2017

CyberPDX: A Camp for Broadening Participation in Cybersecurity

Wu-Chang Feng
Portland State University

Robert Liebman
Portland State University

Lois Delcambre
Portland State University

Michael Mooradian Lupro
Portland State University, lupro@pdx.edu

Tim Sheard
Portland State University

See next page for additional authors

Citation Details

Britell, S., Delcambre, L.M., Feng, W., Liebman, R., Lupro, M., Recktenwald, G., & Sheard, T. "CyberPDX: A Camp for Broadening Participation in Cybersecurity." ASE @ USENIX Security Symposium. 2017.

Authors
Wu-Chang Feng, Robert Liebman, Lois Delcambre, Michael Mooradian Lupro, Tim Sheard, Scott Britell, and Gerald W. Recktenwald

CyberPDX: A Camp for Broadening Participation in Cybersecurity*

Wu-chang Feng[1], Robert Liebman[2], Lois Delcambre[1], Michael Lupro[3], Tim Sheard[1], Scott Britell[1], and Gerald Recktenwald[4]

[1]Department of Computer Science, Portland State University
[2]Department of Sociology, Portland State University
[3]Department of University Studies, Portland State University
[4]Department of Mechanical Engineering, Portland State University

Abstract

With society's increasing dependence on technology infrastructure, the importance of securing the computers, networks, data, and algorithms that run our digital and physical lives is becoming critical. To equip the next generation of citizens for the challenges ahead, an effort is underway to introduce security content early in a student's academic career. It is important that these efforts broaden participation and increase diversity in the field. While many camps and curricula focus on introducing technical content and skills related to cybersecurity, such approaches can prematurely limit how students view career opportunities in the field, potentially limiting those who ultimately pursue it. In addition, it is likely that many problems in cybersecurity can only be addressed in an interdisciplinary manner by those trained in the arts and humanities as well as in technical fields [1].

This paper describes CyberPDX, a residential summer camp that introduces cybersecurity to high school students. Key to CyberPDX is its focus on the range of societal issues that will be impacted by cybersecurity as well as its coverage of the breadth of roles that students can play to help address them. Through four learning threads taught by faculty in Computer Science, Sociology, and Film Studies, the CyberPDX curriculum spans topics from constitutional law, cyberpolicy, ethics, and filmmaking to programming, cryptography, security, and privacy in order to show students how broad cybersecurity issues are and the many ways they can participate in helping to solve them.

1 Introduction

With the impact of recent security incidents such as the 2016 US Presidential Election and the theft of $81 million from Bangladesh's central bank, it is difficult to overstate the importance of cybersecurity to our world's future. To address the challenges posed by cybersecurity, it is critical that we engage our current generation of students to provide them with the skills they need to solve the complex problems they will be facing. Towards this end, this paper describes CyberPDX, a one-week residential camp for teams of high school students and teachers. Similar to other high school camps devoted to cybersecurity, CyberPDX is intended to introduce computer security to students early in order to inspire them to eventually pursue careers in it. CyberPDX has two main goals. The first is demonstrating the importance of cybersecurity by exposing students to some of the emerging problems that their generation will face so that they are motivated to focus on these topics long after the camp is over. The second is giving students the opportunity to try out a diverse number of roles that people can play in tackling these problems and to cultivate competence and confidence in them so that they may be able to participate as cybersecurity professionals in the future.

The role of a cybersecurity professional is a bit of an enigma partly because of the myriad ways one can take part in it. For example, one could be:

- A cryptographer like Shafi Goldwasser or Silvio Micali designing the core underlying protocols that

*This material is supported by the National Science Foundation under Grant No. 1623400. The 2015 CyberDiscovery camp that initially employed this curriculum was supported via the Cyber Discovery Program at the National Integrated Cyber Education and Research Center. The 2016 and 2017 CyberPDX camps that host the current version of the curriculum are supported by NSF and the National Security Agency via GenCyber under Grant No. 206865. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author and do not necessarily reflect the views of the National Science Foundation, the National Security Agency or any supporting agency.

secure Internet transactions.

- A journalist like Brian Krebs, shining light on cybercrime activities throughout the world.
- A software developer like Joanna Rutkowska or Jessie Frazelle, securing operating systems and applications via strong isolation.
- A politician, like Ron Wyden, championing strong encryption and privacy while actively opposing unlawful government surveillance.
- A vulnerability analyst like Tavis Ormandy or Natalie Silvanovich, finding flaws in software.
- A television producer like Sam Esmail, creating award-winning television dramas that expose contemporary issues in computer security.
- A professor like Lorrie Cranor, developing more usable security for end users.
- A lawyer like Susan Hennessey, helping expose and shape issues in cybersecurity laws.
- A cryptanalyst like Juanita Moody, leading the SIGINT response to the Cuban Missile Crisis
- A novelist like Veronica Roth raising awareness of cybersecurity issues in young adults via novels.
- A podcaster like Patrick Gray, bringing attention to the latest developments in cybersecurity.
- A cartoonist like Randall Munroe, explaining complex security issues with humorous illustrations.
- A program manager like Deborah Frincke directing research and education in cybersecurity at the national level.
- A film-maker like Alex Gibney, producing films to highlight the need for laws to govern cyberweapons.

Consequently CyberPDX takes a broad, cross-disciplinary approach in its curriculum design in order to highlight the variety of roles people can play in cybersecurity. Key to its approach are 1) motivating the importance for students to pursue the area, 2) highlighting the diversity of the field to ensure student's view of cybersecurity careers is not overly narrow, 3) providing engaging activities that intrinsically motivate students to find success and gain experience in multiple content areas, and 4) offering memorable experiences to ensure students' first exposure to cybersecurity doesn't turn them away from it.

Specifically, components of the camp include:

- A curriculum that integrates technology and the arts
- Role playing exercises that allow each student to practice different aspects of cybersecurity
- Intrinsically motivating activities that focus on creativity.
- A focus on collaboration and communication amongst students via peer learning and group problem solving
- Scaffolded exercises merging knowledge acquisition with skill development to build competence and confidence in students
- Inclusive targeting of students who are underrepresented in college, in Computer Science programs, and in the field of cybersecurity: women, minorities, and potential first-generation college students.

2 Approach

Based on ideas from educational research, CyberPDX attempts to engage a broad set of students through its use of problem-based learning, cooperative learning, multimodal instruction, and scaffolded activities.

2.1 Problem-based learning

Problem-based learning is a student-centered approach to instruction where learning occurs amongst student groups with teachers stepping back and acting as facilitators. With problems organizing the focus and stimulus for learning, knowledge and skill acquisition can be made more self-directed by the student, leading to positive results [2]. In camp, teams of students engage in solving problems that range from negotiating conditions for an agreement on digital surveillance, to writing a program to break a web site's authentication system, to developing a digital response to an imminent cybersecurity threat, to helping save the city (a fictitious one) from annihilation by cracking cryptographic codes. By developing inquiry-based activities and giving students the independence to pursue them, our goal is to provide students a more effective learning experience.

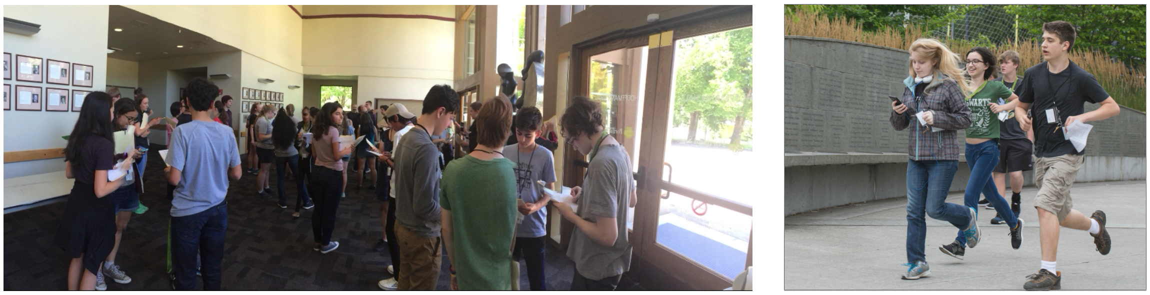

Figure 1: Physical activities used in CyberPDX

2.2 Cooperative learning

Cooperative peer-learning is another approach that has been shown to improve learning outcomes [2]. To this end, CyberPDX creates a non-competitive, team-based environment in order to give students the mind space to focus on the challenging curriculum. A low-threat, high-engagement environment has been shown to maximize attention learning [3]. To cultivate this, the camp uses karma points to recognize and reward teams and individuals for helping each other on a daily basis. In addition, while activities are scored in order to give feedback to students for their work, the camp uses ranking and competition sparingly as many students are turned off by it. For example, while the camp features an Urban Race, the race is set up to allow all finishers to meet the goal of "saving the city" as long as they solve all of the race's challenges.

While a low-threat environment gives students room to learn, the camp also emphasizes peer learning. Students are paired up or placed in groups to collaborate on a daily basis. For example, cryptographic problems are employed in which each student is given part of a message to decrypt. Students then collaborate with the rest of their team to combine all parts of the message to derive the complete decrypted message. This enables those who finish their part of the problem quickly to help others solve theirs. In one exercise, each student in the camp is given one character of a message from Optimus Prime to decrypt and eventually all students in the camp come together to derive the original message. This pattern of student organization extends through the entire camp which includes pair-programming, intra-team collaboration on a digital film response, and inter-team negotiations in a cyberpolicy summit.

2.3 Multi-modal instruction

Studies have shown that students can learn in a variety of ways and that different students have different learning styles. To this end, CyberPDX incorporates a variety of instruction modes including visual, physical, and applied. To engage visual learners, lecture material is given via 3-D presentations (using Prezi) and threads feature visual tools and assignments. Some examples include the programming thread's use of visual block-based programming tools (Blockly and TurtleGraphics) and the filmmaking thread's use of daily video assignments. To engage physical learners, a combination of physical props (such as a Caesar cipher wheel) and physical activities are used. Physical activities range from having campers mingling around the room during the campwide mixer in the cyberpolicy thread to students running around campus during the Urban Race activity in the cryptography thread as shown in Figure 1. Finally, to engage students who best learn by applying what they learn immediately, the camp features frequent hands-on activities interspersed throughout presentations as well as open-ended activities that require students to apply their unique talents and creativity to solve [3, 4].

2.4 Scaffolded activities

One of the goals of CyberPDX is to reach non-traditional students who would not otherwise consider going to college, let alone pursue a career in cybersecurity. As part of the selection process, CyberPDX focuses on underrepresented populations that would be best served by attending the camp. As a result, the camp assumes students have no prior knowledge in computing and provides laptops and computing infrastructure for all who need it.

To ensure that all students eventually obtain competence and confidence in the material, the camp features sets of tightly scaffolded activities that allow them to

Figure 2: Saving the city in the cryptography thread

make consistent progress towards mastery. Exercises and challenges in all threads are designed so that all students can succeed, with the goal of having every student participate in an exercise in every thread. For example, in the cryptography and security thread, a capture-the-flag (CTF) style format is used for homework that consists of 24 levels of cryptographic puzzles of incrementally increasing difficulty. One of the benefits of a CTF format is that it allows students to obtain immediate feedback on whether they are successful, allowing them to move on to the next set of skills to master. By having problems whose complexity matches a student's skill development, a student can quickly develop mastery while avoiding boredom or frustration when levels are too easy or difficult. With proper scaffolding, by the end of the week, students are able to see the progress they have made and then adopt more of a growth mindset for themselves when it comes to cybersecurity.

3 Curriculum

The CyberPDX curriculum includes 4 learning threads: cryptography and security, cyberpolicy, programming, and filmmaking. As happens in the real world, the camp weaves these threads together to show how they influence and inform each other.

3.1 Cryptography and security

The cryptography and security thread consists of 5 modules and a film (The Imitation Game) along with a scaffolded capture-the-flag activity that leads into an Urban Race. To motivate the importance of learning the material, the thread begins with a look back at how cryptography and security (and the lack thereof) have directly changed the course of history such as in World War I with the decoding of the Zimmerman telegram and in World War II with the cracking of the Enigma. Since cryptography is now done mostly in the digital domain, the second module focuses on encoding and decoding schemes such as binary, hexadecimal, and ASCII. The third module introduces simple transposition, monoalphabetic, and polyalphabetic ciphers including the Enigma. After showing campers how the Enigma worked and the core weakness it suffered, as dramatized in the pivotal bar scene in The Imitation Game, students are then shown the full film, allowing them to follow the technical aspects of it while learning about Alan Turing and his role in breaking the Enigma. The fourth module picks up after the Enigma to introduce public-key cryptography, the notion of basing encryption on computationally difficult problems, and the potential challenges that might ensue in the future when those problems are no longer difficult [5]. The final module examines how public-key cryptography can be subverted when the adversary is inside the network performing a man-in-the-middle attack and how this attack vector has been used by governments to break Internet encryption [6].

To help students develop the skills to analyze and decode messages as well as break cryptographic algorithms, modules alternate delivery of conceptual content with group exercises. Specifically, after covering encoding and encryption schemes, students are presented with a message and required to work together to decode or decrypt it. The thread extends these exercises with an engaging CTF which culminates in an Urban Race activity to further reinforce these concepts and skills. To add an additional level of engagement, the exercises use a story based on the Divergent series, a popular young adult novel series by Veronica Roth [7]. In this exercise, students follow Four, one of the Divergent protagonists, in his role as a penetration tester, as he uses a variety of security tools and techniques to compromise the computing systems of both his own clan and those of a rival clan. With this exercise, students research basic security attacks and defenses to identify which ones Four uses in his exploits, with the thread ultimately culminating in campers applying their acquired skills and knowledge to save their city from (fictional) destruction as shown in Figure 2.

3.2 Cyberpolicy

The Cyberpolicy thread looks at the evolution of US cyberpolicy as technology has altered the boundary between private and public communication in our increasingly networked society. Students study the constitu-

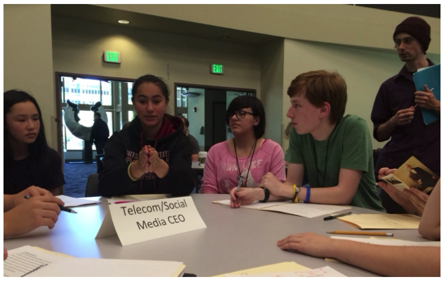

Figure 3: CyberSummit activity

tional framework and historical events that shape policy in the US with regard to security, privacy, and intellectual property.

After being introduced to the basic constitutional principles that US cybersecurity policy must adhere to, they then learn the positions of key stakeholders in the policy debate. With this background, students are brought into a deeper analysis of digital rights and responsibilities by researching and reviewing key stakeholders in the contemporary cyberpolicy sphere. This builds towards the camp's CyberSummit activity: a role-play simulation that is based on President Obama's Summit on CyberSecurity and Consumer Protection held February 2015 at Stanford University. Students watch clips from the actual Summit, are assigned the roles of major actors (President, NSA director, Apple CEO, Telecom/Social Media CEO, ACLU lawyer), and receive role dossiers prepared for them to learn the roles. They then play their roles at a campwide mixer before participating in the CyberSummit where they caucus with students from other schools with the same role in order to discuss the particular interests and responsibilities their role entails (as shown in Figure 3), as well as share potential questions they may face and answers they might give as part of an overall policy negotiation. Then, students move to mixed groups at the negotiating table to frame a cyberpolicy on a major issue like collecting metadata or encryption backdoors. To succeed at the CyberSummit, they must apply what they've learned about programming, cryptography, and constitutional law, and must collaborate with all stakeholders at the table, reckon with competing issues, and attempt to arrive at a consensus decision.

Soon after the summit concludes, students are given a pivot. A loud alert signal calls for teams to respond to a mock, imminent cyber-incident similar to those used in Cyber 9/12 student competitions [8]. They have less than 24 hours to present an action plan to the President that synthesizes and applies what they have learned throughout the camp. Specifically, students are tasked with using what they have learned in the filmmaking thread to script, cast, shoot, and edit a 5-minute film showing how to respond to the incident. The film they create must leverage knowledge of the roles they have studied and address the complexities of digital policy decisions being made in our country. The films are shown at the end of the camp to demonstrate how students have integrated cybersecurity principles, cyberpolicy, the use of computers, and the creative arts.

3.3 Programming

The programming thread aims to take students with no prior experience and helps them develop an ability to understand and write programs. While the thread helps demystify programming and show students that programming language constructs are not difficult to learn, it also allows students to appreciate how challenging it is to ensure a program's correctness and how misplaced trust in a program's correctness can lead to significant problems.

The thread begins by leveraging two well-tested methods for engaging beginners: graphical, block-oriented programming via Blockly as used in code.org and Turtle Graphics as implemented in Python. Both methods were originally designed to teach children, but have also been used successfully to teach adult beginners in introductory CS courses. Key to both of these approaches is the ability to focus on the underlying programming concepts while limiting the need to teach programming language syntax and compilation tools. Another important feature of both approaches is that the program results are visual, thus providing students with immediate feedback. The thread supports the common practice of pair programming, where two students work together to write a program sharing a laptop that we provide to schools that lack them. Students with some programming experience are encouraged to help other students learn with the goal of having every student be able to explain how each line of her or his program works - regardless of the program's complexity. Thus, beginners might write and understand a relatively simple program while more experienced programmers can write and understand more complex ones.

Adopting the applied mode of learning, the lessons include quick explanation and demonstration sessions that are intermixed with student programming challenges. Since code.org puzzles (i.e., programs) can be written by any student in a web browser and since Python is easily installed on most any computing device, students are able to directly apply what they have learned. Basic concepts such as program statements, conditionals, loops, functions, parameters, and return values are introduced along with programming challenges that ask students to apply the concepts. Core cybersecurity principles such as abstraction, modularity, data hiding, and simplicity are taught in the context of programming.

The thread culminates with two large challenges. The first is an open-ended Turtle art program that demonstrates the principles of abstraction, modularity, data hiding, and simplicity. The second challenge ties in with the cryptography and security thread in which students either write a Python program to decrypt text when given the program to encrypt it or write a Python program to perform a brute-force attack against a website's authentication scheme.

3.4 Filmmaking

In our cybersociety, communications media and the creative arts are some of the primary means of influencing public thinking and public policy. Whether through books, movies, news articles, or television shows, the ability to communicate cybersecurity issues effectively is extremely important to raising awareness. The filmmaking thread shows students how impactful films have altered public policy in the past and teaches them the basics of creating compelling digital content of their own design.

Campers are shown how film-makers target affective responses in audiences through three cybersecurity related movies: "War Games", "The Imitation Game", and "Robot and Frank". Using these films as examples, they learn a variety of basic filmmaking techniques in order to script and shoot digital films each day that effectively communicate what they are learning at camp . As part of this process, students are shown how to use video editing software and how to upload and publish their final product on YouTube.

The filmmaking thread eventually merges with the cyberpolicy thread when students are presented with a pivot: a fictitious cybersecurity incident to which campers must create a video that communicates their response. Past scenarios for the pivot have asked student teams to formulate policy responses to 1) a coordinated attack on critical infrastructure and 2) the discovery of an undisclosed backdoor vulnerability in a popular smartphone app (Pokemon Go) being leveraged by government agencies to track an imminent attack. At the end of the camp, the videos are shown to students, teachers, parents, siblings, and school principals at a final dinner where teams are recognized for their creative use of the medium and their demonstration of camp content.

The use of films acts as the glue which ties the threads together and provides touchstones for students in their camp activities. One example is with "War Games". The film, with its rather alarming depiction of a fictitious computer hacking act, impacted both computer crime policy [9], and nuclear disarmament policy under the Reagan administration [10]. Another example is "The Imitation Game" which depicts how a diverse team of codebreakers of varying genders, nationalities, and orientations managed to break the Enigma machine. The movie also shows the impact that the breakthrough had on the course of World War II, the moral conundrum that the government faced in keeping it secret, and the advances in computing that were made in breaking it. The movie also provides a valuable historical context in which students can examine why governments seek to keep security vulnerabilities they discover secret and why they seek backdoors to encryption schemes. Finally, the camp uses "Robot and Frank" as a vehicle for highlighting the impact programming advances are having on society and the need to address the unintended consequences of an increasingly autonomous and robotic future. While students watch the films as a break from the fast-moving pace of camp, they are fully engaged in integrating their learning across threads and seeing how the arts link with the real challenges of a cyber-society,

4 Evaluation

The CyberPDX curriculum originated from the Cyber Discovery [11] program before transitioning to a GenCyber camp in 2016 [12]. A third offering is scheduled for July 2017 through the GenCyber program. The GenCyber program supports a diverse range of camps that include student camps, teacher camps, and combined camps. CyberPDX is run as a combined camp and is offered to rising high-school sophomores with no prior experience assumed. Changes made in the cryptography thread include the collaborative exercises, the scaffolded CTF, and the tie-ins with the film "The Imitation Game" and the book series "Divergent". The robotics thread was replaced with a Python-based programming module that tied more directly into the cryptography and security thread by culminating in students writing a program to brute-force the authentication scheme used on a web site.

Metric	Average rating (1=Strongly Disagree, 5=Strongly Agree)
$Q6$: I know what cybersecurity means	4.19
$Q7$: I know more about cybersecurity than I did before this camp	4.70
$Q8$: I am more comfortable learning cybersecurity concepts now.	4.24
$Q9$: I can explain why cybersecurity is important.	4.26
$Q10$: I learned a lot about cybersecurity.	4.53
$Q11$: I enjoyed learning about cybersecurity.	4.30
$Q12$: I would like to learn more about cybersecurity	4.02
$Q13$: Before this camp I was thinking of a career in cybersecurity.	2.41
$Q14$: This camp has made me more likely to pursue a career in cybersecurity.	3.33
$Q15$: After this camp, I am no longer interested in a career in cybersecurity.	1.94
$Q16$: The teachers in this program made me more interested in cybersecurity.	4.17
$Q17$: My opinions and ideas were respected in this camp	4.17
$Q18$: I enjoyed the projects and activities at this camp.	4.40
$Q19$: I am glad I attended this camp.	4.65

Table 1: Student survey results from CyberPDX 2016

The liberal arts thread was replaced by the CyberSummit role-playing exercise and the pivot which addressed government policies on digital surveillance and strong encryption. The arts thread was modified to teach filmmaking so the policy response to the pivot challenge could be switched from a debate-style presentation in front of camp faculty to a film that is viewed by all camp participants and their families, and later by students at their home schools. Finally, CyberPDX moved from a competitive format which left many students behind to a collaborative format where students from all school teams were encouraged to interact and cooperate in order to create a learning community centered around challenging material.

4.1 Camp survey results

In the 2016 iteration, 10 schools, 20 teachers, and 58 students (58% women, 40% minority) participated. Table 1 lists the results from the student evaluation of the camp via the GenCyber survey that students take upon camp completion. As the table shows, on average, students agreed that the camp impacted their knowledge of cybersecurity ($Q6 - Q9$), that they accomplished positive learning outcomes ($Q10 - Q12$), that their likelihood of pursuing a career in cybersecurity was positively influenced ($Q13–Q15$), and that their overall experience with the camp was positive ($Q16 - Q20$).

CyberPDX uses the same survey that is used to evaluate all other GenCyber camps. While comparing survey results among camps can be a bit of an apples to oranges comparison due to each camp having differing formats and goals, comparisons against camp averages can provide a general indication of the utility of the camp design. Table 2 shows several GenCyber metrics across all camps as reported by GenCyber evaluators. The data was collected from 3,417 students, an 83.1% response rate. The first two metrics ($Q4$ and $Q5$) show the average perceived ability students had in computing and cybersecurity upon entering the camp. As the table shows, CyberPDX students had below average perceived ability, likely the result of the camp targeting underrepresented students. The next two metrics (self-efficacy and perceived learning) show how much growth students felt they gained in cybersecurity by participating in the camp. The self-efficacy metric is the average of $Q6$, $Q7$, $Q8$, and $Q9$ in Table 1 and the perceived learning metric is the average of $Q10$, $Q11$, and $Q12$. As Table 2 shows, both the self-efficacy and perceived learning metrics for CyberPDX students are slightly higher than the GenCyber average, even though camp participants started out with lower perceived ability ($Q4$ and $Q5$). This may be a result of the next metric, camp experience, which is calculated for all camps as an average of $Q16$, $Q17$, $Q18$, $Q19$, and $Q20$. As the results show, CyberPDX has a higher average camp experience than the average GenCyber camp. Based on a paired t-test performed by GenCyber evaluators, the result is statistically significant

Metric	GenCyber Average	CyberPDX
$Q4$: Perceived Ability in Computing (1=Beginner, 4=Expert)	2.52	2.33
$Q5$: Perceived Ability in Cybersecurity (1=Beginner, 4=Expert)	1.93	1.83
$\overline{Q6+Q7+Q8+Q9}$: Self-efficacy	4.23	4.35
$\overline{Q10+Q11+Q12}$: Perceived learning	4.16	4.28
$\overline{Q16+Q17+Q18+Q19+Q20}$: Camp experience	4.15	4.35
$Q13$: Pre-camp Intent to Pursue Cyber	2.78	2.41
$Q14$: Post-camp Intent to Pursue Cyber	3.45	3.33
$Q14-Q13$: Pre-Post delta	0.65	0.92

Table 2: Comparison of CyberPDX to all GenCyber camps (2016)

compared to the mean for all other camps. The final metrics in the table measure the impact that camps had on a student's interest to pursue a cybersecurity career. As the table shows, the pre-camp intent to pursue a cybersecurity career is lower for the CyberPDX student compared to the average GenCyber student. In both cases, this is improved after students go through camp. As the table shows, while the raw CyberPDX post-camp score is lower than the GenCyber average score, the CyberPDX pre-post change score (delta) of .92 is larger than the GenCyber average of .65. The result indicates that CyberPDX increases campers' intention to pursue a cybersecurity career to a larger degree than the average GenCyber camp. Finally, while individual comments from participants has not been included for brevity, a sampling of responses to the survey question "Q21: My favorite thing about this camp was..." is available [13].

4.2 Curriculum transfer

As a combined teacher-student camp, CyberPDX attempts to facilitate deeper teacher engagement in developing curriculum that can be included in high-school courses. To this end, teachers complete a project that is presented to camp faculty during the Fall term and can obtain 2 graduate seminar credits through our Graduate School of Education. As part of this activity, teachers produced a broad range of interdisciplinary, cyber-curriculum resources for bringing the content, exercises, and teaching techniques used in CyberPDX to their schools. For example, a math teacher developed a set of micro-curricular cyber units to allow teacher who do not have time to devote large chunks of class to cybersecurity, the ability to administer small, self-contained units during ad hoc, odd time periods that arise from assembly days and late openings. A history teacher developed a unit on cryptography through history, showing how encryption has changed over time and how encryption has impacted the course of history. Finally, a media arts teacher developed a section for his musical production students on how audio could be used to pass encrypted messages. In each case, teachers were able to draw from their experiences at camp to develop projects relevant to their work in their schools. Thus, in addition to students bringing their camp learning back to their schools, teachers were able to amplify the reach of the curriculum at each participating school. A repository of all of the projects is publicly available [14].

5 Conclusion

With an increased need for a diverse cybersecurity workforce, CyberPDX is an attempt at exposing the broad field of cybersecurity to underrepresented groups. Initial results have shown that the camp has positively influenced its participants. The resources used for the camp are currently available for public use in camps and high-schools [14, 15].

References

[1] S. Hartley, *The Fuzzy and the Techie: Why the Liberal Arts Will Rule the Digital World*, Houghton Mifflin Harcourt, 2017.

[2] K. Smith, S. Sheppard, D. Johnson, and R. Johnson, "Pedagogies of engagement: Classroom-based practices," *Journal of Engineering Education*, vol. 94, no. 1, pp. 87–101, 2005.

[3] S. Barkley, "Instructional strategies motivate and engage students in deeper learning," *SREB Publications*, April 2013, http://publications.sreb.org/2013/13v06w.pdf.

[4] S. Freeman, S. Eddy, M. McDonough, M. Smith, N. Okoroafor, H. Jordt, and M. Wenderoth, "Active

learning increases student performance in science, engineering, and mathematics," *Proceedings of the National Academy of Sciences*, vol. 111, no. 23, pp. 84108415, 2014.

[5] P. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM J. Comput.*, vol. 26, no. 5, pp. 1484–1509, October 1997.

[6] B. Schneier, "New NSA Leak Shows MITM Attacks Against Major Internet Services," 2013, `https://www.schneier.com/blog/archives/2013/09/new_nsa_leak_sh.html`.

[7] W. Feng, "A Divergent-themed CTF and Urban Race for Introducing Security and Cryptography," in *USENIX Advances in Security Education*, August 2016.

[8] Atlantic Council, "Cyber 9/12 Student Challenge," 2017, `https://atlanticcouncil.org`.

[9] S. Rosenblatt, "Where did the CFAA come from, and where is it going?," 2016, The Parallax.

[10] P. Beinhart, "Think Again: Ronald Reagan," 2010, `http://foreignpolicy.com/2010/06/07/think-again-ronald-reagan/`.

[11] Louisiana Tech University, "Cyber Discovery Camp," 2015, `http://www.latech.edu/cyberdiscovery`.

[12] GenCyber, "Inspiring the Next Generation of Cyber Stars," `http://www.gen-cyber.com`.

[13] GenCyber Survey Results, "CyberPDX 2016 Q21 Feedback," 2016, `http://crypto.cyberpdx.org/static/2016_Q21.html`.

[14] CyberPDX Project Repository, "Curriculum Projects from Teacher Participants in CyberPDX 2016," 2016, `http://repo.cyberpdx.org/`.

[15] W. Feng, "CyberPDX Cryptography Thread," 2016, `http://crypto.cyberpdx.org/`.