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
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
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
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
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

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

... More labs being developed ...

## perfSONAR

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

## Zeek / Bro

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

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

Virtual environment

Pods

Pod 1
Pod 2
Pod n

HW

Orchestrator (scheduler, user interface, etc.)

Internet

~8-month usage

Pod example

Community Usage

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Reservations Made</th>
<th>Labs Attended</th>
<th>Hours Reserved</th>
<th>Hours Attended</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>default</td>
<td>3880</td>
<td>3637</td>
<td>37419.94</td>
<td>10241.12</td>
</tr>
</tbody>
</table>

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

Job details

Auto req ID: 44719R
Job Title: Industrial Control Systems Security Intern

Description:
SRNL, a multi-program laboratory operating as part of the U.S. Department of Energy's (DOE) Savannah River Site (SRS), develops and deploys innovative technologies to address critical national security, environmental remediation, and complex nuclear materials challenges.

Intern will participate in the development of a virtual network which simulates known environments to research vulnerabilities of industrial control systems (ICS) through scanning and patching industrial controllers and generating documentation to ensure each system meets SRS cyber security requirements and standards.

Preferred Qualifications:
- Knowledge and skill in basic computer applications and coding
- Strong understanding of cybersecurity principles, including but not limited to network security, system security, and application security
- Experience in developing and maintaining virtual environments
- Proficiency in security tools and technologies

Other Qualifications:
- Excellent written and oral communication skills
- Ability to work independently and as part of a team
- Strong analytical and problem-solving skills
- Ability to prioritize and manage multiple projects simultaneously

Minimum Qualifications:
- Bachelor's degree in Computer Science or related field
- Current enrollment in a degree program in Computer Science or related field

Removal Date: 22 May 2019
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