SecurityEmpire: Development and Evaluation of a Digital Game to Promote Cybersecurity Education

Marc Olano Alan Sherman Linda Oliva Ryan Cox Deborah Firestone
Oliver Kubik Milind Patil John Seymour Isaac Sohn Donna Thomas

Cyber Defense Lab
University of Maryland, Baltimore County (UMBC)
Baltimore, Maryland 21250
{olano, sherman, oliva}@umbc.edu

ABSTRACT

SecurityEmpire is a new multiplayer computer game to teach cybersecurity concepts to high school students. We describe the design and implementation of SecurityEmpire, explain how it teaches security concepts, share preliminary evaluative data from students and teachers, and describe our experiences with developing, fielding, and evaluating this educational game. SecurityEmpire challenges each user to build a green energy company while engaging in sound information assurance practices and avoiding security missteps. Sound information assurance practices include: not clicking on unsafe links, encrypting auction bids, authenticating software downloads, performing integrity checks of system software, keeping antivirus protection up-to-date, and choosing strong passwords. In contrast with traditional teaching methods, educational games hold promise for greater student engagement and learning. We pilot tested an initial version of the game in computer science classes at partner high schools and in an undergraduate gaming class at our university. The preliminary data suggest that the game is engaging and increases awareness of cybersecurity practices.

1 INTRODUCTION

Safe cybersecurity practices are essential skills for all computer users. Two significant threats to cyber safety are: (1) Users act without thinking about the consequences of their actions, including ignoring warning messages, visiting unsafe websites, communicating with unauthenticated entities, and running untrustworthy software. (2) Users lack awareness of basic Information Assurance (IA) concepts, including confidentiality, authentication, integrity, and availability, leading to risky decisions. We address these threats by increasing awareness of safe cybersecurity practices through a fun and competitive game that can be replayed many times. Our work is based on evidence that students are more motivated and learn more efficiently when engaged in interactive hands-on experiences. Our thesis is that a multiplayer competitive computer game with a non-security goal where sound IA practices are important to achieve the goal provides a compelling environment for students to learn information security concepts.

We are designing and developing SecurityEmpire, a multiplayer computer game that teaches IA concepts to high school students, assuming no prior training in cybersecurity. Our multi-disciplinary team has expertise in IA, game development, graphic arts, and education. Taking inspiration from classic card and board games, we designed an interactive game that is playable and fun–each student grows a green energy company by collecting parts to build solar, geothermal, or wind-powered energy systems. Students learn fundamental concepts of IA in an authentic and well-motivated fashion. Players who use sound security practices gain an advantage in the game.

Unlike the single-player computer game CyberCIEGE [1], or the Elevation of Privilege card game [2], SecurityEmpire is a multi-player competitive game focusing on high-level user behaviors rather than on detailed technical knowledge of system software. The games Control-Alt-Hack [3,4] and [d0x3d!] [5] aim to reach more people by not requiring the player to have access to a computer and they use security vocabulary as backdrop for the game but do not explicitly teach IA concepts. In our setting, essentially all students have access to computers and they spend many more hours playing computer games than traditional board or card games. Computer games are easier to duplicate and disseminate than are other types of games, albeit harder to create.

Our contributions include: (1) A description of SecurityEmpire, our new multiplayer security education computer game. (2) An account of our experiences developing the game. (3) Preliminary reactions from students and teachers who have integrated this game in high school computer science classes.

2 PRIOR WORK ON EDUCATION IN GAMES

Game players spend hours developing and practicing skills that will improve their game performance. They

make this effort for the rewards of winning and because the game experience itself is entertaining and fun. Because games lead people to spend hours learning and honing their skills, it is natural to use them in education. Games for education, when successful, have the promise of increased engagement and improved learning [6,7,8]. Research has shown that "skill and drill," also known as "edutainment" is not as effective as engaging games with a narrative context [7]. Schmidtz *et al.*'s [9] IT-Café that teaches remedial computer skills is a compelling example of the skill and drill style of educational game, while Jianqiang *et al.*'s [10] Farmer's Tale that teaches volunteerism is an example of the later style.

Because developing a fun and engaging game is an iterative art requiring numerous rounds of play testing and refinement [11], many educational games are modifications of existing well-proven non-educational games. Farmer's Tale follows inspiration from Zynga's Farmville Facebook game [10]. <e-Adventure> takes inspiration from the Sims series of games [8]. This model has even been followed outside of computer games, where card and board games provide inspiration for physical games to help teach Data Structures and Algorithms [12].

A wide variety of games can be used for education purposes. High school students typically have a breadth of gaming experience. Cone *et al.* [13] found that those users who had significant game experience are much more likely to delve into the complexity of game structure. The current generation of high school and college students are "digital natives" and are very skilled at using a variety of computer technologies [14]. Thus, to engage our high school students, we should focus on computer games.

Many games for security education have focused on training for security professionals. Attack- and defense-based games for teaching IA concepts assume a level of understanding of computers and security that is beyond most computer users. This is also the case for cyber defense competitions and the CyberCIEGE [1,15,16] educational video game. While some security education games follow the skill and drill model [17], many researchers start from transaction diagrams commonly used in teaching [18,19]. These approaches lead to a direct simulation of the transactions cast into game form, as with the envelope and paper game by Hamey [20], or the attack/defense simulation game of Guimaraes *et al.* [21].

One of the most well known games to date for teaching security concepts is CyberCIEGE. This game is a resource-management simulation game similar to the Tycoon video games, which offer a sequence of campaigns defined in a flexible scenario description language. While this approach has been successful, all simulation-style games require a level of knowledge of the domain area by their users. Instead, we are following the model of games like Cash City [22], a Monopoly-like game where houses and risk squares are replaced by security scenarios, where the user must make choices that affect whether they gain or lose money in the game. By contrast, Elevation of Privilege [2] provides cards for various IA terms and concepts, but relies on players' existing knowledge of security to help experienced users explore weaknesses in their own systems.

At the other end of the spectrum, several less formal games use IA vocabulary, without necessarily addressing behavior at all. For example, Control-Alt-Hack [3,4] is a game with a security theme but does not directly teach security in a similar way SecurityEmpire has a green energy theme but does not try to teach about energy. Control-Alt-Hack could be modified to make IA more central to the game by allowing characters to enhance their capabilities by correctly answering security content questions. Peterson *et al.'s* [d0x3d!] network security board game aims to reach a diverse audience (including students), is limited to four players per game, and places those players in cooperative black-hat roles [5]. Unfortunately, the strategic elements of the game, while fun, do not directly demonstrate security risks that can occur during web-based activities nor do they demonstrate the need to perform safe security practices.

Our goal is to educate a less technically sophisticated student base to make them more conscious of IA in their day-to-day online behavior, rather than to teach specific technical or management skills. This goal is aligned with the Department of Defense and the National Initiative for Cybersecurity Education's goal of every household in the United States being aware and able to respond effectively to cybersecurity threats and exposures when using their computers.

3 SECURITYEMPIRE GAME DEVELOPMENT

The main objective of our project is to design and develop an IA educational game that encourages high school students to stop and think before executing computer commands and to develop awareness of selected fundamental concepts in IA. Additional project objectives include involving our university students in IA education research, strengthening collaboration between our university and our partnering high schools and increasing IA awareness of students at all of these schools.

The schools that we worked with already had a partnership with our Education Department and had an existing infrastructure to facilitate collaboration. One of the high schools had a focus on Homeland Security and the other high school focused on Information Technology, so there was a shared investment in project

activities. We worked with teachers, principals, and county-wide administrators to gain approval for the collaboration in developing and testing the game. School administrators expressed concern about developing and running a web-based game on the well-protected county server. There were a series of meetings to develop a plan to run the game at the schools in a way that was aligned with computer use policies of the schools. The evaluation protocol was approved by the university's Intuitional Review Board.

3.1 Game Concept

We selected a game narrative that could easily engage players in goal directed activities. Nagarajan *et al.* [23] state that a successful cybersecurity skills training program must meet two goals: 1. Get and sustain the users attention for a span of time; and 2. Communicate the training content to user in that span of time. SecurityEmpire accomplishes both of these goals. The task of the game is to build an empire by gathering components and constructing energy systems. Players interact with other players in a marketplace and auction to trade components. The game is fast-paced and multi-dimensional so that players' interest and focus are sustained.

In designing SecurityEmpire, we developed a strong core game narrative that could be easily adapted and extended to teach relevant IA concepts. We created a game that allows us flexibility to create teachable moments that maximize the educational impact. We separated the game theme from the security elements, allowing us to address issues of playability and teaching more independently, while giving us the freedom to expand the educational content of the game without changing the core elements of the game itself. This approach separates the "fun" of the game from the elements we want to teach, while ensuring that the educational elements remain central and that the students will learn them while playing the game.

Designing a brand-new game is difficult, as evidenced by the games created even by large professional developers that are not successful. We chose to base the core gameplay on firmly established existing games. The story of the game sets each player as the owner of a green technology energy company. The choice of green technology is not important to the educational goal, but allows us to set up the competitive nature of the game in a friendly way, and helps the players to learn that IA is important even when players are focused on other goals. *KAOS*, our artificial IA adversary, instigates simulated IA events in the context of authentic game events.

Players buy and sell materials to construct green technology systems and compete with other companies. Each player builds renewable energy systems (solar panels, wind turbines, or geothermal plants) to claim market share, with the ultimate goal of having the most successful company. Each alternative energy system is built from six components. Periodically, players receive new components, which they may trade, buy, or sell to collect the set they will need to make an end product. When a player has collected all of the needed parts for one of the systems, she can build that system and generate more energy to advance her empire.

Many IA elements occur as the players post and visit game websites to advance their business. All trading happens in a common marketplace including links to buy and sell items. Each player must manage her company's budget, including the costs of various types of security. Players with sound IA practices have the advantage; players who make security mistakes incur costs and disruptions to their business activities. In a classroom of 20 to 30 students, the trading game is very fast-paced, so a time penalty for poor IA practices is a major disadvantage. The players must be aware of the possibility of fraudulent offers introduced by KAOS, because following one of these will simulate an infection of their system and delay their progress in the game. They must also weigh the cost of antivirus protection over the penalty of KAOS-triggered virus infection. Players have the opportunity to acquire energy units at an auction and can choose to encrypt their bids to gain an advantage.

In the high school classroom, the teacher initiates a game session. During the game, the teacher has a summary page showing who has built renewable energy systems and who has suffered from security lapses. The teacher can pause the game at any time to discuss game events, can control the pace by distributing additional money or green energy items, and can control the onset of security events such as classroom-wide virus attacks. The system or teacher (not any player) triggers all simulated negative actions, attributed in the game to the KAOS adversary.

3.2 Summary of Security Concepts and How They are Integrated into Gameplay

Learning objectives of the game focus on the Department of Homeland Security's message, "Stop. Think. Connect." [DHS], with additional exposure to selected fundamental concepts from the Certified Information Systems Security Professional (CISSP) knowledge bank, including confidentiality, authentication, integrity, and availability.

SecurityEmpire does not artificially reward players who comply with instructions to perform security measures. Instead, the need for safe cybersecurty practices are demonstrated in an authentic manner; they

are presented as the players engage in goal directed activities. Players who use sound security practices gain an advantage over those who do not. For example, if a player fails to encrypt auction bids, a competitor might eavesdrop to win the bid at lower cost. If a player fails to authenticate a new version of her antivirus software, her computers might become infected with malware, costing time and money to repair the damage. In every simulated negative result, the player is informed of what she could have done to prevent it.

SecurityEmpire has a Security Center where players can learn about and buy security products. Players must decide how to invest their money in gadget parts and security products. The economic aspects of the game introduce an additional authentic dimension that mirrors the unsolved real-world challenge of how to assign meaningful costs to security choices.

3.3 Player Incentives and Rewards

We have created opportunities in the game to provide continuous feedback to players. Existing literature on game design [24, 25,26] emphasizes the need for short-term, medium-term, and long-term goals. These goals should match with the rhythm of play, with multiple short-term goals accomplished in one session, medium term goals in a day or two over several sessions, and long-term goals over weeks or longer.

Our reward schedule is adapted to the single class-period game length, but includes all three types of goals and rewards. In SecurityEmpire, an individual sale, trade, or purchase is a short-term goal. Succeeding in a purchase to get closer to building one of the energy systems is its own reward and we observe students celebrating verbally when they win a bid for that final piece. Constructing a renewable energy product will take a few trades and constitute a medium-term goal. For each renewable energy product built, the player sees a brief animation of the product being built and producing energy (Fig. 1).

Achieving this animation is the secondary reward. Multiple completed renewable energy products will be needed to achieve the long-term goal of securing a high rank on the leader board or winning the game. For example, when the player builds a photovoltaic system, each piece of the system first drops into place on the screen (solar panels, inverter, and battery). Wires then appear, connecting each part. An image of the sun appears, causing the solar panels to glow and the battery to emit sparks, signifying that the machine is running and producing power. The animation runs in a continuous loop until the player closes the pop-up window. The continuous animations add a fun dynamic to the game, informing the player that he has a recently completed an energy system. We added another subtle educational element by giving the player a basic idea of how machines produce clean energy.

4 How Players Learn Security Concepts

Students learn IA concepts in SecurityEmpire through our principles for integrating security concepts, leveraging learning moments, teacher monitoring, the Security Center, and how we integrate specific IA concepts. Players learn security concepts through gameplay in an authentic and motivating fashion: players

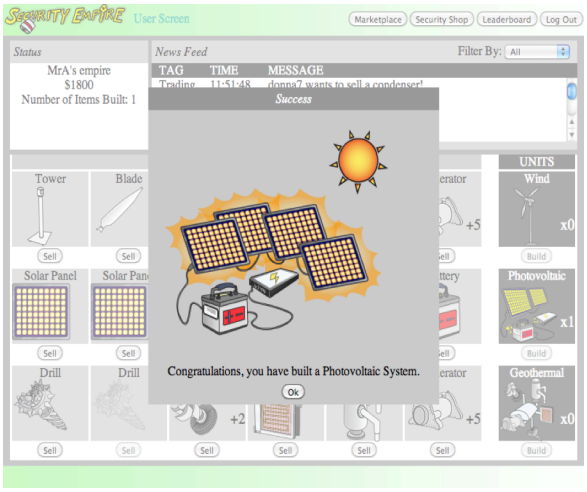


Figure 1. Animation pop-up for complete energy unit

with good security practices are at an advantage and players must always consider the costs of security (or lack thereof) in terms of money and time.

We have aligned learning outcomes of the game with national and state standards, including the Maryland Technology Literacy Standards for Students, Digital Citizenship Howard County, Maryland, the Association for Computing Machinery, Computer Science Teacher Association's K-12 Computer Science Standards, and the International Society for Technology in Education.

At the Security Center, players may purchase a variety of security solutions, including software packages that enable encryption, digital signatures, virus protection, integrity protection of system software, and data backup. For each product type, there are typically three different solution choices with different price-performance characteristics. For example, the player must be a wise consumer to decide what product makes the most sense for his or her budget and application. The Security Center's product information offers useful explanations about security threats, available solutions, product characteristics, and sound practices.

During gameplay, security incidents create powerful learning opportunities. For example, a player receives a pop-up notification that she has won a free component of

an energy system. If the player clicks on the scam and if her antivirus software is not adequate or up-to-date, then a message appears explaining that her computer has been infected with malware, which will cost $200 to repair and will result in downtime during which she will be unable to conduct business transactions. The message will also direct the player to an appropriate section of the Security Center for more information and security solutions. If the player declines to click on the scam, then a positive-reinforcement message appears informing the player that she has successfully avoided a dangerous scam by not clicking on the suspicious link.

The system logs all activity and provides appropriate summaries to individuals, the group, and the teacher. These summaries inform the teacher and players about their security behaviors. For example, the summary includes the number of times a player avoided or fell victim to a pop-up scam. News feeds broadcast incident reports of security events during gameplay.

In addition to pop-up scams, we have included other security learning activities. When updating security software (e.g., antivirus software), if a player does not check the authenticity of the software (using digital signature verification), she is at risk for attack by malware embedded in the update. Periodically, auctions take place where a complete system is sold to the highest bidder. All bids are posted on a public auction site. If a player does not encrypt her bid, other players can read her bid and take advantage of that information.

KAOS periodically launches simulated attacks that subvert system software by modifying the operating system. If a player does not invest in security software to monitor the integrity of her system software, she may lose time and money recovering from such an attack. Players who do not invest in suitable backup and recovery software are at risk for losing time and money when their systems are devastated by fire, earthquakes, flood, or theft.

During a one-time initial registration process before playing, each player creates a username and password. This password is also used within gameplay, for example, to sign into the player's account at the Security Center. KAOS sometimes tries to guess these passwords using standard password cracking tools, such as John the Ripper or RainbowCrack. When KAOS guesses a player's password correctly, the player is at risk to lose time and money to recover from an intrusion, and the player is encouraged to reset her password, guided in part by a password policy and strength monitor. The system also provides positive reinforcement to players who chose passwords that KAOS was unable to crack.

Sometimes, KAOS attacks a player with targeted spearfishing messages based on the player's activities. For example, if KAOS notices that a player is interested in buying a particular part, KAOS might offer to sell such a part at a discounted price. As with pop-ups, players must avoid clicking on such scams and losing time and money.

The security events that occur throughout the game provide timely opportunities to explain consequences and deliver information to the players. This ability to provide players immediate and specific feedback based on their decisions optimizes learning by explaining how their errors occurred and how their expectations failed [27]. Players also receive positive feedback when they make sound cybersecurity choices.

5 Implementation and Development Cycles

We implemented SecurityEmpire with server software running the game and a client running on the students' web browsers.

5.1 Server

SecurityEmpire is hosted on a dedicated server. The server is running a LAMP stack (Linux, Apache, MySQL and PHP). Since the server for a security-focused game is an attractive target for hacking, we take standard precautions for server security: remotely backed-up logs, salted hashes for all game passwords, and database configuration in non-web-accessible locations. In addition, no persistent data are on the server, so at any time we can easily wipe the server and re-install the LAMP stack and game code.

5.2 Client

When the player runs SecurityEmpire, she sees a web client, built as an AJAX application. The high school computers already have a web browser, so with a web-based client, no new software packages need to be installed. In addition, a web client allows us to add, change, and implement features to the game quickly. The client only shows a view of the game state. All game logic resides on the server.

5.3 Development Cycles

We have been designing SecurityEmpire iteratively, alternating focus on appearance and interface with new game features. For example, the first version of SecurityEmpire play tested at the partner high school had a pure-text web interface. Student feedback included requests for a greater variety of security features, increased speed, and better graphics.

The second development cycle focused on the visual appearance of the game, including images for all of the parts and green energy units. We adjusted many smaller elements of the game from the news feed, to the organization of market place, and accelerated gameplay. We also added short animations to mark significant events in the game.

Third, we created visual representations of products in the marketplace, pop up virus attacks, and the log-in

screen. These illustrations and animations focus the players' attention and make the SecurityEmpire experience more enjoyable. We gave the Agent of KAOS a visual representation to signal a security breach.

Throughout the development process, we are working closely with high school partners, including students, computer science teachers, and school and county administrators. Access to the game at the high school is controlled. Students do not have general access to the Internet, are not exposed to dangerous software, are unable to send inappropriate messages to other students, and are unable to perform malicious activity against other students during gameplay. The teacher can monitor the game and the game does not impose undue loads on the school's network.

In the next cycle, we will implement a new graphical user interface, with more indications of the player's progress, such as an energy icon that will "grow" as the player builds more machines, and a progression of lock/safe/fortress representing their security success, based on the number of security lapses and IA incidents avoided. We would also like to incorporate additional security concepts, including physical security and the "insider" threat. As the narrative of the game develops, the complexity and scope of the security issues it can encompass will expand.

6 Evaluation

We placed significant attention on evaluation throughout the creation and development of SecurityEmpire. Each step of the game development cycle was iterative. We field-tested the game several times early in its development at a high school computer science class. As the game developed to a stable version, we tested it more formally. The evaluation methodologies include a review of gameplay metrics, player surveys about their experiences playing the game, observations of research team during game play sessions, open ended questionnaires, and semi-structured group interviews.

Our subjects were high school students at two local high schools. We also tested the game with undergraduate students in a gaming class at UMBC. We introduced the game to students with minimal instructions. We wanted to ensure that students could easily engage in SecurityEmpire as soon as the teacher releases the game. There was no hesitation or delay as the students initiated play and most of them succeeded in building energy systems.

The evaluation sessions consisted of an introduction to the game and then two game play periods of approximately fifteen minutes each. Then players were asked to complete a short survey about their gameplay experience. Students were asked to rate their level of agreement to the evaluative statements on a scale of 1 (strongly disagree) to 5 (strongly agree).

We also collected a variety of gameplay metrics including ones dealing with security concepts as well as standard quantitative metrics typically collected by game designers. We looked for patterns of gameplay events typical of the leaders and poor performers to evaluate their strategies. For example, we measured statistics about which security errors players make, which errors players repeat, how their errors change over time within a game and over multiple games, and how these errors relate to their prior knowledge.

During the gameplay sessions, the development team and our collaborating teachers carefully watched the students play the game. All students were engaged in the game and there was a lot of communication between players as they developed their strategies to acquire the parts they needed. Researchers then conducted semi-structured group interviews to elicit more specific and in-depth perspectives on the game.

Survey responses reflected favorable ratings of many aspects of the game, particularly the level of engagement/focus they felt during the game. (Appendix A reports the preliminary data). The fast-paced and engaging nature of the game was also verified by responses to open-ended questions and semi-structured interviews. The game metrics confirmed that the leaders in the game had more proactive security choices and fewer security breaches than the other players.

7 Future Work

The scope and depth of the evaluation will be enhanced as the game develops. Continued evaluation will use before- and after-testing and in-game feedback through pop-up questions.

During gameplay, brief multiple-choice pop-up questions will periodically appear at critical events. In addition, we will record and analyze in-game metrics to see how the use of IA concepts evolves with gameplay. Both in-game questions and metrics have been successfully used in evaluating previous games and simulations [28,29]. Because this project involves collaboration with both K-12 teachers and faculty from our university's education department, there is a wealth of pedagogical and methodological expertise to generate valuable data and to use that data for continual improvement of the game design, usability, and value. We will require iteration and refinement to ensure the game is balanced and playable by both novice and skilled players.

Leveraging the power and popularity of social media, we are creating another version of the game as an application for the general population. Whereas the

original SecurityEmpire game is for classroom use without using social media, a multiplatform version of the game would have the potential to reach a broader scope of players. The game will require changes to support non-simultaneous play by a potentially far larger player pool. By accommodating users with limited knowledge of computers and computer security, SecurityEmpire will reach more people than other games that require computer expertise.

As we develop this version of the game for use outside the classroom, this project will be in a unique position to make direct comparisons between in-classroom guided use of a game and open free play of an educational game. Because the game will be systematically evaluated in the classroom version and in the online version, we will compare both versions of the game by analyzing the evaluation data, game metrics, and qualitative user reactions.

We also plan to create a collection of teacher materials including teacher notes, background reading for teachers and students, and guidance for using the game inside or outside the classroom. Materials will include information on DHS's "Stop. Think. Connect." and on the concepts of confidentiality, authentication, integrity, and availability [30]. This information will allow even teachers who are not strong on the security concepts to offer lessons using the game. Schools will be able to use the game from our server. We will also provide the game for download, along with server specifications and directions for system administrators, to schools that want to serve the game entirely within their own closed Internet environment.

8 Conclusions

We have developed a new multiplayer interactive computer game and deployed it in high school computer science classes. Preliminary survey data demonstrate that players found SecurityEmpire to be an immersing and enjoyable game. Although the potential of SecurityEmpire to improve actual cybersecurity practices is yet unproven, the engaging nature of the games makes it a very promising curriculum resource.

Partnering with high schools to create and evaluate the educational game provided us with a productive development environment and enhanced relationships between our university and the schools. The collaborative development gave us the opportunity to change elements of the game based on high school student feedback and observations of their play. High school students and teachers learned more about our university, interacted with some of its faculty, and witnessed the creation and development of an interactive computer based game.

SecurityEmpire demonstrates that students with no prior experience in computer security can learn about cybersecurity through a competitive challenge in which making wise security choices in authentic settings gives them an advantage in the game. We will continue to develop the game and to evaluate its effectiveness at improving the security awareness, understanding, and behaviors of students who play it.

9 Acknowledgments

We thank Anne Arundel County Public Schools and, in particular, Pam O'Meara and James Hopper of Meade Senior High School and Lisa Shifflet at Chesapeake High School. We also thank William Byrd and Russ Fink for helpful comments on earlier drafts. Sherman, Olano, Oliva, Patil, Seymour, Sohn, and Firestone were supported in part by the Department of Defense under IASP Grants H98230-11-1-0473 and H98230-12-1-0454; Sherman and Kubik were supported in part by the National Science Foundation under SFS grant 1241576 and supplement.

References

[1] Cynthia E. Irvine, Michael F. Thompson, and Ken Allen, 2005. CyberCIEGE: Gaming for information assurance. IEEE Security & Privacy, 61-64. http://calhoun.nps.edu/public/bitstream/handle/10945/7126/05paper_cciege.pdf?sequence=1

[2] Microsoft, 2013. The Elevation of Privilege (EoP) Card Game. http://www.microsoft.com/security/sdl/adopt/eop.aspx

[3] Tamara Denning, Tadayoshi Kohno, and Adam Shostack, 2012. Control-Alt-Hack™: A card game for computer security outreach, education, and fun. Dept. of Computer Science and Engineering, Univ. of Washington, Technical Report UW-12-07-01.

[4] Tamara Denning, Adam Lerner, Adam Shostack, 2013. Control-Alt-Hack: The Design and Evaluation of a Card Game for Computer Security Awareness and Education. Proceedings of the 2013 ACM SIGSAG, 915-928. *https://homes.cs.washington.edu/~tdenning/files/papers/ccs479-denning.pdf*

[5] Zachary Peterson, Mark Gondree, and Ann Gallenson, 2012. [d0x3d!] A network security game. https://github.com/TableTopSecurity/d0x3d-

the-game/blob/master/instructions/d0x3d-rules.pdf?raw=true

[6] DENIS GUILLAUME AND PIERRE JOUVELOT, 2005. Motivation-driven educational game design: Applying best practices to music education. In: Proc. 2005 ACM SIGCHI Int'l Conf. Advances in Computer Entertainment Technology, ACE '05, New York, NY, 462–465. http://doi.acm.org/10.1145/1178477.1178581.

[7] MARY JO DONDLINGER, 2007. Educational video game design: A review of the literature. Journal of Applied Educational Technology, vol. 4, no. 1.

[8] PABLO MORENO-GER, DANIEL BURGOS, IVAN MARTINEZ-ORTIZ, JOSE LUIS SIERRA, AND BALTASAR FERNANDEZ-MANJON, 2008. Educational game design for online education. Computers in Human Behavior, vol. 24 (September 2008), 2530–2540. doi:10.1016/j.chb.2008.03.012.

[9] BIRGIT SCHMITZ, ANDRÉ CZAUDERNA, ROLAND KLEMKE, AND MARCUS SPECHT, 2011. Game based learning for computer science education. In: Computer Science Education Research Conference (CSERC '11), Gerrit van der Veer, Peter Sloep, and Marko van Eekelen (Eds.). Open Universiteit, Heerlen, Open Univ., Heerlen, The Netherlands, 81-86.

[10] DON SIM JIANQIANG, XIAOJUAN MA, SHENGDONG ZHAO, JING TING KHOO, SWEE LING BAY, AND ZHENHUI JIANG, 2011. Farmer's tale: A Facebook game to promote volunteerism. In: Proc. 2011 Annual Conf. on Human Factors in Computing Systems (CHI '11). ACM, New York, NY, 581-584.

[11] BRIAN WINN AND CARRIE Heeter, 2007. Resolving conflicts in educational game design through playtesting. Innovate: Journal of Online Education. 3(2), (January 2007), 6 pp.

[12] LASSE HAKULINEN, 2011. Using serious games in computer science education. In: Proc. 11th Koli Calling Int'l Conference Conf. on Computing Education Research (Koli Calling '11). ACM, New York, NY, 83-88.

[13] BENJAMIN D. CONE, CYNTHIA C. IRVINE, MICHAEL F. THOMPSON, AND THUY D. NGUYEN, 2007. A video game for cyber security training and awareness. Computers & Security. 26(1), 63-72.

[14] PRENSKY, M. (2003) Digital game-based learning. Comput. Entertain., 1 (1), p.21–21. Entertain., 1 (1), pp.21–21

[15] CYNTHIA IRVINE AND MICHAEL THOMPSON, 2003. Teaching objectives of a simulation game for computer security. In: Proc. Informing Science and Information Technology Joint Conf., Pori, Finland (June 2003), 779-791. http://cisr.nps.edu/downloads/03paper_cciege.pdf

[16] CYNTHIA IRVINE AND MICHAEL THOMPSON, 2007, CyberCIEGE: The information assurance training and awareness video game. IA Newsletter: The Newsletter for Information Assurance Technology Professionals, 10(2) (Summer 2007), 22-26. http://iac.dtic.mil/iatac/download/Vol10_No 2.pdf

[17] W.A. LABUSCHAGNE, N. VEERASAMY, I. BURKE, AND M.M. ELOFF, 2011. Design of cyber security awareness game utilizing a social media framework, Information Security South Africa (ISSA), 1-9, 15-17 http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6027538&isnumber=60275 04, doi:10.1109/ISSA.2011.6027538

[18] XIAOHONG YUAN, PERCY VEGA, YASEEN QADAH, RICKY ARCHER, HUIMING YU, AND JINSHENG XU, 2010. Visualization tools for teaching computer security. Trans. Comput. Educ. 9(4), Article 20 (January 2010), 28 pp.

[19] Y. AL-BASTAKI, A. HERATH, K. AL-MUTAWAH, M. BAQER, S. HERATH, AND R. GOONATILAKE, 2012. e-learning of security and information assurance with sequence diagrams. In: Proc. 2012 Joint International Conference on Human-Centered Computer Environments (HCCE '12). ACM, New York, NY, USA, 19-22.

[20] L.G.C. HAMEY, 2003. Teaching secure data communications Using a game representation. In: Proc. Fifth Australasian Computing Education Conf. (ACE2003), Adelaide, Australia. CRPIT, 20. T. Greening, and R. Lister, Eds. ACS. 187-196.

[21] MARIO GUIMARAES, HUWIDA SAID, AND RICHARD AUSTIN, 2011. Using video games to teach security. In: Proc. 16th Annual Joint Conf. on Innovation and Technology in Computer Science Education (ITiCSE '11). ACM, New York, NY, 346-346. doi:10.1145/1999747.1999860 http://doi.acm.org/10.1145/1999747.1999860

[22] THOMAS MONK, JOHAN VAN NIEKERK, AND ROSSOUW VON SOLMS, 2010. Sweetening the medicine: Educating users about information security by means of game play. In: Proc. 2010 Annual Research Conf. of the South African Institute of Computer Scientists and Information Technologists (SAICSIT '10). ACM, New York, NY, 193-200

[23] AJAY NAGARAJAN, JAN M. ALLBECK, AND ARUN SOOD, 2012. Exploring game design for cybersecurity training. Cyber Technology in Automation, Control and Intelligent Systems. May 27-31, 2012. Bangkok, Thailand.

[24] ELIZABETH LOSH, 2008. In polite company: Rules of play in five Facebook games. In: Proc. 2008 Int'l. Conf. on Advances in Computer Entertainment

Technology (ACE '08). ACM, New York, NY, 345-351.

[25] AKI JÄRVINEN, 2009. Game design for social networks: Interaction design for playful dispositions. In: Proc. 2009 ACM SIGGRAPH Symp. on Video Games (Sandbox '09), Stephen N. Spencer (Ed.). ACM, New York, NY, 95-102.

[26] HEIKKI TYNI, OLLI SOTAMAA, AND SAARA TOIVONEN, 2011. Howdy pardner!: On free-to-play, sociability and rhythm design in FrontierVille. In: Proc. 15th International Academic MindTrek Conference: Envisioning Future Media Environments (MindTrek '11). ACM, New York, NY, 22-29.

[27] JAMES GEE, 2009. Deep learning properties of good digital games: How far can they go? In U. Ritterfield, M. Cody, P. Vorderer (Eds.), Serious Games: Mechanisms and Effects. Routledge/LEA Press, 65-80.

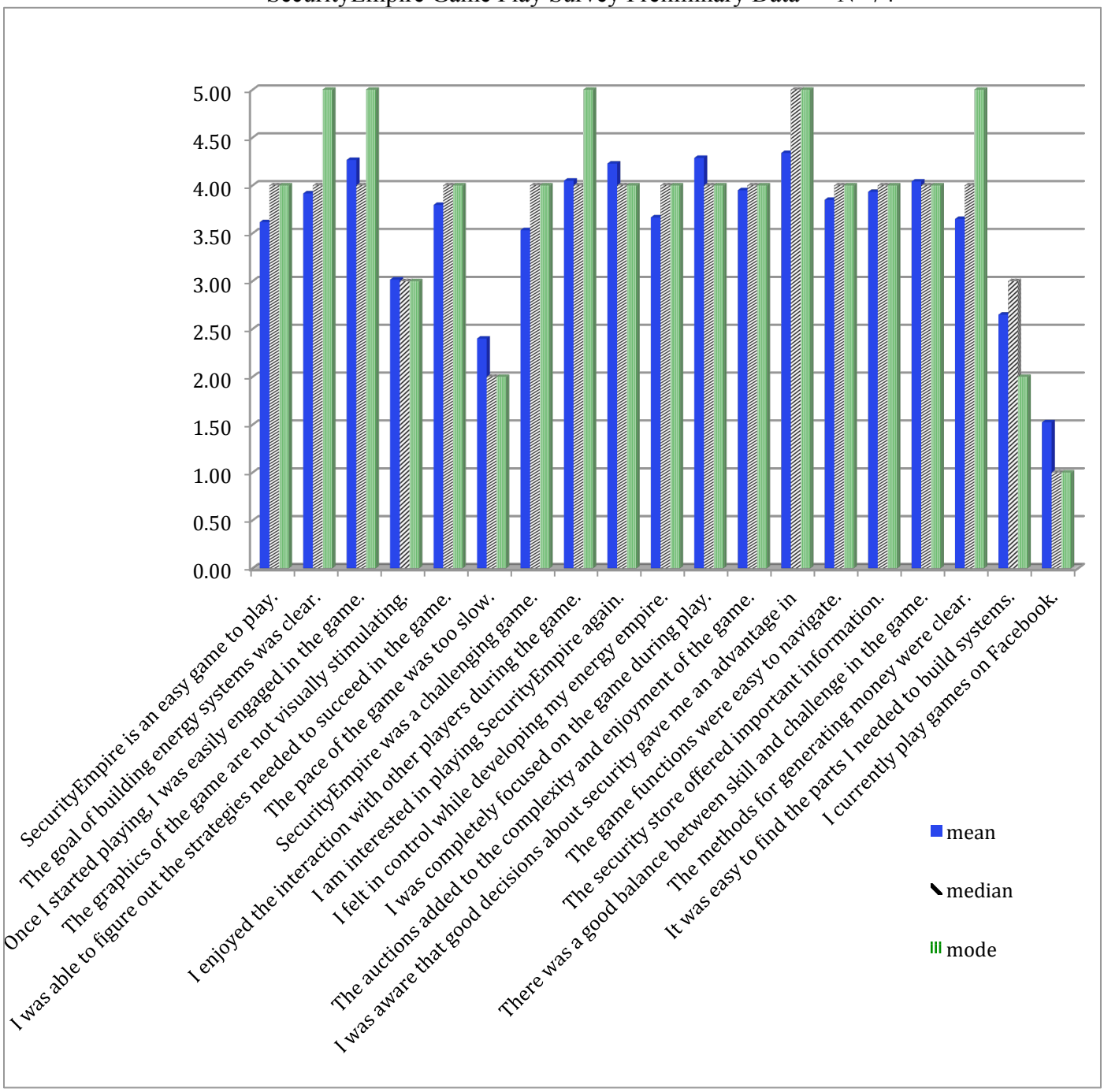
[28] DAVID KAUFMAN, LOUISE SAUVÉ, AND ALICE IRELAND, 2007. New tools, new tricks? Evaluating games and simulations from multiple perspectives. In Organizing and Learning Through Gaming and Simulation: Proceedings of Isaga, 167–174.

[29] ANDERS DRACHEN AND ALESSANDRO CANOSSA, 2009. Towards gameplay analysis via gameplay metrics. In: Proc. 13th Int'l MindTrek Conf.: Everyday Life in the Ubiquitous Era (MindTrek '09). ACM, New York, NY, 202-209.

[30] . http://www.stopthinkconnect.org/2

Appendix A

SecurityEmpire Game Play Survey Preliminary Data N=74



Scale:

1 - Strongly Disagree	2 - Disagree	3 - Neutral	4 - Agree	5 - Strongly Agree