

Cyber Security Education for Liberal Arts Institutions

Xenia Mountrouidou
mountrouidou@cofc.edu
Department of Computer Science
College of Charleston
66 George St., Charleston, SC

Xiangyang Li
xyli@jhu.edu
Information Security Institute
Johns Hopkins University, Whiting School of Engineering
3400 North Charles Street, Baltimore, MD 21218-2608

Abstract - Cybersecurity is a broad, dynamic, and ever-changing field that is difficult to integrate into undergraduate Computer Science (CS) curriculum. The absence of sanitized labs coupled with the requirement of specialized faculty to teach the subject pose obstacles many primarily undergraduate colleges face in adopting cybersecurity education. In this paper we describe a set of labs that have been implemented using the Global Environment for Network Innovations (GENI) cloud infrastructure as a solution to teaching experientially with low overhead. These labs are developed for different levels of experience, based on Capture The Flag (CTF) competitions that include short questions and answers, scenario based exercises, and upper level research skills. Curriculum for Liberal Arts Institutions is presented starting from the core general education as a vehicle to bring cyber security to a diverse population of non-CS majors and moving to introductory and upper level CS courses. These labs and curriculum are part of the project CyberPaths (Cyber security Paths) with goal to broaden the path to cybersecurity profession for a diverse population of Liberal Arts students.

Keywords

Cyber Security Education, Experiential Learning, GENI, General Education, Liberal Arts

1 INTRODUCTION

Recently cyber security has received attention in the news that has been unprecedented. Attacks on critical infrastructure, data breaches, ransomware, cybercrime and cyber warfare, privacy and encryption, are a constant reminder in the media that brings more visibility to the field. Due to the publicity, academic institutions and Computer Science (CS) departments have been increasingly urging for the creation of cybersecurity programs.

The ACM curriculum guide [1] has made cybersecurity a mandatory knowledge area and CS departments are seen with various initiatives of integrating it to their curriculum. Furthermore, there are increasing efforts to create new undergraduate, accredited programs in computer security [2]. All these efforts strive to meet an increasing demand of cybersecurity professionals with a much faster job growth at 18%, compared to the national average of 7% [3].

Although there is increasing interest in the field, teaching cybersecurity, in small, primarily undergraduate, liberal arts institutions, is not a trivial task. One of the difficulties to add more topics is that the undergraduate curriculum is already overloaded with fundamental CS topics. Furthermore, introductory courses CS1 and CS2 are already overloaded with material on programming and fundamental problem solving. Faculty hiring is not always feasible due to budget constraints. Furthermore, considered to be one of most effective pedagogical methods, experiential education of cybersecurity requires lab experimentation in sophisticated, sanitized labs. This may be impractical for primarily undergraduate, liberal arts schools that do not have an engineering school with funding and labs available.

There are several relevant education projects that aim to offer solutions to address the above challenges. Security Injections [4] is a project that teaches secure

coding early, starting from the intro to programming CS1 and CS2 courses. However, these programming courses are already overloaded with material for problem solving, object-oriented principles, and data structures, which makes it hard to add one more topic, such as security. SecKnitKit [5] is an education project with the goal to add cybersecurity modules to upper level CS courses, such as computer networks, operating systems, and databases. This project uses Virtual Machines (VMs) that lack realism and discovery opportunities for the students. EduRange [6] is a project based on the amazon cloud that aims to teach cybersecurity experientially. This project is an interesting approach on using the cloud, however not all network attack and defense experimentation is feasible in a commercial cloud infrastructure. Catalyzing Computing and Cybersecurity in Community Colleges (C5) [7] is an NSF-funded project with goal to create a nationwide network of community colleges that have met the national standard Center of Academic Excellence in Cybersecurity (CAE). The project offers materials, such as exercises and slides, to facilitate teaching the CAE knowledge areas [8] that have been defined by the National Security Agency.

Different to the above, the project CyberPaths¹ aims to add cybersecurity in a non-intrusive way in the general education and to create customized learning opportunities for further study of cybersecurity, while minimizing the requirement of investment in faculty and equipment and avoiding radical changes to existent curriculum. First, this project overcomes the lack of sanitized labs by adopting a cloud infrastructure to introduce experiential cybersecurity learning labs. These cloud-based labs offer real and not virtual machine experimentation in contrast to SecKnitKit [5]. Second, it offers multiple educational paths for students to be exposed to and learn cybersecurity topics. It starts with standalone educational modules that are integrated in general education courses, then offers cybersecurity courses that are inclusive for any major, and finally builds up expertise through upper level courses and capstones.

¹ <http://blogs.cofc.edu/cyberpaths/>

We leverage the power of cloud computing infrastructures, such as the Global Environment for Network Innovations (GENI) for emulation experimentation and discovery learning. GENI is an academic cloud, therefore research experimentation with cyber-attacks and programmable Software Defined Networks offer a flexibility unparalleled to a commercial cloud such as Amazon cloud used by EduRange [6].

One critical goal of this project is to introduce security in early stages of general education courses in CS and other disciplines, such as political science and economics. Thus, it has the potential to attract talents of diverse background to consider education and career in cybersecurity and, more generally, in STEM.

This paper is organized as follows. In Section 2 we describe the project CyberPaths in detail, its goals and what has been done so far. Section 3 gives a detailed description of the GENI cyber security labs and the general education modules. Section 5 presents the general education course and cyber security curriculum that offers an opportunity to non-CS majors to experience the field.

2 PROJECT CYBERPATHS

The project CyberPaths [9] (Cybersecurity Paths) aims at taking advantage of the general education arena to create a diverse population of cybersecurity professionals. Understanding cybersecurity through the core disciplines of political science, business, and humanities. Cybersecurity is introduced in the context of multiple disciplines; to additional technical courses that may lead towards a CS cybersecurity degree or concentration. Several paths to cyber security education are offered as options to the interested students. As seen in Figure 1, students attend a general education class where they get introduced to a concept through a cyber security module (Cohort A), continue further and take a CS intro to cyber security course (Cohort B), complete a CS minor or major (cohort C.1, C.2).

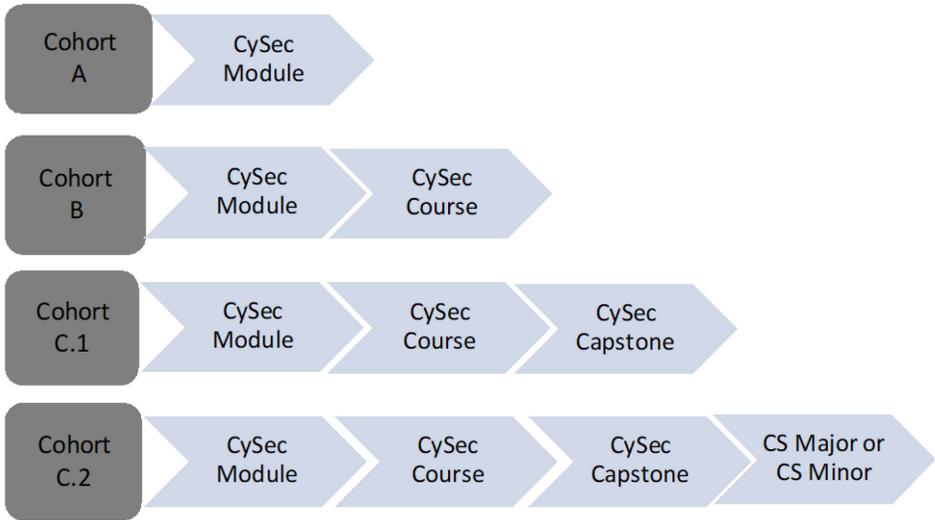


Figure 1: Paths to cybersecurity education.

The goal is not necessarily to turn every student who takes the initial core class into a cybersecurity major over their college careers; rather it is to provide greater reach to students with a baseline understanding of what cybersecurity is and why it matters, while simultaneously developing a new pipeline for recruiting (and retaining) students with diverse qualifications and interests. Its vision is to develop not just technicians, but also policy makers and business professionals who understand cybersecurity fundamentals of how to protect themselves and their organizations. In addition to technical lab modules, the CyberPaths project suggests several non-technical modules that can be integrated in general education courses as seen in Table 1. For example, a general education class related to international conflict may include a module on cyber-conflict; a general education class on finance may include cybersecurity investment module.

General education is a flagship of liberal arts colleges in order to develop student personalities and prepare well-rounded citizens with an appreciation of the basic sciences, humanities and arts. Implementations of general educations in Liberal Arts

schools vary from groups of knowledge areas, to groups of courses, to specific courses. The most common knowledge areas of general education are: aesthetic and interpretive understanding, culture and belief, empirical reasoning, ethical reasoning, science of living systems, science of physical universe, societies and the world, the United States and the world. Thus, most schools include a law, policy, humanities, social or political science requirement in their core curriculum. Moreover, a large majority of schools have a technology requirement that needs to be satisfied within every major. Thus, the standalone introductory course modules seen in Table 1 revolve around: policy, law, privacy, social, and economical issues of cyber security, as well as some introductory technology concepts. The goal is to facilitate any school to use these materials in their general education curriculum.

Table 1:
 Learning modules for general education courses

Standalone Module	Topics	LIA Curriculum
Legal issues	HIPPA/FERPA, Computer Security Act, Laws and Authorities, US Patriot Act	Political Science International Studies Social Science
Management	Operational, Tactical, Strategic Plan and Management, Business Continuity / Disaster Recovery	Economics Leadership Social Science
Human Factors	Privacy, Passwords, Usable Security	Humanities Social Science

Table 1:
Learning modules for general education courses

Standalone Module	Topics	LIA Curriculum
Attacks and Defense	IDS, Traffic, Log Analysis, performance	Technology

3 CYBERSECURITY LABS AND MODULES

In this Section we describe in detail the content and learning outcomes of the GENI experiential cyber security learning labs and the general education modules of the project CyberPaths. A public website is available in [9] with all the materials described below.

3.1 GENI Cyber Security Labs

The Global Environment of Network Innovations (GENI) [7] is a cloud infrastructure that was created for academic research experimentation. GENI allows at-scale network experiments, with testbeds that span around the US. Heterogeneous GENI resources permit users deep programmability throughout the network and are shared among multiple users. Compute, storage and networking resources are provisioned in concert (as slices) to support repeatable experimental activities. Users can reserve resources such as Virtual Machines (VMs), PCs, and switches, stitch networks in different locations, and install any software they need for their experiments.

GENI resources can be reserved using XML (RSpec). The RSpec is highly customizable as it can contain installation instructions, download files, and prepare the environment for an experiment that will require minimal setup. Several tools exist that facilitate the experimentation, such as Jacks GUI for topology reservation,

GENI desktop for experiment visualization, and omni a command line tool with an API for programmable reservation of resources.

GENI has been used extensively in research, however only in the past few years there has been systematic development of education resources. Currently, there are education resources for computer networking, wireless, and distributed systems experimentation [10]. The CyberPaths experiential learning labs are part of this group of novel education materials that can be used by any teacher with an approved GENI project account.

Lab Title	Outcomes	Topology
Passwords	<ul style="list-style-type: none"> Apply crypto, hashing, weak passwords concepts Use password cracking tools 	Multiple VMS interconnected with a switch
Ransomware	<ul style="list-style-type: none"> Understand malware Reverse engineer 	Single VM
DDoS Sniffing	<ul style="list-style-type: none"> Apply network protocol concepts in attack Use Wireshark, tcpdump 	
Snort IDS	<ul style="list-style-type: none"> Create an IDS rule based on attack signature 	
Digital Certificate	<ul style="list-style-type: none"> Understand CA Use LAMP 	
Metasploit	<ul style="list-style-type: none"> Apply a CVE Use Metasploit framework 	
Correlation & Mitigation with SDN	<ul style="list-style-type: none"> Apply SDN for security Automate security with scripting 	
Covert Communication	<ul style="list-style-type: none"> Understand covert communication and encoding 	

Table 2: GENI Labs Outcomes and Network Topologies

The GENI labs are shown in Table 2, including the network topologies and learning outcomes where applicable. The network topologies include local networks with a OpenFlow Virtual Switch (OVS). They can be adjusted based on the experimentation needs. We have categorized the labs based on the student

academic level. Every lab includes prerequisite knowledge that includes videos and network resources, instructions and an XML RSpec to setup the lab topology, guiding screenshots, and critical thinking questions. There are three types of labs:

1. *CTF-style*: these labs are based on short, manageable tasks modeled from Capture The Flag (CTF) competitions.
 - a. Passwords: students start from pivot machine guessing a weak password, then scavenge through files with hidden passwords. They have to crack these passwords that are weakly encrypted or hashed using a tool of their preference.
 - b. Ransomware: students run a python script that encrypts previously readable files. They are asked to reverse engineer the script.
2. *Scenario based*: these labs are based on a security scenario such as sniffing an active attack or setting up an Intrusion Detection System (IDS).
 - a. Distributed Denial of Service (DDoS) traffic: students generate a flooding attack, sniff the packets with tcpdump, and analyze them with Wireshark.
 - b. Intrusion Detection with Snort: students install Snort on a dedicated monitoring machine where all traffic is duplicated with an SDN rule. Then they write a custom rule to detect a DoS flooding attack.
 - c. Digital Certificate: students setup Linux, Apache, MySQL, PHP (LAMP) development stack, then they create a digital certificate, and experience the effects of certificate corruption.
 - d. Metasploit: students gain root privileges using Metasploit framework and a known CVE².
3. *Research oriented*: these labs are based on scholarly research [11], [12], and can be used in special topics undergraduate and graduate courses to inspire research in cyber security.

² <https://www.cvedetails.com/cve/CVE-2015-1328/>

- a. Correlation & mitigation of attacks with SDN: students use Python scripts to actively monitor Snort alerts, communicate with the SDN control plane with OpenFlow rules, and block an attack that is entering from a specific port.
- b. Covert Communication: students create covert messages by manipulating TCP flags and analyze them with Wireshark.

These GENI labs may be used in introductory general education technology courses or introduction to cyber security CS courses (CTF-style), upper level CS (Scenario Based), and even graduate or advanced undergraduate classes (Research Oriented). These labs aim at creating awareness, critical thinking, and deep understanding of security concepts through experiential learning.

3.2 General education modules

The general education modules aim to cover the gap in colleges that may not have the flexibility to introduce technology in their general education core. These modules are standalone and can be added in a non-CS class such as political science, finance, or ethics. The modules include slides, useful videos and references on the topic, role playing or research exercise in class, and a homework assignment.

We have developed three general education modules:

1. *Cyber war*: this module can be taught as part of a political science or international law class. It includes case studies such on the Stuxnet worm³ and the malware that shut down the Estonian electric grid. An in-class role play exercise initiates the conversation on whether these case studies constitute an act of war, how should international laws be updated, what is the responsibility of law makers, politicians, and citizens. A research

³ <https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet/>

homework assignment is given where students research international laws related to cyber conflict and cyber war.

2. *Gordon-Loeb*: this module can be part of a finance, economics, or management class. The Gordon-Loeb [13] finance model is presented to the students. This model aims at mathematically modeling cyber security investment. Students work on a spreadsheet exercise for a specific startup company that they choose, then populate different fields, such as assets and liabilities of the specific company, and finally they estimate the upper bound investment that this company should make on their cyber security infrastructure.
3. *Human factors*: this module can be taught in a sociology, ethics, or psychology class. It includes an introduction to the Social Engineering (SE) framework⁴ where students learn about all the stages of SE, such as information gathering, psychological principles, attack vectors, and social engineering tools. An in-class role play exercise is assigned where students give permission to their pair to look at their social network profiles and then using techniques from the framework try to guess something personal, such as a password or technology that they may use. Ethics is part of the learning outcomes of this module; students are not allowed to find personal information that would violate a person's privacy during the in-class exercise. Students are cautioned about unethical behavior by explaining passive and active reconnaissance and penetration testing versus hacking.

4 CURRICULUM FOR THE LIBERAL ARTS

We have introduced three different courses that have been taught at the College X and Y College. We have studied the student learning experience with pre and post surveys that include questions on demographics, self-evaluation, and evaluation

⁴ <https://www.social-engineer.org/framework/general-discussion/>

of the course materials. The results of the surveys are presented in [14], [15]. In this Section we describe the courses and how they can be adjusted to Liberal Arts Colleges based on our experience.

4.1 General Education Course

A First-Year Experience (FYE) course at the College X is a general education class that every freshman has to take either in a fall or spring semester. Any professor may teach an FYE course and there is flexibility on the topics to cover, as long as it satisfies the writing and research learning objectives of the general education curriculum.

We used the FYE general education course as a vehicle to experiment with the ideas of the project CyberPaths. Our objectives were (i) to introduce non-CS majors to cybersecurity concepts that included both hard technology skills and soft, interdisciplinary competences, (ii) to inspire any major to contribute in the field of cybersecurity even if they did not choose to study CS. The class was designed as a combination of traditional CS course that includes technical labs and a semester project, but in addition included literature readings and writing essays.

For the technical part of the class, students completed CTF-style and some scenario-based labs on GENI. Students completed the lab on passwords, ransomware, and DDoS attack packet sniffing. For the non-technical part of the class we used modules on cyber conflict, ethics, and human factors in security from project CyberPaths, as discussed in the previous Section.

4.2 Computer Science Courses

Two computer science courses have been introduced at the College X as shown in Table 3. The Table includes core competencies taught in the course and how these are covered by GENI and other hands-on labs. Many liberal arts colleges, such as the College X, may be unable to introduce an additional major or track to the curriculum. Thus, we adjusted the curriculum based on the college profile: an introductory cyber security course that is mandatory for Computer Information

Systems (CIS) students and a mandatory upper level (junior/senior) course for the Computer Science (CS) students.

The introductory course serves two purposes. First, the CIS students that are looking at the CS field from the perspective of business and project management acquire basic knowledge on the cyber security field by registering for this course. Second, as a course without prerequisites, it can be taken by non-CS majors that are interested in cyber security (Cohort B in Figure 1). As can be seen in Table 3, a variety of concepts are covered in this class at the introductory level.

The “Computer and Network Security” course is an anthology of computer topics covered in depth, such as cryptography and number theory, networking concepts and security, web application security, and software security. Several scenario-based labs are completed on GENI or using other platforms such as Docker container and Kali Linux VMs. Note that a student may also use a GENI VM with Kali Linux installation.

Table 3:
New Cyber Security courses for LIA, including GENI modules where applicable

Course	Cyber Security Core Competencies	GENI and other projects
Security 101	Basic Data Analysis	Gather traffic, performance metrics, logs (GENI)
	Cyber Defense	Install Intrusion Detection System, write simple rules (GENI)

Table 3:
New Cyber Security courses for LIA, including GENI modules where applicable

Course	Cyber Security Core Competencies	GENI and other projects
	Cyber Threats	Emulate DDoS attack with automation scripts (GENI)
	Intro to Cryptography	Passwords hands on exercise in encryption, decryption, hashing (GENI)
	IT System Components	Create and test complex topologies that include network components (GENI)
Cryptography and Network Security	Web Application Security	Docker container for web application security project (e-commerce website)
	Network Security Administration	DNS poisoning, DDoS Slowloris, and IDS (GENI)
	Mobile Technologies	Wireshark assignment – frames, WPA handshake & Krack attack

Table 3:
New Cyber Security courses for LIA, including GENI modules where applicable

Course	Cyber Security Core Competencies	GENI and other projects
	Advanced Cryptography	Hands on exercises from Kryptos ⁵ Mathematical competition
	Software security	Smashing the stack buffer overflow

5 CONCLUSIONS AND FUTURE WORK

We have presented our work on the project CyberPaths, with goal to facilitate teaching cyber security in Liberal Arts colleges and exposing a diverse population to the field. Our work includes experiential learning cloud-based labs on the GENI infrastructure, that can be used with no resource overhead. Furthermore, it includes general education standalone modules to expose non-CS liberal arts majors to the field. Finally, we have presented curriculum that offers options to LIA institutions to inject security non-intrusively.

In the future, we plan to deploy the general education modules to different courses at the College X and use course surveys to study the cyber security learning experience of non-CS majors. We will continue developing GENI labs related to different concepts such as: forensics, firewalls, and steganography.

⁵ <https://www.cwu.edu/math/kryptos>

REFERENCES

- [1] Joint Task Force on Computing Curricula Association for Computing Machinery (ACM) IEEE Computer Society, "Computer Science Curricula 2013," ACM, 2013.
- [2] "ACM Joint Task Force on Cybersecurity Education," 2015. [Online]. Available: <http://www.csec2017.org/>. [Accessed 2016].
- [3] B. o. L. Statistics, "Occupational Security Handbook," [Online]. Available: <http://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm>. [Accessed 2016].
- [4] "Security Injections @Towson – Cybersecurity Modules for Computer Science Courses," [Online]. Available: <http://cis1.towson.edu/~csecinj/>. [Accessed 2016].
- [5] "Security Knitting Kit," [Online]. Available: <http://blogs.cae.tntech.edu/secknitkit/>. [Accessed 2016].
- [6] "EDURange: A Cybersecurity Competition Platform to Enhance Undergraduate Security Analysis Skills," [Online]. Available: <http://blogs.evergreen.edu/edurange/>. [Accessed 2016].
- [7] NSF #1548315, "Catalyzing Computing and Cybersecurity in Community Colleges (C5)," 2018. [Online]. Available: <https://www.c5colleges.org/>. [Accessed 2018].
- [8] NSA, "National Centers of Academic Excellence in Cyber Operations Advanced," 6 November 2017. [Online]. Available: <https://www.nsa.gov/resources/educators/centers-academic-excellence/cyber-operations/advanced/index.shtml>. [Accessed 2018].
- [9] NSF #1700254, "CyberPaths," 2018. [Online]. Available: <http://blogs.cofc.edu/cyberpaths/>. [Accessed 2018].
- [10] F. Fund, "GENI Classroom Exercises," 2018. [Online]. Available: <http://www.cs.unc.edu/Research/geni/geniExercises/>. [Accessed 2018].
- [11] X. L. X. M. Josephine Chow, "Raising Flags: Detecting Covert Storage Channels Using Relative Entropy," in *IEEE International Conference on Security Informatics (IEEE ISI)*, Beijing, China, 2017.
- [12] X. M. X. L. K. X. Tommy Chin, "An SDN-Supported Collaborative Approach for DDoS Flooding Detection and Containment," in *International Conference for Military Communications (MILCOM 2015)*, Tampa, Florida, 2015.
- [13] M. L. Lawrence Gordon, "The Economics of Information Security Investment," *ACM Transactions on Information and System Security*, vol. 5, no. 4, p. 438–457, 2002.

- [14] X. M. X. L. Harrison Ledford, "Denial of Service Lab for Experiential Cybersecurity Learning in Primarily Undergraduate Institutions," in *Consortium for Computing Sciences in Colleges, Southeastern Regional (CCSC-SE 2016)*, Asheville, NC, 2016.
- [15] X. L. Q. B. Xenia Mountrouidou, "Cybersecurity in Liberal Arts General Education Curriculum," in *ACM Conference on Innovation and Technology in Computer Science Education (ITiCSE 2018)*, Larnaca, Cyprus, 2018.
- [16] J. S. C. L. L. A. N. M. O. D. R.-. h. R. R. a. I. S. M. Berman, "GENI: A federated testbed for innovative network experiments," *Computer Networks*, vol. 61, pp. 5-23, 2014.
- [17] "GENI Education," [Online]. Available: <http://www.cs.unc.edu/Research/geni/geniEdu/>. [Accessed 2016].