Exploring Ethical Hacking from Multiple Viewpoints

Dr. Radana Dvorak, University of Portland

Dr. Dvorak received her Ph.D. in computer science from the University of London, Queen Mary College, and Master's degree in AI from the University of Sussex. Dr. Dvorak has been working in IT, higher education, academic industry and program development for over 25 years. She has served as a researcher, university professor and dean in the US, UK, and the Cayman Islands. Currently, Dr. Dvorak is the Director of the University of Portland Shiley School of Engineering Bachelor of Computer Science Post-Baccalaureate program, and an instructor in computer science, teaching various CS courses. Her current research interests are related to teaching in STEM fields. She advises the cybersecurity club, and is a member of several organizations including OWASP-Portland Chapter. Dr. Dvorak is passionate about teaching, technology, career pathways and student success.

Dr. Heather Dillon, University of Portland

Dr. Heather Dillon is an Associate Professor in Mechanical Engineering at the University of Portland. She recently served as the Fulbright Canada Research Chair in STEM Education. Her research team is working on energy efficiency, renewable energy, fundamental heat transfer, and engineering education. Before joining the university, Heather Dillon worked for the Pacific Northwest National Laboratory (PNNL) as a senior research engineer.

Dr. Nicole Ralston

Dr. Nicole Ralston is an Assistant Professor and co-Director of the Multnomah County Partnership for Education Research (MCPER) in the School of Education at the University of Portland in Portland, Oregon. She received her Ph.D. in Educational Psychology with an emphasis in Measurement, Statistics, and Research Design from the University of Washington. An elementary school teacher at heart, she now teaches educational research and STEM methods to undergraduate and graduate students. Her research focus involves bringing active learning strategies to STEM, best practices of research-practice partnerships, and applied research in partnership.

Jeffrey Matthew Welch, University of Portland

Jeff Welch is a doctoral student in educational leadership at the University of Portland (Oregon, USA).

Exploring Ethical Hacking from Multiple Viewpoints

Abstract

The Shiley School of Engineering, Dept. of Computer Science is using the KEEN module to develop an entrepreneurial mindset while meeting technical objectives in a 300 level Unix/Linux tools course. This paper describes a work-in-progress module for students to explore issues related to ethical hacking and its impact in the field of information security and cybersecurity. Ethical hacking was analyzed from multiple viewpoints including industry, governments and regulatory authorities, n white hat, grey hat and black hat hacking, and analyzing trends and perspectives from industry and research. Student engaged in activities including four corners to explore ethical hacking before and after reading case studies, and also participated in group and classroom discussions. After the initial exploration, students engaged in practical exercises exploring Kali Linux and learning basic penetration and defense techniques which introduced them to tools and skills utilized in the cybersecurity industry. The objectives and the design of the survey was to explore if the module increased students' curiosity and awareness of ethical hacking as they will be confronted with security issues in their software engineering careers. Students were asked to rank the learning objectives on a Likert scale of 1 to 5 where 1 was the worst ranking and 5 was the best ranking Generally, the results of the survey demonstrated students ranked the objectives well, with the lowest score for the objective about developing an action plan for ethics indicating ways to improve the module in future course offering. The highest values were given to considering multiple viewpoints, indicating the mindset aspects of the project may have been successful.
Based on the outcome and student feedback recommendations for future implementation of the module in the curriculum is discussed.

Introduction

This paper describes a classroom module designed to develop computer science and engineering student thinking about ethical hacking. The complexity of ethical hacking is an important topic for students to consider as they pursue careers in information security and cyber security.

Students were given definitions of the type of ‘hackers’ classified by industry. White hat hacker is an ethical hacker, usually a security professional utilizing hacking skills to locate weaknesses and vulnerabilities for defensive purposes. The goal is to duplicate the intent and actions of malicious hackers; they are an authorized hacker that has the legal right to break into a system on behalf of companies. They can be contracted internally or externally, and in addition to look for vulnerabilities, they test and perform audits. Other terms used for white hat hackers are ‘penetration testers’, ‘intrusion testers’, or ‘red team members’ (red team hack, blue team defend).

A Grey hat hacker is one that does not have authorization to break into a system. This is usually illegal, but their intentions are most often ‘good’ due to reporting the vulnerabilities. This is dangerous ground for hackers to take because they risk being arrested, fined, and sent to jail. A number of arrests in the last few years of ‘well intentioned hacking” highlighted the ‘grey area’.

A black hat hacker illegally breaks into a system for any number of reasons, e.g. money, fame, protest, revenge, sabotage, thrill seeking. This could be an individual, military, government or business. Recent media coverage has exposed these attacks and the worrying implications for all individuals, companies and governments world-wide.

Traditional computer science education has mainly focused on case studies of black hat hacking and prevention mechanisms. This module was designed to provide a more nuanced view point for the students, by asking them to engage in activities and a rich discussion around the ethics of hacking, teach them tools ethical hackers utilize in industry, and inform them to future career opportunities in a growing and much needed field of cybersecurity. Computer Science departments, world-wide, have not prepared students to meet the demands of industry. In August 2018, the Forbes Technical Council published an article, "The Cybersecurity Talent Gap Is An Industry Crisis", stating 3.5 M jobs world-wide will not be filled by 2021 [10]. A recent workforce study published in 2019 by (ICS)2, [11] the world's largest non-profit association that certifies cybersecurity professionals, reported that in order to meet the needs of cybersecurity workforce globally, skilled cybersecurity professionals needs to grow by 145% to meet the demand. The report further stated that in order to meet the crucial needs of American businesses, the US cybersecurity workforce needs to grow by 62%!

The module was embedded in a junior level computer science class required to be taken by all computer science and electrical engineering students. The course introduces Unix commands and tools for software development and testing. Students learn to use Unix commands for directory navigation, creating files, compiling programs, and setting file permissions. Course includes design, construct, and testing programs using scripting languages.

The module was also designed to help students develop an entrepreneurial mindset [1]. The entrepreneurial mindset is a broad term for how students grow and change into the computer scientists of the future, with a mindset focused on creating value for society in a broad way. Creating value includes helping students develop character traits that will make them ethical decision makers in the future. To address this goal, the module was designed to help the students build strong habits and skills about complex ethical issues.

In the business discipline, an alternative viewpoint on ethics education has been articulated by Mary Gentile [2]. She argues that students often have a strong ability to identify an ethical challenge, but they may not have the skills needed to articulate it in a professional context. For engineering and computer science students, this means that most students can easily determine that they should not hack a large company's database. However, the professional culture may mean it is difficult for them to articulate concerns; Gentile believes that students need to practice discussion of ethical issues so they are prepared for this challenge in industry.

The module developed had several learning objectives:

1. Analyze social engineering methods using Kali Linux.
2. Explain common physical security weaknesses.
3. Observe trends about the changing world with a future-focused orientation/perspective. Classify key players in security and predict future trends

4. Consider a problem from multiple viewpoints. Analyze current security issues and ramification of decisions taken by companies/governments.
5. Develop an action plan to modify or address an ethics or character issue.

The research goal of the project was to determine if a structured module in a computer science course could help students enhance and practice skills for discussing ethics. This module is also part of a larger effort at the University of Portland to embed the entrepreneurial mindset across the curriculum.

Background

Many prior authors have published in the field of computer science and ethics. Logan and Clarkson wrote early discussions on the ethics of teaching students about hacking methods [3]. Many authors advocate for ethical hacking as an important tool that should be taught to students [4–6]. Salhenia recently surveyed students about the ethical issues in computing [7].

A summary of prior work on teaching ethics of hacking is shown in Table 1. No research was found on instructors focusing on allowing students to determine the ethics of hacking from multiple viewpoints, or work that focused on student mindset growth in this context.

Table 1. Summary of engineering ethics methods from the literature.

Author	Year	Pedagogical Methods	Ethics Focus Area
Conti [8]	2011	Hacking Competition	
Wang et al. [9]	2017	Lab module	Vulnerability scanning
This Study	2019	Active learning, case studies, discussion, laboratory project	Ethical hacking and entrepreneurial mindset

Ethical Hacking Module Design

A two-week module was designed and delivered by Radana Dvorak with the goal of students developing an entrepreneurial mindset while exploring issues related to ethical hacking and its impact in the field of information security and cybersecurity. The problem was analyzed from multiple viewpoint exploring white hat, grey hat and black hat hacking, and analyzing trends and perspectives from industry and government. The module included practical exercises exploring Kali Linux and learning basic password cracking, creating a private key, analyzing networks, and collecting information using scanning techniques. The module was designed to increase students' curiosity and awareness as they will be confronted with security issues in their software engineering careers. The module also explored industry needs and students were presented with data depicting unfilled cybersecurity jobs globally, and the US.

The module started in the eighth week of a semester course due to students first needing to develop Unix skills and acquire a solid understanding of the file structures, permission setting and scripting. Weeks eight and nine also aligned with the National Cybersecurity Awareness Month in October.

The module was delivered as follows:

1. Students were placed in teams of four, and first part of the 'four corners exercise was introduced. Teams were asked to discuss whether it's ethical to hack, and then add their names under one of the four statements given the phrase "It is Ethical to Hack". (students did not have to come to a unanimous agreement in their teams):
    a. Strongly agree
    b. Agree
    c. Strongly disagree
    d. Disagree

2. Case studies were handed out; each group had a different type of case study, all related to ethical hacking and how the ethical hacker was treated by company and/or government, and the authorities. Each group was required to:
    a. Read the case study and discuss in group (15 minutes)
    b. One group member presented the case to the whole class
    c. Class discussion followed about the actions taken by the hacker, and whether they acted 'ethically'; actions taken by the companies and/or government, and why they were taken. This created a very rich discussion.
3. Students were asked to go back to the white board where the statement "It is Ethical to Hack", was stated, and if they changed their mind from their first thoughts, they placed their name in one of the categories above (using a different color marker). Approximately twenty percent (20%) of the students changed their minds[1].
4. A lecture was delivered defining information security, cybersecurity and defined the 'type' of hackers. The lecture also highlighted industry and government issues society is faced with. Students asked questions and discussion continued throughout the lecture.
5. Lab 1 followed the lecture. The lab introduced students to Kali Linux. Students were required to complete a set of exercises which included:
    a. Logging into the VM and Kali, familiarizing themselves with Kali Linux
    b. Linux file systems & applications in Kali Linux
    c. Generating a private key
    d. Password cracking basics - using Kali wordlist and hashcat
    e. If students completed the above before the end of the lab, they were instructed to practice their skill with OverTheWire Wargames, Bandit and Natas [12]. These games are designed to teach cybersecurity skills in a game environment.
6. Lab 2 was delivered a week later. It included:
    a. Short lecture highlighting the lab requirements

[1] Data was not formally collected for this exercise, so 20% is an estimate.

b. Analyzing networks and introduced to 'dig'
c. Using tools such as NMAP and ZenMAP for network information gathering.
d. Continue (or begin) the OverTheWire cyber games introduced in the previous week.

Participants

The student participants were all juniors in computer science with a few electrical engineering students. Forty students completed the survey, 86.95% of the total enrolled. Due to the relatively small size of the class, the survey design did not include gender and ethnicity questions. For the Shiley School of Engineering in total, the student population is 641 students, 27% female and 44% underrepresented minorities. The course instructor was an experienced computer science faculty member with over 20 years of experience.

Assessment Methods

To determine if students had met the learning objectives the module was designed to address, a student survey was delivered to assess specific learning objectives. Table 2 gives an example of the type of survey question students were asked. The questions were modified slightly for each objective.

Table 2. Example of a student survey questions where students were asked to consider each learning objective on a Likert scale.

*For the learning objective listed below, please rank the extent to which your capacity increased **during this class**. (circle one) Then, please elaborate with a specific example.*

Question	Not at all	Very Little	To a Small Extent	To a Moderate Extent	To a Great Extent
To what extent has your ability to explain key ideas of ethics and character formation increased during this class?	1	2	3	4	5
Describe a specific example of how your knowledge of ethics and character formation increased in this class.					

Results

The module was implemented in Fall 2019 as part of a junior level course in computer science. The observer assessment and survey results have been summarized below.

Student Survey Assessment

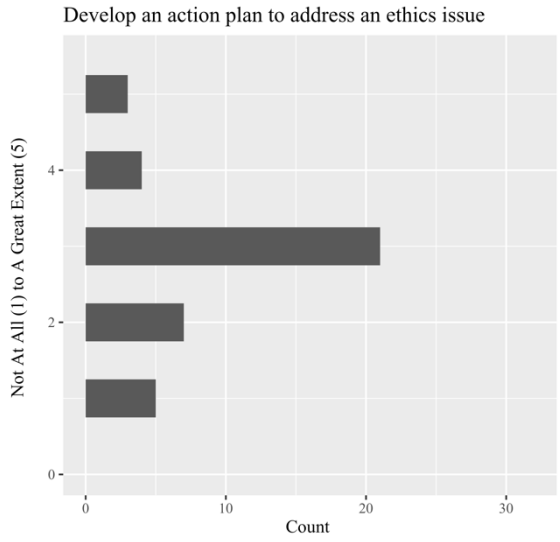
An optional student survey was also conducted to determine how effective this module was for overall student learning for the subject of ethics.

The summary of the Likert questions has been included in Table 3 and Figures 1-3. Students were asked to rank the learning objectives on a Likert scale of 1 to 5 where 1 was the worst ranking and 5 was the best ranking. In general, the students ranked the objectives well, with the lowest score for the objective about developing an action plan for ethics. This might indicate ways to improve the module in future course offerings. The highest values were given to considering multiple viewpoints, indicating the mindset aspects of the project may have been successful.

For each learning objective student were also asked to describe a specific example. The student essays were summarized using a natural language processor and a word cloud of the responses is shown in Figure 4. Students highlighted terms like "perspective" and "trends", but terms well aligned with the goals of the ethics module.

Table 3. Summary of the Likert question results in the student survey.

Objective	*n*	*Mean*	*Standard Deviation*
Observe trends about the changing world with a future-focused orientation/perspective	40	3.13	1.09
Consider a problem from multiple viewpoints	40	3.55	1.20
Develop an action plan to modify or address an ethics or character issue	40	2.83	1.03



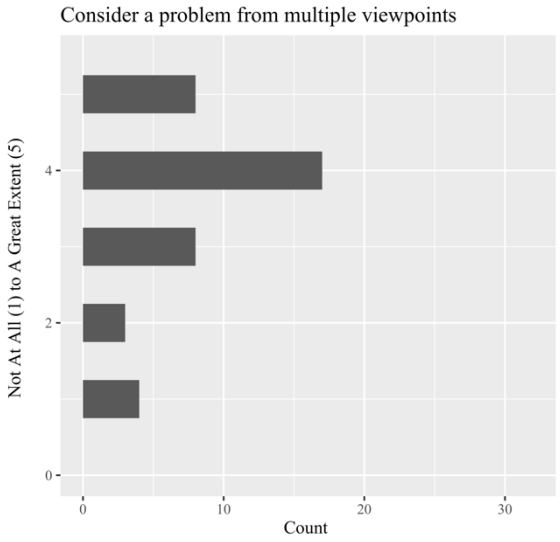


Figure 1. Student responses to the learning objective "Develop an action plan to modify or address an ethics or character issue".

Figure 2. Student responses to the learning objective "Consider a problem from multiple viewpoints".

Student Comments and Trends

The essay section of the student comments was reviewed by an educational expert and summarized by learning objective. For the objective "Observe trends about the changing world with a future-focused orientation/perspective." the students reported the KEEN module helped them to better understand the rise of cyber hacking in the real world and the potential for careers in cybersecurity (48%; n = 19 students). Characteristic student comments:

- "Classes on cybersecurity is helpful in helping me see what problems exist and will evolve into the future."
- "Working with a lot of different programs has allowed me to think about trends to make the world more efficient."
- "We discussed the growth in demand for cybersecurity professional on both the personal/individual and institutional levels."
- "I have been able to understand how CS is in every industry. In accounting, CS can be powerful in data manipulation and protection. We also went over real case examples from the news which were applicable."

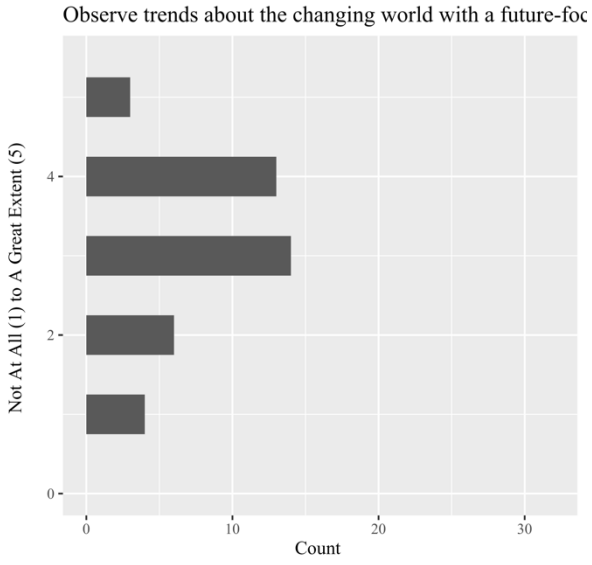


Figure 3. Student responses to the learning objective "Develop an action plan to modify or address an ethics or character issue".

Figure 4. Student natural language summary of the open-ended essay questions.

For the learning objective, “Consider a problem from multiple viewpoints” many of the students described how the KEEN module helped them to see problems from multiple viewpoints, including both the ethics of hacking and solutions to problems (55%, 22 students).

- “Every lab my partner and I have different solutions to the same problem.”
- “All labs have ways to think differently about problems.”
- “There are many times where I saw many possibilities of outcomes either for specific class project for assignment topic that was introduced in class.”
- “I believe that the assignment's solution possibilities allow for students to think outside the box, and to consider different viewpoints in regard to different problems.”
- “During our conversations about the sentences of ethical hackers, I learned about both the hacker's perspective and the company's perspective and the ways they differed.”
- “We learned about how to differentiate grey-hat, white-hat, and black-hat hacking.”

For the learning objective, “Develop an action plan to modify or address an ethics or character issue” students again referenced how the KEEN module helped them think about hacking from different viewpoints, referencing white hat, grey hat, and black hat ethics (38%, 15 students).

- “I have the ability to understand better the implications of an ethics issue in my class through expanded skills and as such can better address the issue.”
- “Learning about the white hates and black hats hackers and the morality/legality of hacking.”
- “By viewing previous cases of ethical grey areas regarding hacking, I have seen punishments for "hackers" that are extreme. This made me think about adequate responses to cases of ethical hacking.”
- “We went over ethics of cybersecurity in great detail. That was the only lab we covered ethics. I have a better idea of when it is ethical to hack, the laws in place, and the consequences.”

A few students used the open response area to provide more general feedback on the module. Most of the responses were positive, with students offering appreciation for the complexity of this assignment when compared with the more traditional lab elements. Other students observed that working in teams was helpful for them to understand other viewpoints.

Conclusions

A novel project was developed for computer science students to help them develop specific skills for ethical hacking and entrepreneurial mindset. Students in a junior level computer science course tested this module in the fall of 2019 and the educational methodology was a success. The module was successful in all aspects; student enjoyed the labs, they learned valuable concepts and skills, in addition to being confronted with the complex issues associated within the cybersecurity area of Computer Science. One of the discussions centered around ‘with great power comes great responsibility’, and how the tools, such as Kali Linux can be used ethically or illegally.

Students reported that the module was most helpful for learning to consider a problem from multiple viewpoints, an excellent outcome for mindset grown in computer science students.

Future work will include adjusting this module to address the planning aspects of ethics in more detail. The instructor noted that the activity might benefit from additional course time, moving from two weeks to three weeks during the course. There are few changes the instructor will make next time this is delivered. One of the issues the four corners exercise highlighted is that a number of students had knowledge about the different types of hacking practices. They questioned having to choose one of the categories without specific details. This exercise would have worked better, for instance, if students were given case studies without the outcome and then complete the four corners exercise answering 'the hacker's actions were ethical' strongly agree, agree, disagree and strongly disagree, and discuss what outcome should have been taken by companies, authorities, etc.,. After this discussion, then provide the students the second half of the case studies which included the actions taken, and then record if students' viewpoints change and why.

Future research will also focus on helping students articulate the difference, distinctions, and overlap between ethics and law. The instructor plans to deliver the module in the 2020-2021 academic year and built on what was learned, and the outcomes from the surveys. The work in this module will serve as a reference for enhancing student thinking about ethics of hacking.

Acknowledgements

Thanks to the W.M. Keck Foundation for funding this study. Thanks to the many undergraduate students who made this project and paper possible.

References

1. KEEN. KEEN - The Framework [Internet]. [cited 2020 Jan 16]. Available from: https://engineeringunleashed.com/mindset-matters/framework.aspx
2. Gentile MC. Giving Voice to Values: How to Speak Your Mind When You Know What?s Right [Internet]. Yale University Press; 2010 [cited 2015 Mar 30]. 256 p. Available from: http://books.google.com/books/about/Giving_Voice_to_Values.html?id=Y7yrKBVflgkC&pgis=1
3. Logan PY, Clarkson A. Teaching students to hack: curriculum issues in information security. In: 36th SIGCSE technical symposium on Computer science education [Internet]. 2005 [cited 2020 Jan 16]. p. 157–161. Available from: https://dl.acm.org/doi/abs/10.1145/1047344.1047405
4. Saleem SA. Ethical hacking as a risk management technique. In: Proceedings of the 2006 Information Security Curriculum Development Conference, InfoSecCD '06. 2007. p. 201–3.
5. Radziwill N, Romano J, Shorter D, Benton M. The Ethics of Hacking: Should It Be Taught? 2015 Dec 8 [cited 2020 Jan 16]; Available from: http://arxiv.org/abs/1512.02707
6. Pashel BA. Teaching students to hack: Ethical implications in teaching students to hack at the university level. In: Proceedings of the 2006 Information Security Curriculum Development Conference, InfoSecCD '06. 2007. p. 197–200.
7. Salehnia A, Salehnia S. Ethical Issues in Computing: Student Perceptions Survey. In: 2016 ASEE Annual Conference & Exposition Proceedings [Internet]. ASEE Conferences; [cited 2020 Jan 16]. Available from: http://peer.asee.org/26740
8. Conti G, Babbitt T, Nelson J. Hacking competitions and their untapped potential for security education. IEEE Secur Priv. 2011 May;9(3):56–9.
9. Wang Y, Yang J. Ethical hacking and network defense: Choose your best network vulnerability scanning tool. In: Proceedings - 31st IEEE International Conference on Advanced Information Networking and Applications Workshops, WAINA 2017. Institute of Electrical and Electronics Engineers Inc.; 2017. p. 110–3.
10. The Cybersecurity Talent Gap Is An Industry Crisis Forbes Technology CouncilBrian NeSmith Forbes Councils Member Forbes Technology Council https://www.forbes.com/sites/forbestechcouncil/2018/08/09/the-cybersecurity-talent-gap-is-an-industry-crisis/#26548da6b367, Aug 9, 2018,
11. "Strategies for Building and Growing Strong Cybersecurity Teams" (ISC)2 Cybersecurity Workforce Studey, https://www.isc2.org (2019)
12. OverTheWire Wargames https://overthewire.org/wargames/