Preparing the Next Generation of Engineers: Adjusting the Curriculum for Cybersecurity Education

A Technical Report submitted to the Department of Computer Science

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Jason Lee

Spring, 2024

Technical Project Team Members

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Rosanne Vrugtman, Department of Computer Science

Briana Morrison, Department of Computer Science

Preparing the Next Generation of Engineers: Adjusting the Curriculum for Cybersecurity Education

CS4991 Capstone Report, 2024

Jason Lee
Computer Science
The University of Virginia
School of Engineering and Applied Science
Charlottesville, Virginia USA
jl5bwn@virginia.edu

Abstract

Cybersecurity threats in the United States and globally have increased with the rapid advance of computer technology. To address this issue, I propose that the University of Virginia adjust its curriculum to provide more in-depth security education for all future CS and Engineering students. I suggest adding mandatory security courses as part of the CS program, along with optional electives dealing with non-traditional hosts that can be easily exploited. Additional education can have positive effects on security threats, but catching possible security vulnerabilities in programs and technology before they are produced would reduce the cost of patching the code later. Future work developing a curriculum and/or major specifically focused on cybersecurity would lessen the load on current CS professors and allow those with an interest in cybersecurity to dive more deeply into these topics.

1. Introduction

The internet is pervasive in our modern society, from replacing restaurant menus to being implemented in every household appliance. The current CEO of Google, Sundar Pichai, describes it as a great equalizer (The Verge 2015). In the realm of cybersecurity, this statement could not be more true.

Smaller nations, such as Iran, Israel, North Korea, and other countries (while small in size) have a well-trained group of hackers that prey on larger nations' software vulnerabilities. That is not to say that larger nations do not have their own claims on cyberspace. Chinese hackers have targeted a variety of opponents, including a successful phishing attack on UVA in 2016. Russian hackers are almost constantly on the news and incident reports regarding cybercrimes. A recent report by ABC news found that Russian hackers were using compromised routers from Ubiquiti (EdgeRouters) to accomplish their cyber operations (Barr 2024, Feb 28). They have a vulnerability with their default settings, leaving them with minimal protection from potential cyber attacks. This was not a clever hacking job: it is a symptom of a lack of security-minded thinking.

2. Related Works

Yan et. al (2018) have a great discussion on the topic of cybersecurity judgments, with their paper examining and benchmarking undergraduate students and their competence in avoiding potentially risky behaviors. They examined whether cybersecurity judgment had any correlation with either intuitive or rational thinking.

They concluded that the reason most undergraduate students did not score above a D in their examination was due to their lack of knowledge on the subject. This is where my inspiration for the curriculum adjustment originated, as the weakest link in a security environment is the untrained/unprepared users.

Further readings by Micco & Rossman (2002, February) proposed an upper level series of security classes labeled simply "cyberwar lab" and the lessons learned from attempting to implement it at the Indiana University of Pennsylvania. Their labs were hands-on, having an attack component, a defense component, and a conviction component to determine the online law that was violated. They also listed their recommendations for future classes regarding this topic, including keeping networking components simple in order to minimize issues, using diverse systems instead of a standard Linux environment for everything, having good foundational programming and networking knowledge, and emphasizing the importance of risk management.

Along with this, Jang-Jaccard & Nepal's (2014) paper on cybersecurity trends highlighted emerging, non-traditional methods of attacks, such as cloud-computing attacks and USB attacks . This was the inspiration for the IoT elective proposed, and another inspiration for the curriculum adjustment.

3. Curriculum Redesign

The first change that could be implemented is the addition of mandatory security courses, as education and awareness are two factors that have proven effects on response time and vulnerability to phishing attacks. The second change is adding courses that discuss non-traditional internet-connected hosts ("Internet of Things"), as "Things" are a quickly growing section that has a plethora of security issues which can be easily exploited. Finally, the current curriculum should either strongly recommend or require Introduction to Cybersecurity (CS 3710) for CS candidates to graduate. Below, the above two courses are outlined in more detail.

3.1 "Keeping Your Systems Secure" – Mandatory Security Training

This course should be required for all prospective Engineers and CS candidates.

3.1.1 Topics to Discuss

This course should focus on high level and abstract concepts, instead of focusing on low-level, coding-focused topics such as C or Assembly programming. The topics should include discussions of common vulnerabilities and exploits, phishing attacks, and social engineering attacks. Vulnerabilities and exploits include common software exploits such as buffer overflows, and methods of delivery such as Trojans and other disguised malware. Along with this, the class should cover the current NIST cybersecurity framework (NIST, 2024 February 26).

3.1.2 Structure

In order to ensure a sufficient level of security awareness in all CS candidates, a pass/fail system should be implemented. The pass/fail is determined by three separate equally weighted examinations. Each exam focuses on one of the topics discussed above, except for the NIST cybersecurity framework. Unlike a traditional pen/pencil exam, these exams are taken online in a simulated environment. Similar to Micco & Rossman's (2002, February) gamification of cybersecurity labs, the examinations should also be gamified. Several online video games simulate a desktop environment but lacked the technical details to mimic real-life attacks. "Keeping Systems Secure" will

stick to the technical details, but at a higher and abstract level to lessen confusion and technical jargon.

The first exam, focusing on the topic of common vulnerabilities and exploits, will be based around spotting malicious programs. Some possible avenues include checking Task Manager for CPU usage to find a Bitcoin/Data Miner, checking network traffic through a "program" on the simulated desktop to spot a keylogger or other backdoor malware attacks, or verifying the checksum and file size of a large executable to check for Trojan malware. A possible environment is demonstrated in Figure 1.

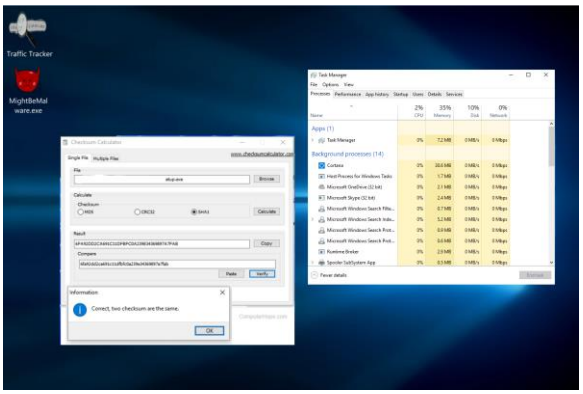

Figure 1: A crude example screenshot of an example Exam 1 in progress.

The second exam will be mainly focused on online social interactions, where the user must spot the difference between fake and real users' messages. Tested skills include checking and verifying email addresses and spotting malicious downloads or links. The differences should be displayed when the grades are released, helping the students spot what they missed during the examination.

The third exam will cover safe browsing online, and how to spot malicious links and spoofed websites (shown in Figures 2). Like the exam above, the differences should be posted after the grades for the exam are released.

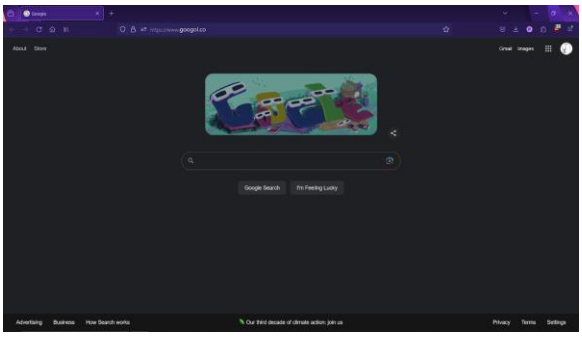

Figure 2: An example spoofed website. In this question, the student must spot the difference in the URL (googol.co) to determine that this is not the correct website.

In order to pass the course, the students must average 85% among the three exams, which would demonstrate proficiency in all three topics. This cutoff is currently arbitrary, and can be adjusted based on the pass/fail rates of previous years. A better cutoff may be found in the future after several reworks.

3.2 "Protecting the Things" – Optional Elective

"Protecting the Internet of Things", or "Protecting the Things" should be offered to CS students (and should be extended to Computer Engineering students in the future) who have already completed CS 3710. The course should also be added as a prerequisite for those looking to go on the Cybersecurity Focal Path for CS undergrads.

3.2.1 Topics to Discuss

The course's focus is on designing secure systems on non-traditional devices, such as smartphones, cloud computing devices, USBs, "Smart" devices, or anything else that is in part of the broad definition of "Internet of Things".

A significant portion should focus on mobile device security, as mobile devices are quickly making their way into the hands of a large number of people. One result is the increase in mobile and two-factor

authentication for web security. However, these methods can be easily exploited given the right tools and experience (Dmitrenko et. al, 2014). Discussion of attack venues and defenses are a must, especially when UVA also relies on these two-factor authenticators to keep our systems safe.

Further topics include attacks by non-traditional means, such as the attacks highlighted by Jang-Jaccard and Nepal (2014). Hardware defenses and secure pseudo-random number generation, securing Wifi and Wifi-routers, and other defenses should also be discussed. These hardware defenses represent the last line of defense before a malicious program infiltrates a device, therefore necessitating discussion.

3.2.2 Structure

In contrast to CS 3710, where the focus is split between both theory and hands-on activities, "Protecting the Things" is primarily lab-focused. The structure of the course has instructors demonstrating attacks in action, and tasking the students in creating defenses to protect against them. This hands-on approach is more akin to the skills that employers require from undergraduate students, while also approaching the latest malware problems from a different angle than the rest of the curriculum.

4. Anticipated Results

The anticipated results of these curriculum changes is a group of engineers and CS graduates that are better trained and more security conscious. Requiring CS 3710 should give everyone a baseline knowledge of cybersecurity topics. The mandatory security course should lead to a class of engineers with a greater focus/baseline knowledge of how to keep themselves and their devices secure on the internet. The gamification has the potential to attract/motivate more individuals to pursue cybersecurity, but it may follow Micco & Rossman's results where a gender gap in the field may appear and be exacerbated through this approach (2002, February). Discussion with a diverse group of instructors and members of the student body on the content of the exam might mitigate this issue, but further research is needed to properly address it. "Protecting the Things" may prepare engineers for a diverse and expanded environment. Results of this could include creation of more secure devices, which can lead to a reduction of weak links in a secured network, thus leading to less security incidents.

5. Conclusion

In order to combat the growing threats of cybersecurity, additional cybersecurity courses for CS undergrads would be an investment for future security in the technological sphere. Covering modern topics is an important facet of keeping up with developing attacks. Additionally, gamifying/incorporating lab elements that require students to be hands-on with their learning would engage the students in the field more while also addressing and simulating scenarios which may mirror their future work. Taking care of the weakest link through widespread education is a small but necessary step in keeping our critical systems and infrastructure safe.

6. Future Works

Several courses could branch off from the broad category of "Protecting the Internet of Things". Mobile Device Security could be further developed into its own class. There could also be a split between CpE and CS students, with the CpE section focusing on hardware safeguards in smart devices while CS students focus on producing security-robust software.

References

[1] Barr, L. (2024, February 28). *Russian hackers using "compromised" internet routers for cyber operations, US, international law enforcement warn*. ABC News.https://abcnews.go.com/US/russian-hackers-compromised-internet-routers-cyber-operations-us/story?id=107616396.
[2] Dmitrienko, A., Liebchen, C., Rossow, C., & Sadeghi, A. R. (2014). On the (in) security of mobile two-factor authentication. In *Financial Cryptography and Data Security: 18th International Conference, FC 2014, Christ Church, Barbados, March 3-7, 2014, Revised Selected Papers 18* (pp. 365-383). Springer Berlin Heidelberg.
[3] Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of computer and system sciences*, *80*(5), 973-993.
[4] Micco, M., & Rossman, H. (2002, February). Building a cyberwar lab: lessons learned: teaching cybersecurity principles to undergraduates. In *Proceedings of the 33rd SIGCSE technical symposium on Computer science education* (pp. 23-27).
[5] National Institute of Standards and Technology. (2024, February 26). *The NIST Cybersecurity Framework (CSF) 2.0*. https://doi.org/10.6028/NIST.CSWP.29
[6] The Verge. (2015, May 29). *The future of Google with Sundar Pichai* [Video file]. Retrieved from https://youtu.be/TguamcqrQjI?si=pLcXUJdoQt1Ev74R
[7] Yan, Z., Robertson, T., Yan, R., Park, S. Y., Bordoff, S., Chen, Q., & Sprissler, E. (2018). Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment?. *Computers in Human Behavior*, *84*, 375-382.