“TRAINING COURSES NEEDED TO KEEP TECHNICAL STAFF CURRENT”

J. Crichigno
Department of Integrated Information Technology
University of South Carolina

NTU Technical Workshop
Arizona State University
Tempe, AZ, July 31, August 1, 2019
Agenda

• The Information Technology (IT) Discipline
• Traditional and pillars-first IT program
• The Networking pillar
• Promoting lifelong learning
• Current training at University of South Carolina
Background

- According to the Guidelines of the ACM and IEEE Computer Society, networking is a **pillar** of IT\(^1,2\)

- Networking identified as a knowledge area with **core** units in the guidelines of programs such as Computer Engineering\(^3\) and Computer Science\(^4\)

---

IT Programs

- How should programs be built?
- Consider the pre-requisites for an introductory course in computer networks
IT Programs

• Traditional emphasis on pre-requisite requirements
• Introduce students to the computer networks area (or other technical areas) at their senior year
• Students exposed at a relative abstract level
• Gap between industry and academia
IT Programs

- Program must prepare students for an undetermined future
- It must be flexible and remain as small as practical, allowing for freedom as needed by stakeholders
- Essential competencies; supplemental competencies for additional depth (e.g., high-performance computing)
The Networking Pillar

- The IEEE / ACM guideline for IT programs considers networking a pillar of the IT discipline
  - Foundations of networking
  - Networking and interconnectivity
  - Routing, switching, and internetworking
  - Application networking services
  - Network management
The Networking Pillar

- General-purpose (essential topics) vs high-performance networks (supplementation)
### The Networking Pillar

#### General-purpose vs high-performance networks

<table>
<thead>
<tr>
<th></th>
<th>General-purpose</th>
<th>Science DMZ</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>WANs</strong></td>
<td>➢ Limited bandwidth by commercial ISPs</td>
<td>➢ Connection to Internet2/NRENs</td>
</tr>
<tr>
<td></td>
<td>➢ Routers/switches not optimized for performance</td>
<td>➢ 10-100 Gbps paths</td>
</tr>
<tr>
<td></td>
<td>➢ Congestion</td>
<td>➢ Routers/switches optimized for performance</td>
</tr>
<tr>
<td></td>
<td>➢ Routing achieved independently by ISPs</td>
<td>➢ Predictable performance</td>
</tr>
<tr>
<td></td>
<td>➢ Typical frame size is 1,500 bytes</td>
<td>➢ End-to-end routing optimization</td>
</tr>
<tr>
<td></td>
<td></td>
<td>➢ Jumbo frames are supported</td>
</tr>
<tr>
<td><strong>Switches / routers</strong></td>
<td>➢ Rates lower than 10 Gbps</td>
<td>➢ Rate higher than 10 Gbps</td>
</tr>
<tr>
<td></td>
<td>➢ Recommended buffer size equals BDP/√N</td>
<td>➢ Recommended buffer size equals BDP</td>
</tr>
<tr>
<td></td>
<td>➢ Cut-through is used as forwarding method</td>
<td>➢ Store-and-forward should be used for forwarding</td>
</tr>
<tr>
<td></td>
<td>➢ Many switches use shared memory for buffering</td>
<td>➢ Buffer allocation should be port-based</td>
</tr>
<tr>
<td></td>
<td>➢ Switching methods include shared-memory, bus fabrics</td>
<td>➢ Recommended fabric is crossbar</td>
</tr>
<tr>
<td><strong>Transport</strong></td>
<td>➢ Stop-and-wait protocol behavior acceptable</td>
<td>➢ pipelined behavior essential for performance TCP buffer size must be greater than BDP</td>
</tr>
<tr>
<td></td>
<td>➢ TCP buffer size has small impact on performance</td>
<td>➢ Rate-based congestion control has positive impact</td>
</tr>
<tr>
<td></td>
<td>➢ Mostly window-based congestion control used</td>
<td>➢ Pacing, parallel streams improve throughput</td>
</tr>
<tr>
<td></td>
<td>➢ No pacing, no parallel streams</td>
<td></td>
</tr>
</tbody>
</table>

*BDP* stands for *Bandwidth Delay Product*, which is a measure of the bandwidth and the average delay required for data transmission.
### The Networking Pillar

- **General-purpose vs high-performance networks**

<table>
<thead>
<tr>
<th>Applications</th>
<th>General-purpose</th>
<th>Science DMZ</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Variety of applications</td>
<td>Small set of applications</td>
</tr>
<tr>
<td></td>
<td>General-purpose data transfer tools</td>
<td>Specialized data-transfer tools (Globus)</td>
</tr>
<tr>
<td></td>
<td>(SCP, FTP)</td>
<td>Multi-domain performance monitoring (perfSONAR)</td>
</tr>
<tr>
<td></td>
<td>Single-domain monitoring application</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(SNMP, Syslog)</td>
<td></td>
</tr>
<tr>
<td>Security</td>
<td>Online devices (IPSs, firewalls) are typical</td>
<td>Online devices are not used</td>
</tr>
<tr>
<td></td>
<td>IDS and ACLs used as complement to IPS and firewalls</td>
<td>ACL used as primary defense</td>
</tr>
<tr>
<td></td>
<td>Frequent application changes and updates</td>
<td>Flow-based IDS is attractive</td>
</tr>
<tr>
<td></td>
<td>Multimedia, image, data processing, conde execution</td>
<td>Changes are not frequent</td>
</tr>
<tr>
<td></td>
<td>(HTML, XML, SQL, etc.)</td>
<td>Limited operations over data (file operations mostly)</td>
</tr>
</tbody>
</table>


The Networking Pillar

- The subject of networking is complex and evolving
- Many topics covered in supplemental units (e.g., Science DMZ) evolve from general-purpose networks
- The curriculum must promote critical thinking, lifelong learning, self-directed professional development
Promoting Lifelong Learning

- The subject of networking is complex and evolving
- Many topics covered in supplemental units (e.g., Science DMZ) evolve from general-purpose networks
- The curriculum must promote critical thinking, lifelong learning, self-directed professional development
Promoting Lifelong Learning

• As students learn more about the underlying real-world IT issues, they become more interested in their studies
  ➢ Real-world capstone projects for external clients, external judges
  ➢ Laboratory experiences with workplace relevance
  ➢ Internship experiences
  ➢ Research agenda emerges from the practice
Promoting Lifelong Learning

- Incorporating professional practice into the curriculum serves as a catalyst to stimulate student’s interest in the IT profession
- Experiential learning promotes leadership and help develop interpersonal skills
Capstones and Professional Presentations
Internships

Welcome to the 2019 SRNL Interns Research Poster Session
July 24, 2019 • 1-4 PM
SRNL Applied Research Center
Garden Room and Lobby

Interns will present research projects from a variety of internship programs including:
- Aiken Co-ops
- JCE Weapons Testing Facility
- JCE Co-ops – Florida Community College
- DOE-SC Office of Science – Savannah River Site Nuclear Energy Office
- DOE-SC Office of Science – Savannah River National Laboratory
- Department of Energy Office of Science
- Savannah River National Laboratory Internships
- Savannah River National Laboratory Cyber Security Internships

Cyber Security: the Internship

Why is policy important?

Standards and policy are even prevalent in the cybersecurity domain and beyond. Without regulations, you would have to rely on a manager’s judgment of what is needed and how it should be accomplished. Lasting policies are used to communicate values, emphasize priorities, and impart understanding of what is expected outside the daily routine. They also help to ensure that sensitive information is protected.

Web Development

Another great opportunity was attending to web development. Learning about domain names and how to host a website on them is a great starting point and can be extended with additional knowledge. Best practices include using HTTPS, ensuring a secure connection, and keeping the backend updated and secure.

Sharepoint

In general, I was in great communication with the team, especially a work group on cybersecurity. We would discuss our strategy and implementation on a daily basis. Communication is key, and it’s important to keep up with the team’s current projects and progress. Sharing information helps to ensure that everyone is on the same page and working towards the same goal.

Change Control

The team is responsible for the management of all cybersecurity efforts. Updates and security fixes are regularly being updated and implemented. Policies and procedures need to be updated as needed. Change requests are coordinated through a process called Change Request Management. This process involves documenting the change request, reviewing it for any potential issues, and then implementing it. The process is important to ensure that changes are properly documented and approved before being implemented. Another great experience working with this process.

Updating Computer Systems Using Image Backups

The team was responsible for updating the computer systems using image backups. The process involved creating an image backup of the existing system, testing it, and then applying the changes. This process is important to ensure that the system is up-to-date and secure. The team was able to identify and fix any issues before implementing the changes, ensuring a smooth transition.

Internships
Current Training at USC

- Employers, alumni, partners
Nurturing Success: Northern New Mexico College Student Lands Dream Job At LANL

Submitted by Carol A. Clark on July 17, 2017 - 10:00am

Los Alamos Daily, July 17, 2017

Science DMZ team, from left to right
Chase: Comp. Sys. Professional 2, LANL; Joseph: Scientist 1 at LANL, GA Tech Master program; Sergio: graduate in Fall 2017, intern at LANL, Analysis, Intelligence, and Technology, GA Tech Master program

NM college lands funding to launch high-growth tech field program

Albuquerque Business First, Aug. 24, 2017

LANL – NNMC: Internship program, Biology and Information Engineering Technology, Spring 2018

1st place award, Bioinformatics; 2016 NM IMBRE conference

Co-PI Biology team, NM IMBRE ‘16 Conf.

Top: Maria, Colo. State Research Symp. ’16, 2nd place award
Bottom: Britney, NM Biomedical Symp. ‘16
Current Training at USC

- Initially targeted for students, IIT’s material helps to train IT staff and self-pace learners from other departments
- Provide foundations, including state-of-the-art technology
  - E.g., when covering the network layer, include Software-defined Networking (SDN)
  - P4 programmable data plane switches (master, PhD level)
- Facilitate the use of hands-on tools
  - Agreements with Cisco, Palo Alto, Juniper, VMware, Amazon, Barefoot Networks
  - Theoretical concepts reinforced with material developed by vendors
  - Develop material for training not provided by vendors (traffic analysis tools, Bro, high-speed networks, programmable data plane switches)
Current Training at USC

• Train students to be a problem solver, skilled practitioner
• Promote applied research using professional tools and platforms
  ➢ Ease the transition from academia to the workplace
  ➢ Some vendors offer excellent tools that complement theory, at no cost
  ➢ Vendor-specific certifications are practice-oriented, highly technical in nature; used as a complement for core concepts
  ➢ Many open source applications are highly recognized
<table>
<thead>
<tr>
<th>Comments by attendees of 2017 NSF CC meeting⁴</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Working with researchers… HPC, Science DMZ, DTN, Big Data and/or GPU platforms”</td>
</tr>
<tr>
<td>“Very difficult to find, or nonexistent - difficult to retain (CI engineers)”</td>
</tr>
<tr>
<td>“time to hire (CI engineers)... ended up taking 10 months”</td>
</tr>
<tr>
<td>“Combination of education and experience”</td>
</tr>
<tr>
<td>“At least one tour of duty as an intern or apprentice”</td>
</tr>
<tr>
<td>“System and network engineering, user support experience, good communication…”</td>
</tr>
<tr>
<td>“Routing and switching (e.g., Juniper, Cisco), …training in security (e.g., Palo Alto or similar), cabling”</td>
</tr>
<tr>
<td>“Working knowledge of theory and practice underlying VLAN/LAN/WAN… Windows and Unix/Linux”</td>
</tr>
<tr>
<td>“We get great mileage out of community college student interns for tasks at the system / network admin”</td>
</tr>
</tbody>
</table>

Current Training at USC

- Introduction to Networks
- Routing and Switching
- High-speed Networks
- perfSONAR

- SOC cyber-operations
- Next-generation Firewalls
- Traffic Analysis with Bro
- Introduction to Cryptography

- Linux Essentials
- Introduction to Virtualization
- Virtualized Datacenter

...
Hands-on Training

Introduction to Cryptography

PAN / Next-generation Firewalls
Introduction to Zeek / Bro

perfSONAR
Hands-on Training

Cyber-operations

Network Tools and Protocols (High-speed Networks)

Intel Xeon Gold 6130 CPU, 2.1 GHz
Labs Series: Networks Tools and Protocols

- Lab 1: Introduction to Mininet
- Lab 2: Introduction to iPerf
- Lab 3: Emulating WAN with NETEM I Latency, Jitter
- Lab 4: Emulating WAN with NETEM II Packet Loss, Duplication, Reordering, and Corruption
- Lab 5: Setting WAN Bandwidth with Token Bucket Filter (TBF)
- Lab 6: Understanding Traditional TCP Congestion Control (HTCP, Cubic, Reno)
- Lab 7: Understanding Rate-based TCP Congestion Control (BBR)
- Lab 8: Bandwidth-delay Product and TCP Buffer Size
- Lab 9: Enhancing TCP Throughput with Parallel Streams
- Lab 10: Measuring TCP Fairness
- Lab 11: Router’s Buffer Size
- Lab 12: TCP Rate Control with Pacing
- Lab 13: Impact of Maximum Segment Size on Throughput
- Lab 14: Router’s Bufferbloat
Lab Series: perfSONAR

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

- Lab 1: Introduction to the Capabilities of Zeek
- Lab 2: An Overview of Zeek Logs
- Lab 3: Parsing, Reading and Organizing Zeek Files
- Lab 4: Generating, Capturing and Analyzing Network Scanner Traffic
- Lab 5: Generating, Capturing and Analyzing DoS and DDoS-centric Network Traffic
- Lab 6: Introduction to Zeek Scripting
- Lab 7: Advanced Zeek Scripting for Anomaly and Malicious Event Detection
- Lab 8: Preprocessing of Zeek Output Logs for Machine Learning
- Lab 9: Developing Machine Learning Classifiers for Anomaly Inference and Classification
- Lab 10: Profiling and Performance Metrics of Zeek
Labs Series: NGFW - PAN

• Lab 1: Initial configuration
• Lab 2: Interface configuration
• Lab 3: Security and NAT policies
• Lab 4: Protecting networks using Application ID
• Lab 5: Protecting networks using Content ID
• Lab 6: URL filtering
• Lab 7: Decryption
• Lab 8: Sandbox malware execution
• Lab 9: User identification
• Lab 10: Global protection
• Lab 11: Site-to-site VPN
• Lab 12: Monitoring and reporting
• Lab 13: Active/Passive High-availability
Labs Series: SOC Cyber-operations

- Lab 1: Identify Running Processes
- Lab 2: Exploring Processes, Threads, Handles, and Windows Registry
- Lab 3: Windows Tools
- Lab 4: Linux Shell
- Lab 5: Linux Servers
- Lab 6: Log Files
- Lab 7: Navigating the Linux File System and Permission Settings
- Lab 8: Tracing a Route
- Lab 9: Wireshark: Ethernet frames, TCP 3-way handshake
- Lab 10: Exploring NMAP
- Lab 11: UDP DNS Captures
- Lab 12: HTTP and HTTPS (Sguil Network Security Analysis)
- Lab 13: Attacking a mySQL Server
- Lab 14: Snort and Firewall Rules
- Lab 15: Regular Expressions
- Lab 16: Isolate Compromise Host using Flow’s 5-tuple
Building a Cloud / Portal for Training

- Distributed cloud integrated into a Learning Management System
  - Learn: learner selects a self-pace training module
  - Teach: instructor selects a module to incorporate into course