A User Experience Study of MeetingMayhem: A Web-Based Game to Teach Adversarial Thinking

Shan Huang
sh69@illinois.edu
University of Illinois, Urbana-Champaign
Urbana, Illinois, USA

JiWoo Lee
jiwool4@illinois.edu
University of Illinois, Urbana-Champaign
Urbana, Illinois, USA

Chenyan Zhao
victorsss.orz@outlook.com
University of Illinois, Urbana-Champaign
Urbana, Illinois, USA

Geoffrey L. Herman
glherman@illinois.edu
University of Illinois, Urbana-Champaign
Urbana, Illinois, USA

Marc Olano
olano@umbc.edu
University of Maryland, Baltimore County
Baltimore, Maryland, USA

Linda Oliva
oliva@umbc.edu
University of Maryland, Baltimore County
Baltimore, Maryland, USA

Alan Sherman
sherman@umbc.edu
University of Maryland, Baltimore County
Baltimore, Maryland, USA

ABSTRACT

We report on our experiences fielding MeetingMayhem, an interactive game that we developed, which introduces students to fundamental concepts in network security, cybersecurity, and adversarial thinking. The game is intended for students who do not necessarily have any prior background in computer science. Assuming the role of agents, two players exchange messages over a network to try to agree on a meeting time and location, while an adversary interferes with their plan. Following the Dolev-Yao model, the adversary has full control of the network: they can see all messages and modify, block, or forward them. We designed the game as a web application, where groups of three students play the game, taking turns being the adversary. The adversary is a legitimate communicant on the network, and the agents do not know who is the other agent and who is the adversary. Through gameplay, we expect students to be able to (1) identify the dangers of communicating through a computer network, (2) describe the capabilities of a Dolev-Yao adversary, and (3) apply three cryptographic primitives: symmetric encryption, asymmetric encryption, and digital signatures. We conducted surveys, focus groups, and interviews to evaluate the effectiveness of the game in achieving the learning objectives. The game helped students achieve the first two learning objectives, as well as using symmetric encryption. We found that students enjoyed playing MeetingMayhem. We are revising MeetingMayhem to improve its user interface and to better support students to learn about asymmetric encryption and digital signatures.

ITiCSE 2024, July 8–10, 2024, Milan, Italy

ACM ISBN 979-8-4007-0600-4/24/07.
https://doi.org/10.1145/3649217.3653538

CCS CONCEPTS

• **Applied computing** → **Interactive learning environments**; **Education**; • **Security and privacy** → **Network security**; **Cryptography**.

KEYWORDS

cybersecurity education, educational game, network security

ACM Reference Format:
Shan Huang, JiWoo Lee, Chenyan Zhao, Geoffrey L. Herman, Marc Olano, Linda Oliva, and Alan Sherman. 2024. A User Experience Study of MeetingMayhem: A Web-Based Game to Teach Adversarial Thinking. In *Proceedings of the 2024 Innovation and Technology in Computer Science Education V. 1 (ITiCSE 2024), July 8–10, 2024, Milan, Italy*. ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3649217.3653538

1 INTRODUCTION

Adversarial thinking involves thinking and reasoning about adversaries' actions and goals in a certain context [15]. Many consider adversarial thinking to be the core concept of cybersecurity [9, 15, 18, 21], and it is useful for everyone. For example, people who lack adversarial thinking may not realize that joining an unencrypted "free" public wifi network risks revealing their personal information. Despite widespread agreement on the importance of teaching adversarial thinking, the existing academic curriculum guidelines neglect this aspect of cybersecurity education [8]. Curricula that include adversarial thinking mainly focus on students in STEM majors [9]. Therefore, although adversarial thinking is significant for everyone, there is a lack of opportunities for students with limited technical backgrounds to learn it.

To address this lack, we developed MeetingMayhem, a web-based educational game for college students focused on adversarial thinking in the context of network security. In MeetingMayhem, three students take on the roles of two agents (Alice and Bob) and

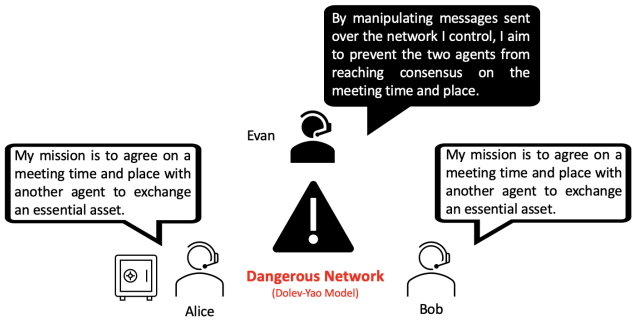

Figure 1: Game overview of MeetingMayhem, where Evan is the adversary, and Alice and Bob are agents.

an adversary (Evan) (See Figure 1). MeetingMayhem is designed based on the *Dolev-Yao (DY)* model [6]. This model has been used by others to teach about adversarial thinking [2, 12]. The DY model is a strong network intruder model [6]: Protocols proven free of structural weaknesses in the DY model are likely to be free of such weaknesses in realistic deployments [6].

In the model, all participants are legitimate communicants. Agents and the adversary have authorized access to the network. All users in the model can apply basic cryptographic primitives, including encryption or decryption and application of digital signatures [1]. The adversary (Evan) can block or repeat any message. They can also insert or modify messages that are not cryptographically protected but cannot defeat the cryptographic primitives. Because the adversary controls the network, Alice or Bob cannot directly send plaintext messages to each other. Instead, they send a message to the network. The adversary may or may not allow messages to proceed to the other agent and may or may not modify messages.

The goal of the agents is to agree on a time and location to exchange an asset. The adversary is successful if they prevent the agreement. The agents do not need to hide the meeting time and location from the adversary. The agents communicate through a network controlled by the adversary without knowing the adversary's identity. Thus, Alice is unaware of the identity of the adversary, which may be either Bob or Evan. However, Alice does know that two agents and an adversary are present in the network.

Our contributions include: (1) We developed a novel educational game MeetingMayhem that teaches adversarial thinking and targets students with limited technical backgrounds. (2) We analyze and discuss the qualitative and quantitative results from our preliminary evaluation.

2 BACKGROUND

2.1 Adversarial thinking

There is no commonly agreed upon definition for adversarial thinking. Some vaguely define adversarial thinking as "thinking as hackers" [8]. Dark [4] defines adversarial thinking as: "Let's say that adversarial thinking is the ability to look at system rules and think about how to exploit and subvert them as well as to identify ways to alter the material, cyber, social, and physical operational space." [4]. Schneider [17] defines adversarial thinking as "the very essence of game theory. In it, actions by each player are completely specified; for cybersecurity and safety-critical systems, identifying possible player actions is part of the central challenge" [17].

We can see how Dark emphasizes "system rules" and "operational space" and Schneider focuses on "player actions". Combining their definitions, we define adversarial thinking as reasoning about the adversary's actions and goals under certain system rules and operational environments.

2.2 Cybersecurity Games

Previous researchers [11] have proposed a game-based approach to teach adversarial thinking and related cybersecurity concepts.

Most early cybersecurity games were simulation-based games exemplified by Defcon's Capture the Flag [3] and CyberCIEGE [10]. These simulation-based games used simplified representations of security concepts to engage players with limited technical backgrounds. To maintain the faithfulness of the simulation, players had little freedom in playing, which may decrease the enjoyability of the games.

Other games focused more on creating enjoyable and sociable experiences, but may sacrifice some fidelity or depth in the cybersecurity concepts taught [5, 7]. [d0x3d!] [7] is a game where students act as white-hat hackers to fetch digital assets from an adversarial network encoded by the game's mechanics. SecurityEmpire [14] introduces high school students to cybersecurity concepts by having students manage a company in the presence of cybersecurity risks.

Distinct from the previous approaches, MeetingMayhem is a short game that seeks to teach students with limited technical backgrounds about adversarial thinking through a technically simplified context and sociable environment.

3 LEARNING OBJECTIVES

By the end of the game session, students should be able to:

(1) Identify the dangers of communicating through a computer network.
(2) Describe the capabilities of a Dolev-Yao adversary.
(3) Apply the following cryptographic primitives that can mitigate dangers in a Dolev-Yao network: symmetric encryption, asymmetric encryption, and digital signature.

4 IMPLEMENTATION

The MeetingMayhem system comprises a frontend and backend. The frontend is deployed using HTML, and JavaScript with Jinja templates. The backend functionality is implemented with the Flask framework. During the focus group study, we deployed the MeetingMayhem server on an online virtual machine to allow access at the same time through the Internet by three participants. We also make MeetingMayhem available as a docker image.

In MeetingMayhem, we provide three cryptographic tools: symmetric encryption, asymmetric encryption, and signature. Table 1 shows example key names and their uses for Alice.

We define (1) ***shared symmetric keys*** as keys pre-shared by two players, and (2) ***public and private keys*** as key pairs generated by algorithms where public keys are available to everyone on the network and private keys are only known to players themselves.

Symmetric encryption is an encryption type where a communicant encrypts or decrypts the message with a shared symmetric

	Shared Symmetric Key	Public Key	Private Key	For Recipient Bob	For Recipient Evan
Symmetric Encryption	*Alice_Bob, Alice_Evan*	*N.A.*	*N.A.*	*Alice_Bob*	*Alice_Evan*
Asymmetric Encryption	*N.A.*	*Alice, Bob, Evan*	*Alice*	*public_Bob*	*public_Evan*
Signature	*N.A.*	*Alice, Bob, Evan*	*Alice*	*private_Alice*	*private_Alice*

Table 1: Keys available to user1 for three types of cryptographic tools, and corresponding correct keys to be used for different recipients.

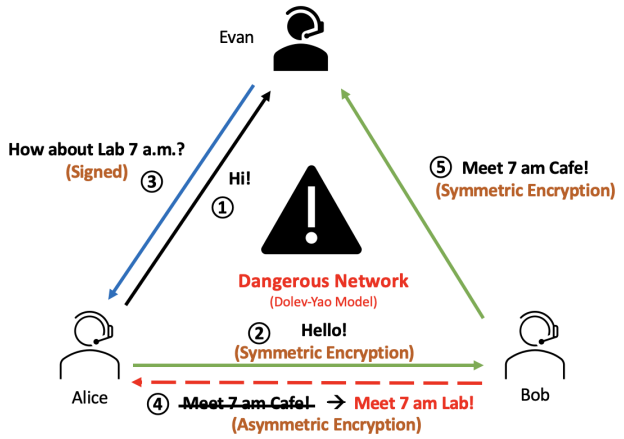

Figure 2: Illustration of an example round, where the number indicates the sequence of the messages; the dashed line denotes messages edited by the adversary; blue indicates correct signature; green indicates correct encryption; and red indicates incorrect encryption.

key between the sender and the recipient. For symmetric encryption, only symmetric keys may be used. Therefore, if a student uses the wrong shared symmetric key, the recipient cannot decrypt the message.

Asymmetric encryption is an encryption type where the sender encrypts the message with the recipient's public key and the recipient decrypts the message with their own private key.

Signature is used to authenticate the identity of the sender of a message. The message is signed with the sender's private key, and the signature is verified with the sender's public key.

The adversary can choose to delete, forward, or edit a message as shown in the edit message part of Figure 3. When forwarding a message, the adversary can change the sender and recipient of the message to masquerade as others. When editing a message, the adversary can modify the content only if the message is not encrypted or signed, or if the adversary has the necessary keys. The adversary can apply new cryptography for unencrypted messages.

5 EXAMPLE GAME PLAY

To help readers understand how MeetingMayhem works, we describe an example round of the game and illustrate it in Figures 2 and 3. Alice, Bob, and Evan are the players; Evan is the adversary. As agents, Alice and Bob aim to agree on the time and location of a meeting. Alice sends a simple greeting to Evan to start. Because Alice has no background in cybersecurity, she sends her first message "Hi" to Evan ① without the use of cryptographic tools. In her user interface as shown in Figure 3, she checks Evan in the recipient box in A, selects cafe and 7 a.m. as the location and time in B, enters "Hi" in the message box in D, and clicks "Send Message."

Next Alice sends a similar greeting message ② to Bob. This time, she has noticed the cybersecurity tools and recalls that she needs to protect her messages from the adversary. She looks up the information on the "About" page of the game and decides to use symmetric encryption. She sends another greeting message to Bob by selecting cafe and 7 a.m. with the content "Hello!" She symmetrically encrypts the message ② with the correct key "shared_Alice_Bob" by using the cryptographic panel in C to Bob.

Evan can review every message in the network. In his interface (Figure 4), he receives the two messages (① and ②) just sent by Alice in the "Message to be Processed." He reads the plain greeting message ① from Alice and replies to the message by sending a new message ③ to Alice by using a similar message interface in Figure 3. To make himself appear trustworthy, Evan uses the signature tool. He signs his message with his own private key and asks Alice "How about Lab 7 a.m.?" in the message content.

Next Evan looks at message ② sent by Alice. Because message ② is protected by symmetric encryption, Evan cannot decrypt the message, so he can only delete or forward the message. Evan chooses to forward message ② to Bob.

Bob receives message ② from Alice and symmetrically decrypts the message with the "shared_Alice_Bob" key. He reads the message from the adversary and replies with "Meet 7 a.m. Cafe!" to indicate his choice. Unfortunately, he incorrectly asymmetrically encrypts with his private key and sends message ④. To make sure all the agents meet at the same time and location, Bob sends message ⑤ with the same content to Evan but uses symmetric encryption.

Evan receives message ④. Because Bob's public key is available for everyone, Evan decrypts message ④ and modifies it. He uses the "Edit a Message" panel (Figure 4) to change the message to "Meet at Lab 7 p.m." to prevent Bob and Alice from meeting at the same location. Evan re-encrypts the message and keeps the sender as Bob. For message ⑤, Evan just decrypts it and reads it.

Alice receives messages ③ and ④. Because Evan's message was signed and Bob's message was encrypted, she mistakenly thinks that means both messages are trustworthy. Because the messages agree on the time and location, she votes Lab at 7 a.m. by clicking the "Ready to Vote" (Figure 3). Bob, however, votes to meet Cafe at 7 a.m. Due to the mismatch in location, the adversary wins the game.

6 DATA COLLECTION

We describe our procedure for data collection. We conducted focus groups to evaluate the user interface and the effectiveness of MeetingMayhem in helping students achieve the learning objectives.

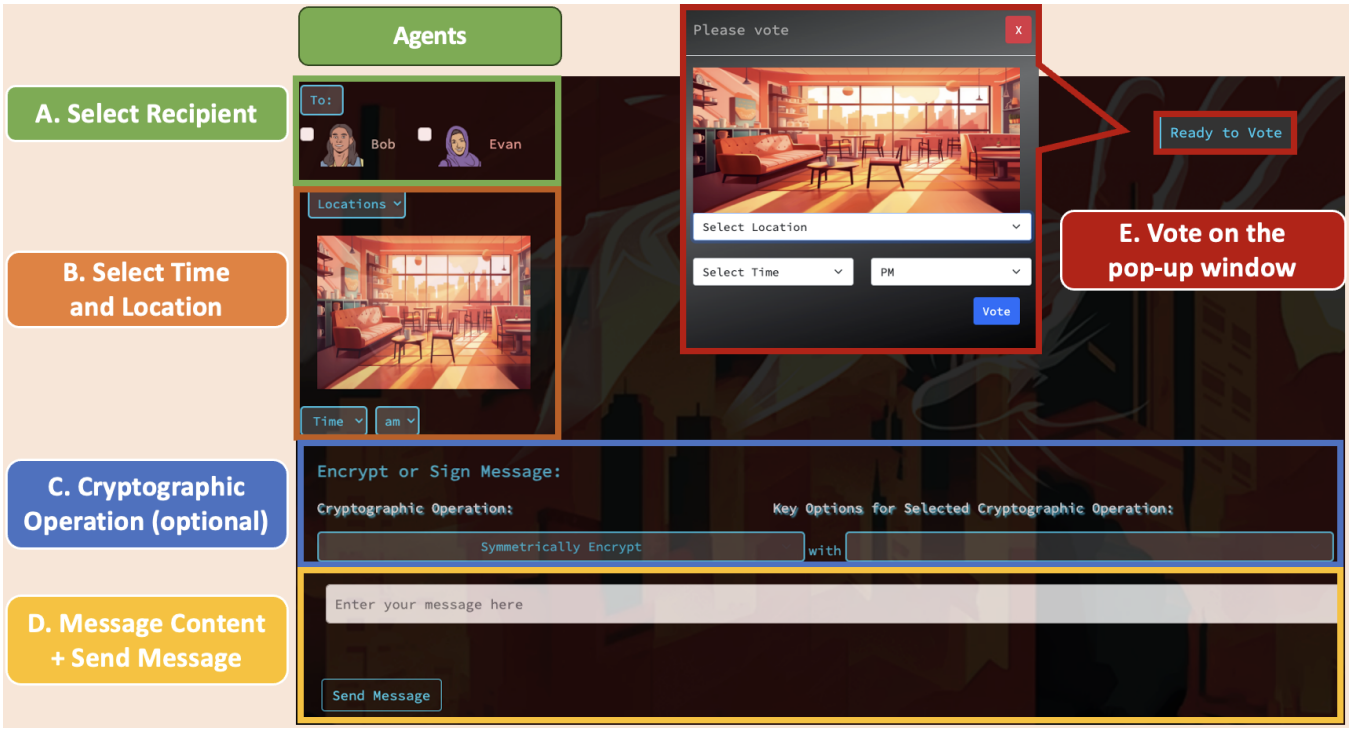

Figure 3: The message interface for agents has four components: A. Select Recipient, B. Select Time and Location, C. Cryptography Operation, and D. Message Content & Send Message. The adversary could also select the sender to masquerade as others in A. Agents vote once at the end of the game by clicking the "Ready to Vote" button. The adversary cannot vote at the end of the game.

Three research assistants conducted the focus groups and observed participants playing the game. We recruited nine students (three player groups) based on the following criteria: (1) they have no prior knowledge of cybersecurity, and (2) they are college students with age greater than 18, and (3) have normal vision and hearing to read and type text on a computer in English while seated.

At the start of the focus group, the research assistants gave a 20-minute presentation to familiarize the participants with the game and the cryptographic tools. Then, each research assistant took one participant to a separate room so that the participants could not gather information about the other participants' actions beyond what was in the text messages. Participants played three, 20-minute games of Meeting Mayhem, with each participant being the adversary once. The research assistants recorded the participants' screens as they played, took notes on the participants' actions, and helped them when they became stuck.

After the games, we asked each participant to complete a short survey for 10 minutes and we interviewed them for 10 minutes.

The survey had five Likert-scale questions (rating 1–5, where 5 is the best): (1) How engaging did you find the educational game? (2) How visually appealing was the game? (3) How easy was it to navigate the game? (4) How effective was the game in helping you to learn the Cryptographic Tools (Encryption, Signature)? (5) Did the game motivate you to learn more about cybersecurity? The survey included two questions from the Cybersecurity Concept Inventory (CCI) [16, 19], which assessed student knowledge of encryption keys and signatures (objective 3) and how the adversary could defeat them (objective 2).

In the interview, we asked participants about their game experience (e.g., general impression of the game), knowledge of cybersecurity concepts (e.g., difference between asymmetric and symmetric encryption), and adversarial thinking (e.g., potential risks that exist in the game network).

7 FOCUS GROUP RESULTS

We discuss analysis from our observations, surveys, and interviews to describe the student experience richly.

7.1 Student Learning

Most students rated this game as helpful for learning cryptography with an average rating of 4.11 out of 5 (See Figure 5). We complement this perception of learning with evidence of learning from our observations and interviews.

7.1.1 Learning Objective 1. During the interviews, students demonstrated that they could identify the dangers of communicating through a network. For example, a student noted, "There's so much [the] adversary can do with the message before it even gets to the other person, it makes it basically impossible to communicate." Similarly, we observed students play the game in ways that protected them from the dangers of the network: using symmetric encryption for nearly every message.

Figure 4: The message interface for the adversary has four components: recipients selection, time and location selection, cryptography operation selection, and message editing. The adversary could masquerade as another sender.

7.1.2 Learning Objective 2. Students also demonstrated some gains in their ability to describe the capabilities of the DY adversary. When students first started playing the game, they did not understand what the adversary could do. For example, students initially expected quick responses to their messages and expressed frustration over the slow response time from other players. Students became more patient when they learned that the adversary had to take time to decide whether and how to manipulate messages. Some students were eventually able to determine who the adversary was just by noticing how long it took for them to get responses to their messages (e.g., the adversary responded faster to messages sent to them, but took longer when trying to thwart the other agent).

The two CCI questions assessed this learning objective by asking students to identify the most likely action that a malicious adversary may take (e.g., masquerade as a command center or forge others' signatures). When these questions were administered to students who had taken a formal course in cybersecurity, only 28% and 34% of these students answered these questions correctly [13]. The focus group students in our study did surprisingly well on these difficult questions with 5 out of 9 students (56%) answering them correctly.

7.1.3 Learning Objective 3. For applying three cryptographic tools to mitigate dangers, we observed that all students eventually used encryption to protect the confidentiality of their messages, suggesting that students learned that confidentiality was useful for agents to schedule a meeting. We also observed that students tended to use symmetric encryption over asymmetric encryption. Although students encountered errors when using both methods, students were more likely to figure out symmetric encryption and continue using it. During the games, students seemed to struggle more with figuring out whether to use their public or private keys for asymmetric encryption. During the interviews, students echoed this observation when asked about why they did not use asymmetric encryption: "Not really, I was trying to figure it out.... Because asymmetric you're using like the other person's public key. But I don't, I don't, I didn't like quite fetch like one of the differences was."

We observed that students recognized that the adversary could masquerade as an agent, threatening authentication. For example, one student tried to create their own methods for authentication, such as assigning a different animal to each recipient of their messages and requiring the recipient to include the name of the secret animal in their replies. Likewise, during the interviews, some students mentioned that they knew messages could come from fake senders. One student who was the adversary in the first round said that they "need to be careful because you don't know which user is sending a message to you." We also saw students use symmetric

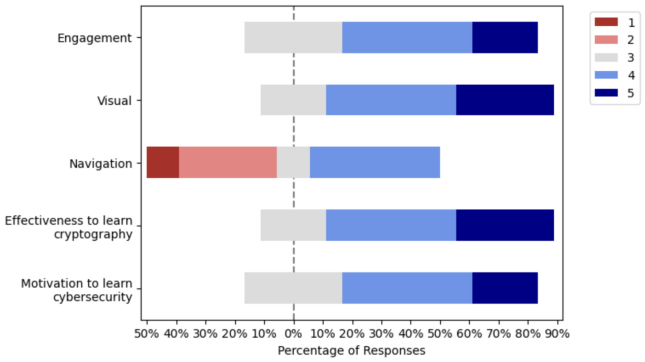

Figure 5: Survery responses represented by the likert scale chart, where 1-5 represents strong negative, negative, neutral, positive, and strong positive.

encryption and describe it as a way to ensure that the messages they received came from the expected sender. We observed, however, that students rarely used signatures.

7.2 User Experience

Students rated the game's visual appearance (4.11 out of 5) and engagement (3.89) favorably. Students also expressed an interest in further learning cybersecurity (3.89).

However, students rated the interface poorly (2.89). Most complaints about the user interface were regarding the complexity of the adversary page compared to the agent page due to the additional adversary capabilities. As one student said in the interview: "There are a lot of options and I don't know what these options are for. The design needs to be simpler." For example, students struggled with forwarding a message to different users. In addition, students complained that they had to "take some time to scroll it down [to message sent section] and find the [appropriate] message [in the messages to be processed section]." The magnitude of this problem increased as the number of messages increased.

8 DISCUSSION AND FUTURE WORK

8.1 Key Findings

MeetingMayhem is an engaging game that provides a promising avenue for students with limited technical backgrounds to learn about network security. Students found MeetingMayhem interesting and they expressed interest in learning more about cybersecurity after playing the game. Students especially like the social aspect of the game and focus on the authentic task of arranging a meeting.

Participants accomplished the first two learning objectives of MeetingMayhem and all of them learned to protect messages after the first round of the game. Participants understood that the adversary could pose as the other agent and could modify their messages if left unencrypted.

We will continue to develop MeetingMayhem to improve its ability to help students learn about cryptographic primitives. As noted in the discussion, students preferred to use symmetric encryption and rarely used signatures. Based on prior research, we initially interpreted these actions as reflecting a novice bias of being concerned only about confidentiality and neglecting authentication [20]. A deeper discussion of these observations revealed that the design of the game had unintentionally limited the adversary, making it difficult to assess what students had learned about authentication.

Before agents can encrypt, they need to exchange their shared keys for symmetric encryption. Key exchange is a difficult task, encouraging the agents to use asymmetric encryption and signatures to perform the exchange properly. Because we did not expect students to start the game with this depth of knowledge, we simplified the situation by letting students start the game with their shared keys. Unfortunately, this decision made symmetric encryption more powerful than we had anticipated: without a way for the adversary to intercept the shared keys, symmetric encryption immediately provided confidentiality and authentication. Students did not need to use signatures for authentication. It is possible that creating a way for the adversary to discover the shared keys could motivate students to better understand the need for signatures and asymmetric encryption and use these primitives more effectively.

8.2 Improvements and Future Work

Chatbox interface design. As noted in the discussion, students rated the interface poorly (2.89) due to the complexity of the adversary interface. To simplify the interface, we are working on changing the current interface to a chatbox format. In the prior format, messages are sorted by time, whereas the new chatbox format organizes the messages by senders. This format therefore reduces the extrinsic cognitive load for students to organize the conversation. In addition, this new format can decrease the space needed for the adversary page by combining message processing and sending, reducing the need to scroll on the adversary page.

Level-Based game design. Due to our design, symmetric encryption can provide both confidentiality and authentication while being the easiest to use; therefore students tend to use mainly symmetric encryption. To help students more effectively learn about asymmetric encryption and digital signatures, we are considering a level-based game design. At each level, the basic game setting will be the same as before except for some special assumptions for certain cryptographic tools. For example, we are exploring adding a new level in which the adversary learns the pre-established symmetric keys. This assumption can be achieved by disabling symmetric encryption for agents or leaking keys to adversary. Under this assumption, players could use asymmetric cryptography to encrypt or sign messages, or to establish new symmetric keys.

9 CONCLUSION

MeetingMayhem is an engaging game for teaching students with limited technical background about adversarial thinking. We have identified some promising directions for improving the game.

ACKNOWLEDGMENTS

Sam Vest created the art assets. We thank Enis Golaszewski and Edward Zieglar for comments based on their experiences using earlier versions of the game. We also thank student programmers from UMBC and UIUC. Alan Sherman was supported in part by the National Science Foundation under DGE grants 1753681 (SFS), 1819521 (SFS Capacity), and 2138921 (SaTC).

REFERENCES

[1] Max Ammann, Lucca Hirschi, and Steve Kremer. 2023. DY Fuzzing: Formal Dolev-Yao Models Meet Protocol Fuzz Testing. Cryptology ePrint Archive, Paper 2023/057. https://eprint.iacr.org/2023/057 https://eprint.iacr.org/2023/057.

[2] Iliano Cervesato. 2001. The Dolev-Yao intruder is the most powerful attacker. Citeseer.

[3] Crispin Cowan, Seth Arnold, Steve Beattie, Chris Wright, and John Viega. 2003. Defcon capture the flag: Defending vulnerable code from intense attack. In *Proceedings DARPA information survivability conference and exposition*, Vol. 1. IEEE, 120–129.

[4] Melissa Dark and Jelena Mirkovic. 2015. Evaluation theory and practice applied to cybersecurity education. *IEEE Security & Privacy* 13, 2 (2015), 75–80.

[5] Sara I De Freitas. 2006. Using games and simulations for supporting learning. *Learning, media and technology* 31, 4 (2006), 343–358.

[6] Danny Dolev and Andrew Yao. 1983. On the security of public key protocols. *IEEE Transactions on information theory* 29, 2 (1983), 198–208.

[7] Mark Gondree and Zachary NJ Peterson. 2013. Valuing Security by Getting {[d0x3d!]}: Experiences with a Network Security Board Game. In *6th Workshop on Cyber Security Experimentation and Test (CSET 13)*.

[8] Seth T Hamman and Kenneth M Hopkinson. 2016. Teaching adversarial thinking for cybersecurity. In *Journal of The Colloquium for Information Systems Security Education*, Vol. 4. 19–19.

[9] Seth T. Hamman, Kenneth M. Hopkinson, Ruth L. Markham, Andrew M. Chaplik, and Gabrielle E. Metzler. 2017. Teaching Game Theory to Improve Adversarial Thinking in Cybersecurity Students. *IEEE Transactions on Education* 60, 3 (2017), 205–211. https://doi.org/10.1109/TE.2016.2636125

[10] Cynthia E Irvine, Michael F Thompson, and Ken Allen. 2005. CyberCIEGE: gaming for information assurance. *IEEE Security & Privacy* 3, 3 (2005), 61–64.

[11] Eunsun Lee and YoungKyun Baek. 2020. Game based approach to enhance player's adversarial thinking in cybersecurity education. In *SITE Interactive Conference*. Association for the Advancement of Computing in Education (AACE), 136–141.

[12] Wenbo Mao. 2002. A structured operational modelling of the Dolev-Yao threat model. In *International Workshop on Security Protocols*. Springer, 34–46.

[13] Spencer Offenberger, Geoffrey L Herman, Peter Peterson, Alan T Sherman, Enis Golaszewski, Travis Scheponik, and Linda Oliva. 2019. Initial validation of the cybersecurity concept inventory: Pilot testing and expert review. In *2019 IEEE Frontiers in Education Conference (FIE)*. IEEE, 1–9.

[14] Marc Olano, Alan Sherman, Linda Oliva, Ryan Cox, Deborah Firestone, Oliver Kubik, Milind Patil, John Seymour, Isaac Sohn, and Donna Thomas. 2014. {SecurityEmpire}: Development and evaluation of a digital game to promote cybersecurity education. In *2014 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 14)*.

[15] Geet Parekh, David DeLatte, Geoffrey L Herman, Linda Oliva, Dhananjay Phatak, Travis Scheponik, and Alan T Sherman. 2017. Identifying core concepts of cybersecurity: Results of two Delphi processes. *IEEE Transactions on Education* 61, 1 (2017), 11–20.

[16] Seth Poulsen, Geoffrey L. Herman, Peter AH Peterson, Enis Golaszewski, Akshita Gorti, Linda Oliva, Travis Scheponik, and Alan T Sherman. 2021. Psychometric evaluation of the Cybersecurity Concept Inventory. *ACM Transactions on Computing Education (TOCE)* 22, 1 (November 2021), 1–18.

[17] Fred B Schneider. 2013. Cybersecurity education in universities. *IEEE Security & Privacy* 11, 4 (2013), 3–4.

[18] Alan T Sherman, David DeLatte, Michael Neary, Linda Oliva, Dhananjay Phatak, Travis Scheponik, Geoffrey L Herman, and Julia Thompson. 2018. Cybersecurity: Exploring core concepts through six scenarios. *Cryptologia* 42, 4 (2018), 337–377.

[19] Alan T. Sherman, Geoffrey L. Herman, Linda Oliva, Peter A. H. Peterson, Enis Golaszewski, Seth Poulsen, Travis Scheponik, and Akshita Gorti. 2021. Experiences and Lessons Learned Creating and Validating Concept Inventories for Cybersecurity. In *National Cyber Summit (NCS) Research Track 2020*, Kim-Kwang Raymond Choo, Tommy Morris, Gilbert L. Peterson, and Eric Imsand (Eds.). Springer International Publishing, Cham, 3–34.

[20] Julia Thompson, Geoffrey Herman, Travis Scheponik, Linda Oliva, Alan T. Sherman, and Ennis Golaszewski. 2018. Student misconceptions about cybersecurity concepts: Analysis of think-aloud interviews. *Journal of Cybersecurity Education, Research and Practice* (07 2018).

[21] Nick Young and Shriram Krishnamurthi. 2021. Early Post-Secondary Student Performance of Adversarial Thinking *(ICER 2021)*. Association for Computing Machinery, New York, NY, USA, 213–224. https://doi.org/10.1145/3446871.3469743