

Monday September 19, 01:00-03:00pm, Central Time

Organizers	**Venue**
Engagement and Performance Operations Center (EPOC)	Renaissance Minneapolis Hotel, The Depot
University of South Carolina (UofSC)	Minneapolis, Minnesota

Preparing Cyber Warfare Professionals by
Integration of Curriculum, Experiences, and Internships
Support: Office of Naval Research (ONR)

Purpose: cyberwarfare - workforce development (undergraduates)

2023 - 2026

Preparing Cyber Warfare Professionals by Integration of Curriculum, Experiences, and Internships

- Recommended for funding – ONR, 2023 – 2026 ($600,000)
- USC will become the hub for Cyber Warfare preparation
- The project will have a national impact, targeting diverse audience
  - ROTC cadets
  - Veterans
  - STEM students
  - Communities of practice: Lawrence Berkeley National Laboratory (LBNL) and Internet2
  - Self-paced learning material

Preparing Cyber Warfare Professionals by Integration of Curriculum, Experiences, and Internships

- Objective 1: Advance formal and informal cyber communities and connect relevant organizations

Audience	Activity	Learning Setting	Partners	Subject	Outcome
ROTC cadets and midshipman at USC, UTSA, SCSU	**a.** Six 16-week academic courses embedded in academic programs at USC, SCSU, UTSA (formal learning); **b.** 12-week C4ISR research experience (formal learning)	Courses in CS, CI, and IT that will include virtual labs on topics relevant to the DoN and DoD	ROTC programs at USC, UTSA, SCSU	Cybersecurity, warfare, networks, communications, virtualization	ROTC graduates (BSc) with MOS, DoD credentials
Veterans at USC, UTSA, SCSC			Veteran Center at USC, UTSA, SCSU		Veterans with MOS, DoD credentials
STEM students at USC, UTSA, SCSU			CS, CI, IT, Math, Engr. programs interested in a minor in cybers, IT, and topics relevant to DoN / DoD		STEM graduates with skills relevant to DoN / DoD
CELL and Internet2 COPs	**c.** Workshops (informal learning)	Workshops + self-paced learning	EPOC / ESnet, Internet2	Advanced communications, networks, warfare	IT professionals with skills on advanced technologies
Open to learners interested in intro., inter-mediate, and advanced IT	**d.** Self-paced learning (informal learning) for - National Guard - General Public	Self-paced; potential periodical meeting for general discussion	National Guard, NDG	Communications, cybersecurity, networks, virtualization	IT professionals, National Guard personnel at all levels, workforce with advanced skills, MOS, certificate credentials

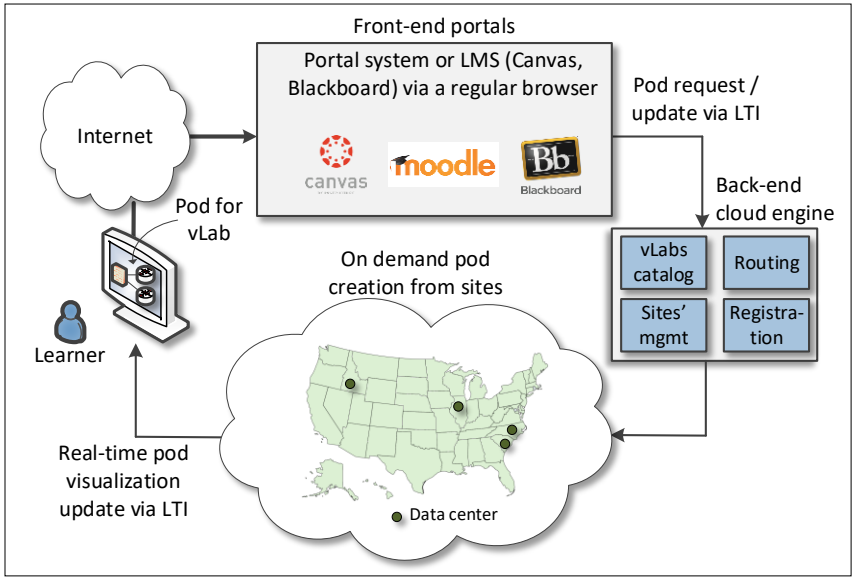
Preparing Cyber Warfare Professionals by Integration of Curriculum, Experiences, and Internships

- Objective 2: Develop a multi-state internship program, leveraging and strengthening the Naval Research Enterprise Internship Program (NREIP)
  - Common pre-internship seminars for USC, SCSU, and UTSA students (14-week long)
  - Internships to be conducted during the summer – 400 hours
  - Intel, Cisco, VMware, Palo Alto Networks will provide tools and platforms to prepare students for internships and full-time positions

Preparing Cyber Warfare Professionals by Integration of Curriculum, Experiences, and Internships

- Objective 3: Expand the Academic Cloud to support large-scale learning and research nationwide
  - The cloud system supports education and research
  - It was established by USC, Stanly Community College, and the Network Development Group (NDG) in 2019
  - It is currently used by colleges, universities, the National Guard, and multiple agencies

Academic Cloud



Cybertraining on P4 Programmable Devices using an Online Scalable Platform with Physical and Virtual Switches and Real Protocol Stacks

Support: National Science Foundation

Purpose: advanced IT - workforce development (PhD students, IT professionals)

2021 - 2025

Cybertraining on P4 Programmable Devices

- Funded by the National Science Foundation (NSF) ($500,000)
- The project is developing hardware and software apps using P4 processors
- Intel provides tools to program the P4 processors
- The Cyberinfrastructure Lab at USC has unique capabilities on this technology: http://ce.sc.edu/cyberinfra/
- USC training platform and material on P4 are now used across the country (ESnet, ASU, Northeastern, small businesses, campus IT professionals, etc.)
- A DoD SBIR proposal has been recently submitted, to develop cybersecurity applications using P4 processors

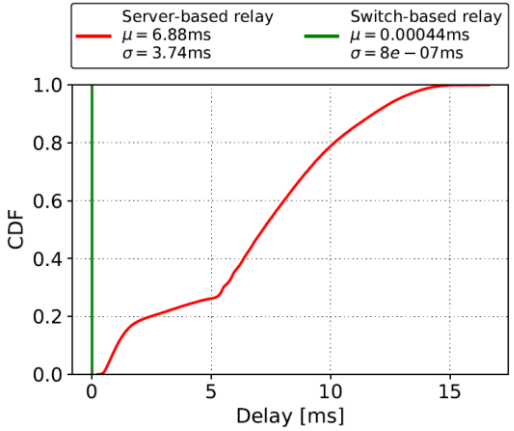
P4 network processor

Cybertraining on P4 Programmable Devices

- Objective: Increase and facilitate the adoption of P4 programmable devices nationwide
  - Network processors provider granular visibility of events (nanosecond resolution)
  - They can detect /process events much faster than general-purpose CPUs
  - Collaboration / agreement with Intel

Application example: voice processing[1]

	Network Processor	General-purpose CPU
Cost	$6,000	$ 10,000 - 25,000
Capacity	~35M connections/chip	~500 connections/core
Latency	440 nanosec	Tens-hundreds of msec



[1]E. Kfoury, J. Crichigno, E. Bou-Harb, V. Gurevich, "Offloading Media Traffic to Programmable Data Plane Switches," IEEE ICC, June 2020.

Cybertraining on P4 Programmable Devices

- Objective: Increase and facilitate the adoption of P4 programmable devices nationwide

INC: In-Network Classification of Botnet Propagation at Line Rate

Kurt Friday[1], Elie Kfoury[2], Elias Bou-Harb[1], and Jorge Crichigno[2]

[1] The Cyber Center for Security and Analytics
The University of Texas at San Antonio, USA
{kurt.friday,elias.bouharb}@utsa.edu
[2] Integrated Information Technology
The University of South Carolina, USA
{jcrichigno@cec, ekfoury@email}.sc.edu

Abstract. The ever-increasing botnet presence has enabled attackers to compromise millions of nodes and launch a plethora of Internet-scale coordinated attacks within a very short period of time. While the challenge of identifying and patching the vulnerabilities that these botnets exploit

IoT Threat Detection Testbed Using Generative Adversarial Networks

Farooq Shaikh[1], Elias Bou-Harb[2], Aldin Vehabovic[1], Jorge Crichigno[3], Aysegül Yayimli[4], Nasir Ghani[1]
[1]*Univ. of South Florida,* [2]*Univ. of Texas San Antonio,* [3]*Univ. of South Carolina,* [4]*Valparaiso University*

***Abstract*—The *Internet of Things* (IoT) paradigm provides persistent sensing and data collection capabilities and is becoming increasingly prevalent across many market sectors. How and function to malicious increased us bot network**

Although IoT-based solutions offer tremendous benefits in terms of productivity and efficiency, they also introduce a plethora of security challenges. Namely

P4DDPI: Securing P4-Programmable Data Plane Networks via DNS Deep Packet Inspection

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

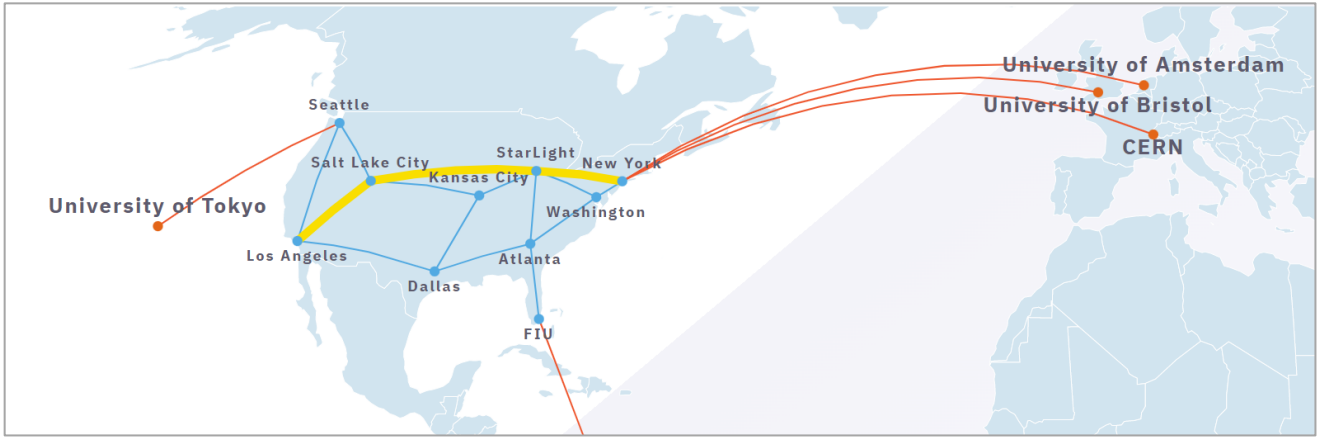
***Abstract*—One of the main roles of the Domain Name System (DNS) is to map domain names to IP addresses. Despite the importance of this function, DNS traffic often passes without being analyzed, thus making the DNS a center of attacks that keep evolving and growing. Software-based mitigation approaches and dedicated state-of-the-art firewalls can become a bottleneck and are subject to saturation attacks, especially in high-speed networks. The emerging P4-programmable data plane can implement a variety of network security mitigation approaches at high-speed rates without disrupting legitimate traffic.**

The security gap incurred by the DNS can be attributed to its ability in handling DNS records transparently, i.e., DNS should not attempt to interpret nor understand the records it is serving. While such transparency is essential for a fast and smooth deployment of new technologies without altering the infrastructure, it leaves the Internet prone to a wide variety of attacks [4].

Traditional enterprise networks use a number of components and approaches to protect against security threats. For exam-

Cybertraining on P4 Programmable Devices

- Objective: Increase and facilitate the adoption of P4 programmable devices nationwide
  - Training material is used by the FABRIC community (FABRIC is a national infrastructure, >$20M investment by NSF) (https://whatisfabric.net/):



FABRIC

Additional Slides

Building a Science DMZ for Data-intensive Research and Computation at the University of South Carolina
Support: National Science Foundation

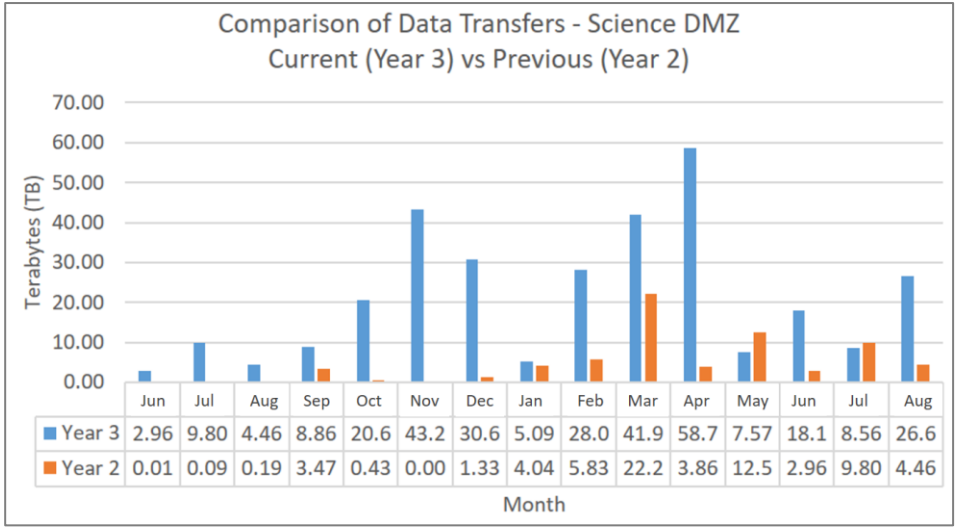
Purpose: deploy a high-speed network at USC, connected to Internet2

Institution: USC

2019 - 2022

Building a Science DMZ

- Funded by the National Science Foundation ($500,000)
- The project developed a 100Gbps high-speed network (Science DMZ) connected to Internet2
- The Science DMZ supports current research moving terabyte-scale data between USC and national labs (e.g., Argonne, Fermi, Oak Ridge, Savannah River, Los Alamos)
- In the last 15 months, the increase of data transfers was over 300% with respect to the previous 15-month period
- Peaks of up to 60TB per month



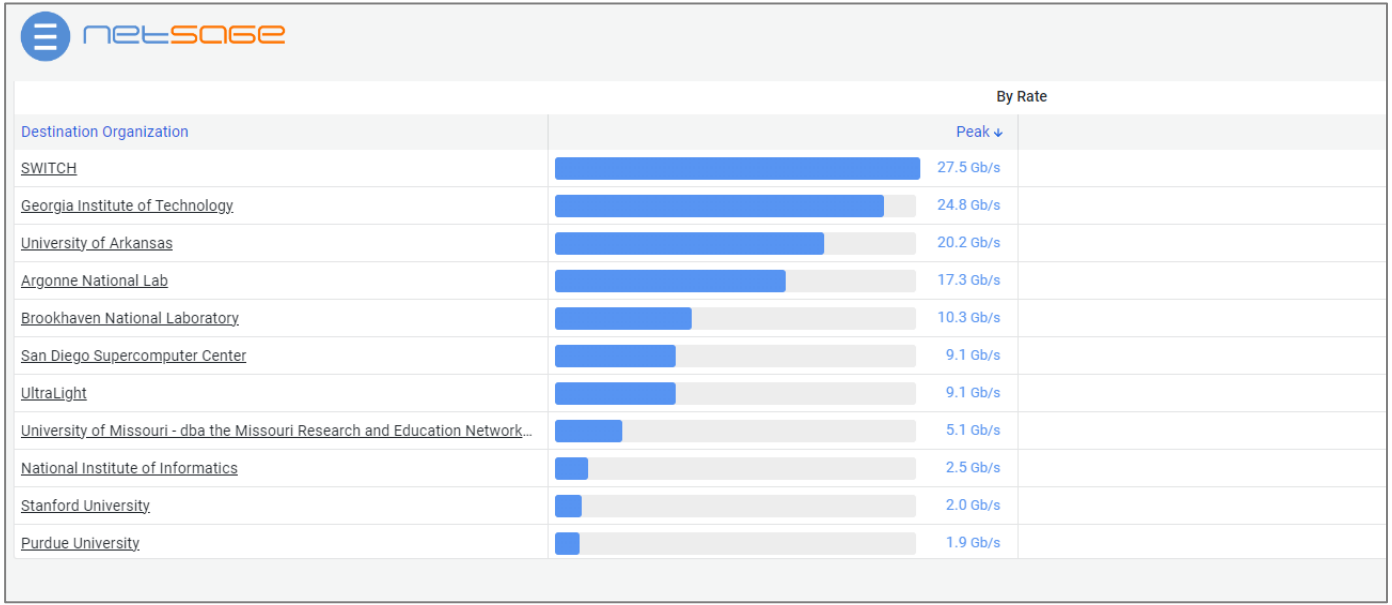
	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug
Year 3	2.96	9.80	4.46	8.86	20.6	43.2	30.6	5.09	28.0	41.9	58.7	7.57	18.1	8.56	26.6
Year 2	0.01	0.09	0.19	3.47	0.43	0.00	1.33	4.04	5.83	22.2	3.86	12.5	2.96	9.80	4.46

Year 3: 2021/2022

Year 2: 2021/2020

Building a Science DMZ

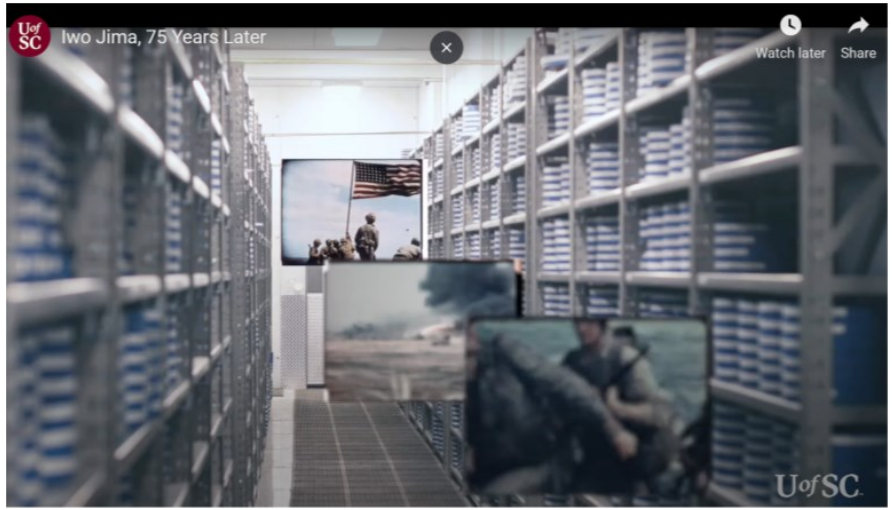
- Prior to this project, data transfers to/from USC were below 5Gbps
- High-speed data transfers enable new research on campus
- Multiple colleges and departments have benefited from the new infrastructure



Example of flow rates from USC to collaborators using the new network (2022)

Building a Science DMZ

- The infrastructure is also used by non-STEM units
- Example: the USC's Moving Image Research Collections (MIRC) library is digitizing films, in partnership with the U.S. Marine Corps History Division
- The process requires high-speed data transfers and high-capacity storage (Science DMZ)



Multi-state Community College, University and Industry Collaboration to Prepare Learners for 21st Century Information Technology Jobs
Support: National Science Foundation

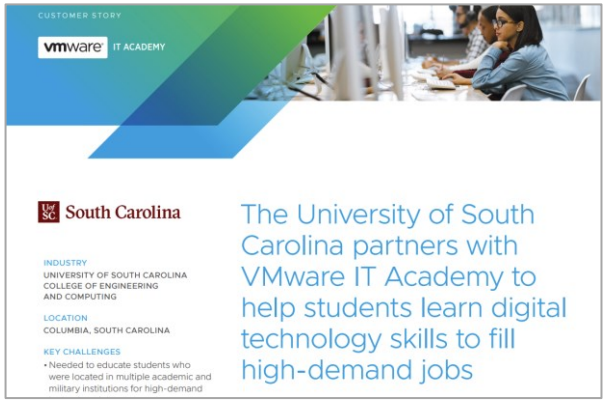
Purpose: Workforce Development at High School, Community College, and University Levels

Institution: USC
Collaborators: VMware, Palo Alto Networks, Cisco Systems, SRNL, Stanly Community College, SC Gov. HS

2019 - 2023

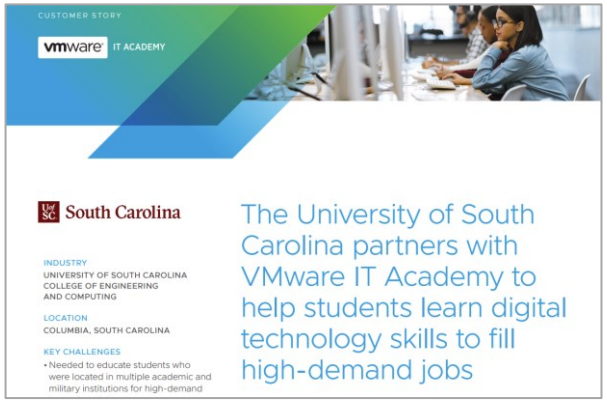
Multi-state Community College, University and Industry Collaboration

- NSF-funded project ($600,000 / $300,000 for USC)
- The project developed a multi-state distributed cloud to support teaching, research
- The distributed cloud pools resources from SC and NC to serve institutions seamlessly
- A 2+2+2 program (HS + College + University) was initiated
- Stackable credentials are now available to students (A+, Cisco, Palo Alto, VMware)
- Weeklong summer workshops are offered to prepare instructors on new technologies



Multi-state Community College, University and Industry Collaboration

- Impact
  - Pedagogical material is now available for highly recognized certificates (networks, cyber, virtualization)
  - The project has trained over 100 instructors who are now teaching the material at their institutions
  - The material has helped over 300 soldiers from the U.S. Army Cyber Signal School, 40+ ROTC cadets, over 1,000 students
  - The material is also used in undergraduate and graduate courses



Summary – Collaborators

Summary

Collaborators	Purpose	Audience
Intel	Advanced training; technology used for DoD (Pronto project https://prontoproject.org/), NSF FABRIC project (https://whatisfabric.net/), PhD research	PhD level / advanced IT professional level
Cisco, VMware, Palo Alto Networks	Workforce development (industry certificates in cyber / networks). Certificates can be completed after one or more 8/16-week course	Undergraduates, veterans, STEM students, IT professionals
Cisco, VMware, Palo Alto Networks	USC trains military personnel who may want to obtain a DoD recognized credential – cybersecurity and networks	National Guard, ROTC, Fort Gordon
LBNL, ESnet, Internet2	Advanced training in IT topics – networks and cybersecurity	IT professionals working on high-performance environments
Amazon	This is a new partnership. USC has access to training material on cloud computing (AWS). This trainings are in high demand	IT professionals, students at all level
SRNL, private companies, NIWC	Internships	Undergraduate students
Network Development Group	NDG is the leading organization in virtual training platforms. USC and NDG collaborate in multiple projects, such as deploying the Academic Cloud	Learners at all levels
Opex Systems	Business partner – DoD proposal has been recently submitted with this organization, to develop advanced applications for DoD	DoD

Impact of the Cyberinfrastructure Lab (2018 – 2022)

Audience	Purpose	# Learners
Military personnel	U.S. Army Cyber Center of Excellence (Fort Gordon). Training on cyber and IT (2019-2022) (approximately 150 per year)	600
ROTC Cadets and Veterans	USC ROTC – USC Students. Training and research on cyber and IT for the military (approximately 20 per year) (2020-2022) (this number only included funded students)	60
National Guard	National Guard – Training on cyber and IT (approximately 75 per year) (2021-2022)	150
Undergraduate Students at USC	Undergraduate students who have used the Academic Cloud platform for course work (approximately 500 per year) (2018-2022)	2,500
IT Professionals Nationally	Advanced training on IT. The audience includes high-skilled IT professionals working on national laboratories, campus networks, research and education networks (approx. 800 per year) (2019-2022)	3,200
Learners*	Learners who access the Academic Cloud platform and pedagogical material (national impact): high school students, community college students, four-year undergraduate students, graduate students, IT professionals (approximately 100,000 per year) (2020-2022)	300,000

* Platform deployed with the Network Development Group (NDG), Stanly Community College (SCC), and Idaho National Laboratory (INL). USC is the leading organization of the NSF-supported project

Impact of Additional Support

Organizations	Outcomes
Middle and High Schools	(1) Enhance middle and high school instruction by providing them access to the Academic Cloud (**virtual laboratory platform for hands-on activities**) and pedagogical material for IT, cybersecurity (2) Pipeline: align pedagogical material for high-school students to 100- and 200-level college courses / **dual credit** (3) Prepare middle-school and high-school students for state and national **cyber competitions** (4) Prepare students with **entry-level IT credentials for the workforce**
Technology Workers	(1) Disseminate IT knowledge developed by USC by creating effective **advanced hands-on training material** (2) Create partnerships to **reskill** workers: **AWS, Cisco, VMware, Palo Alto Networks, Intel, Apple** (3) Coordinate with industry to reskill workers using **professional tools and platforms** be deployed in USC's Academic Cloud (4) Strengthen **partnerships** with Lawrence Berkeley National Lab / ESnet, Internet2, Research and Education Networks (5) Prepare **IT professionals with new skills** on state-of-the-art technology
National Guard, U.S. Army Cyber Center of Excellence (CCOE)	(1) Enhance the **training and education of soldiers** by providing them access to the Academic Cloud (2) Train soldiers on **Military Occupation Specialties (MOS)** (3) Improve **CCOE, Cyber & Information Advantage Battalion (National Guard)** curriculum on MOS (4) Enable soldiers to attain **MOS and advanced degrees**
SBIR - DoD	(1) Produce **prototypes for cybersecurity, network apps** that are easy to operate by soldiers (2) Develop apps exploiting P4 network processors running on **Pronto** (DoD's large-scale infrastructure, https://prontoproject.org/) (3) Promote and support **startups** interested in developing P4 network processor applications

Impact of Additional Support

Organizations	Outcomes
Technical Colleges	(1) Enhance instruction at technical colleges by providing them **access to the Academic Cloud** (virtual laboratory platform for hands-on activities) and pedagogical material for IT, cybersecurity (2) Align pedagogical material to facilitate **transition from 2-year to 4-year programs** (3) Enable students to attain industry **stackable credentials** while completing their degrees
Universities	(1) Enhance instruction at universities by providing them **access to the Academic Cloud** (2) Enable students to conduct **advanced research** on high-speed networks, cybersecurity, and other IT areas **(3) Strengthen partnership with federal agencies** to continue accessing facilities (e.g., FABRIC national infrastructure (https://whatisfabric.net/) (4) Enable students to attain **degrees** with high-market demand (5) Enable student to attain **stackable credentials and DoD's approved certificates** (relevant to ROC, veteran students, students applying to federal agencies and national laboratories)
SC Industry, state workers	**(1) Upskill and reskill** state workers to reduce the widening supply-demand needs of cybersecurity / IT professionals (2) Extend the **agreements** between **USC and industry partners** (Intel, Cisco System, Palo Alto Networks, VMware) to permit state workers to conduct **self-paced training** towards **stackable credentials**, using the Academic Cloud **(3) Promote innovation** and **build infrastructure** capacity to attract IT talent **(4) Reduce the skills gap** in IT and provide businesses with IT talent

Funding Cyberinfrastructure Lab (1 FT Faculty Member)

- Total amount for the period Jan. 1, 2018 – Dec. 22, 2022 (USC share only: $3.4M; total: > $4M)

Support	Purpose	Amount
ONR	(1) Research on applications of P4 network processors for the military (command and control); (2) Training military personal: Veterans, National Guard, ROTC, STEM undergraduates	$600,000
DoD	(1) Accelerating expertise in critical cyber operational skills for future military and civilian leaders	$250,000
NSF	(1) Research on applications of P4 network processors for high-speed networks; (2) Train undergraduate and graduate students, IT professionals	$500,000
NDG	(1) Develop training material for IT and cybersecurity	$20,000
ONR	(1) Develop a minor in cybersecurity to enhance the preparation of ROTC cadets on cyber	$250,000
NSF	(1) Build a high-speed network at USC to move big science data across to collaborators' institutions	$500,000
NSF	(1) Build a virtual platform for training, research, and education	$300,000
NSF	(1) Research on IoT cybersecurity	$500,000
NSF	(1) Research on high-speed networks, protocol development; (2) Training material on high-speed networks	$500,000
NSF	(1) Research on cybersecurity; (2) Training undergraduate and graduate students on cybersecurity	$420,000
		$3,840,000

Funding Cyberinfrastructure Lab (1 FT Faculty Member)

- Expectation for the next 3-4 years is to bring > $3,000,000, by applying to larger programs
- Additional FT faculty with expertise on practical cyberinfrastructure (high-speed networks, network security) may help increase the above amount