Integrating Cybersecurity Labs into Traditional Curriculum Design

Suzanna E. Schmeelk[1], Denise M. Dragos[2]

Department of Computer Science, Mathematics, and Science –
St. John's University, Queens - New York, United States of America[1,2]

Abstract

Cybersecurity topics which make it into textbooks have historically been developed from real world threats which have been actualized in the real world. In fact, most risk management frameworks require cybersecurity threats to be ranked by a probability metric such as a likelihood and an impact score. Cybersecurity therefore is unlike other computing fields as it is most likely not developed in any part in isolation from the real world. This strong real world connection of the field can be emphasized directly to the student through regular cybersecurity lab and demo exercises. Our research contributes an emphasis for cybersecurity learning through regular (i.e. weekly) lab demonstrations by either or both the instructor or students. The paper discusses a curriculum design where both the cloud and local resources are employed for live cybersecurity demos to the students. A cloud service provider such as Amazon, Microsoft, or Google, can be employed in the classroom setting for the cybersecurity teaching and learnings. In some cases, our research has identified that these major cloud service providers offer free services for education. Our research can be used to guide further future curriculum designs gaps in cybersecurity or computing where traditional lab environments and resources are not available to both faculty and students.

Keywords: *Cybersecurity, Software Assurance, Digital Forensics, Innovation, Pedagogy.*

1. Introduction

According to the U.S. Department of Labor (2019), Cybersecurity jobs will increase by 28% from 2016 to 2026 with a median pay of $95,510/year reported in 2017. Weese (2019) however reports that a skills gap still exists across the country so that finding adequate talent continues to be difficult. One important factor, as O'Flaherty (2018) emphasizes, is that diversity in human experiences and backgrounds is essential for reinforcing different perspectives when working on a security team. All too frequently however, as the Infosec Institute (2018) writes, diversity remains unrealized. Thus, our research is in narrowing the cybersecurity skills gap for people of diversity while benefiting students of all backgrounds. One technique we introduce in our paper is to regularly adapt student hands-on learning experiences via labs.

2. Literature Review

Research has shown that outcomes and expertise increases with regular lab interventions. Depending on the learning environments there are many ways students can learn about and advance in their understandings of cyber security topics. We explore techniques published recently in academic venues.

2.1 Cloud-Based Vendor Platforms

Proprietary cloud based learning platforms also exist. Certain vendors, e.g Palo Alto and Fortinet, provide access to online learning content. Dopplick (2015) discusses NETLAB+ (which is partnered with the Center for Systems Security and Information Assurance, a National Science Foundation Advanced Technological Education National Resource Center.) Academic publishers are starting to offer cloud based lab environments that integrate into their digital text books, such as Cengage's MindTap platform (Cengage, 2019).

2.2 Mobile Security

Labs can be setup and executed on a local environment. Mobile security topics labs are introduced by Peruma, Malachowsky, and Krutz (2018) with a set of Practical Labs in Security for (Android) Mobile Applications (PLASMA) at three levels—beginner, medium, and advanced.

2.3 Hybrid Environments

Wenliang Du (2011) has produced the SEED Project where labs are pre-installed on a virtual machine, as well as integrated into a corresponding Cyber Security book. Additional material specific

to Database Security, Network Security, Operating Systems, and Network Management can be found in the NSF sponsored SecKnitKit (Mountrouidou, 2016).

2.4 Cloud-Based Academic Platforms

There exists academic cloud based learning platforms. EduRange is working on publishing an AMI to the Amazon cloud for cybersecurity labs (Mountrouidou, 2016). Global Environment for Network Innovations (GENI) provides emulation experimentation (Mountrouidou, 2016). Try-CybSI, a cyber security experimentation tool produced by Kalyanam and Yang (2017), is a Docker image for running cyber security experiments, specifically ArpSpoof, SSLStrip, and HSTS. DETER, which is an academic consortium between 16 universities, (Dopplick, 2015).

2.5 Outside Exercises

Outside of regular class time exercise, there are other sources of learning such as online capture the flag exercises. Dopplick (2015) names various online exercises as Global Cyber-Lympics, U.S. Cyber Challenge Cyber Quests, National Collegiate Cyber Defense Competition, National Cyber League, U.K. Cyber Security Challenge. Pattanayak et al. (2018) discuss Pink Elephant Unicorn (PEU), which is a Science, Technology, Engineering, and Math (STEM) cybersecurity competition targeted at anyone who has a drive to learn about cybersecurity.

2.6 Frameworks and Early Innovations

Frameworks and curriculum design techniques exist in literature. Gould et al. (2018) discuss additional learning frameworks and early game motivation innovation. Mountrouidou et al. (2018) discuss experiments on the GENI framework and rank student perceptions pre- and post- course material on a Likert scale.

3. Software Assurance

Secure software development is an increasingly important topic in cyber security curriculums and software engineering curriculums. Specifically, organizations are moving to risk management frameworks. One such framework is the NIST Risk Management model. This model works on a likelihood and impact scale to help practitioners manage the risk. Conditions such as budget, time, technology, and human resources are taken into account for managing the risk. Risk starts at application development since all systems rely on development. Analysis of system code can be static, dynamic, or a combination.

3.1 Risk Management

Students should be familiar with writing risk management reports such as a risk assessment. Depending on their software engineering skills they can either use self-developed applications, or can assess free vulnerable web applications (e.g., OWASP WebGoat, etc.) for their reports. There is very little to no research in education in the risk management domain.

3.2 Static Analysis

Students should be acquainted with static analysis tools for analysing source, intermediate, or binary software. Directly analysing code is one of the fundamental techniques for identifying vulnerabilities. Traditionally, this field is considered static analysis since the code is not necessarily executed. Key vendors such as Coverity, Fortify, Black Duck, provide online demos which the student can access for testing vulnerable software. In addition to static analysis, theorem proving tools exist for proving the correctness of code based on inserted assertions. These tools can also be demoed in the Cloud in a visualized environment.

3.3 Dynamic Analysis

Students should be familiar with dynamic analysis tools for analysing their software. Dynamic analysis is geared at finding vulnerabilities by executing code either with a virtualized environment or via Penetration Testing. Tools such as VirusTotal, Palo Alto, and Fortinet provide dynamic SandBox simulations for software.

4. Digital Forensics

Several pre-built forensic Linux distributions are available. Tesla Consulting DEFT (acronym for Digital Evidence & Forensics Toolkit) is a distribution made for Digital Forensics and Incident

Response(DFIR) (Tesla, 2019). The Sans Institute offers the SIFT Workstation as an open source and free project (SANS, 2019). Brian Carrier wrote and the Sleuth Kit front-end GUI, Autopsy (Carrier, 2019). Many commercial forensic software com offer Universities highly discounted licenses to deploy in student labs. Many DFR applications are processor intensive with large data sets that must be recovered from local devices, so a hybrid of local VM and cloud based solutions have been implemented. The cloud based exercises general need the data sets provided to the students with the forensic environment, as transfer of the large files poses a bandwidth issue. Files in the lab are shared using a locally hosted cloud solution.

4.1 Workstation Device and Laptop Devices

Academic Lab licenses enable students to use fully licensed versions of AccessData's Forensic Toolkit suite and BlackBag Forensic's Blacklight tool. Students learn to image hard drives using hardware write blockers and are later provided image files to facilitate additional areas of study. Freeware tools Recuva and PhotoRec augment the data carving lessons. More advanced topics include memory forensics using tools such as DumpIt and Volitliy. Students examine their own Windows Registries and USB device usage using AccessData's Registry Viewer, RegRipper, and Registry Explorer. Volume Shadow Copies are studied using VMware and ShadowExplorer. Many of the free Nirsoft tools are used to analyse applications.

4.2 Mobile Device and IOT Devices

Lab licenses for Blackbag Forensic's Mobilyze and Cellebrite's mobile device forensic suite give students access to the industry standard tools. Students primarily study iOS and Android platforms, but legacy devices, such as blackberry, windows and feature phones are also examined. Smart home, drones, wearables, vehicles, and other devices are inspected. The Santoku mobile forensic linux distro is also introduced. Cloud Forensics using the Belkasoft Acquisition Tool, Cellebrite UFED, and Elcomsoft Cloud forensics tools are reviewed.

4.3 Server and Network Forensics

Traditional forensic methodology is applied to servers and Wireshark, RSA Netwitness Investigator, Netresec AB NetworkMiner are the primary tools used to analyse packet capture files. Pcap samples are provided to students for detailed analysis. Log viewer software and aggregators, such as Splunk are examined. Networks and all the associated types of devices are studied holistically to really demonstrate the overall picture of network intrusions and their investigation. The OSSIM (Open Source Security Information Management) open source security information and event management system to familiarize the students with security information and event management (SIEM) software.

4.4 Malware Analysis

A three prong approach is taken to introduce malware analysis to students. Behavior based, dynamic and static techniques are used. Virtual machines and system snapshots are heavily leveraged in this course, allowing the students to work with live malware samples. Infected system behavior is observed using tools such as regshot, wireshark, ProcessMonitor, and Process Explorer. For dynamic analysis, debuggers such as x64Dbg, OllyDbg, and WinDbg are taught. Ghidra and IDA Pro disassemblers are utilized for static examinations. Online resources including Virustotal.com, Virusscan.jotti.org, Hybrid-Analysis.com, and Reverse.it are used in the classroom. Other tools introduced include PEid, pestudio, and PEview.

5. Information Security Classes

Information Security changes daily. Many security software (e.g. JohnTheRipper, Kismet, Aircrack-ng, etc.) can be run on Linux variants. These labs can be setup for students on many hybrid and cloud-based systems while staying within the freeware service license.

Additionally, students should have awareness for key industry leading technologies. Historically, Gartner has developed a Magic Quadrant for various poplar technology niches. Gartner regularly release Magic Quadrants to emphasize key industry players (e.g., SIEMs, IDS, AntiVirus, Firewalls, etc.). The magic quadrants can help students learn about and examine differences in current vendor leaders. Many vendors provide online demos for students to learn more about specific tools.

6. Conclusions and Future Work

This paper explored current and future hybrid and online learning resources for cyber security. Research, discussed in the Literature Review section, has shown that many students benefit from hands-on lab activities. Our research identifies different free, hybrid, cloud, and proprietary resources, which can be directly integrated into class activities. Online vendors such as Amazon are integrating with VMWare providing additional sources for running labs in the Cloud. Overall, feedback from students indicate that they appreciate hands-on exercises, which they emphasize helps them reinforce learnings.

References

[1] Renee Dopplick. 2015. Experiential cybersecurity learning. ACM Inroads 6, 2 (May 2015), 84-84.
[2] David Gould, Greg Block, and Simon Cleveland. 2018. Using Evolutionary Systems and Ideation Techniques to Enhance Student Cybersecurity Learning. In Proceedings of the 19th Annual SIG Conference on Information Technology Education (SIGITE '18). ACM, New York, NY, USA, 146-146.
[3] Harrison Ledford, Xenia Mountrouidou, and Xiangyang Li. 2016. Denial of service lab for experiential cybersecurity learning in primarily undergraduate institutions. J. Comput. Sci. Coll. 32, 2 (December 2016), 158-164.
[4] Anthony Peruma, Samuel A. Malachowsky, and Daniel E. Krutz. 2018. Providing an experiential cybersecurity learning experience through mobile security labs. In Proceedings of the 1st International Workshop on Security Awareness from Design to Deployment (SEAD '18). ACM, New York, NY, USA, 51-54.
[5] Rajesh Kalyanam and Baijian Yang. 2017. Try-CybSI: An Extensible Cybersecurity Learning and Demonstration Platform. In Proceedings of the 18th Annual Conference on Information Technology Education (SIGITE '17). ACM, New York, NY, USA, 41-46.
[6] Xenia Mountrouidou, Xiangyang Li, and Quinn Burke. 2018. Cybersecurity in liberal arts general education curriculum. In Proceedings of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education (ITiCSE 2018). ACM, New York, NY, USA, 182-187.
[7] Animesh Pattanayak, Daniel M. Best, Daniel Sanner, and Jessica Smith. 2018. Advancing cybersecurity education: pink elephant unicorn. In Proceedings of the Fifth Cybersecurity Symposium (CyberSec '18). ACM, New York, NY, USA, Article 3, 1-7.
[8] Marco Ghiglieri and Martin Stopczynski. 2016. SecLab: An Innovative Approach to Learn and Understand Current Security and Privacy Issues. In Proceedings of the 17th Annual Conference on Information Technology Education (SIGITE '16). ACM, New York, NY, USA, 67-72.
[9] Te-Shun Chou and John Jones. 2018. Developing and Evaluating an Experimental Learning Environment for Cyber Security Education. In Proceedings of the 19th Annual SIG Conference on Information Technology Education (SIGITE '18). ACM, New York, NY, USA, 92-97.
[10] Sherly Abraham and Lifang Shih. 2015. Towards an integrative learning approach in cybersecurity education. In Proceedings of the 2015 Information Security Curriculum Development Conference (InfoSec '15). ACM, New York, NY, USA, Article 11, 1.
[11] Wenliang Du. The SEED Project: Providing Hands-on Lab Exercises for Computer Security Education. In IEEE Security and Privacy Magazine, September/October, 2011. Invited paper.
[12] Infosec Institute. (2018). Minorities in Cybersecurity: The Importance of a Diverse Security Workforce. Retrieved from: https://resources.infosecinstitute.com/minorities-in-cybersecurity-the-importance-of-a-diverse-security-workforce/#gref
[13] Kate O'Flaherty. (2018) How diversity can help fight cyber-attacks. Retrieved from: https://www.information-age.com/how-diversity-can-cyber-123477494/
[14] U.S. Department of Labor. (2019) Information Security Analysts. Retrieved from: https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm
[15] Evan Weese (2019) Cybersecurity pros in high demand but hard to find. Retrieved from: https://www.columbusceo.com/business/20190218/cybersecurity-pros-in-high-demand-but-hard-to-find
[16] Cengage. MindTap. (2019) Training Resources. Retrieved from: https://www.cengage.com/training/mindtap
[17] Tesla Consulting. (2019) De[f]t DFRI Toolkit. http://www.deftlinux.net/
[18] SANS Institute. (2019) SIFT Workstation Overview https://digital-forensics.sans.org/community/downloads#overview
[19] CAINE. (2019) CAINE Computer Forensics Linux Live Distro. https://www.caine-live.net/
[20] Brian Carrier. (2019) Open Source Digital Forensics. http://www.sleuthkit.org/autopsy/