Preparing Cyber Warfare Professionals by Integration of Curriculum, Experiences, and Internships
Project website: https://research.cec.sc.edu/cyberinfra/projects/ONR

Program Officer: Dr. Michael Simpson
Award # N00014-23-1-2245

Jorge Crichigno
University of South Carolina (USC)

April 4, 2024 - McNair Center
Columbia – SC

Motivation

- A key element for the American military to help maintain superiority is the engineering support for information warfare

- Challenges

  - ➤ Shortage of professionals with cybersecurity skills

  - ➤ Difficult to compete for the small number of cybersecurity professionals

  - ➤ Lack of exposure to potential careers in the Navy and federal agencies

  - ➤ Security clearance process may be time consuming

IT capability, Naval Information Warfare Systems Command[1]

---

1. Naval Information Warfare Systems Command, Generic View. February 2022. URL: https://tinyurl.com/4pnpy44n

Objectives

- This project is helping address the shortage of skilled cyber-professionals opting for careers with the DoD

- The project has three objectives:

  1. **Advance formal and informal cyber communities** and connect relevant organizations

  2. **Develop a multi-state internship program**, leveraging and strengthening the Naval Research Enterprise Internship Program (NREIP)

  3. **Expand the Academic Cloud** to support large-scale learning and research nationwide

Objective 1: Advance formal and informal cyber communities

Audience	Activity	Learning Setting	Partners	Subject	Outcome
ROTC cadets	Six 16-week academic courses at USC, SCSU, UTSA, LSU (formal learning); 12-week C4ISR research experience (formal learning)	Courses including virtual labs on topics relevant to the DoN and DoD	ROTC programs	Cybersecurity, warfare, networks, communications, virtualization	ROTC graduates with MOS credentials
Veterans			Veteran Centers		Veterans with MOS credentials
STEM students in general			STEM program students interested in a minor in cyber		STEM graduates with skills relevant to DoN / DoD
Communities of Practice (COPs)	Workshops (informal learning)	Workshops + self-paced learning	ESnet / LBNL, Internet2, IT	Advanced communications, networks, warfare	IT professionals with skills on advanced technologies
Open to military-connected communities	Self-paced learning (informal learning)	Self-paced; periodical meetings for general discussion	National Guard, Naval Information Warfare Center (NIWC) Atlantic	Communications, cybersecurity, networks, virtualization	IT professionals, military personnel with advanced skills, MOS credentials

MOS: Military Occupational Specialty

Academic Courses

Objective 1: Advance formal and informal cyber communities

- Formal academic courses at University of South Carolina (USC), University of Texas San Antonio (UTSA), and South Carolina State University (SCSU)

  Spring 2023:
  - IT 493 IT Security (54 students, USC)
  - IT 742 Enterprise Network Management (7 students, USC)
  - IS 6953 Research Seminar (12 students, UTSA)
  - IS 3033 Operating Systems (40 students, UTSA)
  - CSM 188 Fundamentals of Cybersecurity (15 students, SCSU)

  Summer 2023:
  - IT 493 IT Security (17 students, USC)

  Fall 2023:
  - IT 445 Advanced Networking (65 students, USC)
  - IT 493 IT Security (26 students, USC)
  - CSM 188 – Fundamentals of Cybersecurity (17 students, SCSU)
  - CSC 2362 - Intro to Cybersecurity and Defense (70 students, LSU)
  - IS 3423 - Network Security (54 Students, UTSA)

Objective 1: Advance formal and informal cyber communities

- Twelve-week C4ISR[1] research experience (formal learning)
  - Between 50-75 undergraduates per year conducting research on cybersecurity at the University of South Carolina, South Carolina State University, UT San Antonio, LSU

1. C4ISR: Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance

Objective 1: Advance formal and informal cyber communities

- Twelve-week C4ISR research experience (formal learning)
  - ➢ Between 50-75 undergraduates per year conducting research on cybersecurity at the University of South Carolina, South Carolina State University, UT San Antonio, LSU


1. C4ISR: Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance

Objective 1: Advance formal and informal cyber communities

- Twelve-week C4ISR research experience (formal learning)
  - ➢ Between 50-75 undergraduates per year conducting research on cybersecurity at the University of South Carolina, South Carolina State University, UT San Antonio, LSU

Team	Name	Email	Project
1	Nolan Pelino	npelino@email.sc.edu	Implementing Connection Tracking Service using a P4 Programmable Switch Switch (PDF)
1	Andrew Smith	ats29@email.sc.edu	Implementing Connection Tracking Service using a P4 Programmable Switch Switch (PDF)
2	Yousef Afshar	yafshar@email.sc.edu	Protecting a Web Application against Brute-force Attacks (PDF)
2	Chasey Kilcrease	chaseyk@email.sc.edu	Protecting a Web Application against Brute-force Attacks (PDF)
3	Jacob Sherer	jsherer@email.sc.edu	DDoS Defense using NGFW (PDF)
3	Matthew Kleeman	mkleeman@email.sc.edu	DDoS Defense using NGFW (PDF)
4	Denzel Martin	denzelm@email.sc.edu	Reconnaissance Protection (PDF)
4	Favour Agho	fagho@email.sc.edu	Reconnaissance Protection (PDF)

Objective 1: Advance formal and informal cyber communities

- Twelve-week C4ISR research experience (formal learning)
  - ➢ Between 50-75 undergraduates per year conducting research on cybersecurity at the University of South Carolina, South Carolina State University, UT San Antonio, LSU
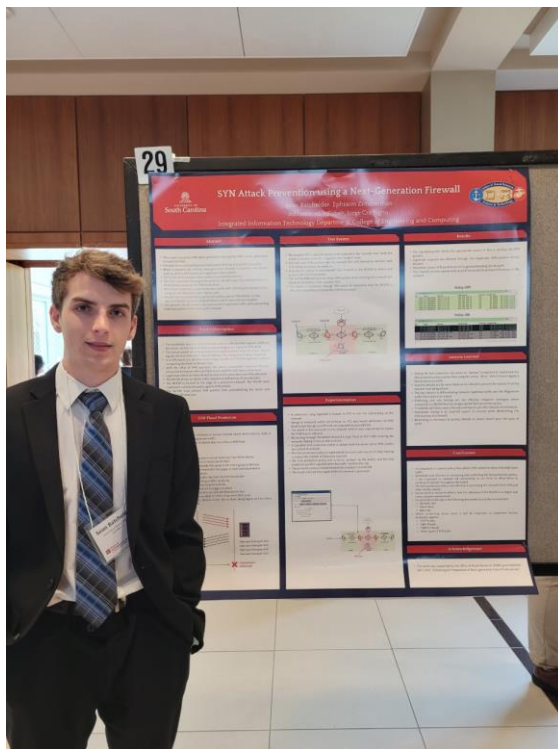
Summer Research Expo – University of South Carolina

Objective 1: Advance formal and informal cyber communities

- Workshops and tutorials (informal learning)

	Workshop / Tutorial	Date / Place	Website and Materials	Att.
1	Workshop on IPv6	Feb. 15-16, 2024, NYC, NY (8am-5pm)	https://tinyurl.com/mt45fasn	35
2	Workshop on Cybersecurity with P4	Feb. 9, 2024, Tampa, FL (8am - 4pm)	https://tinyurl.com/ms229396	30
3	Cybersecurity (Security+) and P4 Programmable Switches Workshop	Jan 4-5, 2024, San Jose, CA (8am-5pm)	https://tinyurl.com/yazac6n6	290
4	Internet2 Technology Exchange Conference - Writing Fine-grained Measurements App with P4 Programmable Switches	Sep. 18, 2023, Minneapolis, MN (8am-12pm)	https://tinyurl.com/uw4t3nca	20
5	Internet2 Technology Exchange Conference - Hands-on Workshop on Science DMZs and Networking for All. Co-organizer: Minority Serving Cyberinfrastructure Consortium	Sep. 18, 2023, Minneapolis, MN (1-5pm)	https://tinyurl.com/3dje732n	20
6	Internet2 Technology Exchange Conference - Security Applications with P4 Programmable Switches	Sep. 18, 2023, Minneapolis, MN (1-5pm)	https://tinyurl.com/58p6yrf6	20
7	Online Workshop on Cybersecurity	Jun. 17 –21, 2023, Online	https://tinyurl.com/yyrwjucj	32
8	FABRIC Community Workshop - Workshop on Security Applications with P4	Apr. 24, 2023, Austin, TX (1-3pm)	http://tinyurl.com/2p8tcw8n	70
			TOTAL:	**517**

Objective 1: Advance formal and informal cyber communities

- Workshops (informal learning)

Workshop on Security Applications with P4, FABRIC Community Workshop, Austin, TX, April 24, 2023.

Workshop on Fine-grained Network Measurements with P4, Internet2 Technology Exchange Conference, Minneapolis, MN, Sep. 18, 2023.

Objective 1: Advance formal and informal cyber communities

- Workshops (informal learning)

Workshop on IPv6 and Cybersecurity, New York State Research and Education Network, NYC, Feb. 15-16, 2024.

Workshop on Cybersecurity (Security+) and P4 Programmable Switches, San Jose, CA, Jan. 4-5, 2024

Self-paced Learning

Objective 1: Advance formal and informal cyber communities

- Training at the U.S. National Guard, National Guard Professional Education Center (PEC), Cyber and Information Advantage Battalion (CIAB)
  - 1. VMWare Virtualization Fundamentals (vSphere ICM 7), Apr. – Jun. 2023: 13 learners
  - 2. VMWare Virtualization Fundamentals (vSphere ICM 7), Jun. – Aug. 2023: 9 learners
  - 3. VMWare Virtualization Fundamentals (vSphere ICM 7), Sep. – Nov. 2023: 16 learners
  - 4. VMWare Virtualization Fundamentals (vSphere ICM 7), Oct. – Dec. 2023. : 2 learners
  - 5. VMware Virtualization Fundamentals (vSphere ICM 7), Feb. – Apr. 2024. : 8 learners

TOTAL: 48 learners

- Veterans Training in Cybersecurity (3-month course)
  - Course on Next-generation Firewalls

TOTAL: 25 Veterans

Objective 2

Objective 2: Develop a multi-state internship program

- Two components
  - ➤ **Pre-internship seminars:** speakers from companies and agencies meet weekly with students and connect to them prior to the summer internships
  - ➤ **Internship:** students work 400 hours (paid internship) on cybersecurity or related fields. Agencies include Savannah River National Laboratory (SRNL), Naval Information Warfare Center Atlantic (NIWC), SOCs, etc.

Pre-internship Seminars	Internships
Spring and Fall semesters (Monday-Wednesday-Friday)	Summer semester (400 hours)

Objective 2: Develop a multi-state internship program

- Features
  - ➢ Students acquire soft skills, teamwork, time management, and communication skills while gaining additional employability skills
  - ➢ For agencies requiring clearance security, starting the process prior to graduation will save time and open opportunities for students
  - ➢ Students may even obtain interim secrecy clearance while completing the internships

Pre-internship Seminars	Internships
Spring and Fall semesters (Monday-Wednesday-Friday)	Summer semester (400 hours)

Pre-internship Seminar

Objective 2: Develop a multi-state internship program

Pre-Internship Seminar - Spring 2024

Pre-Internship Seminar - Spring 2024

Organizers
University of South Carolina (USC)
Lousiana State University (LSU)
South Carolina State University (SCSU)

Venue
Address: 550 Assembly St., Columbia, SC 29201
Building: Innovation Center
Room: 1400
University of South Carolina (USC)

Agenda

Date	Company	Presenter	Presentation	Job Opportunity
Jan-12	Red Hat	Mike Savage	[Video]	
Jan-17	FBI	Carl Cuneo	[Video]	
Jan-19	Pentagon		[Video]	
Jan-22	CEC Career Center		[Video]	

https://research.cec.sc.edu/cyberinfra/ONR/internships

Internship

Objective 2: Develop a multi-state internship program

- By the end of the Pre-internship Seminars (Fall '23 and Spring '24), the goal is to secure 100+ paid internships
- Students from USC, SCSU, and LSU will complete the internships during the Summer '24
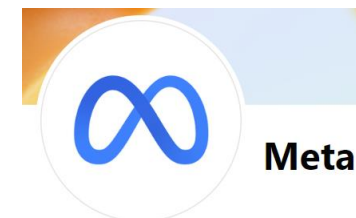
Internship

Objective 2: Develop a multi-state internship program

- By the end of the Pre-internship Seminars (Fall '23 and Spring '24), the goal is to secure 100+ paid internships
- Students from USC, SCSU, and LSU will complete the internships during the Summer '24

Visit to the Defense Information Systems Agency (DISA)
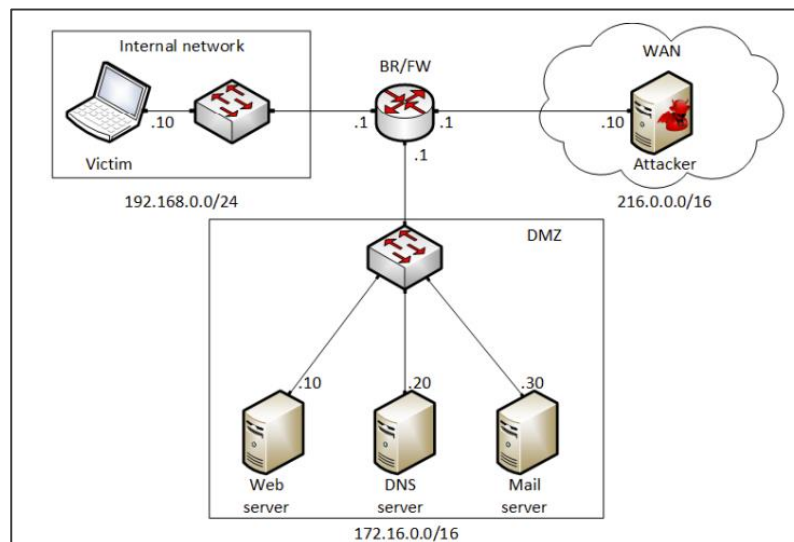August 2nd 2023 - Baltimore, MD

Objective 3: Expand the Academic Cloud

- The Academic Cloud is a purpose-built distributed cloud system for education and research

- Learners only require access to the Internet and to login into the system using a regular browser

- It serves all the organizations involved in this project

Virtual Lab Libraries
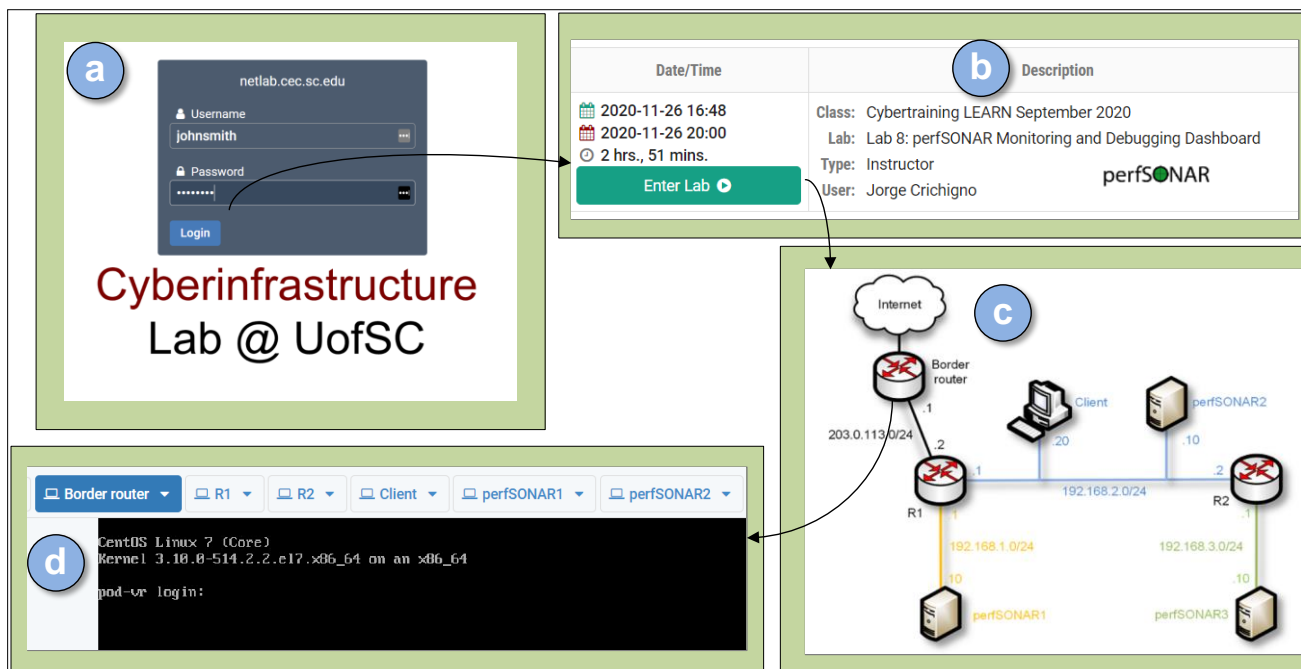
Objective 3: Expand the Academic Cloud

- Virtual labs
  - Systematic lab libraries that cover fundamentals of cybersecurity, networks, virtualization, C4ISR[1], and other topics
  - It also prepares learners for DoD baseline certificate
  - Guided virtual lab experiments + electronic booklet + exercises
- The Academic Cloud is also used by other DARPA- and NSF-funded projects

1. C4ISR: Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance

Objective 3: Expand the Academic Cloud

- Demo – High Resolution Measurements on the Internet

https://youtu.be/cWaWxsqVAgc

Academic Cloud Usage

Objective 3: Expand the Academic Cloud

- The Academic Cloud supports Objectives 1 and 2
- It serves multiple communities (formal and informal learning)

Community usage at USC alone –>
Feb. 1, 2023 – Jan. 31, 2024

📈 Community Usage

Labs Attended	Hours Attended
8550	30899.63
8550	30899.63
8550	30899.63

- The project increases engagement in areas related to C4ISR
  - Communications and networks
  - Cybersecurity operations and warfare
  - Information technology

- The project is training military-connected communities and professionals
  - Veterans
  - ROTC students
  - Military personnel from the U.S. National Guard

- The project is developing technology that is attractive to DoD
  - The project team uses the P4 technology for rapid intrusion detection on a DARPA project (2024-2025)
  - Undergraduate students actively participate in developing commercial and military applications

- Internships will provide learners the opportunity to apply skills on the job

- Internships will focus on positions requiring skills on C4ISR

- Some internships will be conducted at organizations that provide services to the Navy, and at national labs. E.g.,
  - ➤ Naval Information Warfare Center Atlantic
  - ➤ Savannah River National Laboratory

- The expanded Academic Cloud is currently used by colleges, agencies, NIWC, National Laboratories, communities of practice

  - Naval Information Warfare Center Atlantic

  - ESnet

  - National Guard Professional Education Center (PEC), Cyber and Information Advantage Battalion (CIAB)

  - Universities

- New technology will be tested on the Academic Cloud, prior to the deployment on Pronto

- Pronto is a DoD's funded testbed: https://prontoproject.org/

Education sector

Cyber

Private sector

Naval partners, National labs

Description:

This project is helping address the shortage of skilled cyber-professionals opting for careers with the DoD

The project has three objectives:

1. Advance formal and informal cyber communities and connect relevant organizations

2. Develop a multi-state internship program, leveraging and strengthening the Naval Research Enterprise Internship Program (NREIP)

3. Expand the Academic Cloud to support large-scale learning and research nationwide

Naval Relevance:

The project

- Increases engagement in areas related to C4ISR

- Trains military-connected communities and professionals in general on communications and networks, cybersecurity operations and warfare, IT

- Partners with national laboratories and the Naval Information Warfare Center (NIWC) to develop new techniques for detecting cyber attacks

- Creates a pipeline of cyber-professionals from college to Navy and military communities

- Supports communities of practice related to the military by providing a training platform and material relevant to cybersecurity

Major Accomplishments:

- Virtual lab libraries have been deployed in the Academic Cloud system, which supports several formal and informal communities

- Multiple courses from four universities have incorporated material on C4ISR (formal community)

- Undergraduate students conduct research on C4ISR

- Learners nationwide are attending tutorials on cybersecurity covering the material developed in this project.

- Military personnel are trained using the Academic Cloud. They include the U.S. National Guard, Cyber and Information Advantage Battalion (CIAB)

- Veterans are trained on next-generation firewalls technology