# Cybersecurity Shuffle: Using Card Magic to Teach Introductory Cybersecurity Topics

Preston Moore[1] and Justin Cappos[2]
New York University
New York, New York, United States
pkm266@nyu.edu[1] jcappos@nyu.edu[2]

**Abstract**

One of the main challenges in designing lessons for an introductory information security class is how to present new technical concepts in a manner comprehensible to students with widely different backgrounds. A non-traditional approach can help students engage with the material and master these unfamiliar ideas. We have devised a series of lessons that teach important information security topics, such as social engineering, side-channel attacks, and attacks on randomness using card magic. Each lesson centers around a card trick that allows the instructor to simulate the described attack in a way that makes sense, even for those who have no prior technical background. In this paper, we describe our experience using these lessons to teach cybersecurity topics to high school students with limited computer science knowledge. Students were assessed before and after the demonstration to gauge their mastery of the material, and, while we had a very limited set of responses, the results show an improvement on post-test scores. Furthermore, several indicators affirm the students enjoyed the lessons and remained engaged throughout the session.

## 1 Introduction

When teaching technical topics in introductory courses, it can be challenging to present information in a way that makes sense for students of varying experience levels or educational backgrounds. This is particularly true for information security classes where an adversarial mindset is required to fully comprehend the attacks. Thinking in this way may not come naturally to many students, as evidenced by the continuing success of phishing attacks. What is needed

is a way to relate information security concepts in a manner that is engaging enough to build an appreciation for the material, yet relatable enough so the students do not feel lost. To accomplish this, we look towards a pedagogical technique known as scaffolding in which "students are escorted and monitored through learning activities that function as interactive conduits to get them to the next stage [9]."'

In this paper, we employ card magic as a scaffolding device in a series of lessons that teach how three types of attacks – social engineering, side channel attacks, and attacks on randomness – work in the real world. In doing so, we add a new twist to the success other computer science researchers have had in using card magic to explain difficult concepts by allowing the instructor to simulate "attacks" through a non-technical, commonplace activity. In doing so, these lessons can help students safely interact within these attack scenarios. Each demonstration was followed by a short PowerPoint presentation in which the magician makes a connection between the card trick and the very real consequences of the attack it illustrates.

To test the effectiveness of our lessons, we presented them to a group of high school students attending a computer science summer program and assessed mastery using a pre- and post-test. Though our sample size was too small to draw definite conclusions from them, participant scores did increase on the post-test for each subject. Furthermore, based on an opinion survey and presenter observations, participants found the lessons engaging, age appropriate, and helpful in understanding the concepts.

- We create a lesson plan built around three easy-to-perform magic tricks. By using these tricks, instructors can simulate attacks and thus provide a scaffold for teaching these somewhat difficult concepts.

- We test the effectiveness of these lessons by presenting them to a group of high school students in a summer workshop and assessing engagement and improved mastery of the material.

- We note an improved ability to answer questions related to the attacks following our lesson, as judged by pre- and post-test evaluations.

## 2 A Lesson Wrapped in an Illusion

A magician creates an illusion to hide the secrets of his or her tricks. The lessons we have developed reverse this situation by using our tricks to reveal the mysteries behind three cyberattacks. The tricks were chosen because of their relevance to the information security field. Following the principles of scaffolding,

the attacks are presented in order of increasing technical complexity. Video tutorials for each of the tricks are available at: *https://bitly.com/cybersecurityshuffle.* [1]

### 2.1 Social Engineering

In the context of information security, "social engineering" is defined as a set of tactics to manipulate users into giving away personal information that can be used to compromise accounts, reset passwords using security questions, or carry out identity theft. We start with this attack as it is broadly used and affects arguably the greatest cross-section of victims. In our lesson, the magician employs two card tricks as a misdirection and a cover to distract from the amount of personal data he/she is soliciting.

This trick is intended to spark a teachable moment about social engineering and its dangers. Instructors can use this moment to start a dialog with students about the types of information attackers might want and how they could maliciously use it.

#### 2.1.1 From the Audience's Perspective

Our version of this trick is adapted from a magic classic known as "The Red and Black Separation Trick [8]." The magician begins by telling the audience that there is a way to form a psychic bond with a deck of cards. The magician enlists a volunteer and each shuffles the deck before placing one half on top of the other. Next, the magician asks the volunteer a few questions, starting with their birth year, to allegedly "attune" the link between the individual and the deck. The response is used to select one red card and one black card from the deck, each with a numeric value equal to one of the last two digits of the volunteer's birth year. Next, the magician asks for the volunteer's birth month and similarly selects a red card with a numeric value equal to the response (using the jack and queen for November and December, respectively). Finally, the magician asks for the volunteer's birthday and selects a black card with a numeric value equal to the second digit in this day. The magician lays these cards out on the table and asks the volunteer to select one red card and one black card with which they feel most "attuned." The unchosen cards are returned face up to the middle of the deck.

Continuing the pretense of a psychic link with the deck, the magician asks the volunteer to guess the color of each card in the deck. As he/she does so, the magician places each card face down in two piles: red and black. Half-way through the deck, the two face up cards are switched so the black pile becomes

[1] Public domain and GPL-licensed card images used in figures taken from Wikimedia Commons [13].

the red pile and vice-versa. The volunteer continues guessing until all the cards are placed. At that point the magician turns over the face down cards to reveal that the volunteer has guessed **e**very card's color correctly. The magician then reveals the "misdirection" that abetted the trick's true purpose – revealing personal information.

### 2.1.2 Behind the Scenes

Before the trick begins, the deck has already been separated into red and black halves. In the initial shuffling the volunteer is merely scrambling cards of the same color. Therefore, when the two packs are stacked one on top of the other, the two colors remain separate.

In the first portion of the trick the magician pulls out two red and two black cards that reflect the volunteer's answer, and two of these cards are returned to the deck. The magician must return these cards face up exactly between the red and black "sections." This will later signal the magician when all cards of one color have been dealt.

During the prediction phase of the trick, one pile contains all correct guesses while the other is completely incorrect. When the midway point is reached the magician places the red card face up on the black pile and vice versa. An illustration of this arrangement appears in Figure 1. In the reveal the magician flips the correct pile horizontally and the "incorrect" pile forward vertically to reverse the incorrect guesses. The red cards are now paired with the red marker card and vice-versa to complete the illusion that the volunteer correctly guessed **e**very card in the deck.

## 2.2 Side Channel Attacks

As the name implies, a side channel attack strikes a target indirectly by tracking seemingly unrelated phenomena, such as timing information, power consumption, electromagnetic leaks, or even sounds. To mirror this type of attack, the trick demonstrates how an attacker can gather information without directly exploiting a vulnerability. We do so using a deck of cards with a brand logo on the back. When turned upside-down the logo effectively creates the equivalent of a "mark," similar to a "marked" deck of cards. The goal of this trick is to open the participant's eyes to the less obvious avenues an attacker might use to transmit information.

### 2.2.1 From the Audience's Perspective

The magician opens a new deck of cards, removes the jokers and branding cards, and legitimately shuffles it. Several volunteers are asked to select a card

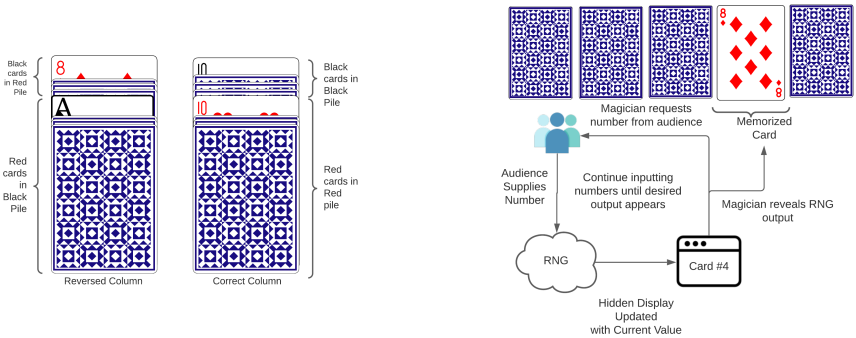


Figure 1: Left: Arrangement of cards after guessing concludes in Trick 1. Right: Use of "random number generator" in Trick 3

from the deck, show it to the audience, memorize it without revealing it to the magician, and then return it to the deck. The magician then shuffles the deck before going through it and finding all of the volunteers' cards. This trick's reveal comes when the magician informs the audience that the cards were found using a secret information side channel present in the deck, opening a door to explore further side channels.

### 2.2.2 Behind the Scenes

The key to this trick lies in the magician's choosing a deck with a logo or text on the back that tips off a card's orientation. Because the trick begins with a fresh deck, all cards are oriented in the same direction. When the volunteers return their cards to the deck, the magician simply has to orient the deck in such a way that the returned cards are upside-down. To complete the trick, the magician finds the card with a differing orientation.

## 2.3 Attacks on Randomness

True randomness is important in many security-sensitive situations. An attacker who is able to predict or influence the output of a random number generator may use this capability to circumvent cryptographic security controls. This trick employs a "forced" card [14] to point out a potential vulnerability that results from a misunderstanding of hash functions.

The purpose of this lesson is to show students the importance of correct randomness that is "fit for purpose," or appropriate for security-sensitive applications. It also shows how an attacker with a small amount of influence, such as when to stop supplying numbers, can compromise a system.

### 2.3.1 From the Audience's Perspective

The trick begins with the magician announcing that it is possible to guess the value of any randomly selected card in a deck by touch. To prove this point, the magician spreads a deck of cards on the table face up, shuffles the deck and deals five cards face down. In order to head off suspicion that the cards are "fixed," the magician declares a software random number generator will be used to select which card will be predicted. Students are asked to shout out numbers to be input into the generator. After a handful of numbers, the magician cuts off input, generates a number, $n$, and correctly predicts the value of the $n$th card from those dealt on the table.

### 2.3.2 Behind the Scenes

There are three components that allow this trick to work. First, spreading the deck on the table allows the magician to memorize one or more of the top five cards in the deck. Next, the deck is shuffled in a way that ensures the top cards remain intact [15]. This ensures that the memorized cards will be amongst the prediction candidates. Finally, the random number generator is engineered to "force" selection of one of the memorized cards.

To make this trick work, the generator has been built with two vulnerabilities. The first is an intermediate output that allows the magician to see what number would be generated, based on the current inputs. Knowing this allows the magician to cut off new inputs once a memorized card would be selected. Second, the generator uses a hash function and modulus to produce its output rather than a cryptographically secure method. This ensures that the magician's desired output will appear after a small number of inputs. Figure 1 shows the generator's use during the trick.

## 3 Study Instrument and Evaluation

**Method** The goal of our study was to judge how effective a non-traditional approach could be in teaching novices about our selected attacks. To do so, we prepared and presented a 90-minute Zoom session as an optional class for high school students in a remote-learning computer science summer camp. Using this particular format was a necessary workaround once COVID-19 restrictions prevented the summer camp from being held live. We discuss the impact of this format switch on our study later in this section.

Once the true purpose of the trick is revealed, the presenter shared a brief lesson that named the attack, separated the attackers' real purpose from the misdirection stated while the trick was in progress (i.e. "creating a psychic bond with the deck"), and shared a real-world example. Though presented as

one session for our study, each of the three modules could be the basis of a single classroom lesson.

To measure any change in the students' mastery of the material, we designed an assessment (a portion of which is shown in Table 1) consisting of 12 multiple choice questions (4 for each topic), 3 Likert-scale survey statements, and a free response section. The assessment, minus the Likert and free response questions, was conducted before the lesson to generate a baseline, and was repeated after the lesson to measure improvement and gather student opinions. In both cases, the participants completed the assessments online and outside of the workshop. We purposely avoided collecting demographic information on the respondents due to the heightened privacy concerns inherent in working with high school students.

| | Question Text | Correct on Pre-test | Correct on Post-test |
|---|---|---|---|
| Q1 | Which of the following is the best definition of social engineering? | 3 (60%) | 5 (100%) |
| Q2 | The act of creating a scenario in order to extract information is called: | 3 ( 60%) | 4 (80%) |
| Q3 | Which of the following pieces of information are dangerous to reveal online? | 5 (100%) | 5 (100%) |
| Q4 | Bad actors can use stolen personal information to do which of the following: | 2 (40%) | 5 (100%) |
| Q5 | What is a side channel attack? | 0 (0%) | 0 (0%) |
| Q6 | Which of the following can give you a hint as to what a computer is doing? | 5 (100%) | 5 (100%) |
| Q7 | What is an example of a common real-world side channel attack? | 4 (80%) | 5 (100%) |
| Q8 | How could you prevent an attacker from stealing a password by using a microphone to listen to keystrokes? | 3 (60%) | 5 (100%) |
| Q9 | Which of the following is a major use of hash functions? | 4 (80%) | 3 (60%) |
| Q10 | Which of the following is an important feature of a good hash function? | 4 (80%) | 4 (80%) |
| Q11 | When passing multiple items sequentially into a hash function, which item has the most influence on the output? | 1 (20%) | 5 (100%) |
| Q12 | What is the term used when two or more inputs to a hash function generate the same output? | 2 (40%) | 5 (100%) |

Table 1: Question text and aggregate scores for each assessment question. Q1-Q4 covered social engineering, Q5-Q8, side channel attacks, and Q9-Q12 attacks on randomness.

**Results** The limited number of assessments completed greatly limits the validity of our results, but does indicate positive trends. Aggregate scores increased across all categories on the post-test. The results in Table 1 show scores for the social engineering and attacks on randomness sections increased by 30%, while the side channel attacks section increased by 15%. The improvement in social engineering scores can be traced to higher scores on Q1, Q2, and Q4, indicating a better understanding of the topic. Smaller improvements on

Q5 and Q9 suggest a need to improve the lesson materials in these specific areas, particularly providing better definitions and examples of side channel attacks real-world use cases for hash functions. On the plus side, accurate responses to Q11 and Q12 suggest the lesson was an effective scaffold for teaching two key properties of hash functions.

On the questionnaire, student shared very positive opinions about the lessons, attesting that the lesson had improved their skills in the covered topics, while also being enjoyable. Free response comments shared described the session as "fun," "entertaining," and "interesting." The instructor also observed that a significant majority of students kept their cameras on, and asked or answered questions about the material – two key indicators of engagement during remote instruction.

**Limitations And Future Work** COVID-19 restrictions, a remote modality, and difficulties handling consent forms drastically reduced participation from a potential enrollment of around 40 students to a group of 15 actual attendees. Of these attendees, only 10 agreed to participate in the study and just 5 completed it. The fall off in study completion can likely be attributed to an inability to do the assessment in person and to follow up about the post-test. It was simply too easy for students to sign off and forget to respond to the post test. This limited completion rate prevents us from making strong statistical claims about the effectiveness of our lessons. However, the positive responses observed by the instructor strongly suggest this approach could be successful in teaching cybersecurity topics.

## 4 Related Work

The idea of scaffolding is to provide a bridge to assist students in mastering material that may be beyond their reach [16] by bringing it into their "Zone of Proximal Development [12]." Given the complexity of computer science topics, it is not surprising that researchers have attempted to "scaffold" these concepts from a familiar base. In a meta-analysis from 2019, Szabo et al. identified 1283 papers in the field that contain scaffolding-related content [4], while Vanderyde et al. argues that increasing and more diverse enrollments in computer science call for greater use of scaffolding practices [11]. Stanier also discusses using scaffolding approaches in higher education to support metacognitive and strategic skills [10]. All the above suggest our demonstrations could work as effective scaffolds for introducing security concepts to novices.

Other researchers have already integrated card tricks into computer science lesson plans, such as using parity bits to detect unintended bit flips, a central technique in error detection and correction. Bell et al. use a 5 by 5 grid of cards

in an exercise that allows students to generate and detect parity errors. [1, 2]. Greenberg et al. were able to create more advanced versions of the exercise using larger grids. Other versions of this activity rely on software assistance to handle more complex computations [7].

In Ferreria et al. a "self-working" card trick called "Are You Psychic?" is used to explain topics in algorithm analysis and design, such as problem decomposition, pre- and post- conditions, and invariants [5]. Each of the trick's steps are mapped onto a formal description of an algorithm. Garcia et al. produced three papers describing a variety of magic tricks, along with the computer science concepts they help teach [6]. Their goal was to help students construct a mental model of how a computer actually works. Similarly, Curzon et al. found success explaining computer science concepts to younger students using magic shows [3].

## 5 Conclusion

In this paper we present a novel approach to teaching an introductory information security that uses card magic to simulate key attacks. By starting with a card trick, we are able to establish common ground even with students who have little knowledge of the field. The trick illustrates how the attack works giving the student a cognitive basis to build upon. After testing this lesson plan in a real-world teaching environment, we see its potential to foster engagement and improve students' mastery of the covered material. We encourage our fellow educators to use the tricks we have developed and to work out new ones as a way to make complex and intimidating material more approachable for novice students. Doing so could potentially improve not only individual performance, but also, by enhancing comprehension, reduce attrition rates among computer science undergraduates.

## References


[1] Tim Bell, Jason Alexander, Isaac Freeman, and Mick Grimley. Computer science unplugged. *The New Zealand Journal of Applied Computing and Information Technology*, 13(1):20–29, 2009.

[2] CS Education Research Group. Cs unplugged: Error detection card flip magic. `https://classic.csunplugged.org/error-detection/\#Card_Flip_Magic`.

[3] Paul Curzon and Peter W McOwan. Engaging with computer science through magic shows. In *Proceedings of the 13th annual ITCSE conference*, pages 179–183, 2008.

[4] Claudia Szabo et al. Review and use of learning theories within computer science education research. In *Proceedings of the Working Group Reports on Innovation and Technology in Computer Science Education*, ITiCSE-WGR '19, page 89–109, New York, NY, USA, 2019. Association for Computing Machinery.

[5] João F Ferreira and Alexandra Mendes. The magic of algorithm design and analysis. In *Proceedings of the 2014 conference on Innovation & technology in computer science education*, pages 75–80, 2014.

[6] Daniel D Garcia and David Ginat. Demystifying computing with magic, part iii. In *Proceedings of the 47th ACM Technical Symposium on Computing Science Education*, pages 158–159, 2016.

[7] Ronald I. Greenberg and Dale F. Reed. Using magic in computing education and outreach. In *2018 IEEE Frontiers in Education Conference (FIE)*, pages 1–4, 2018.

[8] Our Pastimes. How to do the red and black separation card trick, 2017.

[9] Raymond and DeCourcey. *Cognitive Characteristics. Learners with Mild Disabilities.* Allyn & Bacon, A Pearson Education Company, 2000.

[10] Clare Stainer. Scaffolding in a higher education context. ICERI2015 Proceedings:7781–7790, 2015.

[11] James Vanderhyde and Florence Appel. With greater cs enrollments comes an even greater need for engaging teaching practices. *J. Comput. Sci. Coll.*, 32(1):38–45, October 2016.

[12] L.S. Vygotsky. *Mind in Society: The Development of Higher Psychological Processes.* Harvard University Press, London, 1978.

[13] Wikimedia Contributors. Svg playing cards, 2021.

[14] Wikipedia contributors. Forcing (magic) — Wikipedia, the free encyclopedia, 2021. [Online; accessed 12-August-2021].

[15] Wikipedia Contributors. Shuffling — Wikipedia, the free encyclopedia, 2021.

[16] David Wood, Jerome S Bruner, and Gail Ross. The role of tutoring in problem solving. *Journal of child psychology and psychiatry*, 17(2):89–100, 1976.