Teaching and Research on Cybersecurity Using Next-Generation Devices

Jorge Crichigno
Department of Integrated Information Technology (IIT)
College of Engineering and Computing
University of South Carolina

McNair Center
July 29, 2020
Agenda

• Projects at IIT
• Local private cloud to support virtual labs and remote-access capabilities
• Expanding local cloud to a multi-state distributed cloud
• Support for teaching and research using private cloud
• Office of the Naval Research (ONR) project
  ➢ Enhancing the Preparation of Next-generation Cyber Professionals
NSF Cybersecurity

- NSF Cybersecurity (2018)
- Local private cloud for teaching and research in cyber at UofSC
- Build a private cloud
- Real protocol stacks and live traffic experimentation
- Scalable platform, hundreds of users simultaneously
NSF Cybersecurity

- Portal system

Cyberinfrastructure Lab @ UofSC

1. Login to virtual environment
2. Enter the lab at the reserved day and time
3. Perform lab (live experiments and traffic)
NSF Cybertraining

- NSF Cybertraining (2019): Cyberinfrastructure for moving big data
- There is a need for IT technical expertise country-wide
- E.g., ESnet is the network connecting national labs, research institutions
  - Managed by the Department of Energy (Berkeley National Lab)
- Rates of 50 Gbps, emulation of high-performance systems

ESnet

Monthly average traffic volume, ESnet

Three-node network emulation

Intel Xeon Gold 6130 CPU, 2.1 GHz
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 (2 cyber courses)
  - Texas’ Lonestart Education and Research

![Distributed Cloud Diagram]

Distributed Cloud

Portal System integrated into Learning Management System (Canvas, Blackboard)

Learner GSSM HS, SC

Learner SCC, NC

Learner USC, SC

Learner CCCC, NC

Learner SCSS HS, NC

Internet

Content type 1

Content type 2

Content type 3

USC (3 physical servers)

SCC (6 physical servers)

Pod 1

Pod 2

Pod 3

Pod 1

Pod 2

Pod 3

Pod n1

Pod n2

Pod n3

Pod n1

Pod n2

Pod n3

Pod n1

Pod n2

Pod n3

Pod n1

Pod n2

Pod n3
Private Cloud Use

• Portal system, UofSC usage only

![Bar chart showing number of lab experiments and hours attended over years 2018 to 2020]
# Private Cloud Use

- **Private vs public cloud**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Private Cloud</th>
<th>Public Cloud (e.g., AWS)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Granularity to allocate physical resources</td>
<td>Very granular</td>
<td>Not granular (access to the physical resources requires additional fees)</td>
</tr>
<tr>
<td>Easy to create custom pods</td>
<td>Easy</td>
<td>More difficult; hard to design complex topologies</td>
</tr>
<tr>
<td>Cost</td>
<td>Cost effective when used extensively</td>
<td>Cost effective for individual / small virtual machines; costly for large virtual machines over time</td>
</tr>
<tr>
<td>IT Staff</td>
<td>Higher cost</td>
<td>Lower cost</td>
</tr>
<tr>
<td>Application layer for pedagogy and presentation of virtual scenarios</td>
<td>Very flexible</td>
<td>Not flexible; limited to providers’ interface, e.g., command-line interface</td>
</tr>
<tr>
<td>Time-sharing compute resources</td>
<td>The owner controls who can access resources. Easy to implement time-sharing policies</td>
<td>Cloud provider controls who can access resources (typically, a fee is required per user accessing resources)</td>
</tr>
</tbody>
</table>
ONR’s Cyber Project

“Enhancing the Preparation of Next-generation Cyber Professionals” (2020)

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 STEM, ROTC students to obtain a minor in IT
- 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

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

2. Undergraduate applied research
   - CEC faculty, graduate student mentors
   - Advisory entity by NIWC Atlantic, project guidelines

3. Private cloud with professional tools and platforms
   - Hands-on applied research with physical and virtual equipment

4. Collaboration
   - Partnership with Intel, Cisco Systems, Palo Alto Networks, VMware, Juniper
ONR’s Cyber Project

• 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 (NIST)
ONR’s Cyber Project

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

Pod deployed in private cloud

Next-generation Firewall Virtual Machine + licenses
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
✓ Theory
✓ Hands-on expertise Palo Alto

Pod deployed in private cloud

Job search
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
Theory
Hands-on expertise Palo Alto

Additional credentials

Job search
ONR’s Cyber Project

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

Additional credentials

- Bachelor’s degree
- IAT
- Theory
- Hands-on expertise Palo Alto

UofSC’s ROTC
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)
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

---

An emulation-based evaluation of TCP BBRv2 Alpha for wired broadband

Elie F. Kfouri * &1, Jose Gomez * &2, Jorge Crichtino * &2, Elias Bou-Harb * &1

Show more ↘️

https://doi.org/10.1016/j.comcom.2020.07.018

Abstract

Google published the first release of the Bottleneck Bandwidth and Round-trip Time (BBR) congestion control algorithm in 2016. Since then, BBR has gained a
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 connections per switch</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. Kfoury1, Jorge Crichigno1, 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 near the source, thus allowing the network to scale.

The 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 members are also allocated dynamically. Moreover, these dynamic allocations

SONiC Functionalities in Disaggregated Network Switches

Ali AlSahel1, Elie Kfoury1, Jorge Crichigno1, Elias Bou-Harb1
1Integrated Information Technology, University of South Carolina (USC), Columbia, South Carolina, USA
2The 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 with 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].
NIWC Atlantic

- Collaboration with NIWC Atlantic is essential
  - We want to acknowledge Michael Merriken and Captain Sanders
- Advisory entity to the project
- Provide input for undergraduate research projects
- Coordination with UofSC’s ROTC
  - Navy
  - Army
  - Air Force