Hacking as a Game

Dr. Terry Letsche
Department of Mathematics, Computer Science and Physics
Wartburg College
Waverly, Iowa 50677
terry.letsche@wartburg.edu

Abstract

The need for qualified computer and network security personnel continues to expand as the interconnectedness of computing devices grows. This paper presents a case study of a first-time computer security course offering that includes not only lecture and the typical computer lab exercises, but uses card-based tabletop games to motivate topics, foster cooperation, create an atmosphere of active learning, and engage students. These games, student feedback and student learning are discussed.

1 Introduction

Computer security has become a vital curricular topic because of the proliferation of computing devices and their interconnectedness. The Computer Science Curricula 2013 [1] has recognized and responded to these threats by adding a knowledge area in Information Assurance and Security. The shortage of 10,000 – 30,000 computer science professionals with experience in computer and network security [2, 3] has become a government priority. [4] The teaching of security topics is complicated by it being both highly technical, drawing on computer architecture, operating systems, networking, and other advanced topics, and also highly policy driven, e.g. the need for employee training to avoid social engineering attacks, minimum password strengths, etc. Traditional security courses use lecture and some sort of lab activities, whether focused on specific topics or a “Capture the Flag” type of activity. These activities prove valuable because they contribute to learning by motivating topics, reinforcing content and maintaining student engagement.

This paper is a case study of a first offering of a computer security special topics class at a small, four year liberal arts college. Distinguishing this approach is the use of tabletop card-based computer security-related games in addition to a lab component. This paper begins with a brief survey of related gamification work in computer security courses, followed by a discussion of the particular games used in this case study. Following a discussion of student feedback, further work and conclusions are presented.

2 Related Work

The use of games as a pedagogical tool has a rich history. Games can be used to motivate topics in class, as a training tool, as a vehicle for active learning, to engage students in the complexities of computer and network systems, and as a way to promote collaborative learning. [5, 6] Gaming is ideally suited for the area of computer and network security because of the dynamics of the relationships between attackers and defenders. Most classroom approaches to teaching security do not incorporate hands-on real-time recognition and response to threats.

Perhaps the most widely known gaming approach for computer security is the “Capture the Flag” (CtF) scenario. In CtF tournaments, a flag is represented as a data file on a team’s server, which the team defends while others attack. The goal typically is to either corrupt the flag or to replace it entirely with the flag of another team. These sorts of games can be either symmetric, where each side both defends their server while attacking others, or asymmetric, where teams are limited to either offensive or defensive action. [7] Scoring typically occurs either automatically or by the intervention of judges, who periodically poll servers to determine the identity of the flag and update scores appropriately. Additional details on setting up a network for a CtF tournament can be found in [8].

In some forms of CtF, teams are given identically configured server images to secure and defend. These server images are prepared with purposeful security weaknesses to better demonstrate real-world situations. MIT’s Lincoln Laboratory, for example, focuses their CtF exercise on defending and securing WordPress plugins on a LAMP (Linux/Apache/MySQL/PHP) architecture. [6] Here, WordPress is selected as a focus because of its rich API and extensive set of available plugins.

A variant on CtF is called “disturbed playing”, where players are under attack not from other teams, but from trainers attacking under a known threat model. While many of the advantages of CtF are still possible, e.g. practical security experience and teamwork, the ultimate goal is to develop a secure, workable security policy. [9] This disruption of normal play is purportedly closer to the everyday life of IT security experts, where maintaining security is one facet of the job, and developing security policies to maintain security is another.

However, CtF suffers from a number of pedagogical problems – namely, there is a high entry barrier to security proficiency due to the large skill set and background needed across many areas of computer science, i.e. operating systems, database, system administration, networking, etc. [6] One way to obviate this problem is to provide training before the event that relates to the specific skills and environment that will be used. Other, often overlooked, problems are the lack of time to prepare for and conduct the tournament, as well as the cost of networking equipment. While the immersive quality of events with equipment like this may be superior, it does come at a cost. [10]

Catuogno and De Santis [11] make the point that some gaming approaches require too many specific skills (specific, low-level knowledge) than higher and wider levels of knowledge. They propose viewing the game as a cooperative role-play, rather than adversarial effort, in order to accomplish tasks safely and securely over a simulated Internet that was itself neither secure nor reliable. Students learned about real-world security practices and experience managing real, usable services on the “internet,” which is something that CtF typically doesn’t do.

A different approach can be used that employs multiple phases of gaming. In NetS-X [10] and CyberCIEGE [12], players operate avatars in virtual environments, such as an office setting. Players initially learn about their environment and security policy through a scripted series of events, while gaining experience. As their experience grows, increasingly complex tasks are given to them. Assessment of student learning can occur during these games through the inclusion of breaks in the gaming activity where multiple choice questions can be asked. Another single-player security game called CounterMeasures [3] assumes no previous security knowledge and was tested with two hypotheses: training in a more realistic setting is a better learning environment than reading about computer security, and practical knowledge from games is more engaging and less time consuming to master. The creators of CounterMeasures discovered that students using the game learned the same material in half as much time as students using a text and reported higher levels of engagement. Jordan, et al. also report on a wide variety of computer and web-based security games. [3] Both NetS-X and CyberCIEGE allow for the creation or modification of scenarios.

While some sort of lab-based, experiential activities are common in computer security curricula, there is much less work done on table-top card-based games.

3 Case Study

Wartburg College is a selective four-year liberal arts college located in northeast Iowa. The Computer Science and Computer Information Systems majors have approximately fifty students and three full-time faculty. Recognizing the need to discuss security topics in more detail than can be allowed as parts of other classes, the department offered a seminar specifically in computer and network security in the winter semester of 2013. Since a particular seminar course is offered roughly every two or three years, depending on demand, the prerequisites were kept very elementary to maximize enrollment. Since Wartburg’s CS1 class is required for several other majors on campus and also satisfies the general education mathematics requirement, this course had to be geared for students at a variety of levels, from CS 1 to senior computer science majors. As an initial course offering and because of the enrollment (eight students), these results could best be characterized as a case study.

Because of the wide differences between backgrounds, “team” captains were assigned to groups to act as mentors. A computer lab was set up as a sandbox for lab activities. Discarded machines from Information Technology Services were configured with a variety of operating systems, including Windows 98 SE, Windows ME, Windows NT 4, Linux, and a relatively old version of Mac OS. All machines were networked to a hub that the students could connect to with their laptops. Wired network connections outside the lab were forbidden, and students signed an ethics pledge that they would not use the information they learned in the class and its labs in an illegal fashion. Labs were based on a SIGCSE 2013 class [13] in a sandboxed environment with the BackTrack Linux distribution.

In addition to the “typical” lab activities for a security class, card-based table-top games were used to motivate topics and introduce terminology. It was hoped that these games would help bridge the gap between skill levels of the students and enhance the cooperative atmosphere of the class. These card-based games were introduced at different times during the class.

3.1 Hackers and Agents

Hackers and Agents bills itself as a security game where, “The world has been infiltrated with hackers who are out to steal your personal data if they can get their hands on it. The agents are well armed with forensic techniques and sworn to catch these cyberpunks.” [14] The objective of the game is to discard all cards during game play. Remaining cards at the conclusion of the game incur penalty points. Once a player reaches 300 points, the game is over and the player with the lowest penalty score wins.

Players are dealt eight cards from a deck of 108 cards. The deck includes Data Cards in four colors with a rank of zero to eight and Action Cards. Cards must be played by color, action, or rank. Action Cards require a particular action be taken when played. Actions include losing a turn because the hacker has left an encrypted file on the system, and losing a turn and drawing a card because the agent found evidence of an attack in a system log. Lead cards indicate the agent has a lead on the hack and allows the player to play an additional card or change the direction of game play. An SQL Injection action causes a change of color in the game play. A Rootkit action indicates the current player, as a hacker, has pawned the next player’s hand, causing the next player to need to pick up an additional five cards and forfeit a turn. The Hacker card allows the player to swap hands with any other player, while an Agent card allows the current player to request a Lead, Rootkit or SQL Injection card from any other player.

The game website indicates that the core game can be extended by any number of Booster Packs, which include additional cards that change gameplay. One type of card is the Learn card, which represents a ticket to attend a conference called DeckCon. When this card is played, DeckCon cards can be picked up and used to not only increase the player's knowledge about computer security, but it also modify subsequent game play. These cards include a brief lesson (the need for encrypted Wi-Fi connections), an action (an attacker sniffed an e-mail login id and password) and a penalty (as a penalty the player must draw additional cards). These cards can also impact point calculation at the end of the game. [15]

3.2 d0x3d!

d0x3d! means to have one's private data posted publicly online. In this game, someone has stolen your digital assets (authentication credentials, financial data, intellectual property and personally identifiable information) and scattered them across a network of machines and equipment. The players work collaboratively to infiltrate the network, search for the digital assets, and escape undetected. However, admins are watching the network and will patch or even decommission nodes on the network that may have been compromised. Its goal is to create a context for thinking about and discussing issues in network security, geared for informal learning. This game is notable in that it is an open source game, with all game materials available under a Creative Commons License. [16]

The game consists of twenty-four game tiles which depict servers and network equipment that can be either uncompromised or compromised. Game play is between adjacently positioned tiles, so various network topologies can be implemented through the arrangement of network tiles. Players can assume one of six roles, each with unique gameplay properties, including a social engineer, war driver, insider, botmaster, cryptanalyst and malware writer. Players enter the game on predetermined pieces of network equipment, and move through the network based on their role properties. In each turn, players may compromise the network node they're on, drop or pickup lo0t! cards (a way to exchange information or temporarily store tokens), or exchange/give a lo0t card with any player on the same network tile. In the second phase of the turn, a player draws two lo0t! cards. As game-play progresses, network security audits occur randomly by card play. Successive audits raise the infocon level, making it more likely that compromised machines will be patched or decommissioned. Patches to "fix" network nodes can be reversed by players in the third phase of a turn; however, once a node is decommissioned by the network "admins", it remains out of play. Lastly, there is a limit to the number of cards that can be held by each player, so the last phase of a player's turn requires discarding enough cards to remain within the limit. Players move through the network, cooperating to recover the digital assets, without getting "caught" by the network admins. To win, all four digital assets must be recovered, and all players must move through the network to the Internet Gateway node and one player then executes a zero-day exploit. An unsuccessful network attack occurs when the either the infocon level reaches its maximum, or it becomes impossible for players to win because either the Internet Gateway is decommissioned, a hacker is ejected from the network for any reason, or a network node with a digital asset is decommissioned, making it impossible to recover that digital asset.

3.3 Control-Alt-Hack

Control-Alt-Hack bills itself as a card game for computer security outreach, education and fun. [17] Here, three to six players act as white hat hackers in the employ of a security consulting firm. The game's primary goal is to increase computer security awareness to that the players can be better informed consumers. Within this primary goal are four awareness-based subgoals: 1) to help users better understand the importance of computer security and the risks of poor security, 2) to examine the numerous technologies that require computer security, 3) to demonstrate the diversity of threats, and 4) the more general goal that technology brings both benefit and risks. There are also secondary perception and exposure goals: 1) to work against negative stereotypes of people in these fields so that students could vision themselves pursuing a career in security, 2) to highlight the numerous opportunities available to practitioners of these security skills, 3) to help reclaim the word "hack" as a creative and exploratory term, rather than destructive, and 4) the more people that play the game, the greater the chance to increase awareness and/or change perceptions. This game is unique in this case study in that its authors have tied these goals and game play to specific curricular outcomes. [18]

The scenario in Control-Alt-Hack is that the players work for Hackers, Inc., a computer security company that performs security audits and provides consultation services. Game play occurs in rounds where players attempt to complete their assigned missions. Success will gain the player cred points – enough cred points and the player wins the game and becomes CEO of their own consulting company. There are four types of cards that are used. Hacker cards describe the abilities of the characters, mission cards contain tasks to be accomplished, entropy cards alter play by introducing advantages to players or making gameplay more difficult, and attendance cards which indicate whether a player is participating in the regular staff videoconference.

Players are initially dealt three hacker cards, three entropy cards, six hacker cred cards and one each of the attending/not attending cards. Each round has seven phases. Players first get their discretionary budget of $2,000 and draw one entropy card. In the second phase, each player draws a mission card, which is effectively a project assigned by the Hackers, Inc. CEO or an outside customer. Players decide whether to participate in the regular staff video conference. Those in attendance have the opportunity to exchange missions and pick up one more entropy card. Some missions are less desirable and are classified as "newb jobs." Players who skip the meeting get a free re-roll on any one failed roll during their mission. In phase four, players attempt to accomplish their missions by rolling dice and getting a score lower than that stated on a particular mission card. Success may increase hacker cred and failure may decrease hacker cred. Many missions also include gameplay altering conditions for later rounds (e.g. -2 on all rolls next round). After all employees have attempted their missions, a hacker cred bonus/penalty round occurs based on the collective outcome of the missions. Players then discard until they have five cards in their hands, and the round ends with a check to see if the player with the highest hacker cred has at least give more cred points than the next player. If so, that player wins, otherwise check to see if the collective hacker cred of all employees is high enough or low enough for the CEO position to become open. If a player's hacker cred is zero at the end of a round, that employee is "terminated" and the player assumes a new employee identity.

The game discusses how hackers need proficiency in hardware hacking, software wizardry, networking, social engineering, and cryptanalysis. There are additional skills where the employees will have varying levels of ability: barista, connections, web procurement, forensics, lockpicking, search fu, and kitchen sink. Missions consist of one or more activities that must be completed in order, and successful missions require dice roll-based proficiency scores.

4 Analysis and Experiences

Student experiences were collected through reflective writing after each game was played. Qualitative data was collected due to the small class size ($n = 8$). The games were used in the order they appear here at roughly two week intervals.

4.1 Hackers and Agents

Students were asked to list two things they had learned from Hackers and Agents and dox3d! on their first exam. The comment below concerns Hackers and Agents.

"One thing I learned from the game is some terminology for various computer aspects. Things like a Trojan horse which allow you to access parts of the system in the game and also the Intrusion Detection System that monitors whether systems are being broken in to."

4.2 dox3d!

Students were given the following writing assignment.

1. As you play the game, reflect on how network topology (how the cards are arranged) affects the "ease" with which the hackers can achieve their goal. Try playing a couple games with different topologies. In a paragraph or two (a half page?), write up what you discovered about the network topology.

Students quickly focused on the layout of the tiles (the network topology) having a direct impact on the ease of winning the game. A network with a high degree of connectivity between nodes with the digital assets and the Internet gateway led to a higher probability of escape, while placing the Internet gateway at the periphery of the network, or having the gateway connected through only a few nodes greatly increased the risk of not being able to get out of the network. This more visual approach to learning about network topology appears to have helped more students understand the ramifications of particular topological choices.

Two students also commented that increasing the amount of hacker activity on a network made it much more likely to be detected. This point could be reiterated when learning about network monitoring tools.

2. Discuss and identify digital assets important to your life.

The idea of digital assets came very natural to the students, as well as the need to preserve the assets' security and privacy. Authentication credentials for web sites and financial institutions were commonly mentioned. International students were more acutely aware of the need to protect physical identification assets, likely because of their need to produce these documents to verify their visa status so they can work on campus, operate a motor vehicle, etc. There was also concern expressed about identity theft, which demonstrates that students were integrating what they were learning.

3. In the game, players hack into a network to recover assets that they believe belong to them. What are the legal and ethical implications of this?

This question was more problematic for the students. They agreed that individuals entering a network without authorization was not a good idea and was illegal, but could also see how the hackers may think that they should be able to retrieve their digital assets. The consideration of the legal implications depended on the student's grade level. Juniors and seniors tended to describe the legal consequences in more specific ways – one capstone student identified two particular federal laws (18 U.S. Code § 1029 - Fraud and related activity in connection with access devices and 18 U.S. Code § 1030 - Fraud and related activity in connection with computers) that would be applicable. This particular student not only took the time to do an information search to learn this, but also took the time to summarize the possible penalties.

4.3 Control-Alt-Hack

Students were given a writing assignment that asked them to reflect on the game.

1. Reflect on playing the game Control-Alt-Hack in class. What did you learn about computer and network security that you didn't know before?

Students reported that they learned more than they expected playing this game. Several students commented on the size of skillset needed to be proficient at hacking, and were amazed at the variety of skills. One student commented, "Before, I thought hackers just hacked. I never knew how many skills it took to hack something and not get caught." Students also were surprised to learn about hacking culture and the professional connections between hackers, and that hackers may look like everyone else in real life, with real jobs and normal social lives.

2. Playing the game should lead to seven educational outcomes (detailed in section 3.3 above). Briefly address whether each of these goals were met and why.

When asked to reflect on the stated goals by the game authors, most students agreed that the goals had been met. Students were unanimous in their agreement that the awareness goals had been met. The perception goals were more of a mixed bag, as some students felt that the fifth goal concerning negative stereotypes wasn't entirely met because of gender based attributes, e.g. women had more of a social engineering hacking style while men had more technical backgrounds. This finding was surprising as only one student had initially made this observation. A subsequent class discussion on gender differences and stereotypes was particularly interesting, given that two of the eight students were women. Lastly, student opinions on the ability to reclaim the word "hack" were mixed, with some students observing that they hadn't considered the productive and educational aspects of hacking before, while others contended that the word was too entrenched in popular usage.

5 Discussion

Student comments and discussions validated the belief that the use of the card games was engaging. The educational benefits, however, were more varied. Feedback at the end of the semester concerning the three games indicated that d0x3d and Control-Alt-Hack should be used in future course offerings. Feedback on Hackers and Agents was decidedly mixed. It should be noted, however, that there were not yet booster packs available, so that only the core game was played. A student commented, “Hackers and Agents was basically just Uno and not really necessary.”

Almost all students commented on how d0x3d helped them understand the importance of network topology, demonstrating the deep and integrative learning that took place with that facet of the game. Three students also commented that the games helped them put the theoretical knowledge gained from lecture and the book together in a more practical way, just as the lab activities had.

All students reported that at least two of the games had been engaging, interesting, and educational, and observations during class time showed that students were collaboratively engaged.

The games also prompted a class discussion on gender-based stereotypes and computers/hacking that would not have otherwise happened.

“I think all the games helped reinforce important concepts of the class. Enteracting with the games helped me tie what we were learning in class with how it could be used to a certain degree. Also they engaged the students’ interests so they weren’t just reading from a book or listening to a lecture. These games were not only fun but also educational and I would recommend using them in future classes.”

The challenge when using games in classes appears to be balancing the entertainment/motivation factor with solid learning outcomes. These outcomes could be made more prominent in future classes by giving writing assignments at the time of game play rather than later as a reflection. Game play for d0x3d! and Control-Alt-Hack was sufficiently difficult that even assigning the instructions to be read before class was inadequate to make it through the first game in a sixty-five minute class period. Continuing play to a second class day provided ample time to play multiple games once the rules were mastered and committed to memory.

Student feedback demonstrated that they were engaged learners, and certain topics like the relationship between network topology and security were remembered and commented on even after the course had concluded. Observations during the class itself demonstrated that students were actively collaborating and cooperating.

6 Conclusion

This paper discussed the use of card-based games to teach computer and network security. The objectives, rules, and learning outcomes for three different games were described. Student feedback for each of the games was summarized, and educational outcomes were discussed.

There was evidence of deep and integrative learning through the use of the card games. Using card-based games to motivate topics, foster cooperation, create an atmosphere of active learning, and engage students was successful.

Hackers and Agents is an Uno-like game with an option Booster pack to alter game play. d0xed allows students to create their own network topologies and then attempt to recover digital assets from the network without being caught. Control-Alt-Hack is geared more specifically towards education with the game acting as an engaging way to deliver information on computer and network security. Among these three games, students supported the idea of retaining dox3d! and Control-Alt-Hack, while opinions on the usefulness of Hackers and Agents were mixed.

Future work for subsequent security classes includes play-testing Hackers and Agents with Booster Packs, as well as identifying other relevant tabletop games. Educational outcomes between these games and more traditional computer-based games could be compared. Table-top games will be incorporated into other computer science classes, such as d0x3d in a networking class.

References

[1] Joint Task Force on Computing Curricula, Association for Computing Machinery and IEEE Computer Society. *Computer Science Curricula 2013: Curriculum Guidelines for Undergraduate Degree Programs in Computer Science*. ACM, New York, NY, USA, 2013.

[2] Rowe, D. C., Lunt, B. M. and Ekstrom, J. J. The role of cyber-security in information technology education. In *Proceedings of the 2011 conference on Information Technology Education* (West Point, New York, USA, 2011). ACM, New York, NY, USA, 113-122.

[3] Jordan, C., Knapp, M., Mitchell, D., Claypool, M. and Fisler, K. CounterMeasures: a game for teaching computer security. In *Proceedings of the 10th Annual Workshop on Network and Systems Support for Games* (Ottawa, Canada, 2011). IEEE Press, Piscataway, NJ, USA.

[4] *National Initiative for Cybersecurity Education (NICE) Strategic Plan: Building a Digital Nation*. (Washington, D.C.: September 2012) http://csrc.nist.gov/nice/documents/nicestratplan/nice-strategic-plan_sep2012.pdf. Accessed 20 March 2014.

[5] Hakulinen, L. Using serious games in computer science education. In *Proceedings of the 11th Koli Calling International Conference on Computing Education Research* (Koli, Finland, 2011). ACM, New York, NY, USA, 83-88.

[6] Werther, J., Zhivich, M., Leek, T. and Zeldovich, N. Experiences in cyber security education: the MIT Lincoln laboratory capture-the-flag exercise. In *Proceedings of the 4th conference on Cyber Security Experimentation and Test* (San Francisco, CA, 2011). USENIX Association, Berkeley, CA, USA.

[7] Cowan, C., Arnold, S., Beattie, S. and Wright, C. *Defcon Capture the Flag: defending vulnerable code from intense attack*. In *Proceedings of the DARPA Information Survivability Conference and Exposition*, Washington, D.C., April 2003.

[8] Dougherty, M. Making a Game of Network Security. In *Proceedings of the 18th USENIX conference on System Administration* (Atlanta, GA, 2004). USENIX Association, Berkeley, CA, USA, 187-194.

[9] Koch, S., Schneider, J. and Nordholz, J. Disturbed playing: another kind of educational security games. In *Proceedings of the 5th USENIX conference on Cyber Security Experimentation and Test* (Bellevue, WA, 2012). USENIX Association, Berkeley, CA, USA.
[10] Boit, A., Eirund, H., Geimer, T., Mendonca, J. C. d., Ott, E. and Sethmann, R. *NetS-X - The Network Security Experience*. In *Proceedings of the 7th European Conference on i-Warfare*, (Plymouth, UK, 2008).
[11] Catuogno, L. and Santis, A. D. An internet role-game for the laboratory of network security course. *SIGCSE Bulletin*, 40, 3 (June 2008), 240-244.
[12] Thompson, M. and Irvine, C. Active learning with the CyberCIEGE video game. In *Proceedings of the 4th conference on Cyber Security Experimentation and Test* (San Francisco, CA, 2011). USENIX Association, Berkeley, CA, USA.
[13] Jipping, M. J., Haggenmiller, A., Koster, M. and Ostrowski, E. Experiments with network security threats in a safe, easy sandbox. In *Proceeding of the 44th ACM technical symposium on Computer science education* (Denver, Colorado, USA, 2013). ACM, New York, NY, USA.
[14] *http://www.hackersandagents.com*. Accessed 20 March 2014.
[15]*https://s3.amazonaws.com/download.thegamecrafter.com/1396022023/Threat%20AddOn%20Rules.pdf*. Accessed 20 March 2014.
[16] *http://d0x3d.com/d0x3d/welcome.html*. Access 20 March 2014.
[17] Denning, T., Lerner, A., Shostack, A. and Kohno, T. 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* (Berlin, Germany, 2013). ACM, New York, NY, USA, 915-928.
[18] *http://www.controlalthack.com/foreducators.php*. Accessed 20 March 2014.