Cybersecurity Virtual Lab Exercise and Facility Development
School of Information
College of Communication and Information
Faculty Contact: Dr. Shuyuan Mary Ho

1) Vision
As the complexity of cyber-infrastructure increases, the complexity and frequency of cyber-threats increases as well. As a result, corporate victims such as Target, HomeDepot, CitiBank, Sony, and JPMorgan Chase have suffered significant loss of business and reputation. According to the Center for Strategic and International Studies, cybercrime is a growing industry [2]. The Center for Strategic and International Studies [2] suggests that cyber-crime could be costing the global economy as much as $445 billion per year. Current threats include economic transactions, intellectual property and anything tied to the Internet. It is forecasted that automobiles and high-speed trains will also be subject to cyber-attack, as well as smart-grid power distribution infrastructure and nuclear power plants. This is an issue that must be addressed.

It is obvious that cyber-threats can exist both within and outside of information system perimeters (e.g., firewalls). Cybercriminals can penetrate existing security perimeter controls through holes and vulnerabilities in system design, errors in configuration, improper software coding and development, unsuitable architectural deployment, inappropriate business process, and due to attackers’ creativity. The process of securing cyberspace is an ongoing chess game between security professionals and cybercriminals. The threats themselves are dynamic – changing constantly – and so there are very few cookie-cutter responses. As such, we, as an institution of higher education, need to provide a technical skillset accompanied with a mindset that encourages critical thinking and creativity. This is the educational experience we will provide.

The 2013 ISC² Global Information Workforce Study [1] found an ever-widening gap between the supply of qualified information security professionals and the demand for skilled workers to secure critical information and cyberspace in general. The study shows that the workforce will grow at a compound annual growth rate of 11.3% globally between now and 2017, calling for an additional 2 million new workers. Thus far, open information security positions are largely unfilled; 56% of those responding to the survey feel their organizations currently have too few information security workers to manage current threats now, let alone in the future.

Education and technical experience is the best defense in today’s cyber-threat situations. In this proposal, we thus propose to create an educational experience that will directly support students who are preparing to make the transition to the front lines of cybersecurity in the workforce. The need for this was mentioned repeatedly at a recent workshop on Workforce Development at the National Institute of Standards and Technology (NIST) conference held at the University of South Florida [3]. Students need hands-on access to real-world technologies to prepare them for the challenges ahead.
2) Project Description

The project requires three (3) servers to provide a highly customizable virtual computing facility along with five (5) workstations designated for cybersecurity instructional exercises. Most of the information security courses will continue to use the existing School of Information’s instructional computer lab with a maximum 48-student capacity. Students who are members of the FSU Cybersecurity Club\(^1\) will have extended access to the 5 workstations requested herein. These workstations will be available to students within the space dedicated as a Cybersecurity Lab in Room 2011 of the William Johnston Building.

The servers providing the virtual computing environment will be securely housed alongside College of Communication and Information (CCI) production servers at the FSU Information Technology Services (ITS) data center at Innovation Park. These servers will be fully managed by CCI technical staff.

- Server 1: Back-end applications with incident monitoring equipment and simulation of a telecommunications service provider
- Server 2: Front-end applications for individual use, including open source firewalls, intrusion detection, web security, penetration testing, network forensics, honeypot deployment, etc.
- Server 3: Front-end applications for advanced coordinated cyber-defense exercises, including open source firewalls, intrusion detection, web security, penetration testing, network forensics, honeypot deployment, etc.

The proposed virtual lab will provide students with remote and secure access to cybersecurity exercises. Students will be able to work on penetration testing and cyber-defense exercises in a holistic fashion and in a secure manner. The proposed five (5) workstations will provide a jump-start environment for students to prepare for cyber defense competitions (e.g., Collegiate Cyber Defense Competition\(^2\)) and will provide students with thin-client accessibility to the remote exercise servers. There are several national and international competitions that will require the support of these workstations, e.g., CSAW Capture The Flag (CTF\(^3\)). Students will also require several browsers (for PC user) or downloadable applications (for Mac user) to access cybersecurity exercises on these servers. Overall, this project will enhance students’ learning experience regarding complex cyber defense topics with hands-on exercises, and will enable students to accomplish what they cannot (and should not) do in our traditional on-campus instructional lab exercises.

The proposed project will also require one undergraduate student to set up the Cybersecurity virtual lab and exercises. This is work that cannot be done by CCI HelpDesk student staff or project advisors. After initial set-up and development, the CCI HelpDesk will be equipped to support the ongoing activities. The student will be assigned with following front-end responsibilities:

---

\(^1\) Membership of the Cybersecurity Club is interdisciplinary (e.g., Law, Computer Science, Information Technology, Business, Public Administration, Education, Psychology, etc.), and is open to all enrolled FSU students.

\(^2\) National Collegiate Cyber Defense Competition http://www.nationalccdcc.org/

\(^3\) CSAW CTF https://ctf.isis.poly.edu/
• Assisting in physical setup of equipment in the Cybersecurity Virtual Lab.
• Initial configuration and system administration of the above-mentioned servers and workstations under the instructions of Advisors Mr. Garnett and Mr. Penley, and Dr. Ho.
• Development of cybersecurity exercises and instructions under the supervision of the designer Dr. Ho.

The student will benefit from this work experience, and gain professional experience of setting up a Cyber Defense Operation Center.

3) Impact on Instruction
The goal of this effort is to promote hands-on cybersecurity knowledge and skills utilizing industry-accepted best practices that will help students prepare for jobs protecting businesses from cyber-threats. The facility and curriculum is designed to immerse students in real-world simulations that will equip them with concept-oriented knowledge and skills, rather than industry or product-specific information. The curriculum will address intranet, extranet and service infrastructure at multiple levels. The hands-on exercises will be delivered in an isolated sandbox and include introductions to defensive and offensive penetration testing towards systems and networks with possible instructions of big data analysis perspectives and techniques. These exercises will allow participants to identify and quantify cyber-threats using a “big data” set that ties the concept of organizational risk to cybersecurity. The curriculum includes interwoven components that carefully address crafted learning objectives designed to teach students critical thinking skills along with working knowledge of the ever-shifting dynamics of cybersecurity intervention.

Current courses that will utilize the hands-on labs exercises are:

• LIS4774 Information Security
• LIS4777 Advanced Information Security
• LIS5487 Information Systems Management
• LIS5775 Information Security

The School of Information plans to develop new curricula in computing ethics, network forensics, penetration testing, intrusion detection, lawful interception, information systems auditing, and organizational security and privacy to prepare our students as future “Cybersecurity Profession-NOLES.”

4) Number of Students Affected
Students will use their FSUID to securely authenticate to the virtual lab with access the servers. Workstations will be placed in the Cybersecurity Club training and instructional lab currently located at Room 2011 of the William Johnston Building. Students can request access to the facility through the CCI HelpDesk. The annual number of students directly affected by this effort is currently about 600 (expected to increase as STEM-related students are recruited and collaboration across disciplines is encouraged), which includes:

• 253 students in the undergraduate major in Information, Communication and Technology (ICT)
• 219 students in the undergraduate major in Information Technology (IT)
• 29 students in the master of Information Technology (MSIT) and the doctoral programs in Information Science and Technology
• 100+ non-majors currently participating in Cybersecurity Club and events
• Future Cybersecurity Club\textsuperscript{4} participants (open to all FSU-enrolled students).

5) Project Plan
The Cybersecurity Virtual Lab will be installed, configured and administered at the FSU Information Technology Services (ITS) data center facility at Innovation Park. This facility is fully funded by the University and servers can be collocated at no additional cost within existing infrastructure. Access to the data center is secured by FSUCard swipe access. The facility has multiple security cameras for active and logged surveillance. All servers are protected by an uninterruptable power supply system with generator backups in case of power outages.

The Cybersecurity Club training and instructional design will be equipped with the proposed workstations and an immersive multimedia projection system capable of displaying rich multimedia content. Access to CCI RemoteApps, a previously Tech Fee-funded improvement will be fully configured and supported by the CCI HelpDesk and CCI technology staff.

6) Maintenance and Support
The CCI HelpDesk, comprised entirely by student staff and technology specialists, and CCI technology staff will provide ongoing maintenance and support. Failed computer systems over the next 3 years will be replaced under warranties included in the budget below. We will re-evaluate the usability of the Cybersecurity Virtual Lab should the existing equipment require an upgrade or replacement after 3 years. Any unforeseen costs will be paid from the regular College E&G funds.

\begin{center}
\begin{tabular}{|l|l|}
\hline
\textbf{Telephone & Walk-In Support Schedule}$^*$ & \\
\hline
Monday & 8:00 AM – 10:00 PM \\
Tuesday & 8:00 AM – 10:00 PM \\
Wednesday & 8:00 AM – 10:00 PM \\
Thursday & 8:00 AM – 10:00 PM \\
Friday & 8:00 AM – 5:00 PM \\
Saturday & 10:00 AM – 6:00 PM \\
Sunday & 1:00 PM – 10:00 PM \\
\hline
\end{tabular}
\end{center}

\textit{*The CCI Help desk is closed during holidays and home football games.}

7) Project Team
• Richard Garnett, Network Administrator, CCI
• Jason Penley, Manager, CCI HelpDesk
• CCI HelpDesk (student-based staff)
• One undergraduate student for set-up

\textsuperscript{4} Membership of the Cybersecurity Club is interdisciplinary (e.g., Law, Computer Science, Information Technology, Business, Public Administration, Education, Psychology, etc.), and is open to all enrolled FSU students.
Technology Fee Budget for Proposal

Title: Cybersecurity Virtual Lab Exercise and Facility Development
Organization: School of Information, College of Communication and Information

Equipment & Personnel

<table>
<thead>
<tr>
<th>Item Description</th>
<th>Unit</th>
<th>Unit Cost</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>PowerEdge R630 Intel Xeon E5-2603 Processors</td>
<td>3</td>
<td>$6,115</td>
<td>$18,345</td>
</tr>
<tr>
<td>iMac 21.5-inch Workstation</td>
<td>5</td>
<td>$1,338</td>
<td>$6,690</td>
</tr>
<tr>
<td>Undergraduate Student</td>
<td>1</td>
<td>$10/hr for 10-wk</td>
<td>$1,000</td>
</tr>
</tbody>
</table>

Total $26,035

References