# Evaluation of Peer Instruction for Cybersecurity Education

Pranita Deshpande
Department of Computer Science
University of New Orleans
pdeshpa1@my.uno.edu

Cynthia B. Lee
Computer Science Department
Stanford University
cbl@stanford.edu

Irfan Ahmed*
Department of Computer Science
Virginia Commonwealth University
iahmed3@vcu.edu

## ABSTRACT

Peer instruction pedagogy is a student-centric approach that encourages students to read lecture material before coming to class and engages them in class via group discussion and preplanned conceptual questions. Peer instruction has shown promising results in core computer science courses such as Theory of Computation and Computer Architecture, as well as reducing failure rates and improving student retention in computer science major. This paper presents the results of the first-ever attempt to replicate these results in a cybersecurity course, using an action research methodology to implement and evaluate peer instruction in a semester-long cybersecurity course, Introduction to Computer Security. The evaluation consists of quizzes, subjective exams, peer instruction questions, and attitudinal surveys gathered over two control semesters and one peer instruction condition semester. We find evidence of learning gains during group discussion and improvements in dropout and failure rates compared to traditional lecture classes. In attitudinal surveys, most students report that they would recommend that other instructors use peer instruction.

**ACM Reference format:**
Pranita Deshpande, Cynthia B. Lee, and Irfan Ahmed. 2019. Evaluation of Peer Instruction for Cybersecurity Education. In *Proceedings of the 50th ACM Technical Symposium on Computer Science Education, Minneapolis, MN, USA, February 27-March 2, 2019 (SIGCSE '19),* ACM, New York, NY. 6 pages. DOI: http://dx.doi.org/10.1145/3287324.3287403

## 1 INTRODUCTION

Peer instruction is a well-defined teaching protocol designed for active engagement of students in class [3, 26]. It involves conceptual multiple-choice questions and group discussion activities aimed to provoke deep conceptual thinking in students. We aimed to test whether peer instruction could be effective in dealing with the challenges of cybersecurity education, including encouraging out-of-box thinking, developing a mindset of both attacker and defender, and attaining a deep working knowledge of cybersecurity tools and techniques [1, 2, 4–8, 11, 13, 14, 22–25].

Peer instruction requires students to read introductory expository material before coming to class, then engages students in reflection and clarification of the challenging parts of the reading via preplanned conceptual questions on important target concepts. In a peer instruction classroom, lecture is organized into a set of multiple choice questions. To discuss a concept, the instructor poses a question, first giving students a moment to consider and respond individually, then directing students to discuss in small groups to resolve any discrepancies in their responses or reasoning.

A robust body of research, summarized in Section 2, shows that use of peer instruction promotes greater student learning than traditional lecture. Inspired by the success of peer instruction in computer science courses, we implement and evaluate peer instruction in a semester-long cybersecurity course, Introduction to Computer Security. This paper presents the evaluation results of the implementation and compares them with a traditional lecture approach, based on three semesters' worth of data (two traditional lecture, and one peer instruction).

**Roadmap.** Section 2 presents the peer instruction methodology and related work. Section 3 discusses the implementation details in the computer security classes followed by the data collection and analysis results in sections 4 and 5. Section 6 concludes the paper.

## 2 BACKGROUND/RELATED WORK

### 2.1 Peer Instruction Methodology

Peer instruction is a teaching protocol comprised of before-class and in-class activities.

**Before class.** Before-class activities are aimed to have students familiarize themselves with the basics of topics for the next class meeting. They may include reading material, online videos, or other resources. A low-stakes quiz is given with the activities to incentivize the students to complete the work.

**In class.** The instructor divides a lecture into a series of peer instruction questions. Each question targets a certain concept. The instructor typically provides 60-90 seconds to the students to respond to the question individually, and then allows the students to discuss their answers with fellow students in small groups. The discussion typically lasts for two to three minutes. After the discussion, students respond to the question again, possibly changing their answer in light of new information from their peers. Clickers are used to collect the students' responses of on instructor's computer to allow the instructor to gauge classwide performance in real time. As needed, the instructor may choose to further discuss the concept, or move ahead with the next part of the lecture.

### 2.2 Related Work

Peer instruction is widely adopted and studied in many science disciplines. This section limits the scope to the pertinent efforts on the evaluation of peer instruction.

Peer instruction, as described in this paper, originated with Eric Mazur, a physics professor. The superiority of peer instruction over traditional lecture in physics classes was demonstrated in a 10-year, 6000-student study by Crouch *et. al* [10].

[*] Ahmed completed this work while he was at the University of New Orleans

*SIGCSE '19, February 27-March 2, 2019, Minneapolis, MN, USA*
© 2019 Association of Computing Machinery.
ACM ISBN 978-1-4503-5890-3/19/02...$15.00.
DOI: http://dx.doi.org/10.1145/3287324.3287403

Peer instruction is now widely used—and studied—in computer science. In one study, students in a peer instruction course achieved 6% higher grades on the final exam compared to traditional lecture-centric approach [27]. In another, a trio of introductory programming course best practices, including peer instruction, improved retention in the computer science major by 31% [21].

Looking at a broader range of four courses (CS1, CS1.5, Theory of Computation, and Computer Architecture), the use of peer instruction reduced the failure rate by 61% on average [18].

A particular challenge of teaching cybersecurity is the centrality of the need for learners (and practitioners) to apply their knowledge to new and different contexts. Ronald *et al.* Cortright et al. [9] attempted to test the hypothesis that peer instruction enhanced meaningful learning and the student's ability to solve novel problems and the ability to apply the knowledge to different new and existing contexts. They performed the study in an undergraduate physiology class of 38 students. They equally divided the student population into two groups. The lecture consists of short presentations. Each presentation followed a multiple-choice quiz. One group answered the questions individually while the other during peer instruction discussion. Their results validated the hypothesis.

Peer instruction has been deployed and tested in a short cybersecurity course/workshop. Johnson *et. al* [15, 16] developed 108 peer instruction questions for a digital forensics course, and report results from piloting a subset of these questions in a four-hour long workshop to evaluate the peer instruction methodology. Their evaluation results showed the learning gain via quiz and clicker questions by 34% and 13% respectively.

Esper *et. al* [12] adopted peer instruction in a software engineering course that had 189 students. They made slight modification in the standard peer instruction methodology. A clicker question is initially shown without answers and then, the instructor asks the students to call out suggestions for the answers. Both the students and instructor proposed a potential answer choices with discussions of those answers. Their survey results showed that 28% students would not recommend peer instruction for teaching because correct answers are not given and clicker questions are not clear.

## 3 PEER INSTRUCTION IMPLEMENTATION

We gather data over three semesters (Fall 2015, Fall 2016 and Fall 2017) consisting of quizzes, subjective exams, peer instruction questions and surveys. The first two semesters are based on traditional lectures while in the latter semester, the course is revised to incorporate peer instruction methodology.

Peer instruction is evaluated in terms of dropout and failure rates, student learning gain during the group discussion, and survey on students' experience and usage of clickers.

The evaluation results show that peer instruction improves the dropout rate by 4% and the failure rate by 13% and 3% in quizzes and subjective exams on average respectively, when compared with traditional lecture classes. The survey results show that 77% students find the group discussion with fellow students useful to understand the computer security concepts. 70% students would recommend peer instruction be adopted by other instructors.

**Course.** We choose the *introduction to computer security* course to evaluate the effectiveness of peer instruction methodology for cybersecurity education. The course is taught at both undergraduate and graduate levels and provides a broad overview of cybersecurity and covers at least four cybersecurity areas i.e., user authentication, malicious software, buffer overflow, and cryptographic tools. The course is offered regularly once or twice in a year as needed.

**Table 1: Number of students enrolled in the introduction to computer security course.**

| Teaching Method | Student Population |
|---|---|
| Traditional Lecture | 42 |
| Peer Instruction | 33 |

**Table 2: Data collection instruments**

| Quiz Questions | Subjective Exams | Clicker Questions | Survey Questions |
|---|---|---|---|
| 29 | 17 | 18 | 19 |

**Table 3: Survey on students background and interest in computer security**

| Survey Question | Fall 2015 | Fall 2016 | Fall 2017 |
|---|---|---|---|
| Previously taken any coursework related to computer security | 22% | 16% | 28% |
| Intend to specialize in computer security field | 48% | 63% | 49% |
| Intend to take additional computer security course after this class | 70% | 74% | 64% |

**Instructor.** The course instructor is an experienced teacher who taught several cybersecurity graduate and undergraduate courses. The instructor taught the *introduction to computer security* course five times before implementing the peer instruction in the course. The course evaluations by students are typically around 4.5 out of 5.0, which validate the high quality of instruction.

**Peer Instruction Activities.** Recall that peer instruction teaching involves before-class and in-class activities. For the implementation, the students are given reading assignments to cover before-class activities. Each assignment expects the students to read a book chapter of the topic discussed next week in class. The students are given at least one-week time to finish an assignment.

During class, the instructor asks peer instruction questions on a target topic and let students discuss their answers in small groups (consisting of typically four to five students). Clickers are used to collect the responses. The instructor also used his lecture slides to discuss the topics as needed.

## 4 DATA COLLECTION

To assess the effectiveness of peer instruction in terms of student failure rate and learning gain, we develop and utilize four different instruments for data collection i.e., Quiz, Subjective Exam, Clicker Questions and Survey (refer to Table 2 for a summary). Figure 1 shows the timeline of data collection activities in a semester. The semester starts with a before-class reading assignment. The students are given a week to complete it while the instructor uses this week to discuss the syllabus, introduce the course activities, go through

**Table 4: Survey on the reasons for enrolling in computer security**

| Survey Question | Fall 2015 | Fall 2016 | Fall 2017 |
|---|---|---|---|
| Interested in subject matter | 96% | 90% | 88% |
| Times of class is favorable for schedule | 28% | 16% | 27% |
| Other classes wanted were full | 9% | 26% | 30% |
| Prerequisite for other classes | 13% | 37% | 30% |

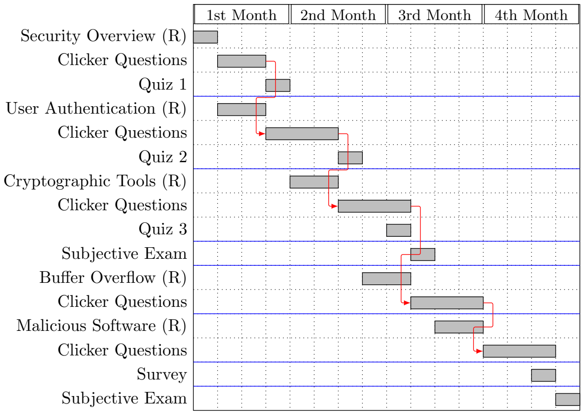

**Figure 1: Timeline of the data collection using quizzes, survey, subject exams, and clicker questions. Each box represents a week. 'R' identifies before-class reading activities on five topics.**

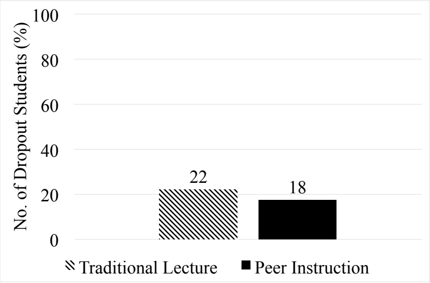

**Figure 2: Student dropout rate for traditional lecture and peer instruction**

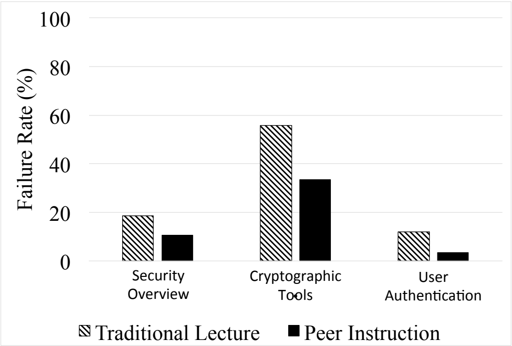

**Figure 3: Failure rate in *quizzes* for peer instruction and traditional lecture in three cybersecurity topics i.e., security overview, user authentication, and cryptographic tools.**

hands-on assignments, and initiate discussion on computer security to raise the students' interest on the subject matter. The rest of the semester comprises of periodic reading assignments and data collection activities.

We have collected the data for three semesters i.e., Fall 2015, Fall 2016, and Fall 2017. The first two uses *traditional lecture* approach while the latter implements *peer instruction*. Table 1 shows the enrollment number for these two approaches. This section further describes the data collection instruments.

**Quiz.** Three quizzes are developed to assess the student knowledge on three topics i.e., computer security overview, user authentication, and cryptographic tools. The students are given (at least a week) time to prepare for the quizzes after the lectures on the respective topics are completed in class. The quiz questions are designed to be straight forward with correct set of choices. To quantify the student responses, each correct question is given one mark.

**Subjective Exam.** The exams are midterm and final tests consisting of subjective questions to evaluate the understanding of the students on five cybersecurity topics, i.e., computer security overview, buffer overflow, user authentication, malicious software, and cryptographic tools. The duration of an exam is one hour and fifteen minutes. The students are advised to provide direct and concise answers to the questions. A standard rubric of correct answers is used to quantify the level of understanding of students on the topics.

**Clicker Questions.** The clicker questions are the peer instruction questions used for the lecture in class. Clickers are used to record the polls of a question before and after the student discussion in small groups. The polling results of the questions are an effective means to measure the learning gains of students at micro-scale as a result of peer discussion. Eighteen questions are used for five topics. Unfortunately, we could not collect the peer instruction data on one topic i.e., security overview. The other data is collected, analyzed and presented in this paper.

**Surveys .** We utilize an attitudinal survey to record the students' experience and opinions on clickers and peer instructions. The survey instrument is provided by Beth Simon and Leo Porter of UC San Diego, and Cynthia Lee of Stanford University. Results from this survey instrument have been published for numerous peer instruction courses, providing useful comparisons for our evaluation of peer instruction for cybersecurity (*e.g.*, [17][19][20]).

The survey gathers information on prior usage of clickers, course preparation, peer discussion, clicker usage, and lecture pacing. It contains 19 questions that are designed with a Likert scale. The survey is given to students at the end of semester in class and provided ample time to complete.

## 5 DATA ANALYSIS

We analyze the data to measure the effectiveness of peer instruction in terms of dropout and failure rates, student learning gain during

**Table 5: Student Survey on Peer instruction lecture preparation, peer instruction, and clicker usage**

| **Survey Questions** | **Average Opinion** |
|---|---|
| Thinking about clicker questions on my own, before discussing with people around me, helped me learn course material. | 70% |
| I read The required material before the lectures. | 60% |
| Most of the time my group actually discussed the clicker question. | 87% |
| Discussing course topics with my seatmate in the class helped me better understand the course material | 77% |
| The immediate feedback from the clickers helped me focus on weakness in my understanding of the course | 77% |
| Knowing the right answer is the only important part of the clicker question. | 30% |
| Generally, by the time we finished with a question and discussion, I felt pretty clear about it. | 80% |
| Clickers are an easy-to-use class collaboration tool. | 77% |
| Clickers helped me pay attention in the class compared to traditional lectures | 73% |
| Using clickers with discussion is valuable for my learning. | 67% |
| I recommend that other instructors use this approach (reading quizzes, clickers, in-class discussion) in their courses. | 70% |

**Table 6: Student survey on peer instruction implementation**

<table>
<tr><td colspan="60">From the point of helping me learn, the content of clicker questions was</td></tr>
<tr><td colspan="12">Much too hard<br>0%</td><td colspan="12">Too hard<br>6.66%</td><td colspan="12">OK<br>80%</td><td colspan="12">Too easy<br>13.33%</td><td colspan="12">Much too easy<br>0%</td></tr>
<tr><td colspan="60">In general, the instructor gave us enough time to read and understand the questions before the first vote.</td></tr>
<tr><td colspan="12">No, far too little time<br>0%</td><td colspan="12">No, too little time<br>0%</td><td colspan="12">OK amount of time<br>80%</td><td colspan="12">Yes, too much time<br>13.33%</td><td colspan="12">Yes, far too much time<br>6.66%</td></tr>
<tr><td colspan="60">Which of the following best describes your discussion practices in this group?</td></tr>
<tr><td colspan="12">I always discuss with the group around me, it helps me learn<br>66.66%</td><td colspan="12">I always discuss with the group around me, I don't really learn, but I stay awake<br>10%</td><td colspan="12">I sometimes discuss, it depends<br>22.33%</td><td colspan="12">I rarely discuss, I don't think I get a lot out of it<br>0%</td><td colspan="12">I rarely discuss, I'm too shy<br>0%</td></tr>
<tr><td colspan="60">The amount of time generally allowed for peer discussion was</td></tr>
<tr><td colspan="12">Much too short<br>3.33%</td><td colspan="12">Too short<br>11%</td><td colspan="12">About right<br>89%</td><td colspan="12">Too long<br>0%</td><td colspan="12">Much too long<br>0%</td></tr>
<tr><td colspan="60">In general, the time allowed for class-wide discussion (after the group vote) was</td></tr>
<tr><td colspan="12">Much too short<br>0%</td><td colspan="12">Too short<br>6.66%</td><td colspan="12">About right<br>70%</td><td colspan="12">Too long<br>23.33%</td><td colspan="12">Much too long<br>0%</td></tr>
<tr><td colspan="60">In general, it was helpful for the instructor to begin class-wide discussion by having students give an explanation.</td></tr>
<tr><td colspan="20">N/A - The instructor rarely did this<br>16.66%</td><td colspan="20">It's not helpful to hear other students' explanations<br>10%</td><td colspan="20">It was helpful to hear other students' explanations<br>73.33%</td></tr>
<tr><td colspan="60">The professor explained the value of using clickers in this class.</td></tr>
<tr><td colspan="15">Not at all<br>0%</td><td colspan="15">Somewhat, but I was still unclear why we were doing it<br>10%</td><td colspan="15">Yes, they explained it well<br>83.33%</td><td colspan="15">Yes, they explained it too much<br>6.66%</td></tr>
</table>

group discussions, and students' experience on clicker usage and peer instruction teaching methodology. Tables 4 and 3 summarize the students' background and interest in computer security. Only 30% students have some prior understanding of cybersecurity. However, 96% students are interested to learn cybersecurity. Around 75% students intend to take more cybersecurity courses and 50% would specialize in this area.

## 5.1 Dropout Rate

At the university, the students may drop the course within two weeks after the semester starts without any official record. After two weeks, the students have six weeks to drop the course with a "W" (or Withdraw) grade recorded.

Figure 2 shows the dropout rate for both traditional lecture classes, and peer instruction classes. We notice that the dropout rate is reduced by 4% in peer instruction classes from the classes taught with the traditional lecture approach.

## 5.2 Failure Rate

To measure the students' performance in the course for both traditional and peer instruction classes, we obtain failure rate in quizzes and subjective exams. The university policy defines that the passing grades are A, B, and C and the failing grades are D, and F. If a student scores less than 70% marks, he/she will be considered failed.

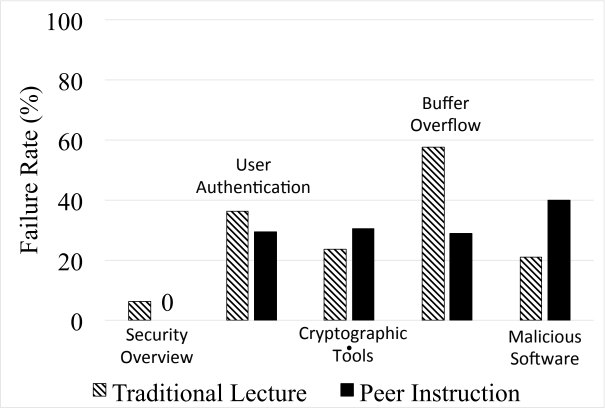

**Figure 4: Failure rate in the *subjective exam* for five topics i.e., introductory computer security, user authentication, and cryptographic tools) in the peer instruction class and traditional lecture class**

**Class Quiz.** Figure 3 presents the failure rate in quiz exams for both traditional-lecture and peer instruction classes. The results show consistent improvements in the failure rates for peer instruction. In particular, failure rate in security overview, cryptographic tools, and user authentication topics are reduced by 8%, 22%, and 8% respectively.

**Subjective Exam.** Figure 4 shows the failure rate of the subjective exams for the five topics (i.e., computer security overview, buffer overflow, user authentication, malicious software, and cryptographic tools) taught at both traditional-lecture and peer instruction classes. We notice substantial improvements in the failure rate. In particular, the failure rate for the topic, security overview is reduced to zero in peer instruction. We also notice some exceptions such as cryptographic tools where the failure rate is increased for peer instruction. We reevaluated the student answers of the questions on this topic. In particular, we found that a significant number of students misunderstood the following question.

*Question on Cryptographic Tools:* `How can message authentication be achieved using one-way hash function with 1) Symmetric encryption and 2) Public-key encryption.`

Apparently, they ignore the one-way hash function and assume that the question asks about the symmetric and Public-key encryption schemes. Some students derive message authentication through encryption without computing and utilizing cryptographic hash values. If the question is rephrased and restructured, it will likely reduce the failure rate on this topic.

Overall, we notice that the peer instruction reduces the failure rate by 3% on average when compared with the traditional lecture classes.

## 5.3 Learning Gain during Group Discussions

Figure 5 presents the results of the clicker responses of the students before and after the group discussions. We notice clear evidence of improvement in the correct answers by the students after the discussions.

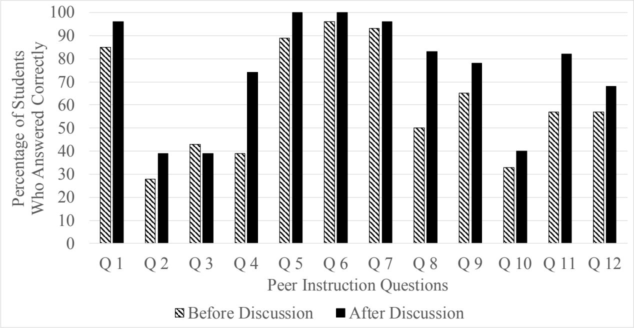

**Figure 5: Percentage of the students who respond to the peer instruction questions correctly**

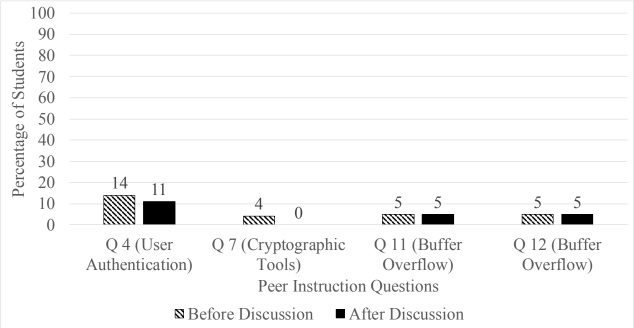

**Figure 6: Percentage of the students who respond to the peer instruction questions with the clicker choices that are not given in the questions**

To our surprise, some students chose an option from clickers that were not given in the questions. In particular, we observed these choices in the questions 4, 7, 11, and 12 on three topics: user authentication, cryptographic tools, and buffer overflow. Figure 6 shows the percentage of the students who have selected unexpected clicker options. Following is an example of such question.

*Question on Buffer Overflow:* `Which of the following describes a buffer overflow attack?`

A Exploiting the traffic flow mechanism in a buffer and blocking packets from reaching their destination.
B Flooding a buffer with server requests and overflowing the network bandwidth.
C Attempting to store more input in a data holding area than capacity allocates.
D An attacker fills the target buffer with malicious code

The above question has four choices: `A`, `B`, `C`, and `D`. However, some students respond with `E` from clickers. It shows that these students do not pay attention to the questions. We also notice in Figure 6 that some of these students change their responses after the group discussions, depicting that they start paying attention during the discussions.

## 5.4 Survey

Table 5 presents the results of the student attitudinal survey portion of the peer instruction evaluation. It shows that the most of the students find it useful to think about a clicker question before discussing it with other students and the discussion helps them understand the concept better. 70% of students would recommend peer instruction be adopted by other instructors.

Table 6 summarizes the students opinion about the peer instruction classes. It shows that the students have a generally positive experience of the classes. They have adequate time to understand the questions and vote for the correct answer. 80% students agree that the allowable duration for group discussions is sufficient.

## 6 CONCLUSION

We implemented and evaluated peer instruction in a semester-long course, introduction to computer security. The evaluation results were compared with traditional lecture classes in terms of dropout rate, failure rate, and student learning gain. Peer instruction showed promising results. The overall dropout rate was reduced by 4% and failure rate by 13% and 3% for quiz and subjective exams respectively when compared with traditional lecture classes. The survey results showed that 77% students found the discussions in small groups useful to understand the computer security concepts. The overall student experience of peer instruction was positive and majority students would recommend peer instruction be adopted by other instructors.

## 7 ACKNOWLEDGEMENT

This work was in part supported by the NSF grants # 1500101 and 1623276.

## REFERENCES

[1] I. Ahmed, S. Obermeier, S. Sudhakaran, and V. Roussev. 2017. Programmable Logic Controller Forensics. *IEEE Security Privacy* 15, 6 (November 2017), 18–24. DOI:http://dx.doi.org/10.1109/MSP.2017.4251102

[2] Irfan Ahmed, Golden G. Richard, Aleksandar Zoranic, and Vassil Roussev. 2015. Integrity Checking of Function Pointers in Kernel Pools via Virtual Machine Introspection. In *Information Security*, Yvo Desmedt (Ed.). Springer International Publishing, Cham, 3–19.

[3] Irfan Ahmed and Vassil Roussev. 2018. Peer Instruction Teaching Methodology for Cybersecurity Education. *IEEE Security Privacy* 16, 4 (July 2018).

[4] Irfan Ahmed, Vassil Roussev, and Aisha Ali Gombe. 2015. Robust Fingerprinting for Relocatable Code. In *Proceedings of the 5th ACM Conference on Data and Application Security and Privacy (CODASPY '15)*. ACM, New York, NY, USA, 219–229. DOI:http://dx.doi.org/10.1145/2699026.2699104

[5] Irfan Ahmed, Vassil Roussev, William Johnson, Saranyan Senthivel, and Sneha Sudhakaran. 2016. A SCADA System Testbed for Cybersecurity and Forensic Research and Pedagogy. In *Proceedings of the 2Nd Annual Industrial Control System Security Workshop (ICSS '16)*. ACM, New York, NY, USA, 1–9. DOI:http://dx.doi.org/10.1145/3018981.3018984

[6] Sajal Bhatia, Sunny Behal, and Irfan Ahmed. 2018. *Distributed Denial of Service Attacks and Defense Mechanisms: Current Landscape and Future Directions.* Springer International Publishing, Cham, 55–97. DOI:http://dx.doi.org/10.1007/978-3-319-97643-3_3

[7] Manish Bhatt and Irfan Ahmed. 2018. Leveraging relocations in ELF-binaries for Linux kernel version identification. *Digital Investigation* 26 (2018), S12 – S20. DOI:http://dx.doi.org/https://doi.org/10.1016/j.diin.2018.04.022

[8] Manish Bhatt, Irfan Ahmed, and Zhiqiang Lin. 2018. Using Virtual Machine Introspection for Operating Systems Security Education. In *Proceedings of the 49th ACM Technical Symposium on Computer Science Education.* ACM, 396–401.

[9] Ronald N Cortright, Heidi L Collins, and Stephen E DiCarlo. 2005. Peer instruction enhanced meaningful learning: ability to solve novel problems. *Advances in physiology education* 29, 2 (2005), 107–111.

[10] Catherine H Crouch and Eric Mazur. 2001. Peer instruction: Ten years of experience and results. *American journal of physics* 69, 9 (2001), 970–977.

[11] Pranita Deshpande and Irfan Ahmed. 2019. Topological Scoring of Concept Maps for Cybersecurity Education. In *Proceeding of the 50th ACM Technical Symposium on Computer Science Education (SIGCSE '19)*.

[12] Sarah Esper. 2014. A Discussion on Adopting Peer Instruction in a Course Focused on Risk Management. *J. Comput. Sci. Coll.* 29, 4 (April 2014), 175–182. http://dl.acm.org/citation.cfm?id=2591468.2591496

[13] Jonathan Grimm, Irfan Ahmed, Vassil Roussev, Manish Bhatt, and ManPyo Hong. 2018. Automatic Mitigation of Kernel Rootkits in Cloud Environments. In *Information Security Applications*, Brent ByungHoon Kang and Taesoo Kim (Eds.). Springer International Publishing, Cham, 137–149.

[14] Salman Javaid, Aleksandar Zoranic, Irfan Ahmed, and Golden G Richard III. 2012. Atomizer: Fast, Scalable and Lightweight Heap Analyzer for Virtual Machines in a Cloud Environment. In *Proceedings of the 6th Layered Assurance Workshop (ACSAC'12)*.

[15] William Johnson, Irfan Ahmed, Vassil Roussev, and Cynthia B. Lee. 2017. Peer Instruction for Digital Forensics. In *2017 USENIX Workshop on Advances in Security Education (ASE 17)*. USENIX Association, Vancouver, BC.

[16] William E. Johnson, Allison Luzader, Irfan Ahmed, Vassil Roussev, Golden G. Richard III, and Cynthia B. Lee. 2016. Development of Peer Instruction Questions for Cybersecurity Education. In *2016 USENIX Workshop on Advances in Security Education (ASE 16)*. USENIX Association, Austin, TX. https://www.usenix.org/conference/ase16/workshop-program/presentation/johnson

[17] Cynthia Bailey Lee, Saturnino Garcia, and Leo Porter. 2013. Can Peer Instruction Be Effective in Upper-division Computer Science Courses? *Trans. Comput. Educ.* 13, 3, Article 12 (Aug. 2013), 22 pages.

[18] Leo Porter, Cynthia Bailey Lee, and Beth Simon. 2013. Halving fail rates using peer instruction: a study of four computer science courses. In *Proceeding of the 44th ACM technical symposium on Computer science education.* ACM, 177–182.

[19] Leo Porter, Dennis Bouvier, Quintin Cutts, Scott Grissom, Cynthia Lee, Robert McCartney, Daniel Zingaro, and Beth Simon. 2016. A Multi-institutional Study of Peer Instruction in Introductory Computing. In *Proceedings of the 47th ACM Technical Symposium on Computing Science Education (SIGCSE '16).* ACM, New York, NY, USA, 358–363. DOI:http://dx.doi.org/10.1145/2839509.2844642

[20] Leo Porter, Saturnino Garcia, John Glick, Andrew Matusiewicz, and Cynthia Taylor. 2013. Peer Instruction in Computer Science at Small Liberal Arts Colleges. In *Proceedings of the 18th ACM Conference on Innovation and Technology in Computer Science Education (ITiCSE '13).* ACM, New York, NY, USA, 129–134. DOI:http://dx.doi.org/10.1145/2462476.2465587

[21] Leo Porter and Beth Simon. 2013. Retaining Nearly One-third More Majors with a Trio of Instructional Best Practices in CS1. In *Proceeding of the 44th ACM Technical Symposium on Computer Science Education (SIGCSE '13).* ACM, New York, NY, USA, 165–170. DOI:http://dx.doi.org/10.1145/2445196.2445248

[22] Vassil Roussev, Irfan Ahmed, and Thomas Sires. 2014. Image-based Kernel Fingerprinting. *Digit. Investig.* 11, S2 (Aug. 2014), S13–S21. DOI:http://dx.doi.org/10.1016/j.diin.2014.05.013

[23] Vassil Roussev, Andres Barreto, and Irfan Ahmed. 2016. API-Based Forensic Acquisition of Cloud Drives. In *Advances in Digital Forensics XII*, Gilbert Peterson and Sujeet Shenoi (Eds.). Springer International Publishing, Cham, 213–235.

[24] Saranyan Senthivel, Irfan Ahmed, and Vassil Roussev. 2017. SCADA network forensics of the PCCC protocol. *Digital Investigation* 22 (2017), S57 – S65. DOI:http://dx.doi.org/https://doi.org/10.1016/j.diin.2017.06.012

[25] Saranyan Senthivel, Shrey Dhungana, Hyunguk Yoo, Irfan Ahmed, and Vassil Roussev. 2018. Denial of Engineering Operations Attacks in Industrial Control Systems. In *Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy (CODASPY '18).* ACM, New York, NY, USA, 319–329. DOI:http://dx.doi.org/10.1145/3176258.3176319

[26] Beth Simon and Quintin Cutts. 2012. Peer Instruction: A Teaching Method to Foster Deep Understanding. *Commun. ACM* 55, 2 (Feb. 2012), 27–29. DOI:http://dx.doi.org/10.1145/2076450.2076459

[27] Beth Simon, Julian Parris, and Jaime Spacco. 2013. How We Teach Impacts Student Learning: Peer Instruction vs. Lecture in CS0. In *Proceeding of the 44th ACM Technical Symposium on Computer Science Education (SIGCSE '13).* ACM, New York, NY, USA, 41–46. DOI:http://dx.doi.org/10.1145/2445196.2445215