GenCyberCoin: An Engaging, Customizable, and Gamified Web Platform for Cybersecurity Summer Camps and Classrooms[*]

Vitaly Ford[1], Ambareen Siraj[2]
[1]Computer Science and Math Department
Arcadia University
Glenside, PA 19095
`fordv@arcadia.edu`
[2]Department of Computer Science
Tennessee Tech University
Cookeville, TN 38505
`asiraj@tntech.edu`

Abstract

Teaching cybersecurity requires dedicating a substantial amount of time and effort to combine both practical and theoretical notions into a coherent and clear chain of thoughts. As a result, educators have been exploring various gamification techniques to spark interest among students and engage them with interactive activities leading to a cybersecurity career. In this paper, we present a GenCyberCoin open-source web platform that can be used as a complementary module to the existing teaching material in cybersecurity summer camps and classrooms. GenCyberCoin aims to facilitate the development of students' interest in cybersecurity by providing students with opportunities to earn and spend digital currency, practice bug hunting, and get rewarded for helping peers and completing tasks. This platform introduces students to real-world concepts such as the blockchain, digital currency markets, banks, cybersecurity principles, open source intelligence gathering, passwords, bug bounty, and social norms and values.

1   Introduction

The cybersecurity field has seen a significant growth of interest from academia and government in recent years. Numerous cybersecurity education programs and calls for grant proposals have been developed, for example, GenCyber[12], CLARK[1], C5[2], NSF SaTC EDU[4], and CyberCorps SFS[5].

Teaching cybersecurity requires dedicating a substantial amount of time and effort to combine both practical and theoretical notions into a coherent and clear chain of thoughts. Consequently, to address the need for developing a cybersecurity workforce pipeline, educators have been exploring various creative gamification techniques to spark interest among students and engage them with interactive activities leading to a cybersecurity career – a career that demands much focus, patience, grit, critical thinking, and aspiration for continuous learning[7, 8, 9, 10, 11, 13, 14, 15].

In this paper, we present a publicly-available GenCyberCoin web platform[6] that can be used as a complementary module to the existing cybersecurity teaching material in cybersecurity summer camps and classrooms. This platform facilitates increasing students' interest in cybersecurity, incentivizes students to complete assignments, promotes exploring cybersecurity on their own, and provides a practical approach to teaching cybersecurity principles with interactive elements. GenCyberCoin is an open-source platform and it assumes no prior experience in cybersecurity from students and teachers.

1.1   Related Work

Weanquoi et al.[15] developed an educational 2D game called "Bird's Life". This game focuses on teaching phishing attacks and defense techniques. The game works on different platforms (PC, web, and mobile). They deployed the game in several courses related to Internet Systems and Computer Usage. The feedback they received demonstrated that students enjoyed the game, learned anti-phishing tips, and increased their interest in learning more.

Jin et al.[10] incorporated game elements into their GenCyber[12] summer camp. They developed four games: a 3D social engineering game, 3D VR secure online behavior game, cyber defense tower game, and 2D GenCyber card game. Their post-camp survey demonstrated promising results in terms of utilizing games as camp activities.

Švábenský et al.[14] designed a cyber range where undergraduate students learned about network attacks and defenses by creating educational games that teach about certain vulnerabilities. Students learned cybersecurity attack and defense methodologies and worked on their own game projects that they later presented in front of students and professors.

Gonzalez et al.[9] developed a classification taxonomy for cybersecurity

training resources that implemented gamified elements. Based on that taxonomy, they classified a number of gamification-related cybersecurity education projects and aligned them with their curriculum in several courses.

Giannakas et al.[8] developed a mobile app called CyberAware for K-6 children for cybersecurity awareness. The topics of the mini-games in this app include firewalls, antivirus, security patches, updates, and email spam filters.

Fouché et al.[7] proposed utilizing the existing Code Hunt framework[13] to teach application security and IT auditing by adding gamification elements. They also discussed how others have been incorporating secure coding into the Code Hunt framework.

Olano et al.[11] developed a multiplayer cybersecurity game called SecurityEmpire for high school students. It teaches about information assurance practices.

2 Motivation and Contribution

In 2017, our initial goal was to develop a web platform that would engage and incentivize students, providing a continuous cybersecurity learning experience throughout a one-week long GenCyber summer camp. GenCyberCoin has since evolved to address the following challenges in a practical way:

- Encourage students to pursue a cybersecurity career.
- Introduce students to the blockchain and digital currency markets.
- Introduce students to the major cybersecurity concepts, including "confidentiality, integrity, availability, defense in depth, keep it simple, and think like an adversary".
- Introduce students to social engineering and reconnaissance.
- Introduce students to bug bounty hunting and software bugs.
- Introduce students to social and ethical norms and values.
- Introduce students to password attacks and management practices.
- Provide an incentive for students to go an extra mile in participating in the activities and assignments.

2.1 Features

Additional features of GenCyberCoin include:

- Rewarding participation by allowing students to earn digital coins.
- Allowing students to show appreciation to peers.
- Allowing GenCyberCoin administrators to customize:
  - the marketplace with real products of their choice that students can purchase with their earned GenCyberCoins;

- the reconnaissance and social engineering questions that students can answer, earning GenCyberCoins;
- the activities that can be assigned to students who receive a custom number of GenCyberCoins when they successfully complete an activity.

- Being open-source and freely available on GitHub[6] with detailed instructions on how to set it up locally, through docker[3], and in the cloud.
- Having an intuitive, responsive, and easy to use web/mobile interface.

3 GenCyberCoin Web Platform

Some of the major goals of GenCyberCoin are to raise interest in cybersecurity, capture students' attention, and make the cybersecurity assignments engaging. To achieve these goals, the platform provides students with opportunities to explore and learn the cybersecurity principles in a hands-on way via the integrated account, wallet, blockchain, bug bounty, hall of fame, reconnaissance, feedback, and market modules. Additionally, it provides teachers (administrators) with modules to generate registration and reward codes, add and edit market/activities/reconnaissance, nominate activities, view student orders, manage students, change settings, and view feedback. The student view of the home page is shown in Figure 1.

3.1 Initial Setup

When teachers log into their accounts, they can perform multiple actions, such as preparing Activities, Market Items, and Reconnaissance/social engineering questions. It is not necessary to set up any of these for students to start learning about cybersecurity, however, we recommend to at least add a few new Activities and Reconnaissance questions to fully engage students.

Activities can represent badges, achievements, or completed assignments (gamification features) that can be later nominated to students upon teachers' discretion. Teachers have full control of what information they put on each Activity (picture, name, and description). Every Activity can also have a different GenCyberCoin value assigned to it.

Market Items are real goods that teachers decide to give away. Those items can be things that teachers receive from conferences, school swag, etc. Students can purchase those items on the Market, using their GenCyberCoins.

Reconnaissance and social engineering questions can be used to increase curiosity, break the ice, and teach about open source intelligence gathering. These questions can be anything that the teachers would like to ask; they can be about the teachers themselves, some random facts related to someone

Figure 1: Home page of GenCyberCoin in "student" view.

famous, cybersecurity puzzles, etc. For example, "where did Dr. Leo spend her vacation this year", "how old is our school", "decode: scaegneig oilniern", and "what is the company name of the watch that Dr. Craig is wearing". When a student correctly answers a reconnaissance question, the student automatically receives a GenCyberCoin reward, the value of which is set by the teacher in Settings.

3.2 Registration and Reward Codes

Teachers can create registration and reward codes that can be generated automatically or manually. The registration codes would allow students to register on the website whereas the reward codes (custom-named by teachers or auto-generated by the platform) would allow teachers to give those codes to students for various reasons, such as successfully completing assignments, finishing within a certain time period, helping peers, being a good team player, being a good listener – in other words, teachers have the absolute freedom to choose for what reasons they give the reward codes.

3.3 Bug Bounty and Hall of Fame

Bug Bounty is an autonomous module that introduces bugs on the website in various places on the platform. Students are provided with hints on where and what types of bugs to search for, whereas teachers do not need to know how to find those bugs. This module does not break anything on the website but when a student finds a bug, the platform automatically lets the student know what this bug allows to do in the real world and then rewards the student with GenCyberCoins for discovering the bug. Additionally, the student's bug hunting record is timestamped and captured on the Hall of Fame page that is visible to all students and teachers. At the time of writing, the platform contains 18 different bugs and we are in the process of adding more.

Additionally, the Hall of Fame links every found bug with the external resources so that students could further investigate the secure coding topics.

3.4 Blockchain

Every transaction happening on the platform is captured in a Blockchain. Students and teachers can transfer coins to anyone in their Wallets. Also, when students complete Reconnaissance questions or find a bug, they automatically receive GenCyberCoins. All of the aforementioned transactions are recorded in the Blockchain, representing a public digital ledger that is available for everyone to view. The transactions in the Blockchain are not reversible.

3.5 Settings

Teachers have full control over all settings including Market On/Off, Bug Bounty On/Off, Reconnaissance On/Off, custom reward value for bug bounty, custom reward value for correctly answering reconnaissance questions, and others. They can also customize the title and description of the platform's header text, located at the top of every page.

3.6 Feedback

Students can leave anonymous comment/feedback about anything they have in mind and teachers can view that feedback on a separate page.

3.7 Account, Password, and Wallet

Students can view their Activities and personal information on the Account page. The password manager is also available on that page, leading students to learn about the importance of password complexity and where to securely check if a real personal password has been compromised as a result of a data

breach. The Wallet page represents a digital bank where students can transfer money and redeem reward codes as GenCyberCoins that they can later use to purchase real goods on the Market.

GenCyberCoin has a password recovery option and if a student answers two out three security questions correctly, the student will be automatically logged into the account without a password prompt. This could be an effective learning example of how hackers can log in to a bank account by obtaining personal information of a victim. Consequently, teachers can talk about the ethical implications of possibly knowing the answers to security questions of peers, friends, and relatives.

3.8 Social Ethics and Norms

GenCyberCoin lays the foundation for a social ethics and norms discussion. For example, Bug Bounty teaches students about ethical hacking versus unethical hacking, the difference between which can be described with one word: permission (did the person receive permission before performing the attack?) Also, Bug Bounty demonstrates the concept of responsible disclosure. Reconnaissance and Password Recovery teaches about privacy and its potential violation as a consequence of targeted social engineering and open source intelligence gathering attacks.

4 Learning Outcomes

At the end of all activities in this platform, the students will learn about:

- Confidentiality, integrity, availability, "defense in depth", "keep it simple", and "think like an adversary" concepts.
- Fundamentals of the blockchain technology and digital currency.
- Open source intelligence gathering and social engineering tactics.
- Password complexity and data breaches that leak passwords.
- Social ethics and norms.

5 Case Studies

We have deployed GenCyberCoin in multiple venues and its first use case was at the NSA/NSF GenCyber summer camp in 2017, Tennessee Tech University. It has also been deployed at the same camp in 2018. Both camps were one week long and GenCyberCoin was introduced on the first day, engaging students from the very beginning. Separately from GenCyberCoin, Tennessee Tech University GenCyber team (faculty, staff, students) has prepared many different activities with Raspberry Pis, virtual machines, console-based chat

systems, CryptoBoxes, and cyber defense games. We integrated some of those activities (especially cryptography-related) into GenCyberCoin in such a way that upon completing them, the students automatically obtained reward codes that they were able to redeem in the Wallet on the platform.

In spring 2019 semester, we integrated GenCyberCoin in the Introduction to Practical Security Assessment course at Arcadia University. We used the platform for making extra credit assignments, teaching about web attacks, and rewarding GenCyberCoins based on how active students have been in the class.

Additionally, we ran a three-hour long outreach event at a Lower Merion High School in Philadelphia, PA in January 2019. A part of the event was dedicated to a mini-competition on GenCyberCoin, in which students had to find answers to reconnaissance questions and search for as many bugs as they could find, engaging them to interact with each other and ourselves.

The overall feedback we received from students across all above-mentioned events was that they felt much more interested in studying cybersecurity. The GenCyberCoin motivated them to continuously learn more about security topics, search for bugs on the platform, complete the activities, and be good team players. The following is the anonymous anecdotal feedback from high school students and teachers who attended our camps and outreach activities:

> I think GenCyberCoin is a great way to learn about bugs and collect points.
> Wow!! Hope you get to make the coin for all camps.
> The website was a creative way to get us to learn about digital currency and other stuff. Love it. This was pretty cool.
> The coins both make the camp competitive and fun. It takes a lot to get teens focused, and even more to keep focus. You've done both.
> I'd love to figure out how to modify it for my classes.

Some other feedback we got was more peculiar:

> I will give you all of my coins for information of a bug.
> If I pay you 15$, can I have 15 coins.

The gameplay metrics gathered automatically in GenCyberCoin demonstrated that more than 90% of all students (across all venues where GenCyberCoin was presented) answered all Reconnaissance questions regardless of their difficulty and found more than half of the Bounty Bugs.

6   Conclusion and Future Work

We have developed a GenCyberCoin web platform that engages students in practical learning of the major cybersecurity principles, blockchain, digital cur-

rency, reconnaissance, ethics, and bug bounty. The engaging elements of the platform make it a promising tool for cybersecurity education at summer camps (for instance, GenCyber[12]) and classrooms. This platform is freely available on GitHub[6] and is constantly maintained. New features are being added and code-base is being improved. Also, GenCyberCoin has been used in multiple GenCyber camps in 2019 across the nation. Our next steps are to disseminate this work, receive and address the feedback, and continue making it a better web platform for raising students' interest in cybersecurity.

7 Acknowledgments

References

[1] CLARK. Effective cybersecurity curriculum at your fingerprints. `https://clark.center`.

[2] C5 Cyber Curriculum Development. The c5 project has brought together computer science faculty and cybersecurity educators to develop new course content that integrates the two disciplines. `https://www.c5colleges.org/index.php/cs-course`.

[3] Docker. Enterprise container platform for high-velocity innovation. `https://www.docker.com/`.

[4] NSF SaTC EDU. Proposals that focus entirely on cybersecurity education. `https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=504709`.

[5] CyberCorps Scholarship for Service. Scholarship for service is designed to recruit and train the next generation of it and security professionals to meet the needs of the cybersecurity mission for federal, state, local, and tribal governments. `https://www.sfs.opm.gov`.

[6] Vitaly Ford. GenCyberCoin GitHub Repository. `https://github.com/vitalyford/gencybercoin`.

[7] Sandro Fouché and Andrew H Mangle. Code hunt as platform for gamification of cybersecurity training. In *Proceedings of the 1st International Workshop on Code Hunt Workshop on Educational Software Engineering*, pages 9–11. ACM, 2015.

[8] Filippos Giannakas, Georgios Kambourakis, and Stefanos Gritzalis. Cyberaware: A mobile game-based app for cybersecurity education and awareness. In *2015 International Conference on Interactive Mobile Communication Technologies and Learning (IMCL)*, pages 54–58. IEEE, 2015.

[9] Hugo Gonzalez, Rafael Llamas, and Francisco Ordaz. Cybersecurity teaching through gamification: Aligning training resources to our syllabus. *Research in Computing Science*, 146:35–43, 2017.

[10] Ge Jin, Manghui Tu, Tae-Hoon Kim, Justin Heffron, and Jonathan White. Evaluation of game-based learning in cybersecurity education for high school students. *Journal of Education and Learning (EduLearn)*, 12(1):150–158, 2018.

[11] 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.

[12] NSA/NSF GenCyber Program. Inspiring the next generation of cyber stars. `https://www.gen-cyber.com`.

[13] Microsoft Research. Code hunt is a serious gaming platform for coding contests and practicing programming skills. `https://www.microsoft.com/en-us/research/project/code-hunt/`.

[14] Valdemar Švábenskỳ, Jan Vykopal, Milan Cermak, and Martin Laštovička. Enhancing cybersecurity skills by creating serious games. In *Proceedings of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education*, pages 194–199. ACM, 2018.

[15] Patrickson Weanquoi, Jaris Johnson, and Jinghua Zhang. Using a game to improve phishing awareness. *Journal of Cybersecurity Education, Research and Practice*, 2018(2):2, 2019.