Creation of a Security in Web Development Course
(Technical Topic)

The Ethical Problems Associated with Teaching Hacking Techniques
(STS Topic)

A Thesis Project Prospectus Submitted to the

Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements of the Degree
Bachelor of Science, School of Engineering

Eric Sakmyster

Fall, 2020

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.

Signature _____Eric Sakmyster_____

Approved by:
Kathryn A. Neeley, Associate Professor of STS, Department of Engineering and Society

Approved by:
Aaron Bloomfield, Professor, Department of Computer Science

Introduction

Reliance on online web services by the world continues to increase as computing power gets stronger. As a consequence, the public's personal data has never been more exposed then it is today. According to a Pew Research study, Americans feel like their data today is less secure than it's ever been, and almost a third of respondents said that they have had a data breach in the past twelve months (Anderson, Auxier, Kumar, Perrin, Rainie, and Turney, 2019). In order for people's data to be kept private, developers need to make websites secure. However, the majority of web developers today do not have security at the forefront of their mind because they have not been reinforced with a security mindset prior to getting a job (Romeo, n.d.). Uniquely, Norwich University Online mentions how 90% of online attackers are amateurs, not professional hackers like many would suspect (2020). Web attacks are particularly prevalent now because of the amount of people working remotely. Ransomware attacks, one form of web attacks, have been on the rise across the globe in 2020, and if the web doesn't become more secure, attacks will continue to increase (Sophos, 2020).

To confront the problem of web developers not having security as a top priority when constructing websites, the technical project of this prospectus hopes to create a course on security in web development. The course will combine concepts from two University of Virginia (UVA) classes, Introduction to Cybersecurity and Advanced Software Development, to give students the tools needed to perform secure programming, while also being able to recognize types of attacks that hackers attempt. The STS part of the prospectus will examine the ethics associated with hacking and what drives someone to become a hacker. This research will improve people's understanding on why amateurs choose to be hackers, as well as if teaching

hacking techniques in a class, like the technical project proposes, could potentially lead people to become hackers.

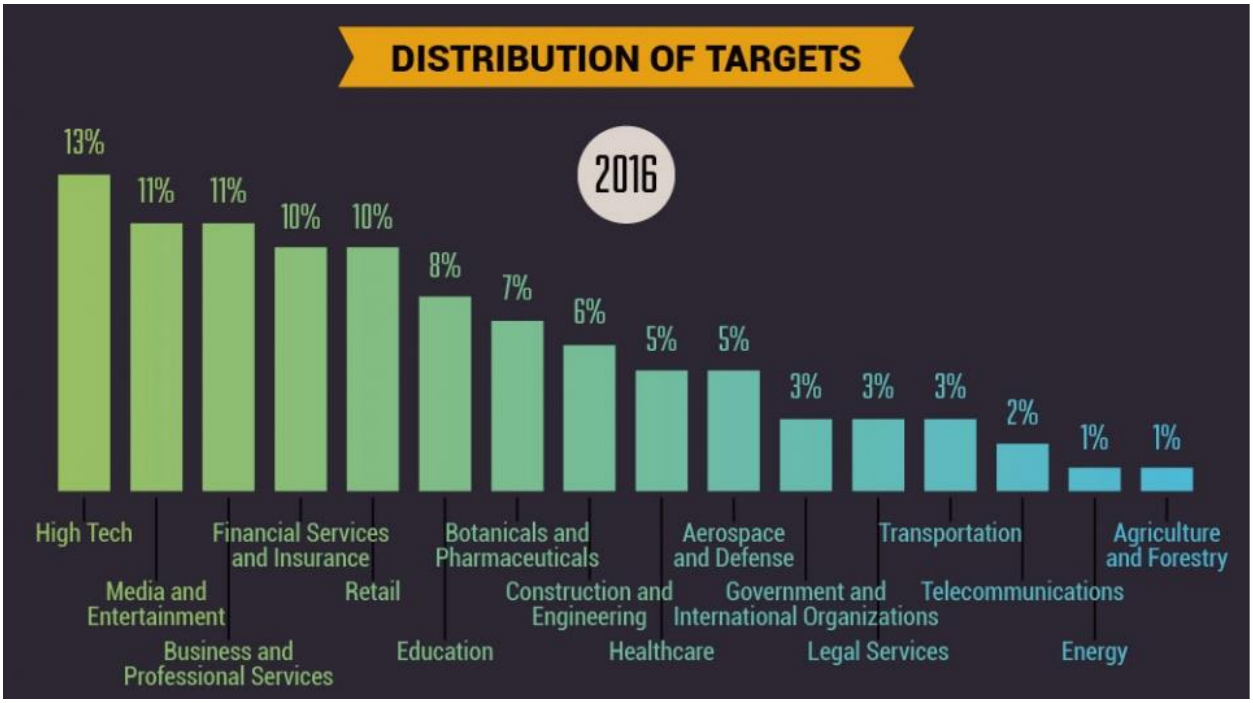
Technical Topic: Creation of a Security in Web Development Course

Hackers are always finding new and sophisticated ways to attack websites, but much of what they use is knowledge that is already known. Most websites are made using particular frameworks that give a programmer a starting structure so that they can focus more on the logic of what they want on their website. Unfortunately, many web developers think these frameworks are a substitute for good security. Vulnerabilities of a variety of web frameworks are readily available online for web developers to learn (Boyer, 2018). However, these vulnerabilities are also available for hackers to tap into someone's website. Most hackers use variations of different types of cyber-attacks, such as SQL injections or buffer overflow attacks, that are also easily accessible online. Luckily, quality ways of preventing them can be implemented into web programs, like using encryption or firewalls (Priest, 2017). In order for security to be ensured on the web, developers need to be able to anticipate and understand how they can be attacked by hackers.

The main problem with computer science education in America is that security is either not being emphasized, or isn't being taught altogether. In fact, a 2015 study done by CloudPassage found that, "out of the top ten computer science programs in the U.S., not a single program requires a cybersecurity course to graduate" (White, 2016). Another issue that arises from this study is that security is not being incorporated into all computer science classes and is only being taught as a separate class. If there's no incorporation, computer scientists will learn through a solution-based mindset, when they should have a security outlook on all problems built

into their thinking (Romeo, n.d.). Unfortunately, hackers are only getting better at what they are doing, while universities are lacking in equipping students with the tools necessary to fight back.

Attacks by hackers are increasing every year at the expense of businesses and the public. In SiteLock's 2020 security review, they found that websites are attacked on average 94 times per day, up 52% from 2019. These attacks are very cheap for the hackers, but Oliver Rochford, Director of Research at Tenable, estimates the global cost of damage to businesses can be up to $6 trillion (Swinhoe, 2020). Additionally, cyber-attacks are not focused only on tech companies. As the figure below notes, most working sectors are affected by cyber-attacks, with some, such as Agriculture and Forestry, less affected than others (Norwich University Online, 2020).



Target distribution of cyber-attacks by working sector in 2016. The figure shows some industries, such as tech and media, are more often attacked than others, but overall, most industries are affected by attacks (Norwich University Online, 2020).

However, the sectors that are attacked less have the potential to have higher costs than other sectors as they are not as focused on security as a technology company might be. These consequences will only continue with a lack of security on the web.

The technical project aims to provide a solution to these problems with the creation of a web development course that emphasizes security throughout all stages of the material. Currently at UVA, as well as many other universities, web development courses are taught completely separate from cybersecurity classes with no overlap. The new course I will propose seeks to integrate the two classes, as well as add additional material. The course would focus on three main overarching goals: how to do secure web development programming, how to handle well-known cyber-attacks, and how to incorporate security principles into any computer science project. The main challenge with this course will be making it seem as if the student isn't taking two courses, but that the topics feel like they are meant to be together in order to produce a security mindset in each student. All security principles taught in the class would be from the widely accepted Saltzer and Schroeder's 1975 design principles. These principles are the basis of a lot of companies' security policies, so it will be beneficial for students to learn and implement them in their own work (Smith, 2012). For the course, I will work on the creation of a syllabus, lecture material for a week, and assignments corresponding to the lecture material.

STS Topic: The Ethical Problems Associated with Teaching Hacking Techniques

Researchers are trying to understand what characteristics or experiences persuade someone to be a hacker. One study focusing on people's predispositions suggests that there is a positive association between someone's willingness to create and understand systems, and hacking skills and expertise. This study emphasizes that hackers do not just have a base knowledge of the branch of computer science they take on, but instead tend to have a desire to know all factors that go into the particular computer science system they are focusing on (Harvey, Bolgan, Mosca, Mclean, Rusconi, 2016). These aren't necessarily negative qualities to have, but they are indicators that someone might be interested in taking on a hacking profession.

Most people think of a hacker as a person with malicious intent, but a type of good hacker is on the rise called an ethical hacker. An ethical hacker uses tactics a bad-intent hacker would use to diagnose vulnerabilities in a company's online system to improve their security for possible future attacks. Additionally, Mohd. Ehmer Khan, from the Department of Information Technology at Al Musanna College of Technology in Sultanate of Oman, ranks ethical hacking among some of the best forms of security testing for a company (2010). It is important to understand ethical hacking in the context of this STS project because those with the skills to be a hacker need to be aware that they have legal ways that they can apply those skills. In general, the skillset of good and bad hackers is the same, but currently more people are choosing the wrong side.

Most people when they begin hacking do not have ill-will. They normally learn hacking techniques from school and clubs, but end up believing it's a game to exploit web pages (Radziwill, Romano, Shorter, and Benton, 2015). For example, Turgeman-Goldschmidt (2008), in a study about what hackers gain from their activities, concluded that hackers have a feeling of competition with other hackers that drives them, giving them adrenaline comparable to a thrill seeker. Because of this behavior, even though ethical hackers have good intentions, many universities oppose teaching hacking altogether because of the dangers associated with teaching it to young people who don't fully understand the ethics associated with it. Unfortunately, if students are taught hacking techniques without ethics reinforcing what they shouldn't do with that knowledge, they can face serious legal issues and be completely unaware they were doing something wrong (Radziwill, Romano, Shorter, and Benton, 2015).

The STS project's goal is to research how to teach hacking techniques to web developers without contributing to creating bad hackers. This can only be accomplished by understanding

the mindset of a hacker and the profession of ethical hacking, both of which I will build off of previous research from Harvey, Bolgan, Mosca, Mclean, and Rusconi (2016) and Radziwill, Romano, Shorter, and Benton (2015), respectively. In order to understand a hacker, it is important to understand the context in which they are created. To achieve this, I will create an analysis of the actor-network associated with a hacker system. Some actors I anticipate I will have to research further is the hacker themselves, including their typical way of thinking and their experiences, as well as those who can influence them, such as professors, friends, and other hackers. For a course like the one proposed in the technical project to not inadvertently make bad hackers, ethics associated with hacking and the web as a whole must be stressed. I will examine what ethics should be included in such a course through research into ethical hacking principles, which could include speaking to ethical hackers themselves.

Conclusion

For the technical portion of my prospectus, I will design a course that will focus on secure web development programming, handling well-known cyber-attacks, and using security principles in computer science projects. I will create a syllabus, lecture material for a week, and assignments that relate to that lecture material. For the STS project, I will research how to teach hacking techniques to students without causing them to become bad hackers themselves. In order to do this, I will create both an analysis of the actor-network for a hacker system and a set of ethics that should be taught in a class similar to the one presented in the technical project.

The course proposed by the technical project has the potential to help web developers know the impact of their coding by giving them a security mindset. Web developers that gain this mindset coming out of college can lead to a more secure web for both businesses and the

public. It is also important to understand hackers and how to teach students hacking techniques with ethics so that hackers who have bad intent can either be prevented or deterred by countermeasures to ensure less attacks are made on websites.

References

Anderson, M., Auxier, B., Kumar, M., Perrin, A., Rainie, L., Turner, E. (2019, November 15). *1. How Americans think about privacy and the vulnerability of their personal data*. Pew Research Center. https://www.pewresearch.org/internet/2019/11/15/how-americans-think-about-privacy-and-the-vulnerability-of-their-personal-data/

Boyer, J. (2018, July 17). *How secure are popular web frameworks? Here is a comparison*. Veracode. https://www.veracode.com/blog/secure-development/how-secure-are-popular-web-frameworks-here-comparison

Harvey, I., Bolgan, S., Mosca, D., McLean, C. and Rusconi, E. (2016, May 17). Systemizers are better code-breakers: self-reported systemizing predicts code-breaking performance in expert hackers and naïve participants. *Front. Hum. Neurosci.* 10:229. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4868920/

Khan, Mohd. E. (May 2010). Different forms of software testing techniques for finding errors. *International Journal of Computer Science Issues* 7, no. 3:11-16. http://ijcsi.org/papers/7-3-1-11-16.pdf

Norwich University Online. (2020, September 30). *The rise of cyber threats*. https://online.norwich.edu/academic-programs/resources/rise-cyber-threats

Priest, C. (2017, September 25). *Why web security should no longer be overlooked in the web development stage*. Cloud Secure Tech. https://www.cloudsecuretech.com/web-security-no-longer-overlooked-web-development-stage/

Radziwill, N., Romano, J., Shorter, D. and Benton, M. (December 2015). The ethics of hacking: should it be taught? *Software Quality Professional*, 18(1), pp. 11-15. https://arxiv.org/abs/1512.02707

Romeo, C. (n.d.). *4 steps to transforming developers into security people.* Tech Beacon. https://techbeacon.com/security/4-steps-transforming-developers-security-people

SiteLock. (2020). *2020 annual security review*. https://www.sitelock.com/download/SiteLock_AnnualSecurityReview_5-12-20.pdf

Smith, R.E. (2012). A contemporary look at Saltzer and Schroeder's 1975 design principles. *Security & Privacy*, 10(6), pp. 20-25. https://doi.org/10.1109/MSP.2012.85

Sophos. (May 2020). *The state of ransomware 2020*. https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf

Swinhoe, D. (2020, May 1). *How much does it cost to launch a cyberattack?* CSO. https://www.csoonline.com/article/3340049/how-much-does-it-cost-to-launch-a-cyberattack.html

Turgeman-Goldschmidt, O. (2008). Meanings that hackers assign to their being a hacker. *International Journal of Cyber Criminology*, 2(2), 382. http://www.cybercrimejournal.com/Orlyijccdec2008.pdf

White, S. (2016, April 25). *Top U.S. universities failing at cybersecurity education*. CIO. https://www.cio.com/article/3060813/top-u-s-universities-failing-at-cybersecurity-education.html