Cyber-training, Research, and Education Opportunities at the University of South Carolina

Jorge Crichigno
Department of Integrated Information Technology (IIT)
University of South Carolina
jcrichigno@cec.sc.edu
http://ce.sc.edu/cyberinfra

SC Cyber-Security Webinar Series
October 8, 2020
Agenda

• Department of Integrated Information Technology at UofSC
• Academic programs
• Virtual platform
• Industry collaboration
• Research
IIT Department

• The Department of Integrated Information Technology (IIT) is within the College of Engineering and Computing (CEC) at the University of South Carolina (UofSC)
• IIT offers undergraduate and graduate degree programs
• Its research focuses on the areas of cyber infrastructure, database systems, data analytics, health information technology, and human-computer interaction
• It is more practical than theoretical; IIT emphasizes operations, applications
• Partnership with industry for internships, materials
Academic Programs

- BSc In Integrated Information Technology
- ABET accredited
- 120 credit hours
- 400-hour internship
- Curriculum includes
  ✓ Cybersecurity
  ✓ IT Business Operations
  ✓ Databases
  ✓ Networking
  ✓ Project Management
  ✓ Web Development
- The department is developing a fully online BSc
Academic Programs

• Minor in Integrated Information Technology
• 18 credit hours
• Several concentrations
  ➢ Cybersecurity Operations
  ➢ IT Business Operations
  ➢ Databases
  ➢ Networking
  ➢ Project Management
  ➢ Web Development

Courses map learning objectives to the U.S. NICE framework (ITEC 293, ITEC 445, ITEC 493)

The National Initiative for Cybersecurity Education (NICE) Framework is a national-focused resource that categorizes and describes cybersecurity work.
Academic Programs

- Minor in Integrated Information Technology
- 18 credit hours
- Several concentrations
  - Cybersecurity Operations
  - IT Business Operations
  - Databases
  - Networking
  - Project Management
  - Web Development
Academic Programs

• Minor in Integrated Information Technology
• 18 credit hours
• Several concentrations
  ➢ Cybersecurity Operations
  ➢ IT Business Operations
  ➢ Databases
  ➢ Networking
  ➢ Project Management
  ➢ Web Development

#### Minor Requirements

<table>
<thead>
<tr>
<th>Course</th>
<th>Title</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Databases</td>
<td>18</td>
</tr>
<tr>
<td>IT 101</td>
<td>Thriving in the Tech Age</td>
<td></td>
</tr>
<tr>
<td>IT 233</td>
<td>Introduction to Computer Hardware and Software</td>
<td></td>
</tr>
<tr>
<td>IT 264</td>
<td>Computer Applications in Business I</td>
<td></td>
</tr>
<tr>
<td>IT 265</td>
<td>Introduction to Databases</td>
<td></td>
</tr>
<tr>
<td>IT 370</td>
<td>Database Systems in Information Technology</td>
<td></td>
</tr>
<tr>
<td>IT 570</td>
<td>Database Management and Administration</td>
<td></td>
</tr>
</tbody>
</table>
Academic Programs

• Minor in Integrated Information Technology
• 18 credit hours
• Several concentrations
  ➢ Cybersecurity Operations
  ➢ IT Business Operations
  ➢ Databases
  ➢ Networking
  ➢ Project Management
  ➢ Web Development

### Minor Requirements

<table>
<thead>
<tr>
<th>Course</th>
<th>Title</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Networking</td>
<td>18</td>
</tr>
<tr>
<td>ITEC 101</td>
<td>Thriving in the Tech Age</td>
<td></td>
</tr>
<tr>
<td>ITEC 233</td>
<td>Introduction to Computer Hardware and Software</td>
<td></td>
</tr>
<tr>
<td>ITEC 245</td>
<td>Introduction to Networking</td>
<td></td>
</tr>
<tr>
<td>ITEC 445</td>
<td>Advanced Networking</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Select two of the following:</td>
<td></td>
</tr>
<tr>
<td>ITEC 293</td>
<td>Cybersecurity Operations</td>
<td></td>
</tr>
<tr>
<td>ITEC 493</td>
<td>Information Technology Security for Managers</td>
<td></td>
</tr>
<tr>
<td>ITEC 545</td>
<td>Telecommunications</td>
<td></td>
</tr>
</tbody>
</table>
Academic Programs

• Minor in Integrated Information Technology
• 18 credit hours
• Several concentrations
  ➢ Cybersecurity Operations
  ➢ IT Business Operations
  ➢ Databases
  ➢ Networking
  ➢ Project Management
  ➢ Web Development

<table>
<thead>
<tr>
<th>Course</th>
<th>Title</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>ITCS 101</td>
<td>Thriving in the Tech Age</td>
<td>18</td>
</tr>
<tr>
<td>ITCS 233</td>
<td>Introduction to Computer Hardware and Software</td>
<td></td>
</tr>
<tr>
<td>ITCS 264</td>
<td>Computer Applications in Business I</td>
<td></td>
</tr>
<tr>
<td>ITCS 362</td>
<td>Introduction to Web Systems</td>
<td></td>
</tr>
<tr>
<td>ITCS 560</td>
<td>Project Management Methods</td>
<td></td>
</tr>
<tr>
<td>ITCS 564</td>
<td>Capstone Project for Information Technology</td>
<td></td>
</tr>
</tbody>
</table>
Academic Programs

• Minor in Integrated Information Technology
• 18 credit hours
• Several concentrations
  ➢ Cybersecurity Operations
  ➢ IT Business Operations
  ➢ Databases
  ➢ Networking
  ➢ Project Management
  ➢ Web Development

<table>
<thead>
<tr>
<th>Course</th>
<th>Title</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Web Development</td>
<td>18</td>
</tr>
</tbody>
</table>

- ITEC 101: Thriving in the Tech Age
- ITEC 233: Introduction to Computer Hardware and Software
- ITEC 262: Introduction to Web Systems
- ITEC 562: Advanced Web Support Systems

Select one of the following:

- ITEC 245: Introduction to Networking
- ITEC 264: Computer Applications in Business I
- ITEC 265: Introduction to Databases

Select one ITEC elective
Academic Programs

• The Department is developing
  ➢ A PhD in Informatics (approval expectation in 2021)
  ➢ Undergraduate and graduate certificates

• More practical than theoretical

• Partnership with industry
  ➢ Cisco Network Academy
  ➢ Palo Alto Networks Cybersecurity Academy
  ➢ VMware IT Academy
  ➢ Intel's Barefoot Academy
  ➢ Juniper Networks

• Flexible program
Virtual Platform

- IIT programs incorporate much hands-on activities
- The IEEE and ACM are the main societies which guide IT education
  - IT curriculum should emphasize “learning IT core concepts combined with authentic practice” and “use of professional tools and platforms”
- Physical labs are typically used to teach and train IT students
- COVID exacerbated the needs of efficient technologies for hands-on education in IT
- UofSC works with the Network Development Group (NDG), VMware, Palo Alto Cybersecurity Academy, Cisco, and others to virtualize labs
- A virtual platform enables an institution to move traditional curriculum relying on physical labs into an online format

Virtual Platform

- Virtualization is a technology by which the software portion of a device (e.g., PC, routers, etc.) can execute on a general-purpose physical server as a virtual machine.
- A pod is a set of virtual machines needed for the completion of a virtual lab exercise.
- The pod can be as simple as a single isolated virtual machine, or as complex as autonomous systems with live traffic flowing to/from the Internet.
Virtual Platform

- USC (SC), SCC (NC), and NDG are building a distributed virtual platform
- The goal is scalability, using the resources available on campus networks
- Since January 2020, the distributed platform has served more than 7,000 learners
Virtual Platform

• There are multiple types of pods
  ➢ Pods to learn concepts traditionally covered by academic programs
  ➢ Pods to learn skills and techniques covered by certificate programs
  ➢ Pods to perform research

• Industry partners are essential
Virtual Labs – Zeek Intrusion Detection

- The Zeek labs provide hands-on experience on Intrusion Detection System (IDS)
- Zeek is a passive, open-source network traffic analyzer
- It is primarily used as a security monitor in national labs, campus networks, enterprises, research labs

<table>
<thead>
<tr>
<th>Lab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lab 1</td>
<td>Introduction to the Capabilities of Zeek</td>
</tr>
<tr>
<td>Lab 2</td>
<td>An Overview of Zeek Logs</td>
</tr>
<tr>
<td>Lab 3</td>
<td>Parsing, Reading and Organizing Zeek Log Files</td>
</tr>
<tr>
<td>Lab 4</td>
<td>Generating, Capturing and Analyzing Network Scanner Traffic</td>
</tr>
<tr>
<td>Lab 5</td>
<td>Generating, Capturing and Analyzing DoS and DDoS-centric Network Traffic</td>
</tr>
<tr>
<td>Lab 6</td>
<td>Introduction to Zeek Scripting</td>
</tr>
<tr>
<td>Lab 7</td>
<td>Introduction to Zeek Signatures</td>
</tr>
<tr>
<td>Lab 8</td>
<td>Advanced Zeek Scripting for Anomaly and Malicious Event Detection</td>
</tr>
<tr>
<td>Lab 9</td>
<td>Profiling and Performance Metrics of Zeek</td>
</tr>
<tr>
<td>Lab 10</td>
<td>Application of the Zeek IDS for Real-Time Network Protection</td>
</tr>
<tr>
<td>Lab 11</td>
<td>Preprocessing of Zeek Output Logs for Machine Learning</td>
</tr>
<tr>
<td>Lab 12</td>
<td>Developing Machine Learning Classifiers for Anomaly Inference and Classification</td>
</tr>
<tr>
<td>Lab Manuals</td>
<td></td>
</tr>
</tbody>
</table>
Virtual Labs – BGP

- These labs provide a detailed, hands-on experience to understand the Border Gateway Protocol (BGP), adjust its attributes, and control traffic on the Internet
- Routers use Free Range Routing (FRR) routing stack
- FRR is an open-source protocol stack that provides IP-based routing services

<table>
<thead>
<tr>
<th>Lab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lab 1</td>
<td>Introduction to Mininet</td>
</tr>
<tr>
<td>Lab 2</td>
<td>Introduction to Free Range Routing (FRR)</td>
</tr>
<tr>
<td>Lab 3</td>
<td>Introduction to BGP</td>
</tr>
<tr>
<td>Lab 4</td>
<td>Configure and Verify EBGP</td>
</tr>
<tr>
<td>Lab 5</td>
<td>BGP Authentication</td>
</tr>
<tr>
<td>Lab 6</td>
<td>Configure BGP with Default Route</td>
</tr>
<tr>
<td>Lab 7</td>
<td>Using AS_PATH BGP Attribute</td>
</tr>
<tr>
<td>Lab 8</td>
<td>Configuring IBGP and EBGP Sessions, Local Preference, and MED</td>
</tr>
<tr>
<td>Lab 9</td>
<td>IBGP, Next Hop and Full Mesh Topology</td>
</tr>
<tr>
<td>Lab 10</td>
<td>BGP Route Reflection</td>
</tr>
</tbody>
</table>

17
Virtual Labs – MPLS and Advanced BGP Topics

- These labs provide a detailed, hands-on experience to understand advanced concepts and protocols
- Examples include MPLS, Multi-protocol BGP, BGP hijacking, virtual private networks (VPNs), Ethernet VPNs, and Segment Routing

<table>
<thead>
<tr>
<th>Lab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lab 1</td>
<td>Configuring Multiprotocol BGP</td>
</tr>
<tr>
<td>Lab 2</td>
<td>IP Spoofing and Mitigation Techniques</td>
</tr>
<tr>
<td>Lab 3</td>
<td>BGP Hijacking</td>
</tr>
<tr>
<td>Lab 4</td>
<td>Introduction to MPLS</td>
</tr>
<tr>
<td>Lab 5</td>
<td>Label Distribution Protocol (LDP)</td>
</tr>
<tr>
<td>Lab 6</td>
<td>Virtual Routing and Forwarding (VRF)</td>
</tr>
<tr>
<td>Lab 7</td>
<td>MPLS Layer 3 VPN using MP-BGP</td>
</tr>
<tr>
<td>Lab 8</td>
<td>Ethernet VPN (EVPN) using MP-BGP</td>
</tr>
<tr>
<td>Lab 9</td>
<td>Introduction to Segment Routing over IPv6 (SRv6)</td>
</tr>
<tr>
<td>Lab Manuals</td>
<td></td>
</tr>
</tbody>
</table>
Virtual Labs – MPLS and Advanced BGP Topics

• These labs provide a detailed, hands-on experience to understand advanced concepts and protocols
• Examples include MPLS, Multi-protocol BGP, BGP hijacking, virtual private networks (VPNs), Ethernet VPNs, and Segment Routing

<table>
<thead>
<tr>
<th>Lab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Configuring Multiprotocol BGP</td>
</tr>
<tr>
<td>2</td>
<td>IP Spoofing and Mitigation Techniques</td>
</tr>
<tr>
<td>3</td>
<td>BGP Hijacking</td>
</tr>
<tr>
<td>4</td>
<td>Introduction to MPLS</td>
</tr>
<tr>
<td>5</td>
<td>Label Distribution Protocol (LDP)</td>
</tr>
<tr>
<td>6</td>
<td>Virtual Routing and Forwarding (VRF)</td>
</tr>
<tr>
<td>7</td>
<td>MPLS Layer 3 VPN using MP-BGP</td>
</tr>
<tr>
<td>8</td>
<td>Ethernet VPN (EVPN) using MP-BGP</td>
</tr>
<tr>
<td>9</td>
<td>Introduction to Segment Routing over IPv6 (SRv6)</td>
</tr>
<tr>
<td></td>
<td>Lab Manuals</td>
</tr>
</tbody>
</table>
Virtual Labs – Software-defined Networking

• These labs provide a detailed, hands-on experience to Software-defined Networking (SDN)
• Devices and protocols include Open Virtual Switch (OVS), Open Network Operating System (ONOS) controller, VXLAN, and VPLS

<table>
<thead>
<tr>
<th>Lab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lab 1</td>
<td>Introduction to Mininet</td>
</tr>
<tr>
<td>Lab 2</td>
<td>Legacy Networks: BGP Example as a Distributed System and Autonomous Forwarding Decisions</td>
</tr>
<tr>
<td>Lab 3</td>
<td>Early efforts of SDN: MPLS Example of a Control Plane that Establishes Semi-static Forwarding Paths</td>
</tr>
<tr>
<td>Lab 4</td>
<td>Introduction to SDN</td>
</tr>
<tr>
<td>Lab 5</td>
<td>Configuring VXLAN to Provide Network Traffic Isolation</td>
</tr>
<tr>
<td>Lab 6</td>
<td>Introduction to OpenFlow</td>
</tr>
<tr>
<td>Lab 7</td>
<td>Routing within an SDN network</td>
</tr>
<tr>
<td>Lab 8</td>
<td>Interconnection between Legacy Networks and SDN Networks</td>
</tr>
<tr>
<td>Lab 9</td>
<td>Configuring Virtual Private LAN Service (VPLS)</td>
</tr>
<tr>
<td>Lab Manuals</td>
<td></td>
</tr>
</tbody>
</table>
Virtual Labs – Palo Alto NG Firewall

• These labs enhance the student’s understanding of how modern firewalls work, referred to as Next-generation Firewalls (NGFWs)
• Students gain hands-on experience deploying, managing, and monitoring firewalls in a (virtual) lab environment, using live traffic
• Material also prepares students for certificates
• The IEEE/ACM group “acknowledges the value of vendor and industry certifications and encourages students to pursue them as they see necessary”

Virtual Labs – Palo Alto NG Firewall

• These labs enhance the student’s understanding of how modern firewalls work, referred to as Next-generation Firewalls (NGFWs)

Pod deployed in private cloud
Virtual Labs – Palo Alto NG Firewall

• These labs enhance the student’s understanding of how modern firewalls work, referred to as Next-generation Firewalls (NGFWs)

Pod deployed in private cloud

Job search
Virtual Labs – Palo Alto NG Firewall

• These labs enhance the student’s understanding of how modern firewalls work, referred to as Next-generation Firewalls (NGFWs)
ONR’s Cyber Project

• Office of Naval Research (ONR) is funding the project “Enhancing the Preparation of Next-generation Cyber Professionals”

• South Carolina cybersecurity needs
  ➢ Naval Information Warfare Center (NIWC) Atlantic, SRNL, Fort Jackson, Shaw Air Force Base

• Recruiting the American military’s cyber force is more difficult than ever
  ➢ DoD has been struggling to hire more than 8,000 cyber positions (2018)¹

• The College of Engineering and Computing is addressing the workforce needs:
  ➢ Encourage Reserve Officers’ Training Corps (ROTC) students to obtain an IT minor
  ➢ Undergraduate applied research

ONR’s Cyber Project

1. Minor in IT – Cyber specialization
   - Option to earn DoD’s approved baseline certificates for Information Assurance Technical (IAT)
   - Self-contained specialization; no pre-reqs

2. Undergraduate applied research

3. Private cloud with professional tools and platforms

4. Collaboration with industry
ONR’s Cyber Project

- Undergraduate students work 18 hours per week, 15 weeks, $18 per hour ($4,050)
  - Applied research
  - Professional tools, platforms, market validation
  - Cisco Systems, Palo Alto Networks, VMware, Juniper, Intel
  - Focus on relevant technology, customized scenarios; e.g., IPsec-based VPNs with NGFWs
Graduate Projects

• Development of new techniques against attacks targeting “Internet-of-Things” devices
• Agreement with the Center for Applied Internet Data Analysis (CAIDA) (San Diego)
Graduate Projects

• Development of new techniques against attacks targeting “Internet-of-Things” devices
• Agreement with the Center for Applied Internet Data Analysis (CAIDA) (San Diego)

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 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
Graduate Projects

- Performance testing Google’s new communication protocol
- Feedback to Google (used in Youtube, Chrome, and other apps)
- Emulating behavior in private cloud before Google’s protocol public release
Graduate Projects

• Improving system’s performance using next-generation switches
• Offloading computational tasks to network switches
  ➢ Orders of magnitude faster than general-purpose CPU
  ➢ Very limited instructions set (e.g., no multiplication, no division, simple operations)
• Agreement with Intel (chips, software development environment)

Application example: media (voice) relay server

<table>
<thead>
<tr>
<th></th>
<th>Programmable Switch</th>
<th>General-purpose CPU</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cost</td>
<td>$6,000</td>
<td>$10,000 - 25,000</td>
</tr>
<tr>
<td>Capacity</td>
<td>~35,000,000 connections per switch</td>
<td>~500 connections per core</td>
</tr>
<tr>
<td>Latency</td>
<td>400 nanoseconds</td>
<td>Tens to hundreds of milliseconds</td>
</tr>
</tbody>
</table>
Graduate Projects

• Improving system’s performance using next-generation switches
• Offloading computational tasks to network switches
  ➢ Orders of magnitude faster than general-purpose CPU
  ➢ Very limited instructions set (e.g., no multiplication, no division, simple operations)
• Agreement with Intel (chips, software development environment)

Offloading Media Traffic to Programmable Data Plane Switches

Elie F. Kfoury*, Jorge Crichigno*, Elias Bou-Harb¹, Vladimir Gurevich¹
¹Integrated Information Technology, University of South Carolina, USA
²The Cyber Center For Security and Analytics, University of Texas at San Antonio, USA
³Barefoot Networks, an Intel Company, USA

Abstract—According to estimations, approximately 80% of Internet traffic represents media traffic. Much of it is generated by end users communicating with each other (e.g., voice, video sessions). A key element that permits the communication of users that may be behind Network Address Translation (NAT) is the relay server.

This paper presents a scheme for offloading media traffic from relay servers to programmable switches. The proposed scheme relies on the capability of a P4 switch with a customized parser to de-encapsulate and process packets carrying media traffic. The switch then applies multiple switch actions over the packets. As these actions are simple and collectively emulate a relay server, the scheme is capable of moving relay functionality to results [8] reveal that CGN has a widespread adoption and that over half of operators have deployed or will deploy CGN. NAT 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 (voice, video), the user must wait and accept incoming connections at a well-known port. With NAT, the user is not reachable because it is assigned a private IP address. Furthermore, port numbers are also allocated dynamically. Moreover, these dynamic allocations...

32
The END