Editors: Melissa Dark, dark@purdue.edu | Jelena Mirkovic, mirkovic@isi.edu | Bill Newhouse, newhouse@nist.gov

Peer Instruction Teaching Methodology for Cybersecurity Education

Irfan Ahmed and Vassil Roussev | University of New Orleans

Effective cybersecurity professionals continuously adapt to the fast-changing security landscape; this requires deep analytical skills and an agile mindset. In contrast, it has been documented that the traditional lecture approach does not sufficiently engage the students in class and largely fails to stimulate the necessary thinking processes that would enable learners to quickly understand dynamically shifting attack vectors and to devise effective countermeasures in real time. In other words, students come out of security classes nominally knowing the material, yet are largely unprepared mentally for the daily rigors of the high-stakes competition between attackers and defenders.

In our experience, *peer instruction*, a well-defined teaching protocol originally developed by Eric Mazur at Harvard University,[1] holds a significant promise to deliver better cybersecurity education effectively. Peer instruction has been widely used in several disciplines such as philosophy, psychology, geology, and biology, and showed promising results on student learning. Recently, it has been explored for core computer science courses, such as Theory of Computation and Computer Architecture, and found effective in improving students' grades by 6 percent, reducing failure rates by 61 percent, and retaining students in a computer science major by 31 percent.[2–4] The students not only value peer instruction but also recommend that more instructors use it at both small colleges and large schools.

This article presents the application of peer instruction in a cybersecurity curriculum. We have developed the peer instruction material for three cybersecurity courses and evaluated them in a small group setting for a pilot study. The evaluation results show significant promise for the peer instruction in cybersecurity. The material is available at https://github.com/ahmirf/peer-instruction-questions-for-cybersecurity.

The Peer Instruction Method

In a peer instruction class, the instructor divides the original lecture into a series of questions; each question focuses on a target concept and follows the same format. The one critical prerequisite for the success of the method is a pre-class reading assignment; that is, students are required to read up on the topic covered in the class *ahead* of time. Thus, the class can be assumed to have some basic knowledge on the topic, enough to comprehend the questions during the lecture and discuss the answers with other students. The actual per-topic instruction process follows four major points:

- The instructor poses a multiple-choice question to students and gives them two to three minutes to respond individually. *Clickers* are commonly used to facilitate the logistics. They are handheld transmitters that send radio frequency signals to a receiver attached to the instructor's computer. Clickers allow students to easily respond to the question; the classroom response system automatically collects and summarizes the results for the instructor.
- If a non-trivial fraction of the responses is incorrect, the instructor asks the students to discuss their answers with a group of students sitting close by. Research shows that the real learning occurs during the discussions in this step.[5]
- In about three to four minutes, the instructor stops the discussion and polls for the answers again.
- The instructor presents the correct answer to the students and, based on the poll results, may further discuss it with them.

Developing Peer Instruction Questions for Cybersecurity

Our team studied the application of peer instruction in cybersecurity[6,7] and developed 280 peer instruction question for three courses—Introduction to Computer Security, Network Penetration Testing, and Digital Forensics, offering an introduction to *security concepts*, a *defensive view* of cybersecurity, and an *offensive view* of cybersecurity, respectively. The first is closest to the traditional lecture format, whereas the second and third are intensive hands-on classes; together, they

Copublished by the IEEE Computer and Reliability Societies

form the basis of a broad skillset in security.

Based on our experience, we identified a basic methodology for developing peer instruction questions systematically. It consists of four steps: concept identification, concept trigger, question presentation, and question development.

Concept Identification

The first step to create a question is to identify a target concept. The student discussion during a peer instruction process and multiple choices in the question should help the students understand the concept.

Concept Trigger

After identifying a target concept, we introduce one or more concept triggers to provoke a student's thinking process and to set the desired direction for the student discussion. For instance, we deliberately introduce some ambiguity in answer choices and expect the students to identify it, bringing it to the discussion with other students. Table 1 presents a brief list of concept triggers originally proposed by Beatty and colleagues.[8]

Table 1. List of common concept triggers.*

Concept triggers	Brief description
Compare and contrast	Compare and draw conclusion from multiple situations
Identify a set or subset	Identify a subset that fulfills some criteria
Omit necessary information	Insufficient information to answer a question
Use "none of the above"	A choice to reject other options
Trap unjustified assumptions	Facilitate the identification of potential unjustified assumptions by the students
Deliberate ambiguity	Ambiguous answer choices for a question
Trolling for misconceptions	Answer choices have common misconceptions by the students
Oops-go-back	Pair of questions; first traps the students with a common error; the second clarifies it
Require unstated assumptions	A question misses required assumption, potentially leading to multiple defensible answers

** A comprehensive list is presented in Beatty and colleagues'[8] and Johnson and colleagues' work.[6,7]*

Question Presentation and Development

After identifying the potential concept triggers for a question, we determine how the question should be presented to students to facilitate understanding. A question can be presented in different ways including scenario, example, or diagram. The question is then articulated consisting of the text and multiple choices along with any other supporting content such as diagram, graph, and so on.

Example Peer Instruction Questions

The following examples of peer instruction questions cover a cyberattack, reverse engineering, and digital forensics; each example also presents a brief analysis of the questions in terms of concept trigger and each question's presentation.

Q1: Cyberattack

Which of the following represents an example of an attack?

a) A web application is vulnerable to cross-site scripting.
b) A successful denial-of-service attack takes down a login page for a full day.
c) A database administrator implements a system to encrypt data stored in the database.
d) A SQL injection vulnerability is used to obtain sensitive information by an unauthorized user.
e) More than one of these.

Analysis of Q1: This question uses the concept trigger "identify a set or subset," because both B and D are examples of an attack, and thus, the correct answer is E. The question is presented as an example, and an important detail here is that the examples are in the choices rather than the question description.

Q2: Reverse Engineering

After executing the instructions in Figure 1 while single-stepping inside a debugger on an 80486 processor, what is the value of the 16-bit word at location `loc_10129+5`?

a) 168h
b) 152h
c) 4D4Ch
d) Value is unknown
e) None of the above

Analysis of Q2: The question uses the concept trigger "analysis and reasoning" to allow students to discuss the answers based on whether instruction prefetch caching is enabled. It also provides "none of the above" to allow students to discard other choices. If prefetch caching is enabled, the correct answer is 4D4Ch.

```
1.    Start:
2.    mov word ptr loc_10106 + 1, 152 h
3.    loc_10106: ;DATA XREF
4.    mov ax, 168h
5.    mov word ptr loc_10129 + 5, ax
6.    loc_10129:  ;DATA
7.    mov word ptr es: 0, 4D4Ch
```

Figure 1. Self-modifying code snippet.

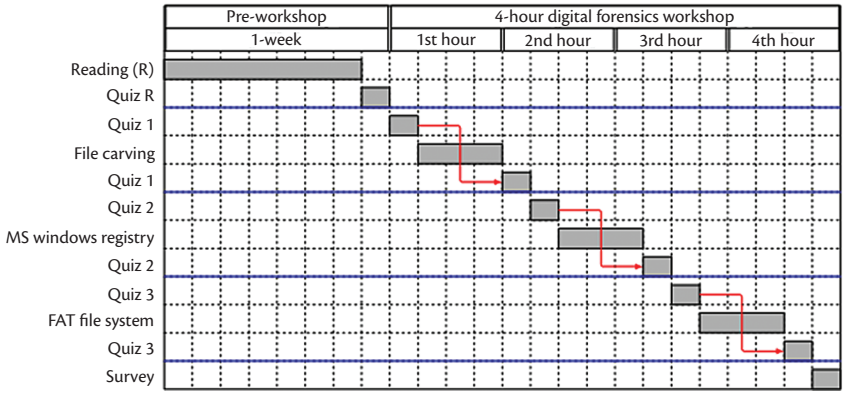

Figure 2. Timeline of the workshop activities including quizzes, survey, and peer instruction lectures on three digital forensics topics, file carving, MS Windows registry, and FAT filesystem.

Q3: Digital Forensics

In which of the following situations is file carving most effective?

a) The targeted drive is highly fragmented.
b) The targeted drive has been defragmented before carving.
c) The system being used to examine the drive has low free disk space.
d) The system being used to examine the drive has high free disk space.
e) More than one of the above

Analysis of Q3: This question has a choice "More than one of the above" to utilize the concept trigger "identify a set or subset." It also uses "trolling for misconceptions" because the defragmentation rearranges data in contiguous disk blocks; however, it may lose some deleted files. The correct answer is D because high free disk space leads to less fragmentation, which helps file carving recover more data.

Peer Instruction Evaluation

As already mentioned, we developed 280 questions for three cybersecurity courses—Introduction to Computer Security, Digital Forensics, and Network Penetration Testing. We used a small subset of the forensics questions in a four-hour workshop on digital forensics to perform a pilot study on the effectiveness of peer instruction for a cybersecurity course. The workshop covered three topics—file carving, MS Windows registry, and FAT filesystem. Figure 2 presents the timeline of the workshop activities. Twelve undergraduate students attended the workshop, consisting of 11 males and one female, who had never taken any prior computer forensics course. We provided reading material to the students on the topics a week before the workshop. We also distributed a quiz of five questions on the material using Google Forms and asked the students to complete the quiz before the workshop. We used the quiz to ensure that the students read the material.

During the workshop, the students were divided into four groups for peer discussion. The entire workshop was centered on seven peer instruction questions: two for each topic and one for the introductory discussion on computer forensics. The clickers were used to collect student responses on the questions.

For the evaluation, we used the following metrics: quiz, survey, and clicker responses. The quizzes were presented twice to the students, once before and once after a topic, to quantify student learning. The survey gathered the data on prior usage of clickers, workshop preparation (reading material and quiz), peer discussion, clicker usage, and lecture pacing. We employed a survey developed by Beth Simon and Leo Porter of the University of California, San Diego, and Cynthia Lee of Stanford University that had been used in numerous peer instruction courses.[2,9,10]

In the evaluation results, the quizzes (at the beginning and end of the topics) and peer instruction questions (before and after discussions) showed clear evidence of student learning gain. Table 2 presents the results of the survey.[6] The results were similar to the previous studies of peer instruction in the core computer science courses.[1–4] For instance, 92 percent of students reported that discussions with peers during a lecture helped them understand the workshop material. Ninety-one percent of them not only found the immediate feedback from clickers very useful but also

recommended that other instructors use peer instruction in their courses.

The study showed that the students quickly adapted to the format, found it useful, and highly recommended the approach be extended to a wider range of subjects. To further substantiate our results, we plan to perform a large-scale study of peer instruction on cybersecurity courses.

Although we have a positive experience with peer instruction, we notice that a big challenge for an instructor to adopt this technique is to manage time and maintain an appropriate pace for a class lecture. We encourage other educators to employ peer instruction as an active learning technique in their courses and share their experiences with the cybersecurity education community. ■

Table 2. Results of the peer instruction survey on the digital forensics workshop.

Questions	Average opinion
Discussing course topics with my seatmates helped me better understand the material.	92%
The immediate feedback from clickers helped me focus on weaknesses in my understanding of the workshop material.	91%
I recommend that other instructors use this approach (reading quizzes, clickers, in-class discussion) in their courses.	91%
I read the required material before the workshop.	89%
Clickers are an easy-to-use class collaboration tool.	89%
Thinking about clicker questions on my own, before discussing with people around me, helped me learn the workshop material.	87%
Most of the time my group actually discussed the clicker question.	87%
Clickers helped me pay attention in this workshop compared to traditional lectures.	82%
Generally, by the time we finished with a question and discussion, I felt pretty clear about it.	80%
Using clickers with discussion is valuable for my learning.	80%
The pre-workshop reading quiz helped me recognize what was difficult in the reading.	78%
Knowing the right answer is the only important part of the clicker question.	46%

Acknowledgments

This work was supported by the NSF grant 1500101.

References

1. C.H. Crouch and E. Mazur, "Peer Instruction: Ten Years of Experience and Results," *American Journal of Physics*, vol. 69, no. 9, 2001, pp. 970–977.
2. L. Porter et al., "Peer Instruction in Computer Science at Small Liberal Arts Colleges," *Proceedings of the 18th Annual Conference on Innovation and Technology in Computer Science Education*, July 2013.
3. B. Simon et al., "Experience Report: Peer Instruction in Introductory Computing," *Proceedings of the 41st SIGCSE Technical Symposium on Computer Science Education*, March 2010.
4. B. Simon, J. Parris, and J. Spacco, "How We Teach Impacts Student Learning: Peer Instruction vs. Lecture in CS0," *Proceedings of the 44th ACM Technical Symposium on Computer Science Education*, March 2013.
5. L. Porter et al., "Peer Instruction: Do Students Really Learn from Peer Discussion," *Proceedings of the 7th Annual International Computing Education Research Workshop*, August 2011.
6. W. Johnson et al., "Peer Instruction for Digital Forensics," *USENIX Advances in Security Education Workshop* (ASE 17), August 2017.
7. W. Johnson et al., "Development of Peer Instruction Questions for Cybersecurity Education," *USENIX Workshop on Advances in Security Education* (ASE 16), 2016.
8. L. Beatty, W. Gerace, and R. Dufresne, "Designing Effective Questions for Classroom Response System Teaching, *American Association of Physics Teachers*, vol. 74, no. 1, 2006.
9. C.B. Lee, S. Garcia, and L. Porter, "Can Peer Instruction Be Effective in Upper-Division Computer Science Courses?," *Trans. Comput. Educ.*, vol. 13, no. 3, 2013, pp. 12:1–12:22.
10. L. Porter et al., "A Multi-Institutional Study of Peer Instruction in Introductory Computing," *Proceedings of the 47th ACM Technical Symposium on Computing Science Education* (SIGCSE 16), 2016, pp. 358–363.

Irfan Ahmed is in the Department of Computer Science at the University of New Orleans. Contact at irfan@cs.uno.edu.

Vassil Roussev is in the Department of Computer Science at the University of New Orleans. Contact at vassil@cs.uno.edu.