U.S. National
Science Foundation

Enhancing Cybersecurity Education: Personalized Threat Scenarios for High School Students

---

Introduction

This summer project, spanning approximately three months, aimed to develop threat modeling scenarios that are relatable to high school students to personalize their learning of Identity and Access Management (IAM) technologies. The project design included group brainstorming to identify threat scenarios most suitable for classroom instruction that appeal to students' everyday contexts. Specifically, we aimed to identify threat and attack scenarios that students may regularly face (or are familiar with) related to IAM, like password attacks through shoulder surfing from a classmate or use of biometrics on smartphones. Our hypothesis was that by personalizing learning in this way, student engagement and learning will be positively impacted, as opposed to relying on existing teaching strategies that do not produce consistently positive learning outcomes.

Threat modeling is a process that allows us to identify and understand security threats [12]. By modeling threats, we gain a better sense of how to attack or defend a given system. In terms of teaching cybersecurity, threat modeling provides a way for teachers to give students a real-life scenario to engage with.

With the rise of technology, as well as the ethical considerations that come along with it, teachers are now required to explain cybersecurity and related topics to their students [4]. Unfortunately, there is strong evidence suggesting that teachers struggle to implement this curriculum into their classes [2, 3, 4]. In the Killhoffer study, teachers expressed concerns about a perceived gap in knowledge when faced with the tech-savvy nature of their students, whether or not this divide was real. The Childers study revealed that teachers did not feel comfortable creating engaging lessons on cybersecurity, even after completing professional development courses.

There is a consensus among teachers and parents that it is important to educate students on these topics [3], but there are differing views on how it should be done. Some suggest game-based learning [6, 7, 10], while others advocate for hands-on simulation activities like labs or projects [5, 8, 9, 11], or simply engaging learning experiences [2, 4]. Additionally, most of these studies are conducted as summer programs rather than being integrated into the regular school system [5, 6, 8, 10], or they are tested in the classroom for only a short period of time [7]. Although student enjoyment significantly increases with these programs, it is difficult to evaluate their long-term impact on learning without further study.

This project considers the student perspective in the cybersecurity learning scenario. We examine the preconceived notions that high school students might have about cybersecurity and Internet safety, and explore how lessons can be adapted to be more engaging and relatable. Additionally, we involve students in generating their own ideas for activities, allowing them to create concepts that other students might find interesting and engaging.

Proposed Research Questions

1. **Brainstorming Session 1:**

a. What is threat modeling?
b. Can threat modeling be useful for teaching cybersecurity?
c. How can personalizing the threat scenarios be useful?
    i. How can we personalize learning scenarios?
    ii. How might students respond to personalized threat scenarios?
    iii. How would personalized threat scenarios promote learning?
    iv. What would be the likely takeaway messages by students when using personalized threat scenarios to teach cybersecurity?

2. **Brainstorming Session 2:**
    a. Which scenarios are suitable for classroom instruction, and why?
        i. Are these scenarios truly relatable?
        ii. What makes scenarios relatable, including the media of presentation (e.g., online content, images, videos, slide decks, music, etc.)?
        iii. Which assessments/rubrics should be used for measuring learning?
        iv. What are the potential limitations?
        v. What are the potential benefits?
        vi. What should be improved?

3. **Final Focus Group:**
    a. Which scenarios are most promising for classroom instruction?
    b. If adapting personalized threat modeling for teaching cybersecurity concepts, what should teachers focus on during lesson planning?
    c. In what cases would this approach be most and least appropriate?
    d. Would this approach to teaching IAM work for other cybersecurity topics?

Study Team

- **Tempestt Neal**
  Principal Investigator
  Assistant Professor
  Computer Science and Engineering
  University of South Florida
- **Janelle Yearwood**
  Study Facilitator
  Computer Science Teacher
  Winthrop College Prep Academy
- **Erika Samuel**
  Study Facilitator
  Undergraduate Researcher, Computer Science
  University of South Florida

Participant Recruitment and Demographics

Ten undergraduate students were recruited for this study through various channels, including:

- Email invitations

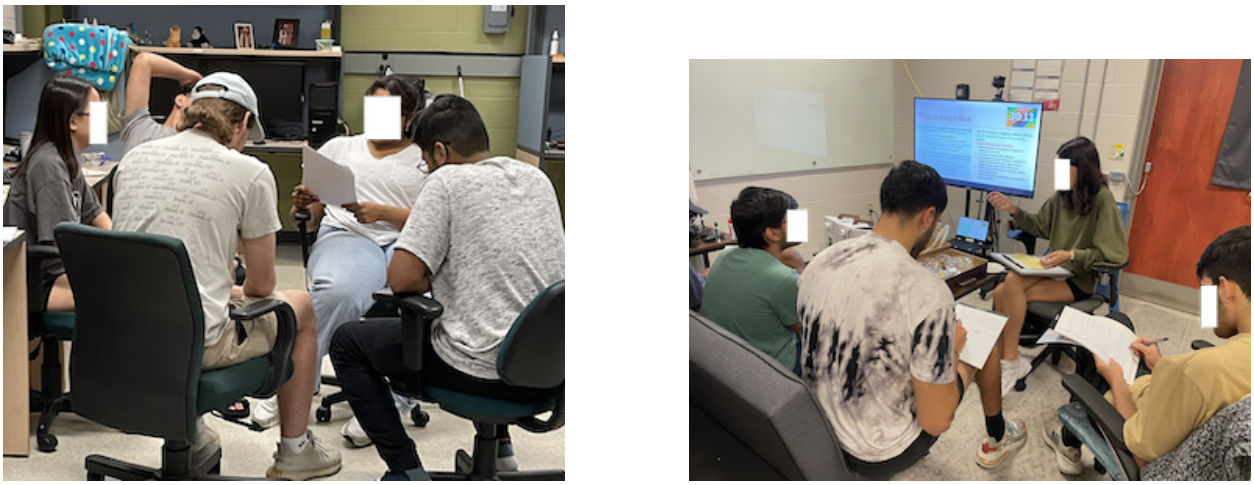

Figure 1: Participants engaged in group brainstorming.

- USF social media platforms
- Paper flyers distributed across campus and within on-campus residence halls
- Campus-wide email distributions
- Recruitment videos

Additionally, study flyers were shared with our established collaborators for dissemination to potential participants and were made available in the university student center. Eight participants reported enrollment in the Computer Science and Engineering program, with two individuals also enrolled in Medical Engineering, all of whom are affiliated with the University of South Florida's College of Engineering.

Each participant completed a Cybersecurity Knowledge Quiz prior to participating in the study to assess their overall cybersecurity awareness. This was important to ensure each participant could effectively participate in discussion during the study.

Each participant received:

- A $75 e-gift card per brainstorming session
- A $50 e-gift card for completing the final focus group

Participant and Engagement Summary

Prior to engaging in the study, each participant completed the Cybersecurity Knowledge Quiz to gauge their overall awareness in the field, ensuring their active involvement in subsequent discussions. The demographic profile of participants reveals a diverse group with varying levels of cybersecurity exposure and expertise. Notably, participants demonstrated strong proficiency in foundational programming concepts, with several individuals having completed relevant cybersecurity courses. The distribution of quiz scores indicates a spectrum of cybersecurity knowledge among participants, suggesting differing starting points for engagement with the study's objectives. These demographics serve as a foundational understanding for interpreting the insights and contributions gathered throughout the study sessions, reflecting a broad spectrum of perspectives and experiences within the cohort.

Participants received a $75 e-gift card per brainstorming session and a $50 e-gift card for completing the final focus group.

Table 1: Participant Demographics

Age	Gender	Ethnicity	Program Year	Cybersecurity Quiz Score	Relevant Cybersecurity Courses
20	Man	Asian or Asian American	Sophomore	90%	Programming Concepts, Python, Program Design
19	Woman	White or Caucasian	Sophomore	90%	AP Comp Sci, Intro to Oriented Programming, Intro to Databases, Programming Fundamentals, Foundations of Cybersecurity
19	Woman	Asian or Asian American	Sophomore	90%	Programming Concepts
21	Man	Asian or Asian American	Junior	100%	Intro to Python
20	Man	Arab/Middle Eastern or Arab American, Asian or Asian American	Freshman	90%	Intro to Python, Google Cybersecurity Certificate, Programming Concepts, Intro to Web Development
21	Man	Asian or Asian American	Senior	100%	Program Design, Data Structures, Database Design
20	Man	White or Caucasian, Hispanic, Latino, or Spanish	Sophomore	70%	Programming Concepts, Program Design, Computer Logic Design, Python, C#, C++
20	Man	Asian or Asian American	Junior	60%	Computer Programming
20	Woman	Asian or Asian American	Junior	80%	Programming Concepts, Program Design, Computer Organization
22	Man	White or Caucasian	Senior	100%	Intro to Programming, Programming Fundamentals, IT Object Oriented Programming, IT Concepts, Foundations of Cybersecurity

Overview of Methodology

Each brainstorming session consisted of:

- Lunch (15 minutes)
- Study overview (15 minutes)
- Brainstorming (45 minutes)
- Discussion (15 minutes)

Lunch was served at the start of the session. Participants were welcomed to continue eating during the study overview, during which the study facilitators presented a slide deck which detailed the study goals, provided an ice breaker, defined fundamental concepts, and established a schedule for the day.

During brainstorming time, participants broke into two groups, during which they were instructed to generate ideas with the following in mind:

- Quantity over quality
- No idea is a bad idea
- Creative and wild ideas are encouraged
- Jot down everything
- Avoid criticizing or praising ideas
- Avoid lengthy discussion
- Use many tools to express your ideas

Participants were provided with a wide array of stationary during all sessions, including markers, mini whiteboards and dry erase markers, pens, paper pads, sticky notes, index cards, and stickers. During discussion, each group would present their ideas and the whole team would reflect and discuss commonalities and the research team would ask questions to gain clarity.

We organized the sessions to scaffold the participants' thought processes by first asking them to assess the feasibility of personalized lessons to teach cybersecurity in high school, having participants generate specific lesson plan ideas according to their previously established assessment of feasibility, and then voting on the most promising ideas. We video and audio recorded each session, using two video cameras to focus on each group. Each session, we also photographed design artifacts and collected notes.

Findings

The objective of the first brainstorming session was to pinpoint threat modeling scenarios tailored specifically to high school students, aiming to facilitate effective cybersecurity education. The session underscored the importance of making content relatable to teenagers, hypothesizing that crafting narratives and scenarios would enhance engagement and comprehension. We emphasized the potential value of using real-world threats to enhance memorability and relevance. Central to this endeavor was the identification of scenarios pertinent to Identity and Access Management (IAM) and user authentication, vital concepts in cybersecurity education. The session's refined goal was to assess the usefulness of personalized threat scenarios for teaching IAM, with questions probing the benefits of personalization, its impact on learning, and student responses. The ultimate aim was to investigate the efficacy of this approach in the session and strategize its implementation for scenario identification in subsequent sessions.

Question 1: Why would personalizing threat scenarios be useful?

Group A Overall, Group A felt that personalizing threat scenarios was crucial for several reasons. They argued that such personalization could compel students to immerse themselves in a scenario, encouraging reflection and improvement for future encounters. Additionally, personalized scenarios might foster a sense of caution and connection by relating directly to personal experiences. They also felt this approach could facilitate easier dissemination of information, enhance understanding of risks, and provide a solid foundation for learning cybersecurity concepts, particularly for non-experts. Specific quotes from Group A members included the following:

- "[Personalizing threat scenarios] forces the individual to be in the scenario, [encouraging them] to think about how to do better next time."
- "[It] teaches them to be more careful."
- "[Personalizing threat scenarios] would be useful to make audiences feel more connected with the message."
- "[It's] useful because it can allow ourselves to be relatable to the audience."
- "[People] would relate to their own personal experiences."
- "[It's] easier to spread information if people care about what they are listening to."
- "[Many] people may know friends or family members that have had similar experiences."
- "[Audiences] can better understand the risks and severity as they see how it applies in their own lives."
- "Facing [threat scenarios] for the first time is tough. If they experience it before[,] it would be better to face the situation."
- "[Personalizing threat scenarios] would make the concept or threat scenarios easier to understand."
- "[It provides a] good foundation to learn."
- "[It] makes the information simpler, making it easier for non-experts to understand."
- "[It involves] open public servers, risk assessment, or even data breaches leading to information."
- "Do not share personal things."

Group B Overall, Group B highlighted the various benefits of personalizing threat scenarios, emphasizing its importance in cybersecurity education. They felt that by informing students about the potential threats to their personal information and raising awareness of cybersecurity issues, personalized scenarios could significantly increase engagement and promote a deeper understanding of the subject. Moreover, Group B felt that personalized scenarios could inspire students to consider cybersecurity as a career path and encourage them to develop solutions to mitigate risks, such as creating cybersecurity software. Additionally, they argued that personalized scenarios could foster social awareness, enhance training, and empower students to take proactive measures against cyber threats, ultimately contributing to a safer online environment. Notable individual comments from Group B included the following:

- "It would inform students about the threat to their personal information."
- "Increased engagement rate."
- "So they are aware that they can pursue it as a career."
- "[This] could probably lead to someone creating a cybersecurity software which minimizes the risk of data being stolen."
- "[Cybersecurity education would be] easily available."
- "[It would] promote learning of cybersecurity."
- "[It would foster] social awareness."
- "[It would] involve more students [in] cybersecurity."
- "[It would provide] enhanced training."
- "[It would aim] to help student not be scared of hackers."
- "[It would serve the purpose of] informing authorities."
- "[It would help students] know about potential threat cyberattacks can pose to them."
- "[It would be implemented] to encourage students to be aware and afraid."
- "[It would emphasize] not sharing information across platforms."
- "So student are aware it could happen to them."
- "[It would help students] know about different types of cyberattacks."
- "So they know the severity of cyberattacks."

When asked why would personalizing threat scenarios be useful, we received the following responses:

	Group A	Group B
Highest Rated	Makes the information simpler, making it easier for non-experts to understand	Easily available
	It would make the concept or threat scenarios easier t understand.	Not sharing information across platforms
	Audiences can better understand the risks and severity as they see how it applies in their own lives	Increased engagement rate
	Useful because it can allow ourselves to be relatable to the audience	It would inform students about the threat to their personal information
	It forces the individual to be in the scenario, think about how to do better next time	So they know the severity of cyberattacks
	Personalizing threat scenarios would be useful to make audiences feel more connected with the message	So students are aware it could happen to them
	Easier to spread information if people care about what they are listening to	Social awareness
	Facing for the first time is tough. If they experience it before it would be better to face the situation.	Involve more students cybersecurity
	Teaches them to be more careful	To encourage students to be aware and afraid
	People would relate to their own experiences	Know about potential threat cyberattacks can pose to them
Lowest Rated	Open public servers, risk assessment, or even data breaches leading to information	Know about different types of cyberattacks

Overall outcomes from Brainstorming Session 1 showed general support for the use of personalized threat scenarios for high school students to teach cybersecurity concepts. Real-world threats were highlighted as essential for enhancing memorability and relevance. However, to conclude Session 1, we held a 15-minute open discussion, which yielded further insights from both groups. Group A raised questions about the feasibility of true personalization, emphasizing the need for engaging activities over personalized ones. They highlighted the discrepancy between current personalized approaches and real-world scenarios, suggesting that effective personalization requires a deep understanding of the individual. As a result, their goal for the next session evolved to develop a set of engaging and relevant activities that promote positive and ethical behaviors among students. Group B's final comments in Session 1 centered on the potential negative consequences of personalized content, including the risk of fostering "bad hacking mentalities" and influencing unethical behavior. As an alternative, they proposed introducing concepts like Blue Teams and Bug Bounty Programs to mitigate these risks while making students more aware of cybersecurity issues like phishing emails. Thus, their objective for the next session also evolved to create a set of large problem-solving projects that address cybersecurity challenges on a broader scale. This file contains the final set of games ideated by the study participants during Session 2 and the final focus group session.

Session Slides

Session 1 Slides
Session 2 Slides
Session 3 Slides

Acknowledgements

This study was approved by USF's Institutional Review Board as Study #005606, and was funded by NSF's Secure and Trustworthy Cyberspace Program, Grant #2039373. We extend our heartfelt gratitude to the participants who contributed their time and insights to this study. Special thanks to our collaborators, colleagues, and the NSF for their support in making this research possible.

References

[1] Anderson, R. (2008). Security engineering: A guide to building dependable distributed systems. John Wiley & Sons.

[2] Childers, G., & Jones, M. (2015). The role of collaborative digital projects in teaching and learning introductory astronomy. Journal of College Science Teaching, 45(1), 55-63.

[3] Clark, S., Logan, K., Luckin, R., Mee, A., & Oliver, M. (2009). Beyond Web 2.0: Mapping the technology landscapes of young learners. Journal of Computer Assisted Learning, 25(1), 56-69.

[4] Haynie, D. (2018). What you need to know about the new SAT. U.S. News & World Report.

[5] Killhoffer, D., & Mohammadian, M. (2018). A new teaching strategy to improve student engagement and learning. Journal of Education and Training Studies, 6(1), 11-19.

[6] Knezek, G., Christensen, R., & Tyler-Wood, T. (2016). Addressing the STEM challenge through game-based learning. Journal of Education and Training Studies, 4(3), 1-11.

[7] Kosa, M., Arpaci, I., & Bahcekapili, E. (2016). Learning effects of educational game design: A case study of a course on computer organization. Computers & Education, 103, 113-123.

[8] Lee, J., & Hammer, J. (2011). Gamification in education: What, how, why bother? Academic Exchange Quarterly, 15(2), 1-5.

[9] Livingstone, S., & Helsper, E. (2010). Balancing opportunities and risks in teenagers' use of the internet: The role of online skills and internet self-efficacy. New Media & Society, 12(2), 309-329.

[10] Smith, M. (2017). Game-based learning. Cambridge University Press.

[11] Whitton, N., & Moseley, A. (2012). Using games to enhance learning and teaching: A beginner's guide. Routledge.

[12] Shostack, A. (2014). Threat modeling: Designing for security. John Wiley & Sons.