TRAINING AND EDUCATIONAL INITIATIVES

Jorge Crichigno
Department of Integrated Information Technology
University of South Carolina

2019 SC Cyber Security Conference
Cooperative Conference Center
Columbia, SC
October 10, 2019

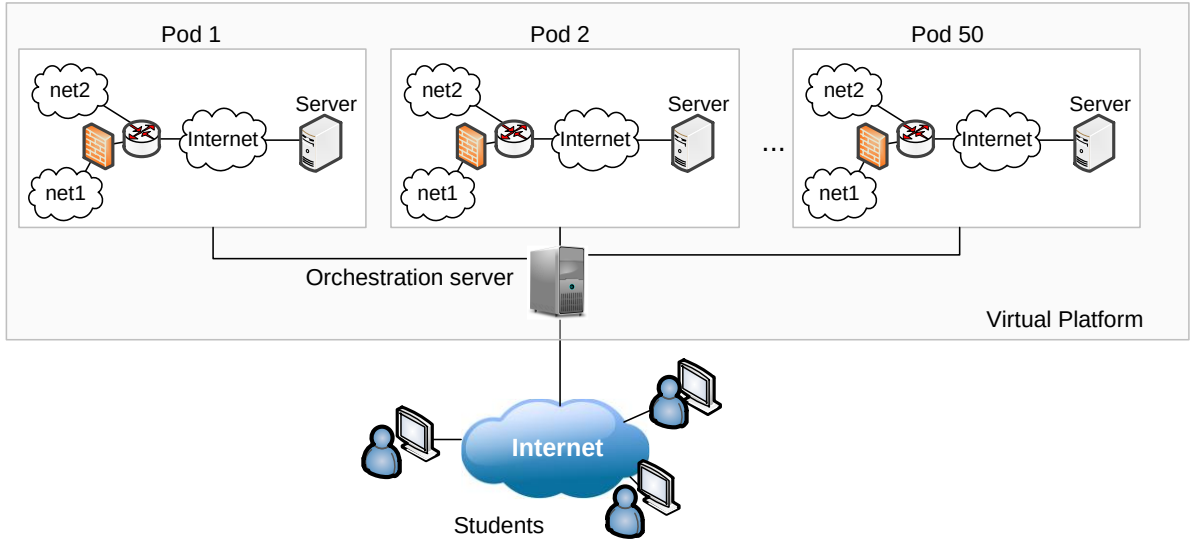
Support – National Science Foundation

1. “Building a Cybersecurity Pipeline through Experiential Virtual Labs and Workforce Alliances”
2. “Devising Data-driven Methodologies by Employing Large-scale Empirical Data to Fingerprint, Attribute, Remediate and Analyze Internet-scale IoT Maliciousness”
3. “Cyberinfrastructure Expertise on High-throughput Networks for Big Science Data Transfers”
4. “Building a Science DMZ for Data-intensive Research and Computation at the University of South Carolina”
5. “Multi-state Community College, University and Industry Collaboration to Prepare Learners for 21st Century Information Technology Jobs”

Virtual Laboratories

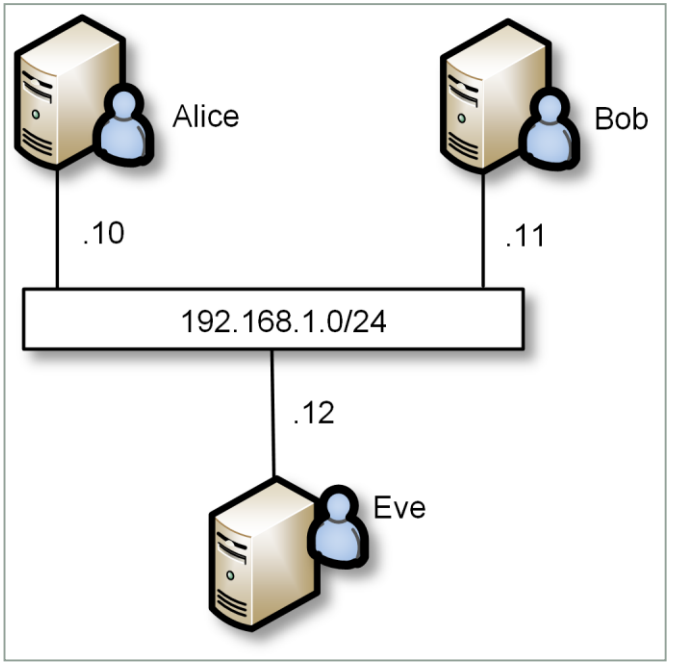
- Virtual platform based on virtual machines (VMs)
- Pods launched on demand on an server hosted in IIT
- Access to the virtual platform via web interface
- Development of custom pods
- Pod elements (computer, firewall, router, equipment) are VMs rather than physical devices

Partnership w/ NDG



Pod Examples – Introduction to Cryptography

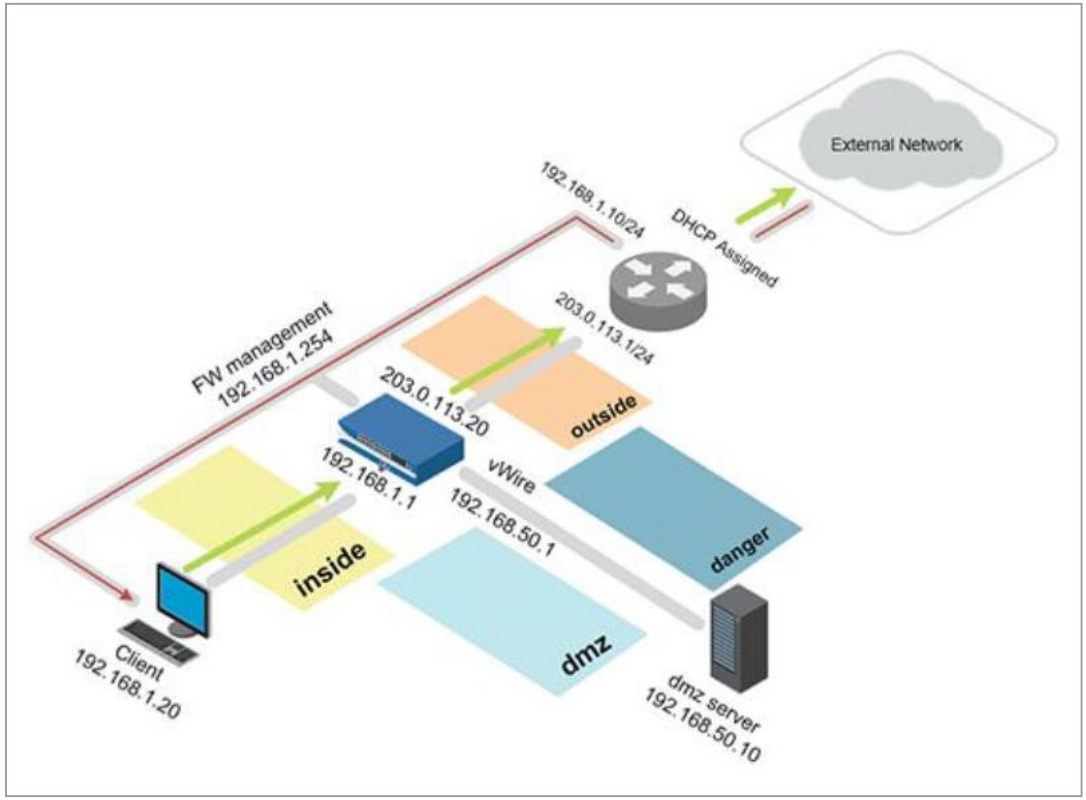
- Symmetric-key encryption
- Generation of public keys
- Public-key encryption
- Certificate authorities
- Digital signatures
- Digital envelopes
- Web of trusts
- Encryption protocols



LAN environment

Pod Examples – Next-generation Firewalls

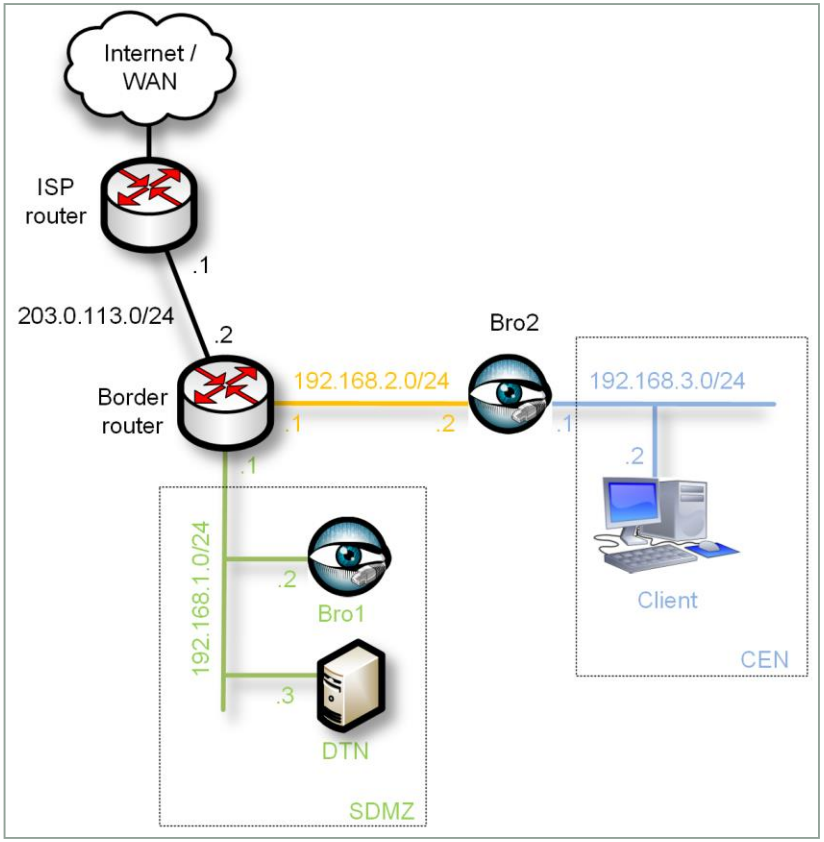
- Firewalls
- Malware analysis
- Application identification
- User identification
- URL filtering
- Virtual Private Networks
- Monitoring and reporting
- Modern techniques for malware identification
- Palo Alto Firewalls provided VMs at no cost



Enterprise network

Pod Examples – Bro Intrusion Detection

- High-performance tools
- Big data transfers
- Access-control lists
- Traffic routing for high speeds
- Intrusion detection systems
- Passive network monitoring



Enterprise network

Workshops

- Professional development workshops are organized periodically
- Activities include presentations and hands-on training
- July 22 – 23 attendance was 70
- National speakers, NSF, SRNL, Berkeley National Lab
- Other states are now replicating these training opportunities

Libraries

	Network Tools and Protocols
1	Introduction to Mininet
2	Introduction to Iperf3
3	Emulating WAN w/ NETEM I: Latency, Jitter
4	Emulating WAN w/ NETEM II: Loss, Duplication, Reord.
5	Setting WAN Bandwidth with Token Bucket Filter (TBF)
6	Traditional TCP Congestion Control (HTCP, Cubic, Reno)
7	Rate-based TCP Congestion Control (BBR)
8	Bandwidth-delay Product and TCP Buffer Size
9	Enhancing TCP Throughput with Parallel Streams
10	Measuring TCP Fairness
11	Router's Buffer Size
12	TCP Rate Control with Pacing
13	Impact of MSS on Throughput
14	Router's Bufferbloat

⋮

More labs being developed

	perfSONAR
1	Configuring Admin Info Using perfSONAR Toolkit GUI
2	PerfSONAR Metrics and Tools
3	Configuring Regular Tests Using perfSONAR GUI
4	Configuring Regular Tests Using pScheduler CLI Part I
5	Configuring Regular Tests Using pScheduler CLI Part II
6	Bandwidth-delay Product and TCP Buffer Size
7	Configuring Regular Tests Using a pSConfig Template
8	perfSONAR Monitoring and Debugging Dashboard
9	pSConfig Web Administrator
10	Configuring pScheduler Limits

	Zeek / Bro
1	Introduction to the Capabilities of Zeek
2	An Overview of Zeek Logs
3	Parsing, Reading and Organizing Zeek Files
4	Generating, Capturing and Analyzing Scanner Traffic
5	Generation, Capturing and Analyzing DoS and DDoS
6	Introduction to Zeek Scripting
7	Advanced Zeek Scripting for Anomaly Event Detection
8	Preprocessing of Zeek Output Logs for Machine Learning
9	Machine Learning Classifiers for Anomaly Classification
10	Profiling and Performance Metrics of Zeek

To access the platform and additional information:

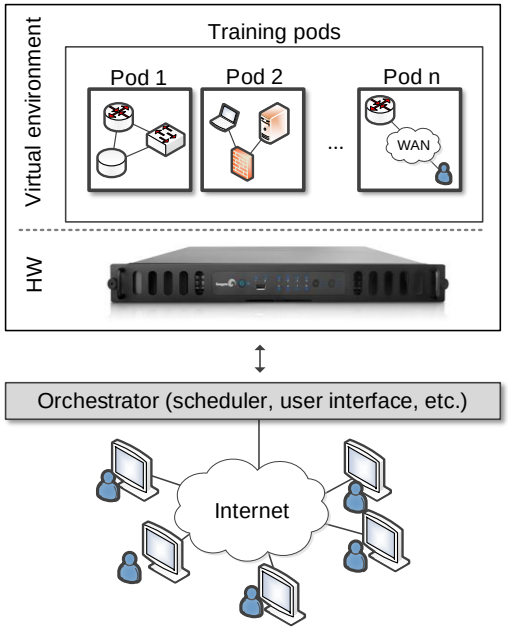
http://ce.sc.edu/cyberinfra/cybertraining.html

Alignment with Industry Certificates

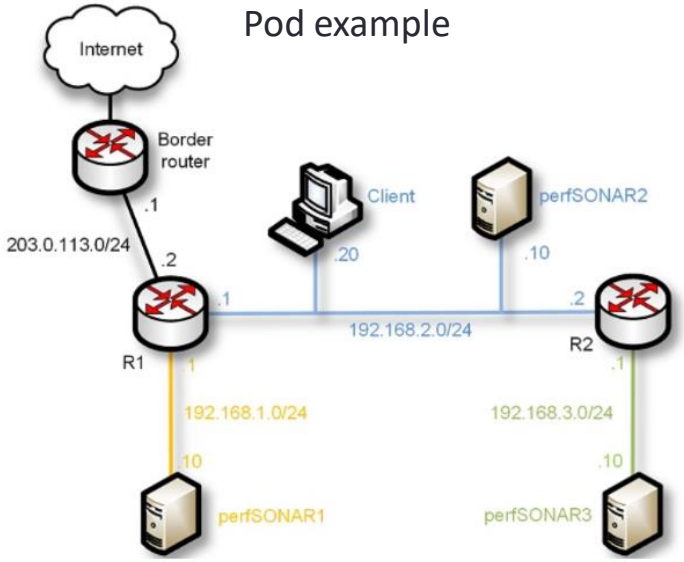
- Professional development aligned with industry certificates
  - Cisco Cyberoperations (cyber-analyst)
  - Cisco CCNA Routing and Switching
  - Palo Alto Networks Next Generation Firewalls
  - VMware Datacenter Virtualization

Platform

Training platform



Pod example



~8-month usage

Community Usage

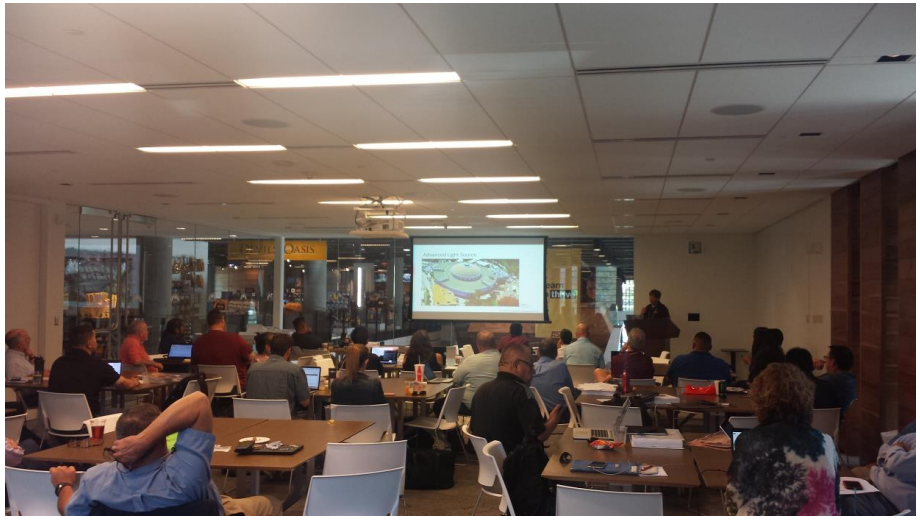
Search

ID	Name	Reservations Made	Labs Attended	Hours Reserved	Hours Attended
1	default	3880	3637	37419.94	10241.12
	Page Total:	3880	3637	37419.94	10241.12
	Table Total:	3880	3637	37419.94	10241.12

Showing **1 to 1** of **1** items

Workshops

- 200+ IT professionals from more than 30 states
- 10,000+ hours of training
- 30+ IT internship opportunities for students



Internships / Workforce

- 50+ internship opportunities for students in IT / cybersecurity / networks (2018/2019)
- Private and public sectors, national laboratories

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

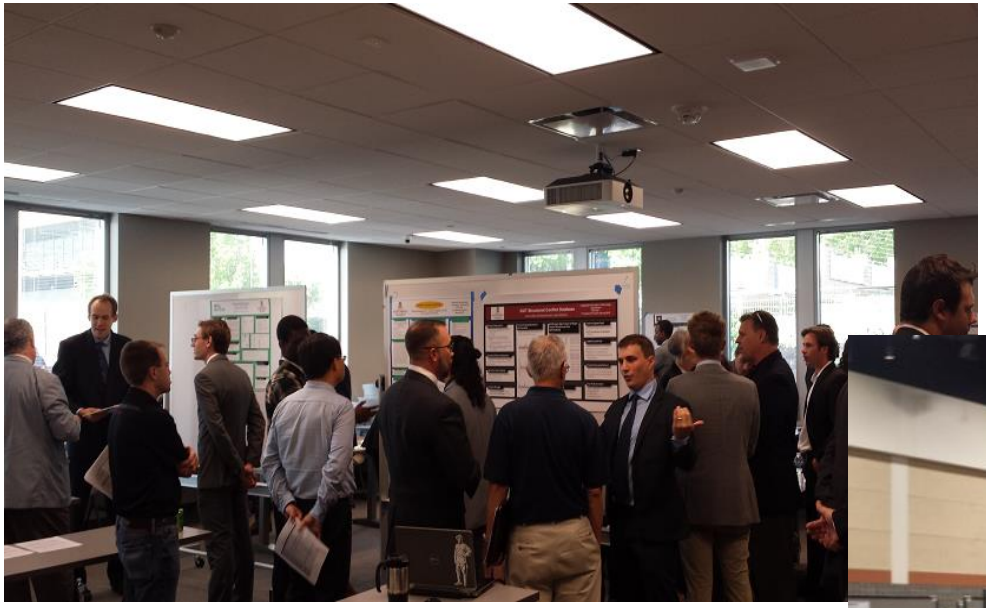
Submit to job | Send to friend | Save to cart | View similar jobs

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-value, cost-e Department of Energy's (DOE) Savannah River Site (SRS), the laboratory develops and deploys innovative technologies to address some Intern will participate in the development of a virtual network which simulates known environments to research vulnerabilities of Industrial C through scanning and patching industrial controllers and generating documentation to ensure each system meets SRS cyber security requi 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 related degree 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

Industry-sponsored Projects

- ~70 students, 2018/2019
- 20 industry-sponsored projects



Access to Training ROTC

- Participation and dissemination at USC's Reserve Officer Training Corps (ROTC)
- Professional development aligned with industry certificates
  - Cisco Cyberoperations (cyber-analyst)
  - Cisco CCNA Routing and Switching
  - Palo Alto Networks Next Generation Firewalls
  - VMware Datacenter Virtualization

Contact Information

Jorge Crichigno

jcrichigno@cec.sc.edu

803-576-6858

Cyber-training Information

http://ce.sc.edu/cyberinfra/cybertraining.html