2014

Building a Virtual Cybersecurity Collaborative Learning Laboratory (VCCLL)

Julien Murphy PhD
University of Southern Maine, jmurphy@maine.edu

Edward Sihler
University of Southern Maine

Maureen Ebben PhD
University of Southern Maine

Glenn Wilson
University of Southern Maine

Building a Virtual Cybersecurity Collaborative Learning Laboratory (VCCLL)

A. Julien Murphy[1], B. Edward Sihler[2], C. Maureen Ebben[3], D. Lynn Lovewell[4] and E. Glenn Wilson[5]

[1]Philosophy, University of Southern Maine, Portland, Maine, USA
[2]MCSC, University of Southern Maine, Portland, Maine, USA
[3]Communication and Media Studies, University of Southern Maine, Portland, Maine USA
[4]MCSC, University of Southern Maine, Portland, Maine, USA
[5]Technology, University of Southern Maine, Gorham, Maine, USA

Abstract - *In fall 2013, the Maine Cybersecurity Cluster (MCSC), was invited to assist the United States Coast Guard with cybersecurity training. MCSC conducted training activities that created the conditions under which Coast Guard personnel could experience and respond to cyber attacks first-hand. A major result of this endeavor was the recognition of two critical needs: 1) the necessity for a flexible, learning laboratory to address the increased security requirements presented by the Internet of Things (IoT), and 2) the need for applied education and training for students going into information assurance professions. To fill these gaps, MCSC designed plans for the creation of a Virtual Cybersecurity Collaborative Learning Lab (VCCLL). The lab would operate inter-institutionally and offer innovative, hands-on, collaborative learning experiences aimed at preventing and mitigating cyber attacks in real time. This paper delineates the background, design, and benefits of the VCCLL.*

Keywords

1. Cybersecurity, 2. Virtualization, 3. Education, 4.Training, 5. Laboratory, 6. Collaboration

1 Introduction

The chief objectives of Maine Cybersecurity Cluster (MCSC) are twofold: 1) to address network vulnerabilities across a spectrum of technologies in public and private sector organizations, and 2) to develop student education and skills around information assurance for workforce development. Central to cyber security education is the skill to detect network vulnerabilities. This skill is best acquired in an applied, dynamic, virtual laboratory, one that allows for students to uncover, understand, and resolve a variety of documented cyber security exploits in a practical manner [1]. The MCSC Virtual Cybersecurity Collaborative Learning Laboratory (VCCLL) will offer the opportunity for students to work in a collaborative culture and to engage in solving challenging cybersecurity problems. Matching student skills with the MCSC objectives, the VCCLL draws on a team of faculty and other expert practitioners to work with undergraduate and graduate students to study and resolve security issues. Students in this program will go on to careers in security work or pursue other IT professions, or, at the very least, will become more aware network users. The latter is vital to our increasingly wired and interconnected society--the Internet of Things (IoT)--that is rapidly becoming the norm.

2 VCCLL Background

The VCCLL concept arose from an earlier pilot project created by MCSC. MCSC built a small cyber range for the United States Coast Guard, Sector Northern New England, to provide training about security issues related to data vulnerabilities under shared network conditions. This training is necessary because there is no way to ensure absolute separation between an individual's online presence inside and outside of a work environment [2]. Constant vigilance is necessary and must include awareness and training beyond the typical worship of the complex password and avoidance of nefarious sites. Temptations for security breaches through the use of public and other outside networks arise, for instance, when employees travel and use networks at airports and hotels. Similarly, vulnerabilities exist in everyday life when individuals visit coffee shops and jump onto open networks. The VCCLL training is aimed at increasing participants' awareness and skills about data security, and is encapsulated in a set of exercises called. "Evil at the Coffee Shop" (ECS). The aim of these exercises is to sensitize participants about myriad cybersecurity exploits that can occur in routine and informal settings.

3 "Evil at the Coffee Shop" became the inspiration for the VCCLL

In order to understand how the "Evil at the Coffee Shop" (ECS) training inspired the creation of the VCCLL, it is helpful to describe its initial design in context. The request from the United States Coast Guard was to target non-IT personnel and provide them with a brief introduction that would make the cyber threat "real." An additional goal was to both supplement and reinforce mandated annual cybersecurity training. The ECS simulation was created to meet these goals. ECS was first deployed at an active US Coast Guard Base, Sector Northern New England. The simulation entailed disabling the Coast Guard network during a staged "crisis." In addition, the simulation was planned to occur at the same time as a disaster drill that included a simulated extreme weather event, an epidemic, and a hypothetical terrorist attack at a harbor or port.

The cyber range developed for the simulation was comprised of two laptops for end users, a wireless router, and two laptops acting as control with various virtual machines (VMs) to handle spoofed web pages and Domain Name System (DNS) changes. During this activity, three scenarios were experienced by participants: 1) control of DNS which sent the participants to a set of spoofed web pages, 2) a Denial of Service (DOS) attack, and 3) a phishing simulation. The experiential activity was followed up with discussion and critique. If time permitted or the participants' questions made it appropriate, a packet capture technique was also demonstrated. The expectation was that two Coast Guard personnel would participate at a time. However, the simulation attracted a group at least twice that size and higher, with the largest group numbering more than thirty Coast Guard personnel. When this consistently occurred, we knew we were on to something.

Synopsis of "Evil at the Coffee Shop":

- Users surf the web
- Activate the spoofed web pages and suggest the Coast
  Guard personnel surf to one of them (i.e., CNN, Fox News, or Yahoo) and discuss how the Domain Name System (DNS) changes impacted the "look and feel" of the page
- Have the group surf to a page that requires a login (e.g., Facebook, Linkedin, etc.); show participants that we could capture their password
- Discussion of https versus http. Demonstration of packet sniffing
- The question of how to get users onto our "bad" or "poisoned" network would always be raised and thus a DOS would be demonstrated and explained
- Phishing techniques were demonstrated. For example, how to read the headers and links for indications of phishing with a fake Amazon email

Several lessons were learned from the "Evil at the Coffee Shop" (ESC) pilot simulation, and these are taken into account for the design of the VCCLL. Lessons include:

- Reviews and observations of the exercise indicated that each participant needs to have his/her own laptop, simply watching others is not nearly as engaging and effective
- Setup time is about 20 minutes with two researchers/instructors helping
- Giving participants about 10 minutes to surf and become comfortable produces a bigger "a-ha" moment when directed to a spoofed page
- Participants almost instantly recognize that the DNS exploit could be executed in any number of public venues
- Exactly what phishers were trying to do is very clear to participants from the earlier DNS exploit
- The logical progression of "this is what can happen in a public place" to "this is what can happen via an email" is why an expired and self-signed certificate are a cause for alarm

4 VCCLL Design

While the "Evil at the Coffee Shop" simulation worked well at a small scale, the plan is to build out this concept to afford more sophisticated training for IT students, as well as offer basic level training for non-IT persons. The VCCLL is designed to be flexible to serve both university students as well as the larger community and organizations. Located within the currently existing MCSC Cybersecurity Research lab, the VCCLL will use remote nodes made up of virtual machines to run different simulations. The virtual machines would be configured to simulate a real-time complex network environment. For on-site nodes, Linux will serve as the base operating system, with virtual machines installed as the user operating system(s). Nodes will be linked via a Virtual Private Network (VPN) to merge the nodes into a single private lab.

The objective is to develop and evaluate the feasibility of an inter-institutional, virtual cybersecurity collaborative learning laboratory to foster teamwork among undergraduate and graduate students across distances [3]. The VCCLL would link three virtual laboratory nodes: one at York County Community College, one at the University of Maine at Fort Kent, and one at University of Southern Maine (head node). Students from remote areas of Maine would be able to work with students from Maine's economic and population center in Portland. This design meets the five criteria for a virtual cybersecurity laboratory: 1) increase advanced, hands-on learning in networking and security courses; 2) reduce cost and the need for specialized computer labs; 3) provide an agile

and secure computer environment for information assurance (IA) education; 4) foster collaboration and teamwork among students in distant locations; 5) enable inter-institutional collaboration for shared resources in cybersecurity education.

The VCCLL is designed to accommodate fifteen to forty-five students depending on the simulation scenario and required roles. To participate in the simulations, students are required to have basic knowledge in networking and related information security. At the outset, students will be given an outline of the goals and objectives of the project and information explaining how these are integral to the goals and objectives of their courses, including the ways in which professional ethics and strategic communication play a role in information security systems and practices.

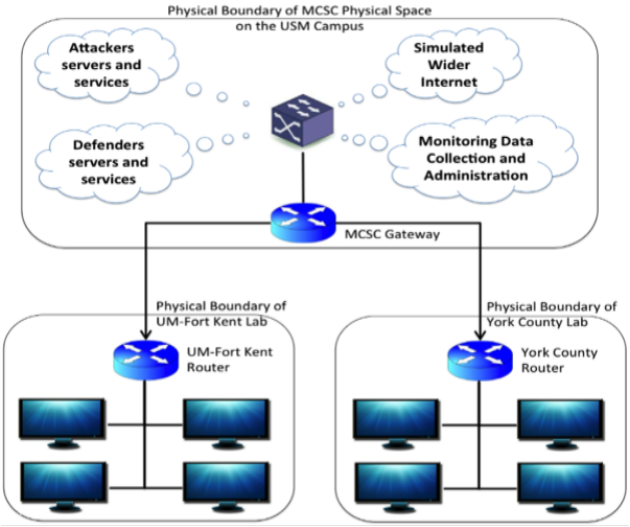

Figure1
Maine Virtual Cybersecurity Collaborative Learning Laboratory
Notes: The elements denoted by clouds within the USM MCSC space are part of the base Cybersecurity Research Laboratory. The links between the sites will take place over VPNs to ensure that the hosting institutions are protected from activities within the lab. The virtual lab does not have any connections to either the hosting institutions networks or the wider Internet.

Figure 1 illustrates the flow of activities in the VCCLL. The expectation is that the VCCLL concept will surpass existing models by developing challenging exploit scenarios that require participants to: 1) learn and exercise highly developed interpersonal, collaborative skills; 2) generate specialized exploit mitigation skills; and 3) blend both of these skill sets while working in a dynamic virtual environment [4]. A unique aspect of the VCCLL is the affordance of achieving the foregoing with students from disparate geographical and cultural regions in Maine through randomizing exploit scenarios and team membership. This closely resembles the real-world conditions which ensue upon the discovery of exploits. The aim is to prepare students for the escalating complexities that emerge before, during, and after exploits, and for students to become accustomed to working in realms where rules and roles change, and lives and major assets are at risk. Further, the VCCLL concept employs a three (3) node network that integrates two scenarios that exemplify common and frequent exploits into cybersecurity classes. These cybersecurity events are integral to the courses, and planned for prior to the event, with role and protocol assignments. They conclude with a debriefing and evaluation session--a post event "hot wash." All students have the opportunity to partner both locally and remotely across virtual distances and will develop techniques and procedures for effective communication and collaboration [5].

5 Creation of simulation scenarios for the VCCLL

The VCLL design and pedagogy builds on the experiences and insights gleaned from the "Evil at the Coffee Shop" (ECS) Coast Guard training pilot. MCSC faculty, staff, and other experts comprise the "Coffee Shop Team" and are charged with the creation of innovative, collaborative, and resource-shared cybersecurity simulation scenarios. Criteria for the scenarios are that they reach across diverse rural and urban cultures to strengthen the foundation of computer offense and defense security knowledge. Each simulation must be designed to last approximately four hours to allow for participants to apply collaboratively offensive and defensive skills and techniques. Distributed Denial of Service (DDOS) and Malware Eradication will continue to be refined as exploit scenarios for the VCCLL. Other simulation scenarios include general and common exploits such as: understanding the impact of Domain Name System (DNS) spoofing; understanding the differences between http and https and why those differences matter; understanding how a Denial of Service (DOS) attack can be used to drive users to a malicious access point, and using basic tools for differentiating phishing emails. The Coffee Shop Team hopes that the training is infectious and spreads to friends, colleagues, and associates of end-users, in part, by the increased awareness of participants and the need to share this so all can act to secure the network. Further examples of VCLL exercises include:

DDOS "Hactivists": In this exercise, participants learn to identify the major components on the network (improve documentation); identify the nature of the attack; select and configure effective teams; request help from outside; deploy help; respond to the attack; and contain the attacks.

Malware Eradication: Participants identify the nature of the outbreak; build and maintain records that reflect spread, investigation, and eradication; select and establish effective teams; use external sources to categorize and identify malware; request external help; deploy help; contain the attack. In addition, participants learn to communicate effectively with management about the event including investigation, efforts to eradicate,

advocacy for contacting outside resources, and communicate effectively with end users about the event.

Integration of Professional Ethics and Strategic Communication Skills: Participants gain increased understanding about when, how, and with whom to communicate network vulnerabilities and security breaches. This aspect of security may be just as important as awareness. The Coffee Shop team for the VCCLL will include a professional ethicist and a communications expert. This interdisciplinary aspect of simulated security attacks will allow participants to explore underlying reasons for responsible use of the internet, the importance of security for the ethical values of privacy and confidentiality that allow for autonomy and maintain civil society.

6 VCCLL Benefits

The VCCLL offers benefits that are lacking in current virtual models. First, the laboratory provides an in-lab experience using real world breaches [6]. This mirrors the working environment found in medium size or larger organizations. The geographic diversity of the ad hoc teams reflect structures often found in government and industry security groups. Using well-established and relatively common exploits in the virtual laboratory, students will experience multi-dimensional / multi-way simultaneous attacks and will be trained to address, correct, and guard against such activities in an ad hoc collaborative setting.

Second, central to the virtual laboratory model, is that students understand and appreciate the value of working in effective ad hoc teams in a highly decentralized laboratory--where they may or may not have peers with their levels of technical expertise physically present. This means that students will have to be confident in their ability to communicate and collaborate using technologies that, as yet, cannot convey the complete subtleties of *in situ* human interaction. This scenario has particular relevance to SCADA systems that are often physically remote and require local personnel to act as the security teams eyes and hands. Students will have to communicate using remote systems, and they will have to make decisions collectively and execute them without the luxury of physical presence. In the traditional classroom setting, an intervention or repair may be difficult, and a team decision will have to be made, but there is comfort for students in that they can discuss the solution in real-time and in each other's presence (with all the non-verbal cues that humans rely upon) in a critical situation.

Third, students and their teams learn to communicate effectively on many levels and often at off hours or during extreme conditions. Such extreme conditions make regular communication difficult or strained. Adding the factors of massive outages of data or physical infrastructure, remote, long distance, and or virtual communications frequently fail. These failures and their solutions are addressed in the VCCLL. Frequently, capacity building models address research and development on a particular topic. In this case, the research and development both targets the virtual environment and uses the virtual environment and its tools, techniques, and culture.

7 VCCLL Integration

Lastly, the VCCLL is fundamentally interdisciplinary integrating tactical knowledge in cybersecurity with fundamental principles in strategic communication and professional ethics. Strategic communication concepts and practices are enacted including proactive, pre-crisis planning, ongoing communication management across work activities and groups, and post-crisis strategic response deployments. Through these activities students gain appreciation of communication behaviors that may influence crisis prevention and outcomes such as patterns of interpersonal and small group communication and decision making, forms and methods of communication with stakeholders, and effective use of media to communicate information about the crisis. Professional ethics are considered in terms of personal privacy, confidentiality of financial and personal information, and the importance of the ethical value of trust, which is often at the heart of all cybersecurity undertakings. Trust is central to maintaining personal autonomy and to securing the integrity of social and virtual networks [7] [8]. Trust includes trusted systems, nodes, and identification, which are all subject to attack or subversion. The model also includes the trusting relationships among students (student to student individually or in teams) or students to machine(s). Without the interpersonal (and person to machine) trust developed transactionally through solid communication practices, collaboration will not take place or will dwindle rapidly.

8 Results

Over time, it is envisioned that the VCCLL concept could be scaled up and applied to training for the general public who are now consumers and users of products and services that inherently carry security risks in the world of the Internet of Things (IoT), including networked homes, schools, libraries, and offices. The chief outcome of any successful VCCLL is increased participant awareness and caution around security along with deeper understanding of the responsibilities of network users to others beyond specific networks. While the VCCLL could be reconfigured to support SCADA breaches, educating non-IT staff using and supporting these systems about cybersecurity would greatly enhance the security of these systems. Anticipated results suggest improvements in the logistical design and implementation in virtual network nodes and information will aid in the successful execution of exploits in a distributed virtual collaborative laboratory over distances.

VCCLL ideas and concepts have been further developed and submitted to the National Science Foundation as a proposal under the CyberCorps Scholarship for Service program.

9 Conclusions

From the work with the US Coast Guard and our students, it is clear that there is a proven and appreciated need for hands on and real-world activities and training on typical cyber security exploits. Such injects are both fascinating to the everyone, whether they are seasoned IT workers or undergraduate students. Moreover, both groups need continued and upwardly scaling (quantity and complexity) experiences across geographic regions, networks, systems, and scenarios. Therefore, the establishment of a highly scalable virtual cyber security collaborative cyber range is a logical next step based on the prelminary work done over the last year at the Maine Cyber Security Cluster. Further, the need for a collaborative interdisciplinary approach is essential to establish effective communication and ethical behavior combined with technical expertise in order to overcome cyber security exploits.

10 References

[1] Nance, K., Hay, B., Dodge, R., Seazzu, A. and Burd, S. (2009). Virtual Laboratory Environments: Methodologies for Educating Cybersecurity Researchers. Methodological Innovations Online, 4(3) 3-14.

[2] Kott, A. (2014). Towards Fundamental Science of Cybersecurity. Network Science and Cybersecurity, Advances in Information Security. Volume 55, pp 1-13.

[3] Bonabeau, E. (2013). Cybersecurity: Human Behavior Matters. Icosystem Corporation. Retrieved from http://www.icosystem.com/cyber-security-human-behavior-matters/ on February 13, 2014.

[4] Viveros, M. and Jarvis, D. (2013). Cybersecurity education for the next generation: Advancing a collaborative approach. Center for Applied Insights. IBM Corporation.

[5] Willems, C., Klingbeil, T., Radvilavicius, L., Cenys, A., and Meinel, C. (2011). A distributed virtual laboratory architecture for cybersecurity training. Published in 2011 International Conference for Internet Technology and Secured Transactions (ICITST). Pp 408-415.

[6] Zlateva, T., Burstein, L., Temkin, A., MacNeil, A., and Chitkushev, L. (2008). Virtual Laboratories for Learning Real World Security. Proceedings of the 12th Colloquium for Information Systems Security Education. University of Texas, Dallas, TX June 2 – 4.

[7] C. Ess and Thorseth, M (2011). Trust and Virtual Worlds. Peter Lang Press.

[8] Vallor, S. (2012). Flourishing on Facebook: Virtue friendship and new social media. Ethics and Information Technology, 14 (3). 185-199.