International Conference
The Future of Education

Integrating Cybersecurity Labs into Traditional Curriculum Design

Authors: **Suzanna E. Schmeelk** & **Denise M. Dragos**

Affiliation: **St. John's University** – Queens, New York (United States)

Session: Technology in Education 14:30 – 16:35 on **June 28, 2019**

Talk Outline

- Overview/Contributions
- Introduction
- Literature Review
- Case: Software Assurance
- Case: Digital Forensics
- Case: Information Security Classes
- Conclusions and Future Work

Research Overview

- Cybersecurity topics in textbooks
  - Historically been developed from real world threats actualized
  - *Risk management frameworks ranked by a probability metrics (likelihood x impact)*
- Cybersecurity topics are not developed in isolation from the real world
- The strong real world connection of the field
  - Emphasized directly to the student through
    Regular cybersecurity lab and demo exercises

Research Contributions

- 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.
  - *Employing a cloud service provider such as Amazon, Microsoft, or Google*
- 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.

Introduction

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

Literature Review

- Research has shown that outcomes and expertise increases with regular lab interventions.
- Techniques published recently in academic venues:
  - Cloud-Based Vendor Platforms
  - Mobile Security
  - Hybrid Environments
  - Cloud-Based Academic Platforms
  - Outside Exercises
  - Frameworks and Early Innovations

Case Study: Software Assurance

- Risk Management
  - Risk Assessment of known vulnerable applications (e.g. Gruyere, WebGoat)
- Static Analysis
  - Free tools (e.g. FindBugs, Apktool, etc.) & Educational Licenses (e.g. Fortify, etc.)
- Dynamic Analysis
  - Free tools (e.g. MobileSandbox, etc.) & Educational Licenses (e.g. WebInspect, Palo Alto, etc.)

Case Study: Digital Forensics

- Workstation Device and Laptop Devices
  - Academic Licenses (e.g. AccessData's Forensic Toolkit suite, BlackBag's BlackLight tool)
  - Freeware (e.g. DumpIt, Volitliy, Nirsoft tools)
- Mobile Device and IOT Devices
  - Academic Licenses (e.g. Blackbag Forensic's Mobilyze and Cellebrite)
- Server and Network Forensics
  - Freeware Licenses (e.g. RSA Netwitness Investigator, Netresec AB NetworkMiner)
- Malware Analysis
  - Free (temporary) licenses (e.g. IdaPro, x64Dbg, OllyDbg, and WinDbg)

Case Study: Information Security Classes

- Information Security changes daily.
- Most 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.
- Students should have awareness for key industry leading technologies. Historically, Gartner has developed a Magic Quadrant for various poplar technology niches (e.g. firewalls, IDS, SIEM, etc.)

Conclusions and Future Work

- Research has shown that many students benefit from hands-on lab activities.
- This paper explored current and future hybrid and online learning resources for cyber security.
- 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.

References

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/