Cyber Attack! A Story-driven Educational Hacking Game

Ersin Dincelli
University of Colorado Denver

Alper Yayla
University of Tampa

Łukasz Kusyk
LUXO Interactive

Abstract

There is an urgent need for cybersecurity professionals as large-scale data breaches and hacks are becoming daily occurrences. However, several perceived barriers prevent the young generation from pursuing a cybersecurity-related career. One of the major barriers is the perception that cybersecurity is a purely technical field that requires expertise in computer science. Attracting young people to join the cybersecurity workforce requires innovative pedagogical methods that go beyond the traditional cybersecurity education, especially to make the field more accessible. We postulate that game-based learning can motivate young generations to learn more about cybersecurity and reduce the perceived barriers that prevent them from considering cybersecurity-related career paths. To pursue this thesis, we developed *Cyber Attack*, a story-driven cybersecurity video game that incorporates various gamification elements that focus on fundamental cybersecurity concepts. This paper details the design principles we followed for the early version of *Cyber Attack*.

1. Introduction

The current cybersecurity workforce consists of 2.8 million professionals, a level much lower than the workforce needed globally [1]. It is estimated that over 4 million cybersecurity professionals are in demand to make up for the labor shortage in the cybersecurity field. In addition to the limited supply of professionals, the need for cybersecurity workforce is being fueled by the increasing number of data breaches and various other cyber crimes [2]. Given this state of the field, the demand for a highly skilled cybersecurity workforce will continue to grow, possibly faster than the supply of cybersecurity professionals for the near future. Therefore, educating a new generation of cybersecurity professionals is an immediate need for all nations.

There are several barriers that hinder the pursuit of cybersecurity-related career paths among young people. A major barrier is the perception that cybersecurity is a highly technical field for nerdy males who have expertise in computer science [3]. Such individual stereotypes may discourage students from starting a cybersecurity-related career. Additionally, ethnicity, income level, and educational level also influence students' interest in cybersecurity careers [4], limiting the diversity of the field and strengthening the existing stereotypes. Another barrier is that traditional teaching methods often fail to motivate and engage students, especially teaching subjects in science, technology, engineering and math (STEM) disciplines [5]. STEM learners first need to be motivated so that they can see the value of the subject matter before they invest their time and effort in learning.

Prior research suggests the use of gamification techniques to increase engagement and awareness of students and improve learning outcomes in teaching cybersecurity [6]. Gamified systems provide a framework for educational programs for enhancing students' motivation in learning tasks and materials that are perceived as difficult [7]. For instance, using game-design elements in non-game system contexts can increase users' motivations, engage them in the learning materials, and help process information easier, thus leads to achievement of learning goals [8]. The use of gamification has been effective in increasing engagement and learning new skills not only in non-technical fields but also in technical fields like cybersecurity training [9]. Video games provide an effective platform to introduce gamification elements for teaching cybersecurity [10]. However, many exiting cybersecurity games are designed for training professionals and require an understanding of fundamental cybersecurity concepts [6]. Therefore, there is a lack of engaging educational video games for young people with little or no knowledge in cybersecurity that can spark their interest and motivate them to learn more about it [11].

Given the state of the cybersecurity workforce and the challenges of young people to enter the field, we developed a cybersecurity video game called *Cyber Attack* that incorporates gamification elements. Following a design science research approach, we developed *Cyber Attack* with the goal of increasing motivation and engagement to explore and learn fundamental concepts of cybersecurity, such as cyber threats, malicious actors, social engineering, information gathering, ethics, Internet of Things (IoT), computer and digital forensics, cryptography, and online safety in a game environment.

USENIX Symposium on Usable Privacy and Security (SOUPS) 2020. August 9 -- 11, 2020, Boston, MA, USA.

Figure 1: Cyber Attack is a story-driven hacking game in which the player controls a team of hackers.

2. Related Work

The use of games is an effective learning method as games can be highly motivational if they are created following specific design principles [12]. One of the important design principles is *reflection*. Reflection is built on the argument that games should provide opportunities for the users to stop and think, or in other words reflect, on the knowledge they have acquired [13]. *Storytelling* is another learning design principle that advocates for the use of narratives and real-life characters in the gamified content to guide users throughout the learning process [13]. The use of storylines with interpreted or experiential narratives stimulates a game-like experience and therefore can be an effective method to change the user's perceptions towards the learning materials positively [14].

Game design elements should be chosen carefully considering the target audience to be able to create the desired user-system interactions, as well as the desired experiential and instrumental outcomes [15]. The taxonomy developed by Helms et al. includes seven broad categories for the design of educational game elements for gamification: *progression*, *rewards*, *rules*, *competition*, *social*, *communication*, and *general* [5]. Careful integration of these game elements into the design of educational materials increases motivation and engagement of users by making learning more interesting and appealing compared to traditional methods [5].

For cybersecurity education, the necessary skills are best acquired with experiential learning techniques that use real-life examples [16] and engaging games [17]. One of the necessary conditions for cybersecurity education is that students should be able to discover and learn a variety of threats, vulnerabilities, and exploits in a safe and protected environment, without the fear of damaging the actual computer systems. This is particularly important to understand ethical issues and consequences in cybersecurity. Therefore, beyond increasing engagement and motivation, the use of games is beneficial in creating the necessary safe learning environment. In the next section, we provide details of *Cyber Attack* and the design of game elements through the design science research lens.

3. Method

Cyber Attack is a story-driven hacking game in which the player controls a team of hackers. The player can intercept communications among individuals, hackers, corporations, or governments around the world. The player can choose to protect people by exposing private messages between malicious actors or exploit highly sensitive information to earn fame and money. The player also has the ability to hack numerous different devices in over seven thousand cities all around the world using an interactive world map. Each dot on the map in Figure 2 represents a city and initiates a quest. The player can hire hackers to establish a hacker team and branch in different cities.

The game was created using the Unity 2019.3 game engine and the C# programming language. The Unity game engine allows easy implementation of gameplay solutions. We used a Unity asset called *World Political Map Globe Edition 2* for the simulation of the interactive 3D world map. *Cyber Attack* is available on Steam, one of the biggest video game digital distribution services.

We used the principles of design science research as a guideline in developing *Cyber Attack*. The main goal of design science research is to build innovative solutions for significant problems. The guideline developed by Hevner et al. [18], which initiated a strong stream of research that produced several generally accepted design science models, describes the activities required to create and evaluate an IT artifact that is intended to solve a problem. The synthesis of the existing models revealed a methodology that categorized the main activities of the design science research as *artifact creation* and *artifact evaluation* [19].

3.1. Artifact Creation

In artifact creation, we followed an iterative design process based on Helms et al.'s taxonomy of educational game elements as shown in Table 1 [5].

Figure 2: Using an interactive world map, the player can choose a quest in over seven thousand cities.

Table 1. Educational Game Elements in *Cyber Attack* (Helms et al., 2015)

Progression	Quests	Players follow non-linear sequence of quests to progress through the game. At the end of each quest, they are asked to make a decision (see Figure 3).
	Storyline	The game includes a non-linear storyline that offers various decisions points. The story develops based on the decisions the player makes at the end of each quest. The decisions affect the player's ***ethics level***, which is an indication of white hat or black hat hacker.
Rewards	Progression points	Each quest rewards the hacker with cumulative ***progression points***, which give the ability to unlock new hacking skills.
	Resources	Each quest also rewards the hacker with ***cryptocurrency***, ***fame***, and ***followers***. Based on her performance, the hacker also collects ***personal data*** during the quest, which she can sell in black market for additional cryptocurrency.
Rules	General rules	Cyber Attack includes basic rules to guide players and constrain their behaviors within the game.
	Time constraints	Each quest has a limited time. The more system the player hacks during this time, the more progression points and resources she earns.
Competition	Leaderboards	The leaderboard compares the achievements and progression points of all the Cyber Attack players.
	Challenge	In addition to the time constraint, each quest includes firewalls that slow down the hacking attempts of the player. Player needs to avoid going through areas with firewall (see Figure 5).
General	Control	Participants have control over how the game develops. The decisions the player makes changes her ethics level, which ranges between -100 and 100. For example, negative values attract more attention from the police.
	Fun	The game aims to be fun to reduce the effort players put into learning.

Progression triggers the intrinsic motivation to progress in a story, which in turn influences the extrinsic motivation to complete the gamified training. With the help of progression, users can see the impact of their actions (i.e., *reflection*), and this, in turn, increases their motivation to focus on the training material. We included two aspects of progression in *Cyber Attack*: *quests* and *storyline*.

The player follows a non-linear sequence of quests by conducting hacks in different cities around the world and progress through the game. In each quest, the player is exposed to fundamental concepts of cybersecurity chosen based on GenCyber *cybersecurity first principles* and *cybersecurity concepts* - two frameworks suggested for cybersecurity curriculum for students at the K-12 level[1]. At the end of each quest, the player is forced to make a decision, which often involves ethical decision-making that teaches about the consequences of certain actions in the context of cybersecurity. The decisions affect the player's *ethics level* and the number of rewards she earns. Ethics level is an indication of being a white hat or black hat hacker. The ethics level ranges from -100 to 100. If the value is less than 0, the law enforcement begins to pursue the player, resulting in possible loss of resources. The quests are designed to increase the motivation of the player by providing her various goals (e.g., being an activist, white hat or black hat hacker). Figure 3 presents an example of an ethical decision-making process.

Figure 3: The decisions players make at the end of each quest affect their ethics level and the rewards she earns.

[1] GenCyber is a cybersecurity summer camp program funded by NSF and NSA. For more information, see www.gen-cyber.com.

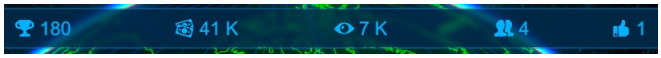

Figure 4: Progress Indicators. From left to right: progression point, cryptocurrency, fame, followers, and ethics level

Cyber Attack also includes a non-linear storyline that offers various decision alternatives that the player can learn from. The story develops depending on the player's ethics level and her decisions. The storyline adds context and relevance to the player's actions throughout the game, and further increase the motivation to play and learn concepts related to cybersecurity and ethical decision making.

Rewards are implemented to create a sense of continuous progress and increase the motivation to complete tasks in gamified systems. We included two types of rewards: *progression points* and *resources*. Figure 4 shows the in-game icon of each progress indicator. Progression point is the main indicator of progress in the game. Each quest rewards the player with cumulative progression points, which give the player the ability to unlock new hacking skills. With new hacking skills, the player can unlock new quests and increase the amount of resources that she earns after completing the quests.

Resources are the second type of rewards that are earned after completing quests. There are three different types of resources: *cryptocurrency*, *fame*, and the *hacker team*. Cryptocurrency can be used to hire additional hackers and to open new branches in the hacking skill tree. Figure 5 presents a part of the hacking skill tree. Certain hacking skills and quests can be unlocked by increasing the size of the hacking team, adding another decision point for the user with respect to choosing resources. Fame rises when more people, other hackers, or governments start to pay attention to the player, which is related to the player's activities and progress. The impact of the player's decisions increases with the amount of the fame she has. Based on her performance, the player can also collect personal data during the quests. Personal data can be sold in the black market for additional cryptocurrency.

Figure 5: A part of the hacking skill tree.

Figure 6: An example of a quest with time constraint and challenges. The player tries to hack as many devices as possible and avoid firewalls during the quest.

Rules are integrated to control players' actions. *Cyber Attack* includes basic rules to guide players and constrain their behaviors within the game. Quests also include time constraints. The player has to complete each quest in a limited time. The more system the player hacks during this limited time, the more progression points and resources she earns.

Competition increases the motivation and engagement to outperform other players, thus increase the learning outcomes. We included two competition elements: *leaderboard* and *challenges*. Players compare their achievements and progression points using the leaderboard. Challenges add an extra layer of difficulty for the quests. Figure 6 presents a quest that includes firewalls that slow down the player. The player needs to avoid firewalls and hack as many devices as possible with limited time.

The **General** category has two game elements: *control* and *fun*. Players have control over how the story develops. Since the player can see the consequences of her actions and how they affect the storyline, her motivation to make proper decisions increases. In turn, the focus on learning the cybersecurity material also increases as they directly affect the success of the player. Fun reduces the effort players put into learning and increases the engagement level. Table 1 maps the game design elements that we used in *Cyber Attack*.

3.2. Artifact Evaluation

The goal of the artifact evaluation is to show the feasibility of the artifact and its success in meeting the design goals based on the data collected through proofs, experiments, simulations, or observations [19]. Our overall proof-of-value of *Cyber Attack* is going to be demonstrated by the following performance criteria: the efficacy of the game will be assessed by interviewing players. Effectiveness will be assessed by conducting a survey that will ask players about the fundamental concepts they learned during their time spent in *Cyber Attack*. We will also collect various usability metrics, such as satisfaction with the game as an educational tool and ease of use and learning [9].

4. Conclusion

One of the main challenges of the cybersecurity field is the availability of qualified professionals. The increasing number of security breaches further highlights the need for systematic changes in cybersecurity education. Based on the findings of the literature, we postulate that combining educational game elements in an engaging video game that is designed to educate people about fundamentals of cybersecurity can increase the interest of young people in cybersecurity-related career paths. *Cyber Attack* is developed parallel to the principles of the design science research and includes carefully integrated game elements that correspond with generally accepted cybersecurity topics. In the next steps of our research, we will evaluate the proof-of-value of our artifact based on the interviews of the players. We believe that *Cyber Attack* provides a compelling alternative as an effective educational platform for cybersecurity.

References

[1] $(ISC)^2$. Cybersecurity workforce study 2019. Accessed May 26, 2020: www.isc2.org/Research/2019-Cybersecurity-Workforce-Study, 2019.

[2] Rob Sobers. 107 must-know data breach statistics for 2020. Accessed May 25, 2020: www.varonis.com/blog/data-breach-statistics, 2020.

[3] Julie M. Haney and Wayne G. Lutters. Skills and characteristics of successful cybersecurity advocates. In *Proceedings of the 13th Symposium on Usable Privacy and Security*, 2017.

[4] Sangmi Chai, Sharmistha Bagchi-Sen, Rajni Goel, H. Raghav Rao, and Shambhu Upadhyaya. A framework for understanding minority students' cyber security career interests. In *Proceedings of the 12th Americas Conference on Information Systems*, 2006.

[5] Remko W. Helms, Rick Barneveld, and Fabiano Dalpiaz. A method for the design of gamified trainings. In *Proceedings of the 19th Pacific Asia Conference on Information Systems*, 2015.

[6] Marc Olano, Alan Sherman, Linda Oliva, Ryan Cox, Deborah Firestone, Oliver Kubik, Milind Patil, John Seymour, Isaac Sohn, and Donna Thomas. 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)*, 2014.

[7] Michael D. Hanus and Jesse Fox. Assessing the effects of gamification in the classroom: A longitudinal study on intrinsic motivation, social comparison, satisfaction, effort, and academic performance. *Computers & Education*, 80: 152-161, 2015.

[8] Horst Treiblmaier, Lisa-Maria Putz, and Paul Benjamin Lowry. Setting a definition, context, and theory-based research agenda for the gamification of non-gaming applications. *AIS Transactions on Human-Computer Interaction*, 10(3): 129-163, 2018.

[9] Ersin Dincelli and InduShobha Chengalur-Smith. Choose your own training adventure: Designing a gamified SETA artefact for improving information security and privacy through interactive storytelling. *European Journal of Information Systems*, 2020. http://dx.doi.org/10.1080/0960085X.2020.1797546

[10] Christopher B. Mayhorna and Patrick G. Nyeste. Training users to counteract phishing. *Work*, 41: 3549-3552, 2012.

[11] Paul Gestwicki and Kaleb Stumbaugh. Design and evaluation of a cybersecurity education game: S^2ERC technical report 318, 2016.

[12] Clark N. Quinn. Engaging learning: Designing e-learning simulation games. John Wiley & Sons, 2005.

[13] Steve Sheng, Bryant Magnien, Ponnurangam Kumaraguru, Alessandro Acquisti, Lorrie Faith Cranor, Jason Hong, and Elizabeth Nunge. Anti-phishing phil: The design and evaluation of a game that teaches people not to fall for phish. In *Proceedings of the 3rd Symposium on Usable Privacy and Security*, 2007.

[14] Paul Ralph and Kafui Monu. Toward a unified theory of digital games. *The Computer Games Journal*, 4: 81-100, 2015.

[15] De Liu, Radhika Santhnam, and Jane Webster. Toward meaningful engagement: A framework for design and research of gamified information systems. *MIS Quarterly*, 41(4): 1011-1034, 2017.

[16] Melissa Dark. Advancing cybersecurity education. *IEEE Security & Privacy*, 12(6): 79-83, 2014.

[17] Tamara Denning, Adam Lerner, Adam Shostack, and Tadayoshi Kohno. Control-Alt-Hack: The design and evaluation of a card game for computer security awareness and education. In *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*, 915-928, 2013.

[18] Alan R. Hevner, Salvatore T. March, Jinsoo Park, and Sudha Ram. Design science in information systems research. *MIS Quarterly*, 28(1): 75-105, 2004.

[19] Ken Peffers, Tuure Tuunanen, Marcus A. Rothenberger and Samir Chatterjee. A design science research methodology for information systems research. *Journal of Management Information Systems*, 24(3): 45-77, 2007.