Overview
Department of Integrated Information Technology
University of South Carolina

Jorge Crichigno
jcrichigno@cec.sc.edu

Center of Advanced Technical Studies
Chapin, SC
November 11, 2021
IIT Program

- B. S. Integrated Information Technology
- 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
- ABET accredited ("quality assurance")
IIT Program

- Programs are more practical than theoretical
- Courses reinforce the theoretical knowledge with hands-on activities
- What do graduates do?
  - They build, maintain, operate, and repair hardware and software associated with computer systems
    - Network engineer
    - Cybersecurity analyst
    - Web design and services
    - User experience / human-computer interaction professional
    - Cloud system specialist
    - Security Operation Center (SOC) analyst
    - Data analytics professional
IIT Program

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

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

- DoD’s Information Assurance (IA) workforce is classified in IA technical (IAT):
  - Level 1 (IAT 1): Computing environment information assurance
  - Level 2 (IAT 2): Network environment information assurance
  - Level 3 (IAT 3): Enclave, advanced network & computer information assurance

- It requires partnership
  - Cisco Systems, Palo Alto Networks, VMware, Juniper, Intel

<table>
<thead>
<tr>
<th>Certificate</th>
<th>Material Covered in</th>
<th>IAT 1</th>
<th>IAT 2</th>
<th>NICE framework</th>
<th>Networks cert.</th>
</tr>
</thead>
<tbody>
<tr>
<td>A+</td>
<td>ITEC 233</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Cyberoperations</td>
<td>ITEC 293</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Security+</td>
<td>ITEC 293</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>CCNA Security</td>
<td>ITEC 493</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>CCNA Routing/Switching</td>
<td>ITEC 245, ITEC 445</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>ACE</td>
<td>ITEC 493</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PCNSE</td>
<td>ITEC 493</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

NICE: National Initiative for Cybersecurity Education
Office of Naval Research (ONR) Project

- “Enhancing the Preparation of Next-generation Cyber Professionals”
- South Carolina cybersecurity needs
  - NIWC Atlantic, SRNL, Fort Jackson, Shaw Air Force Base, private industry
- 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
  - Shortage of cybersecurity professionals
- The College of Engineering and Computing is addressing the workforce needs:
  - Encourage students to acquire “cyber” knowledge
  - Undergraduate applied research
  - Private cloud
  - Collaboration among industry, government, education institutions

Cybersecurity job openings in four metro areas near Columbia, Feb. 2020

ONR’s Cyber Project

• Collaboration
  ➢ Applied teaching and research -> professional tools, platforms, market validation
  ➢ Cisco Systems, Palo Alto Networks, VMware, Juniper, Intel

✓ Bachelor’s degree
✓ IAT credential
✓ Theory
✓ Hands-on expertise
ONR’s Cyber Project

• Collaboration
  ➢ Applied teaching and research -> professional tools, platforms, market validation
  ➢ Cisco Systems, Palo Alto Networks, VMware, Juniper, Intel

✓ Bachelor’s degree
✓ IAT credential
✓ Theory
✓ Hands-on expertise
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
NSF ATE and CC

- NSF Advanced Technical Education (ATE) and NSF Campus Cyberinfrastructure (CC) (2019)
- Development of a multi-state distributed cloud to support teaching, research
- 2+2+2 program (HS + College + University)
- Distributed cloud pools resources from SC and NC, serves institutions seamlessly
- Requests to use the platform
  - Berkeley National Lab
  - SANS institute (“girlsgocyber”)
  - Multiple higher-ed institutions
  - International Networks at Indiana
  - Fort Gordon (PAN’s NGFW, VMware Clouds)
  - Texas’ Lonestart Education and Research

![Diagram of distributed cloud system with节点 Pod 1 to Pod n, USC and SCC servers, portal system integrated into Learning Management System (Canvas, Blackboard), and learner institutions like SCC, NC, USC, and SCSS HS.]
NSF ATE 2021 - …

- National Online Platform
- Consortium of Colleges and Universities
- Industry
  - Palo Alto Networks Cybersecurity Academy
  - Cisco Network Academy
  - VMware IT Academy
  - …

The University of South Carolina partners with VMware IT Academy to help students learn digital technology skills to fill high-demand jobs.
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)

Global distribution of exploited IoT devices; results from this research project

Malware exploiting default credentials
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
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><strong>Cost</strong></td>
<td>$6,000</td>
<td>$10,000 - 25,000</td>
</tr>
<tr>
<td><strong>Capacity</strong></td>
<td>~35,000,000</td>
<td>~500 connections per core</td>
</tr>
<tr>
<td><strong>Latency</strong></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 Cricchigno*, Elias Bou-Harb†, Vladimir Gurevich‡

*Integrated Information Technology, University of South Carolina, USA
†The Cyber Center For Security and Analytics, University of Texas at San Antonio, USA
‡Barefoot 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 network switches.

---

**Implementing SONiC Functionalities in Disaggregated Network Switches**

Ali AlSabe*, Elie Kfoury*, Jorge Cricchigno*, Elias Bou-Harb†

*University of Texas at Austin, 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

Network Operating Systems (NOs), which are conceptualized, designed, developed, and sold by a specific company. The vendor provides the locked-in hardware with a pre-installed NO, preventing the user from tampering it or installing third-party software. This behavior is beneficial among traditional networks where vendors have extensively tested their software before distributing it among clients. However, when it comes to adopting new technologies and scaling the network, vendors become cautious and reluctant due to security concerns, financial costs, and downtime drawbacks that might follow [2].

---

*TNSA: This model is referred to as "disaggregated" as the software and hardware are decoupled; essentially, vendors'