Cyber Operations Education: Building Capacity in a Priority Area

Kara Nance
Department of Computer Science
University of Alaska Fairbanks
klnance@alaska.edu

Robert Wesley McGrew
Department of Computer Science
Mississippi State University
mcgrew@cse.msstate.edu

Abstract

IT systems are, without a doubt, fundamental to almost all facets of modern life, including government operations, commerce and manufacturing, financial systems, education, communications, energy production and distribution, and transportation. However, given the global connectedness of such systems, they are under constant attack from a variety of actors ranging from automated malware and so-called script kiddies, to organized crime and nation states around the world. A great deal of work has been performed to improve cyber security education, with the dual aims of building a workforce to protect our critical infrastructure, and producing researchers capable of meeting the challenges apparent today, and those that we will face in the future. This paper describes some of the challenges associated with developing educational capacity in cyber operations and some approaches that can help to mitigate these challenges.

1 INTRODUCTION

U.S. agencies have invested in many important projects to help to educate the next generation of cybersecurity workers in order to address the important national need to protect our digital assets. This paper describes how some NSF-funded educational successes in cybersecurity have been used as a foundation and adapted to build educational capacity in the emerging field of cyber operations. The goals of this ongoing effort include the following:

1. To produce high-quality easily-deployable cyber operations scenarios and educational materials to educate students nationally on these important topics.

2. To provide educational materials and faculty development opportunities to build faculty expertise nationally in cyber operations.

3. To evaluate and assess the usage of the materials and apply this information in ongoing curriculum improvement.

4. To deploy these materials in the NSF-funded Remotely Accessible Virtualized Environment (RAVE) infrastructure so that they are available nationally to faculty for use in their courses.

2 BACKGROUND

Information assurance (IA) is the use of "measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality and non-repudiation" [1]. IA is both multidisciplinary and multidimensional field of study [2], and as information systems becomes even more embedded in all facets of modern life, IA is an area of vital importance to society at large. In the United States, jobs in Computer Networking, Systems, and Database Administration, all of which have significant IA components, are expected to increase 23% from 2008 to 2018 [3], which is a substantially higher rate than is projected for many other academic disciplines. This growth will be due in part to the increasing need for information security as cyber-attacks are more frequent and more sophisticated. In October, 2009 the Department of Homeland Security announced a requirement to hire an additional 1000 computer security professionals. [4] This announcement was met with a tremendous amount of speculation about the existence of 1000 capable individuals. [5-8] In order to help educate computer security professionals, educators need to provide them with learning scenarios similar to the situations they need to be prepared to handle.

Beyond just the immediate impact on the technology domain, IA is vital to areas of the economy and modern life that are far less obviously dependent on IA.
Manufacturing, finance, education, national defense, energy, transportation, and a host of other economic sectors are dependent on technology for daily operations, research and development, and long-term viability. As such, the ability of our economy to function is quite directly tied to our ability to design, build, and maintain technologies that can withstand the types of cyber-attacks that are even today increasing in volume and complexity.

Given the importance of IA to modern society, it is vital that we prepare students to meet the demands of our technology-dependent workplaces, and to take on the research challenges we still face in the IA domain. To address those requirements, many higher education institutions have incorporated relevant topics into their curricula, either as entire degree programs, one or more stand-alone classes, or by integrating new material into their existing course offerings. Other efforts include many IA-focused research projects at the graduate level, and the development of multiple educationally focused security competitions such as the CCDC, NYU Poly CSAW, and University of California Santa Barbara iCTF [9-11], to name only a few.

The federal government, in an effort to attract more people to the IA profession and improve the state of information security for the nation, has also implemented some programs focused in the IA domain. Through the National Security Agency and the Department of Homeland Security, educational institutions can receive recognition as a Center for Academic Excellence (CAE) in Information assurance, based on an evaluation of their educational, research, and outreach programs [12]. The CAE-IAE program has certainly received its share of criticism over the years, but at a minimum it does provide a community of institutions with capacity in, and a focus on, IA. To address some of the criticisms, and also to increase the breadth of specializations within the program, new CAE designations have emerged supported by various government agencies.

- **CAE/IAE** – Sponsored by the National Security Agency and the Department of Homeland Security, this was the first CAE program and certifies National Centers of Academic Excellence in Information Assurance Education
- **CAE-IC** - The Intelligence Community Centers of Academic Excellence Program was originally sponsored by the Office of the Director of National Intelligence (ODNI), although the program was recently shifted to DIA. This program focuses on a more multidisciplinary approach to building a cadre of scholars for the IC as well as national security positions in industry, public service, federal government, and non-governmental sectors. [13]
- **CAE-R** – Sponsored by the National Security Agency and the Department of Homeland Security, this program certifies National Centers of Academic Excellence in Information Assurance Research
- **CAE2Y** – Sponsored by the National Security Agency and the Department of Homeland Security, this program certifies National Centers of Academic Excellence in Information Assurance 2-Year Education focusing on community colleges.
- **CAE-CO** – The CAE-Cyber Operations program is the newest of the CAE programs and complements the existing Centers for Academic Excellence (CAE) in Information Assurance Education (CAE-IAE) and Research (CAE-R) programs, providing a particular emphasis on technologies and techniques related to specialized cyber operations (e.g., collection, exploitation, and response), to enhance the national security posture of our nation. These technologies and techniques are critical to intelligence, military and law enforcement organizations authorized to perform these specialized operations. [14]

There are several initial challenges for an institution that wants to develop capacity in information assurance. Some basic challenges include faculty development, content development, and providing educational environments in which students can gain valuable hands-on experience. The content described herein provides experiential learning for students and faculty in all of the above programs, as well as for programs who are trying to build capacity to apply for one of the above programs. While the content areas for all of the above overlap, the focus of this effort is developing educational materials and capacity for the Cyber Ops arena with an emphasis on experiential learning. As studies have shown, experiential learning is a key element in increasing the likelihood that students will remember what they have learned [15], hands-on exercises have a strong impact on student learning outcomes [16], and discovery learning helps to develop autonomous learning, an important trait for IA students. Lab exercises are as important to the study of IA just as the use of science labs are important to a complete understanding of the material in many Biology, Chemistry, or Physics courses [17].

However, teaching hands-on IA skills has many challenges [18]. IA activities and labs often involve the deliberate use of tools and malicious software [19], which creates the potential for either a student using unauthorized tools and techniques on external networks and systems, or the inadvertent release of malware into external environments. As a result, proper isolation of an IA lab environment is a vital component of providing hands-on IA lab activities. This requirement can result in IA labs that are difficult to build, require expensive (and
dedicated) equipment and space, and are costly to maintain [20].

These issues are compounded in distance education environments. While it can be challenging to build an IA lab for on-site students, it is even more difficult to provide a suitable IA lab environment for students who may live across town, the nation, and even the planet, particularly in light of the requirement that activities in an IA lab are effectively isolated from access to external systems. However, there are some efforts already underway to address this need, including the currently operational and nationally accessible Remotely Accessible Lab Environment (RAVE) infrastructure. While many institutions are using the RAVE environment for cybersecurity education, the application of this domain to cyber operations is lagging the other areas.

3 CYBER OPERATIONS

Cyber Operations (Cyber Ops) are concerned with technologies and techniques related to specialized cyber operations (e.g., collection, exploitation, and response), to enhance the national security posture of our nation. These technologies and techniques are critical to intelligence, military and law enforcement organizations that are authorized to perform these specialized operations. [21] Since they can be offensively focused, many institutions are unable or unwilling to provide hands-on experiences in this area. This can inhibit the opportunity to build the faculty expertise in this area necessary to champion the creation of more educational programs in cyber operations.

In the original academic criteria for becoming a CAE specializing in cyber operations, ten mandatory content areas were identified [22]:

1. Low Level Programming (C and Assembly Language)
2. Reverse Engineering (Software, Malware Analysis, Tools & Techniques, Communications)
3. Operating System Theory (Internals, Operation, etc.)
4. Networking (Protocols, traffic analysis, etc.)
5. Telecommunications (Mobile, Telephony, Infrastructures, Core Network)
6. Discrete Math (logic graphs, algorithms, statistics, automata)
7. Overview of Cyber Defense (many subtopics)
8. Security Fundamental Principles (domain separation, policies, applied cryptography, etc.)
9. Vulnerabilities (Root causes, Buffer overflow, Privilege escalation attacks, Rootkits, Malware)
10. Legal (Law, Regulations, Directive, Policies, etc.)

Many of the criteria specifically listed hands-on experiences for students as a requirement. That requirement is indicative of the importance that the agencies feel hands-on experience should be given, but providing such experiences does have several inhibiting factors, which can be reduced significantly reduced by sharing the infrastructure and scenario development efforts as follows:

- **Infrastructure Cost:** As discussed previously, the infrastructure required to provide hands-on experiences can be costly to purchase, deploy, and manage, and often sits idle as it often cannot be shared with other activities (such as a shared purpose lab). This project addresses this factor by using the existing (and expanding) RAVE infrastructure.

- **Development and Set-up Time:** Development of high-quality lab exercises can be time consuming (and even beyond the skill-set of many instructors who could otherwise teach the material). Even shared materials can require significant alteration to fit within a new physical environment as they move from institution to institution. This project addresses this factor by deploying materials to a common platform, and allowing institutions to share more easily.

- **Functional Challenges:** The types of activities performed in Cyber Ops exercises can result in systems that are no longer functional (without a reinstall), infested with malware, or otherwise mis-configured. In addition, participants often need full control of the environment (i.e., super user access), and the ability to easily reset to previous states on demand. This project addresses this factor by providing participants with full control over their assigned systems (from the BIOS and virtual hardware level upwards), the ability to for the students, instructors, or administrators to revert to previous states instantaneously, and the ability to deploy systems to large numbers of participants on demand.

- **Instructor expertise:** Instructor expertise is important during both the development of materials and in their delivery to students, and many instructors do not have direct experience in the Cyber Ops domain. This project addresses this factor by providing materials that can be easily shared, and by providing instructor resources (such as recorded, narrated walkthroughs of exercises) and faculty development opportunities and materials.
4 SCENARIO DEVELOPMENT PROCESS

The content developed by the Cyber Ops domain experts is being coupled with the rich array of templates available in the RAVE environment. Together, this results in evolving Cyber Ops educational units that address individual learning topics as well as end-to-end scenarios that incorporate all of the phases of the Cyber Ops life cycle. The ongoing plan for the project includes steps for scenario development, evaluation, and deployment, which is using an evolutionary production model with the following distinct phases:

- **Identify Materials to be Developed**: Based on the needs assessment, the project team develops a set of development priorities, and also determines whether each item in that list requires the development of new content, or can be met by augmenting or updating existing content. These materials may include virtual machines, scenario descriptions, instructions for instructors and students, and assessment materials to evaluate the students’ performance.
- **Identify Scenario Developers**: Once the materials to be developed have been identified and prioritized, the team solicits appropriate domain experts to lead the development effort(s). These may include RAVE personnel (to aid in the deployment of VMs and networks for the scenario) as well as cyber-ops experts from a variety of institutions. These scenario developers have been solicited from the existing CAE-CO institutions, as well as the rich pool of faculty experts who have been successfully developing content for the RAVE environment over the past 5 years.
- **Develop Materials**: Once the development team for a given priority area has been assembled, they are free to develop materials to address the needs of their assigned priority area.
- **Evaluate Materials**: There is an evaluation plan that describes how developed content will be deployed to an initial population in concert with appropriately designed evaluative research instruments, allowing the project team, and the development team, to gain insight into how effectively the materials meet the needs of the priority area. (The results of this step may result in further development work to address any areas of concern.)
- **Deploy Materials**: Once the content has been determined to successfully address the needs of the priority area, it is deployed for widespread use. The primary deployment environment for these materials has been the RAVE, but other options are also be available (including the distribution of OVF formatted virtual machines where appropriate for easy import into a variety of virtualized environments).

5 SCENARIO DEPLOYMENT

By utilizing the RAVE as a deployment environment for the materials developed during this project, institutions throughout the nation will be able to immediately benefit from this effort. RAVE provides accredited nonprofit US colleges and universities with no-cost access to remotely accessible lab environments, and as these new cyber-ops scenarios are added to the RAVE library, they are immediately available for deployment to instructors, students, and researchers nationwide.

In addition, the virtual machines can be exported from the RAVE to other approved environments (allowing, for example, an institution to run local versions of these scenarios on a variety of virtualization platforms, if so desired). We also envision institutions augmenting or updating these scenarios, and in return for the use of RAVE resources, we actively encourage instructors to contribute such derivative works back into the RAVE library (again, making them available to other institutions).

6 MEASURABLE OUTCOMES

The project is being evaluated in a number of ways, with the goal of ultimately determining its impact of the ability for students to perform common cyber operations tasks. Some factors are easy to measure. For example, we can easily measure the number of scenarios developed, and the numbers of students and classes to which those scenarios are deployed. In addition, pre- and post-testing has been applied by some instructors to determine the effectiveness of the scenarios in communicating cyber ops topics to the target student populations. However, we also expect to be able to measure more specific outcomes, such as the extent to which skills learned in the RAVE environment can be transferred to environments in which cyber-ops are typically conducted, thus ensuring that we are not merely teaching students how to “fly a simulator”,
but are instead providing them with skills that transcend the environment in which they were learned.

7 CONCLUSION

This effort builds on a successful NSF-funded infrastructure project (RAVE) to develop, evaluate, and deploy high-quality, culturally appropriate materials focused on Cyber Operations. These materials will be made easily available to instructors and students throughout the nation at no cost (although faculty members who make use of them will be encouraged to share any improvements they make with the wider community). This is an exciting project with the potential for maximum benefit as the RAVE infrastructure is in place to deploy the educational materials at a national level immediately, quickly increasing the nation’s capacity to educate faculty and students in this important area. While the preliminary materials will target educating faculty and students, there are no firm boundaries around the topic or target audiences. The topical subcomponents of cyber operations can be used to strengthen a wide variety of courses in computer science in general and cybersecurity in specific. Further, instructors can modify and readapt the materials to new audiences and contribute the enhanced version back to the RAVE, creating momentum for ongoing capacity building in this important area.

8 REFERENCES


