Control-Alt-Hack: The Design and Evaluation of a Card Game for Computer Security Awareness and Education

Tamara Denning†, Adam Lerner†, Adam Shostack*, and Tadayoshi Kohno†
†Computer Science & Engineering
University of Washington
Seattle, WA, USA
{tdenning, lerner, yoshi}@cs.washington.edu
*adam@homeport.org

ABSTRACT
We scoped, designed, produced, and evaluated the effectiveness of a recreational tabletop card game created to raise awareness of—and alter perceptions regarding—computer security. We discuss our process, the challenges that arose, and the decisions we made to address those challenges. As of May 2013, we have shipped approximately 800 free copies to 150 educators. We analyze and report on feedback from 22 of these educators about their experiences using *Control-Alt-Hack* with over 450 students in classroom and non-classroom contexts. The responses from the 14 educators who reported on their use of the game in a classroom context variously indicated that: their students' awareness of computer security as a complex and interesting field was increased (11/14); they would use the game again in their classroom (10/14); and they would recommend the game to others (13/14). Of note, 2 of the 14 classroom educators reported that they would not have otherwise covered the material. Additionally, we present results from user studies with 11 individuals and find that their responses indicate that 8 of the 11 had an increased awareness of computer security or a changed perception; furthermore, all of our intended goals are touched upon in their responses.

Categories and Subject Descriptors
K.3.2 [**COMPUTERS AND EDUCATION**]: Computer and Information Science Education

Keywords
Card game; computer science education; computer security and privacy; computer security education; game; outreach; privacy; security; security awareness; security education; security outreach; tabletop security; tabletop games.

1. INTRODUCTION
We believe that there is vast benefit to be offered from raising people's awareness of computer security. Exposing many different kinds of individuals to ideas that make them think about computer security—however briefly—could potentially benefit the status of computer security as whole:

Current and Future Users. The more people prioritize security, the more they might express it with their purchasing power, and the more willing they might be to engage in security and privacy behaviors that require time or effort.

Current and Future Developers. The more developers prioritize security, the more willing they might be to take action. This might mean taking security training, refreshing their knowledge of best security practices, taking more care with their code, or simply thinking to reach out to their institution's security team.

Current and Future Management. If management prioritizes security, they might dedicate more resources to developing and maintaining secure products and systems, or reward security-promoting behaviors via the institution's incentive structure.

Future Technologists. We encourage as many people as possible to consider computer security and computer science as a profession, in order to increase the strength of the field as a whole.

There are many avenues to increase people's awareness of security: publicity campaigns, integration into popular culture, and education and training are just a few. In our work, our desire to create an artifact that exposes people to thinking about security and that facilitates ad hoc, social interactions led us to design *Control-Alt-Hack®: White Hat Hacking for Fun and Profit*: a recreational, tabletop card game about computer security. As of May 2013, approximately 800 requested copies of Control-Alt-Hack have been shipped to 150 educators.

We sent these educators surveys, and 22 educators representing over 450 students submitted feedback about their experiences using Control-Alt-Hack inside and outside of the classroom. Analysis of the evaluation data has indicated that we have had some success meeting our design goals. Of the educators who reported using the game in their classrooms: 11 out of 14 indicated in their responses that the game played a role in increasing their students' awareness of computer security; 11 out of 14 indicated that the game was engaging or filled a social role in the classroom; 13 out of 14 indicated that they would suggest the game to others; and 10 out of 14 said that they would use the game in their class again. In terms of reaching new audiences, 2 of the classroom educators reported that they would not have otherwise covered the security material in Control-Alt-Hack. Furthermore, in a user study we conducted with 11 participants, 8 of the 11 provided evidence that they were thinking in new ways about computer security after playing the game.

In this paper, we:

- Describe and explore the manner in which unconventional tools, and specifically a physical game, can reach new audiences—or be used in new contexts—in order to raise overall awareness or alter perceptions about security;

CCS'13, November 4–8, 2013, Berlin, Germany.

ACM 978-1-4503-2477-9/13/11…$15.00.
http://dx.doi.org/10.1145/2508859.2516753

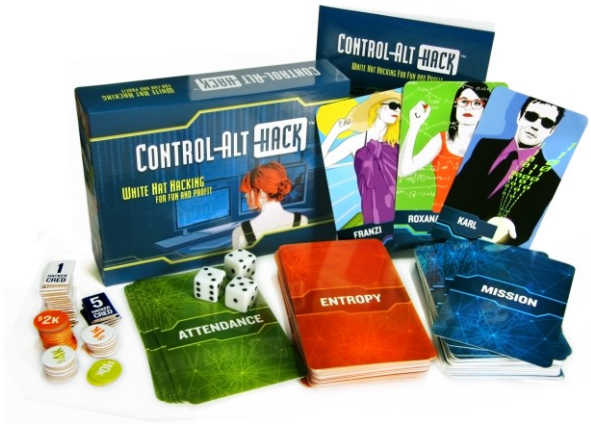

Figure 1. A photo of the game box and contents. Photo Credit: Juliet Fiss. © University of Washington

- Explicate and critique our design process, the constraints that arose throughout its course, and the tradeoffs that we made to further our project goals;
- Present our analysis evaluating the success of our tool in reaching its desired audience and achieving its intended goals;
- Based on our knowledge and our evaluation, discuss the contexts in which the game is less suitable, and our takeaway lessons regarding how this reflects the design tradeoffs that we made to meet our goals;
- Contribute to the knowledge foundation for those interested in creating tools that utilize unconventional methods or reach new audiences, in order to ultimately improve the state of computer security as a whole.

2. PROJECT GOALS

2.1 Goals

Awareness Goals. As motivated by Section 1, our primary goal is to increase people's awareness of computer security needs and challenges, so that they can be more informed technology builders and consumers. This includes:

(1) Increasing understanding of the importance of computer security, and the potential risks with inadequate security safeguards.

(2) Conveying the breadth of technologies for which computer security is relevant, including not only conventional computing platforms like laptops and Web servers, but also emerging platforms like pervasive technologies and cyber-physical systems.

(3) Improving understanding of the diversity of potential threats that security designers must consider and the creativity of attackers.

Perception Goals (Secondary Goal). We additionally seek to show that the information technology community and its professions are open to people of diverse backgrounds. Providing even fictional role-models could help encourage interest in computer science and computer security. More specifically, we aim:

(1) To work against negative, dissuasive, or niche stereotypes about people in these fields, and to allow players to identify with one or more of the characters in order to envision themselves in the field.

(2) To highlight the variety of professional and personal opportunities available to people with these skills.

Exposure Goal. We seek to have as wide an impact with our Awareness and Perception Goals as possible—the more people that play this game, the more opportunities our game has to increase awareness or change perception.

2.2 Why a Game?

We believe that games are well positioned to address our specific project goals. If designed well, we argue that games can be an appropriate tool for seeding a large audience of people with a modest amount of security information. Briefly:

- Games can be fun, which gets people engaged.
- Games can give you permission to explore ideas and ask questions.
- Games are intended to have intrinsic entertainment value, which gets people to pick them up and use them on their own time.

Given the subject matter, it may seem natural to have created a computer game, rather than a physical tabletop game. Both formats have their merits and their limitations, and in creating our tool we chose to explore the problem space via a physical game. Part of our reasoning in doing so was to take advantage of some of the following factors:

- Physical games may appeal to people who do not enjoy computer games.
- Aside from requiring a surface on which to play, physical games generally do not require extensive setup or have resource dependencies.
- Having a game lying around in a physical space provides the opportunity to read through some of the cards, even if the game is not being actively played.

While the following properties are not exclusive to physical games:

- Physical games can create social environments, which can foster interaction and discussion of ideas encountered.
- Because physical games can create interaction between players, they are suitable for use in social gatherings.

2.3 Target Audience

No game strongly appeals to everyone. While we sought to make our game as broadly appealing as possible to raise security awareness within a very large audience, it is most practical to target a specific demographic.

Primary Education Audience. Our primary target audience is people with an affinity for computer science and engineering but without requiring significant computer security education, training, or experience. We target in particular those who are early in their careers, including computer science and engineering undergraduate students, high school students, and recent graduates. For example, a high school student in AP Computer Science might play this game, as might a recent hire in software development, test, or management. This goal means that our primary target audience is technically inclined and consists of roughly 15- to 30-year-olds.

Secondary Education Audiences: High school and undergraduate students in the Science, Technology, Engineering,

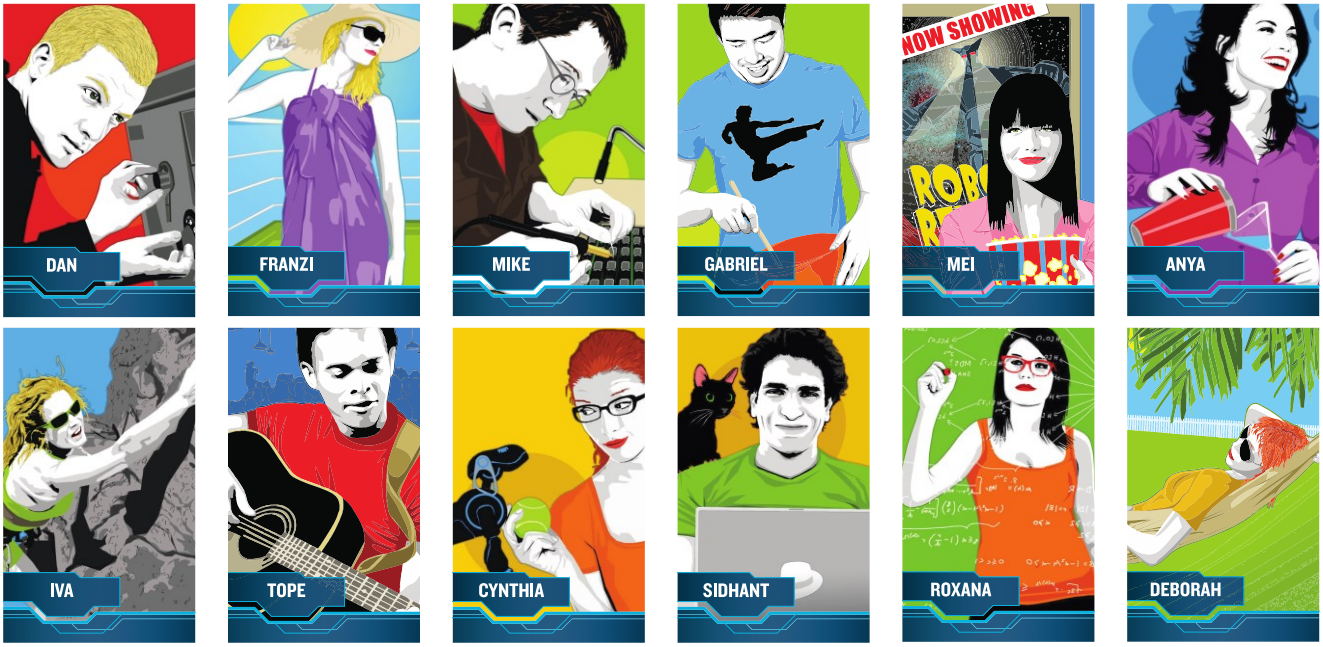

Figure 2. The character art from the portrait side of 12 of the game's 16 Hacker cards. © University of Washington

and Math (STEM) disciplines; software developers; gamers; and the broader public.

Security Community: As a vector for increased dissemination.

3. GAME DESIGN

In this section we give a brief, high-level tour of our game development process.

3.1 Choosing Game Mechanics

A game's "mechanics" includes all numeric and logical elements of the game that contribute to game play; for example, a game's mechanics might consist of its rules, the number and type of game decks, and the numbers or gameplay actions on those cards. It can be challenging to design mechanics that lead to well-balanced games. Variables include: the number of players; the time it takes to learn the rules; the time it takes to play; replay value; cooperative versus competitive paradigms; the ability to rebound from a losing streak; and the variety of winning strategies. The story, flavor text, and art rest on top of the mechanics.

We initially explored creating game mechanics from scratch. However, since we are computer security researchers and not experts in game mechanics, we chose to license a system from a pre-existing game and then create all new game content. This approach allowed us to forgo playtesting the mechanics—a necessary, time-consuming step to ensure game balance and enjoyment. We did do playtesting to review our game content, which we discuss in Section 3.2.

We explored the rules and mechanics of a number of games available for sale in gaming stores for a game that would support our desired design goals. For example, we wanted a game where a player took on the role of a character, so that they could identify with someone in the computer security field (Perception Goals); we immediately gravitated towards games whose characters featured a variety of skills, in order to highlight the somewhat eclectic specializations that can help improve—or break—a system's security. We also wanted a game that would naturally support a variety of textually-heavy scenarios or encounters.

We licensed the *Ninja Burger* mechanic from Steve Jackson Games [28], best known for their *Munchkin* card game and the *GURPS* roleplaying system. Ninja Burger met our above criteria, and we transformed the game into *Control-Alt-Hack: White Hat Hacking for Fun and Profit*. Instead of delivering burgers in fun scenarios in the quest to become the next branch manager, our players tackle a range of technically-themed scenarios with the goal of becoming the next company CEO.

3.2 Feedback Process

We solicited feedback on iterations of the Control-Alt-Hack card deck to gather suggestions to improve the game and assess its ability to meet our goals. These formative evaluations took the form of playtest sessions or "show and tell" sessions, and were conducted with a variety of parties, including: undergraduates in an introductory computer science course (n=10); undergraduates involved in a computer security competition (n=5); graduate students affiliated with a computer security lab (n=8); graduate students (unaffiliated with a security lab) who have an interest in gaming (n=2); computer science professors (n=2); a computer science lecturer (n=1); a former high school teacher of computer science, now an undergraduate lecturer (n=1); outreach officers (n=3); and assorted non-experts (n=14). In response to this evaluation feedback, we: changed specific card text, modified art, and added new cards to help keep track of gameplay decisions.

3.3 Brief Overview of Control-Alt-Hack

The following is the premise of the game:

> *You and your fellow players work for Hackers, Inc.: a small, elite computer security company of ethical (a.k.a., white hat) hackers who perform security audits and provide consultation services. Their motto? "You Pay Us to Hack You."*
>
> *Your job is centered around Missions—tasks that require you to apply your hacker skills (and a bit of luck) in order to succeed. Use your Social Engineering and Network Ninja skills to break the region's power grid, or apply a bit of Hardware Hacking and Software Wizardry to convert your*

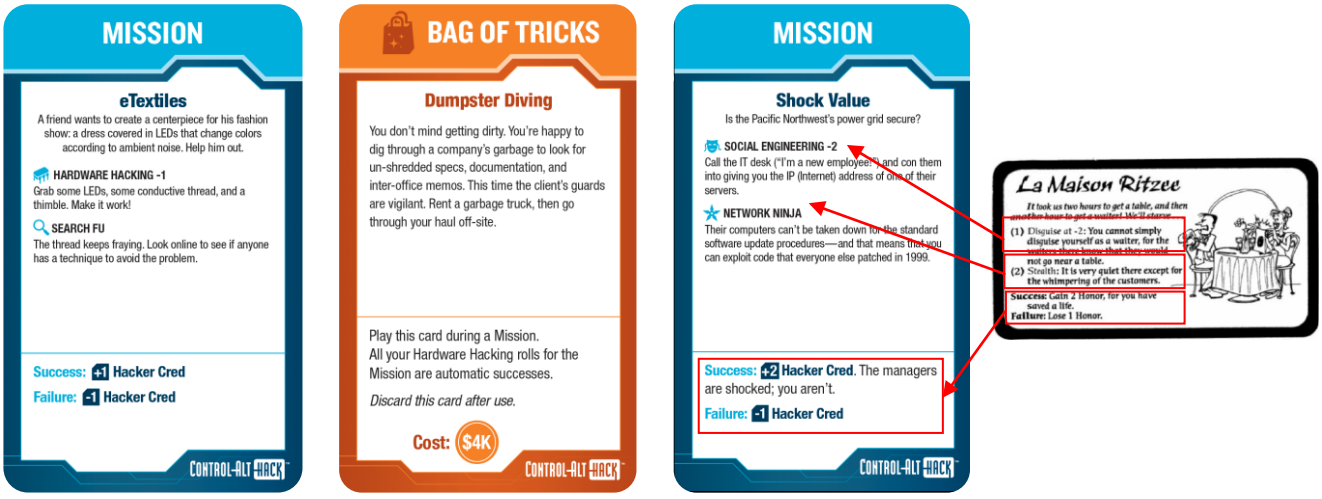

Figure 3. From left to right: (a) a Mission demonstrating the usage of technical skills for artistic purposes (Perception Goal (2)); (b) a Bag of Tricks card illustrating a particular attack threat (Awareness Goal (3)); and (c) a Mission describing a social engineering attack on an SCADA system (Awareness Goals (2) & (3)), along with the mappings to the original Ninja Burger card. © University of Washington

robotic vacuum cleaner into an interactive pet toy...no two jobs are the same. So pick up the dice, and get hacking!

Figure 1 shows the game box and contents. Figures 2 and 3 show some of the game art and card contents.

Each turn each player attempts a single Mission, so players get to see a number of Missions throughout the course of the game. By incorporating a large number of technologies and security threats into the Mission narratives, we communicate a variety of security ideas throughout the course of the game.

3.4 Juggling Design Constraints

Our game creation process was driven by goals and constraints, some occasionally in direct conflict; seeking optimal solutions (or pleasing compromises) took significant effort and iteration.

3.4.1 Text

In creating the cards' textual content, we balanced a number of goals and restrictions: (1) Including Technical Content; (2) Mapping Game Mechanics; (3) Offering Comprehensibility; (4) Maintaining Brevity; and (5) Incorporating Humor.

Including Technical Content. We began by creating a list of the content we wanted to cover in order to address our Awareness Goals and convey the range and depth of computer security issues: we brainstormed lists of technologies, attacks, defenses, attacker types, and the range of human assets that can be impacted by system breaches. Table 7 in the Appendix (Section A.1) gives some sample card titles and topics, along with examples of specific research that inspired their inclusion. We sought topics that would be relevant and interesting to players through personal (e.g., social networks), educational (e.g., browser cookies), or professional experience (e.g., patching) or through the news and media (e.g., credit card theft). During the Feedback Process (Section 3.2), we solicited feedback on the selection and technical accuracy of the content which we portrayed.

Most of the game relates to computer security: of the 56 Mission cards, 44 deal directly with security topics, 6 with technological activities (as in Figure 3a), and the remaining 6 deal with related topics like puzzles, the role of computer security in history, or the value of professional networking. For content balance and enjoyability, we intentionally did not want all of the cards to focus on computer security topics.

Mapping Game Mechanics. The characters, their skills, and the Missions—which require the use of various combinations of those skills—in Control-Alt-Hack are isomorphic to those in Ninja Burger in order to preserve game balance. Significant iteration and exploration was required to create reasonably realistic and fun story justifications for the combinations of skills required for all 56 Missions. See the Mission "Shock Value" in Figure 3(c) for an example where it was necessary to invent an attack requiring Social Engineering and Network Ninja skills, along with a mapping from the original Ninja Burger card. Similar effort was required to create content for the game's 72 Entropy cards and 16 Hacker cards.

Offering Comprehensibility. Given our target audience (Section 2.3), our goal of creating enthusiasm for computer security and computer science (Perception Goals), and our desire to reach a broad audience (Exposure Goal), we needed to make our text understandable to those without extensive security experience—without sacrificing technical integrity. We attempted to always make the meaning of terms implicitly clear, explicitly clear, or irrelevant to understanding the overall gist of the card. For example, "Shock Value" in Figure 3(c) parenthetically defines an IP address as an Internet address, and "Dumpster Diving" in Figure 3(b) defines dumpster diving within the text of the card.

Observe how this latter card also incorporates additional learning content: the card helps illustrate that defensive measures (guards, in this case) are not always effective, and that the creativity of attackers can be surprising (such as renting a garbage truck, which many people may not have thought possible).

Incorporating Humor. We incorporated humor into the game in order to make it more enjoyable. The humor primarily (but not exclusively) took the form of: (1) puns; (2) popular culture references; or (3) sexual innuendo, although we attempted to keep the innuendo tasteful and respectful, and we evaluated the cards with stakeholder groups prior to finalizing them (Section 3.2). For example, "Shock Value" in Figure 4(c) has puns, and "eTextiles" in Figure 3(a) has a popular culture reference in its Hardware Hacking task.

Responding Participant	Course	Class Size	Student Level	Prior Security Experience	Would have covered [the security material in Control-Alt-Hack] otherwise?	Time Taken	Supplementary assignment involving Control-Alt-Hack
E1-classroom	Information Software Technology	30	HS	No / Some Informal	Yes	60 min	No
E4-classroom	Unknown	12	UG	No / Some Informal	Yes	50 min	Yes
E6-classroom	Computer Science	75	HS	Some Informal	No	75 min	No
E7-classroom	Cyber-Security and Information Assurance	56	UG	No / Some Informal	Yes	120 min	Yes
E8-classroom	Computer and Network Security	10	UG, G	Some Informal / Prior Educational	Yes	120 min	No
E9-classroom	Computers and Information Technology	60	HS	Prior Educational	No	75 min	No
E10-classroom	Game Design	65	HS	No / Some Informal	Yes	90 min	Yes
E12-classroom	Computer Security	22	UG	Prior Educational	No*	80 min	Yes
E13-classroom	IT Security	8	UG	Prior Educational	Yes	45 min	No
E14-classroom	Information Security	15	UG	Some Informal / Prior Educational	Yes	120 min	No
E16-classroom	Intro CS Web Design	35	HS	No	Yes	40 min	No
E17-classroom	Cyber Security	2	HS	Prior Educational	Yes	30 min	No
E18-classroom	Fundamentals of Information Security	30	UG	No / Some Informal / Prior Educational / Prior Professional	Yes	75 min	Yes
E19-classroom	Computer and Network Security	27	UG	No / Some Informal	Yes	60 min	No

Table 1. Classroom-based educator activity contexts. The shaded cells represent cases of interest, some of which are discussed in Sections 6.4 and A.4. HS = high school; UG = undergraduate; G = graduate.

*We believe this response to be an error or a misinterpretation of the question's meaning.

3.4.2 Visuals

We directed illustration and graphic design as part of the game's content creation process. We purposefully allocated a non-trivial portion of our resources to these visuals for two reasons: (a) to make it easier for players to identify with and project themselves onto Hacker characters (Perception Goals); and (b) to make the game visually appealing, hopefully attracting players (Exposure Goal) and implicitly showing that a focus on technology does not preclude placing importance on aesthetics (Perception Goals).

In creating Hacker portraits, we addressed the Perception and Exposure Goals by balancing the characters' genders and ethnicities and by showing them engaging in a variety of hobbies. Figure 2 shows the character art from the portrait side of 12 of the 16 Hacker cards.

Table 2. Non-classroom-based educator activity contexts

	Context	Time Taken
E2-ACM	Extra-curricular activity with undergrads in the ACM	150 min
E3-vetting	University instructors vetting the game	150 min
E5-no-play*	Instructor vetting the game with adult friends*	N/A*
E11-checkout	Provided as a checkout for students to play with friend and family	150 min
E15-vetting	Instructor vetting with graduate students, faculty, and staff	60 min
E20-vetting-didn't-read**	Instructor vetting**	N/A**
E21-lunch	Departmental staff lunch	60 min
E22-vetting	Instructor vetting	90 min

*After reading the rules, they did not understand how to play, so they stopped.

**The instructor chose not to read cards or play due to the list of PG-14 cards supplied on the web site.

4. DISTRIBUTION, EXPOSURE, AND PRELIMINARY IMPACT

In order to reach a diverse set of audiences (Exposure Goal), we chose to make Control-Alt-Hack available via two different avenues:

(1) Available for free to educators who submit a request via http://www.controlalthack.com. As of July 2013, the supply of games allocated to educators has been nearly depleted.

(2) Available for sale on Amazon.com via RGB Hats, LLC, which was founded by two of the co-authors and which licensed the game from the University of Washington. This distribution method also allows production of the game to be self-sustaining.

From when the game was made available in November through March, we shipped approximately 800 copies of the game to 150 different educators who requested copies. Approximately 50 copies were also handed out at the SIGCSE 2013 poster session. Together, these educators served as the recruitment pool for our summative evaluation of the game (Section 6). Additionally, over

	Positive Functions		Critiques				
	Social / Engagement	Awareness	Takes a long time to learn	Takes a long time to play	Not enough fun	Not enough educational value	Has inappropriate content
E1-classroom	X	X	X	X			
E4-classroom	X	X					
E6-classroom	X		X				
E7-classroom	X	X					
E8-classroom	X	X				X	
E9-classroom	X	X	X				
E10-classroom	X	X					
E12-classroom		X		X		X	
E13-classroom	X		X			X	
E14-classroom	X	X	X	X			
E16-classroom		X	X				
E17-classroom						X	
E18-classroom	X	X	X				
E19-classroom	X	X					

Table 3. Classroom-based educator survey analysis results.

300 copies have been distributed at a variety of NSF-sponsored job fairs, competitions, and similar events.

We were invited to present a talk on the game at a large web company's internal security training conference, and an optional play session was held at the conclusion of the hands-on training.

5. EVALUATION METHOD

In this paper we present evaluations of Control-Alt-Hack via two methods:

- **Primary:** Feedback surveys from educators who requested copies of the game; and
- **Secondary:** User studies performed with the game.

Both methods were approved by the University of Washington's Human Subjects Institutional Review Board.

5.1 Educator Feedback Surveys

We distributed online feedback surveys via email to the 150 instructors who received educator copies prior to May 2013. Section A.2 in the Appendix shows the questions asked on the educator survey. 22 educators submitted responses to the surveys.

Coding. Two researchers analyzed the survey responses independently and formed preliminary opinions about the categories that emerged from the data. The researchers then compared the categories and formed a cohesive coding scheme via consensus. The primary coder recoded the educator surveys according to this coding scheme. (Complying with our institution's conflict management plan, one of the researchers has no financial interest in RGB Hats, LLC.) In the evaluation, we used the survey in its entirety as the unit of analysis, rather than individual responses; that is to say, if part of an educator's response received the code "Awareness," it did not matter which question on the survey elicited the relevant response, and it did not matter how many times the survey was coded for "Awareness."

The primary coder and the secondary coder had 93% agreement across all educator surveys (N=22) and codes (N=7); there were 11 cases where the primary and the reliability coder disagreed. All cases are provided in the Appendix (Section A.3), along with contextual quotes. Except for one case in which the reliability coder misread the data and coded an error, the primary coder's results—the results reported in the paper—always represent the stricter of the two viewpoints. That is, we report the upper bound on our interpretation of the critiques to the game and the lower bound on the game's role in engagement and awareness.

The primary and secondary coders independently labeled educator activities as classroom-based or non-classroom-based activities; they had 100% agreement. Tables 1 and 2 list information about classroom- and non-classroom-based activities, respectively.

5.2 User Studies

We posted recruitment ads inviting participants to join us for a games study session on: an institution-wide electronic bulletin board; and in the local Craigslist gigs listings. We held two game study sessions: one with 7 people (M=3, F=4) divided into two gameplay groups; and one with 4 people in one gameplay group (M=1, F=3). The participants covered a range of ages (mean=31, min=18, max=50, median=29). 5 of the participants could be categorized as "hobbyist" gamers, and 6 had casual or little gaming experience. Each session lasted approximately 2 hours. Participants were compensated $20 for their time. Following consent paperwork, participants filled out a short pre-gameplay survey. After this participants were shown a 15-minute video introducing them to gameplay; we used a video for consistency between sessions. Participants played for 40-60 minutes, then filled out a short post-gameplay questionnaire.

Coding. Two researchers independently analyzed the survey responses for themes and categories. (Complying with our institution's conflict management plan, one of the researchers has no financial interest in RGB Hats, LLC.) The researchers discussed and came to a consensus regarding the data of interest

in the survey responses. The data in question is presented as direct quotations, and the goal mappings were decided via consensus coding.

6. EDUCATOR SURVEY RESULTS

The 22 educators who responded to the survey used the game with over 450 students at the high school, undergraduate, and graduate levels in computer science, computer security, and game design courses. These courses were primarily, although not exclusively, based in the United States. The educator survey results are the primary evaluation of Control-Alt-Hack in this study.

As previously mentioned, the educator survey responses fell into one of two categories: feedback about an activity using Control-Alt-Hack that took place in a classroom, or feedback about an activity using Control-Alt-Hack that took place outside of a classroom. Many of the reported non-classroom activities were from educators who were vetting the game for classroom use, and subsequently decided not to use the game; the other non-classroom activities were an ACM gathering, a lunch activity, and offering the game to students to check out and take home. Table 1 provides additional information on the classroom activities (N=14), and Table 2 provides additional information on the non-classroom activities (N=8).

6.1 Positive Functions

Appreciation of the game expressed in educator surveys generally described the game as fulfilling one of two functions: being fun or serving a social function (Social/Engagement); or increasing students' awareness of computer security or computer science issues (Awareness).

Social/Engagement (Classroom: 11/14; Non-Classroom: 2/8). "Social/Engagement" was marked when the educator was deemed to be indicating that usage of the game was fun, engaging, and/or contributed to serve a social function, such as an icebreaker or a breather before a test. The following quotes are two examples:

- **E7-classroom (56 undergraduates, Cyber-Security and Information Awareness):** *"It worked as a way to break the ice and get students from diverse majors get to know [sic] each other and get thinking about the topics of the course."*
- **E19-classroom (27 undergraduates, Computer and Network Security):** "*I just wanted to reiterate how great my students thought the game was! The students begged me to leave the game in the student lounge so they could continue to play, and from what I hear it's made a trip or two out to our weekly majors night at the pub."*

Awareness (Classroom: 11/14; Non-Classroom: 1/8). "Awareness" was marked when the educator was deemed to be indicating that usage of the game served to increase students' awareness of security in some fashion, such as: increasing exposure to domain terminology; raising awareness of career opportunities; stimulating discussion; or stimulating critical thinking. The following quotes are two examples:

- **E9-classroom (60 high school students, Computers and Information Technology):** *"The game did not necessarily teach security methods, but it did a great job of teaching vocabulary and literacy."…"It increased awareness of my program, and it got more students interested in computer science."*
- **E19-classroom (27 undergraduates, Computer and Network Security):** *"They really got into it and there was a lot of strategizing"…*"*They were mainly focused on causing pain to their classmates, but as I wandered around the room I heard some great discussions about the tradeoffs of choosing various hackers' skill sets, what various missions meant, etc.*"

Table 3 shows the Positive Functions results from the classroom-based educator responses, and Table 4 shows the results from the non-classroom-based educator responses.

Overall, in the classroom contexts, 11 of the 14 educators indicated that the game served a Social/Engagement role, and a different set of 11 educators indicated that the game served to increase Awareness. For the educators who did not provide responses that indicated that the game raised awareness, two were courses about computer security; these educators also indicated that the game did not have enough educational content (Section 6.2). This suggests that although our design goals were aligned with the intentions of educators not already teaching a computer security course, the goals were not well aligned with some educators' intentions in using the game in security-focused courses.

In the non-classroom contexts, 2 of the educators' responses indicated that the game filled a Social/Engagement role (E2-ACM, E15-vetting), and 1 of the educators indicated that the

	Positive Functions		Critiques				
	Social / Engagement	Awareness	Takes a long time to learn	Takes a long time to play	Not enough fun	Not enough educational value	Has inappropriate content
E2-ACM	X	X				X	
E3-vetting					X	X	
E5-no-play*			X				
E11-checkout						X	
E15-vetting	X		X			X	
E20-vetting-didn't-read**							X
E21-lunch			X				
E22-vetting					X	X	

Table 4. Non-classroom-based educator survey analysis results.

*Educator did not play the game due to not understanding the rules.

**The educator did not read the cards, but responded based on the list of PG-14 cards listed on the website.

game helped increase Awareness (E2-ACM). The relative lack of educators reporting positive game functions in non-classroom activities could be a result of the fact that many of the responses in the non-classroom context were from educators who played the game (or not, in 2 cases) out of the classroom in order to vet it for its suitability for use in the classroom. In many of those cases, the educator decided not to use Control-Alt-Hack in the classroom (Section 6.3 and Table 5), so it is not surprising that they do not comment that the game serves positive functions.

6.1.1 Discussion

Overall, we find that the feedback on the game—in the classrooms in which it was used—shows promising indications that it performs multiple positive functions.

Awareness. In most of the surveys, educators' comments indicated that the game helped raise students' awareness of issues related to computer security. Raising individuals' awareness of the risks, challenges, technologies, and professions involved in computer security was a large part of our purpose in creating the game (Goals, Section 2.1).

Social/Engagement. Again in most of the surveys, educators' comments indicated that the game served a Social/Engagement role in the classroom. This is promising for two reasons: first, it is somewhat correlated with "fun," which can increase engagement or encourage people outside of the classroom to pick up the game. Second, some of the educators used the game specifically because they had need of a non-traditional educational activity; Section 6.4 explores the cases where the educators used the game, but would not have otherwise covered comparable security material. The apparent success of the game's Social/Engagement function, as represented in the evaluation, suggests that the produced game is aligned with our Exposure Goal.

6.2 Critiques and Tradeoffs

The critiques of the game contained in educators' responses were analyzed as falling into one or more of five somewhat self-explanatory statements: (1) Takes a long time to learn; (2) Takes a long time to play; (3) Not enough fun; (4) Not enough educational value; and (5) Has inappropriate content. We discuss the critiques at some length because many of them directly reflect the design tradeoffs that we selected to meet our intended goals.

Takes a long time to learn. Examples:

- **E5-no-play:** *"Honestly, after reading over the rules, we didn't understand how to play it, and we gave up. So sorry!"*
- **E15-vetting:** *"The game itself is too complex to easily teach and use for the first time."*

Following the shipment of the game to educators, we have created a new video that walks viewers through game setup and gameplay in a shorter, clearer format (a video of an hour-long conference talk was previously available which contained an explanation of how to play), which we will publish online; the new video is 10 minutes long. Some of the learning curve is due to the complexity of the game mechanics that we chose (Section 3.1); however, we accepted a level of complexity as a good tradeoff for increased replay value and the in-game opportunities to strategize.

Takes a long time to play. Examples:

- **E14-classroom (15 undergraduates, Information Security):** *"Shorten the game and eliminate some components."*
- **E12-classroom (22 undergraduates, Computer Security):** *"Students reported that they enjoyed the game, but that the hour twenty was pushing the limit."*

Gameplay duration can vary depending upon the number of players, players' familiarity with the rules, and the emergent characteristics of a particular game instance. Potentially long gameplay can make the game unwieldy for the classroom setting; however, the gameplay duration can be an asset in other social settings. Many educators indicated positive results even when playing a version of the game truncated to fit into a class period.

Not enough fun. One example (the only other instance an example of coder disagreement, and is given in the Appendix):

- **E3-vetting:** *"The feedback from the instructors trying the game is that it didn't seem very enjoyable to play or strategic. It may be that more experience will change this, but the first impression was not positive."*

While the players in the above example (adult instructors) are not our primary target audience, there is no guarantee that the instructors' students would have found the game fun. We do not have sufficient data to confidently predict who will or will not enjoy the game; nevertheless, observation and anecdotes suggest at the very least that if the audience is familiar with and enjoys the style of game on which Control-Alt-Hack is based, then it is relatively likely that they will find the game fun.

Not enough educational value. Examples:

- **E11-checkout:** *"The game could use more specificity around computer activity. My students were hoping for a higher level of rigor."*
- **E17-classroom:** *"Since we approached the game expecting to be tested on our knowledge of vulnerabilities and penetration techniques, we were dissatisfied in that manner, but we enjoyed the overall concept."*

We intentionally chose a lower level of technical depth in the design phase in order to further the Exposure Goal and be comprehensible to a wider portion of our target audience; in the case of these classrooms that decision was not well aligned with instructors' intentions. We recognize that the game is not a good fit for students with a more advanced security background who are hoping to learn new material; this would only be accomplished if the game were paired with a supplementary activity, as some educators chose to do (see Section A.4 in Appendix).

Has inappropriate content. There is only one instance of this critique appearing in the data:

- **E20-vetting-didn't-read:** *"I didn't have time to vet the game for appropriateness and, from what I did read on the above site, I felt that the cards significantly contributed to a learning environment hostile to women."*

We do not wish to create an environment hostile to women, and kept gender issues at the forefront of our minds during game development. We took care to make references gender-neutral or gender-balanced: for example, the CEO is a woman, half of the Hacker cards are female, and with one exception, all innuendo is gender-neutral (a Mission card about cell phone security has the title "That's What She Said"). We recognize that innuendo can make an environment more hostile to women, particularly if the environment already has uncomfortable overtones; however, during the design phase we gathered feedback on the appropriateness of our content from multiple parties, including a former (female) teacher of high school computer science and 3 (female) outreach officers (Section 3.2), and incorporated it into

the game. For example, we redid the style of dress of one of the female Hackers in response to their comments. The materials we distribute to educators included a list of PG-14 cards which can be reviewed for content and/or removed from the deck.

6.2.1 Discussion

Table 3 presents the classroom-based educator experiences coded for the goals and critiques; Table 4 presents the same for the non-classroom-based educator experiences.

The most prominent critique was that the game takes a long time to learn (classroom: 4/14, non-classroom: 3/8). From observation and anecdotes, individuals who are familiar with this style of game find it fairly quick to pick up. For example, E13-classroom gave this quote: "*The students with some game experience found it obvious and intuitive. They would say "this is easy."*" Additionally, we suggest that educators could make the start of gameplay smoother by pre-designating individuals to learn the rules and play together ahead of time, so that those individuals can then seed gameplay groups during the activity.

The second most prominent critique was that the game did not have enough educational value (classroom: 4/14, non-classroom: 5/8). As previously mentioned, many of the non-classroom educators reported on the experience wherein they vetted the game, and chose not to use it in their classroom. Control-Alt-Hack may not be suitable for all educational contexts, but its educational value can be increased by pairing it with or using it to bootstrap a level-appropriate supplementary activity, as done by 5 of the classroom educators.

The third most common critique—and the only other critique expressed by educators who used the game in the classroom—was that the game took too long to play. Control-Alt-Hack may not be suitable for all class formats and in all contexts; however, from observation and anecdotes we tentatively find that having more than 4 players in a game significantly extends the duration of gameplay; we therefore suggest staying below 5 players in a game. Responses indicate that there is some value in playing a short game, even if players do not have time to finish; educators who provided as little as 40 minutes of time to play (E16-classroom) reported some positive results. Additionally, gameplay is somewhat modular, with logical periodic stopping points; if players are already familiar with gameplay, then individual rounds are of manageable lengths.

Table 5. Classroom-use and non-classroom-use responses as to whether or not educator would use the game again, and whether or not the educator would suggest the game to others.

	Educator	Would Use Again	Would Suggest to Others
Classroom	**E1-classroom**	Yes	Yes
	E4-classroom	Yes	Yes
	E6-classroom	No	Yes
	E7-classroom	Yes	Yes
	E8-classroom	No*	Yes
	E9-classroom	Yes	Yes
	E10-classroom	Yes	Yes
	E12-classroom	No**	Yes
	E13-classroom	Yes	Yes
	E14-classroom	Yes	Yes
	E16-classroom	Yes	Yes
	E17-classroom	No	No
	E18-classroom	Yes	Yes
	E19-classroom	Yes	Yes
Non-Classroom	**E2-ACM**	Yes	Yes
	E3-vetting	No	No
	E5-no-play	No	No
	E11-checkout	Yes	Yes
	E15-vetting	No	No
	E20-vetting-didn't-read	No	No
	E21-lunch	Yes***	Yes***
	E22-vetting	No	No

*Might instead use with high school students or interns.

**Not in class because of time constraints. Maybe as an out-of-class exercise.

***Yes, but only with additional material, and dependent upon going over it a few more times to understand how to incorporate.

6.3 "Would Use Again"

To serve as an overall assessment of the game's usefulness, we asked educators the following questions on the surveys:

> *Would you use Control-Alt-Hack again in your classroom? Why or why not?*
>
> *Would you suggest Control-Alt-Hack to others? Why or why not?*

Educators' responses are given in Table 5. Overall, the results are promising. 13 of the 14 educators who used the game in their classrooms reported that they would suggest the game to others, and 10 of them reported that they would use Control-Alt-Hack again. E8-classroom responded that they would not use the game with those who already had some familiarity with the subject, but might with high school students or interns, and E12-classroom clarified that they would not use the game again in class due to time constraints, but might as an out-of-class exercise; for both of these educators, this suggests that they still find merit in the game, even if it is not an appropriate match for their instructional needs. E17-classroom indicated elsewhere in responses that the game did not contain sufficient educational content (Table 3), so we surmise that is why they will not use the game again or recommend it to others. As mentioned in the previous section, the educational level of our game was an intentional decision related to our Primary Audience and Exposure Goals (Section 2).

For the non-classroom experiences with the game, 5 of the educators were playing the game with other instructors, friends, graduate students, or staff to vet its use, and did not subsequently report on using the game in their classrooms. The remaining 3 educators would use the game again and would suggest it to others (E2-ACM, E11-checkout, and E21-lunch). E21-lunch clarified that they might use the game again and recommend it to others, but only with supplementary educational material and after further consideration. These three scenarios—an extracurricular club, a checkout, and a staff lunch—are highly aligned with the social, ad hoc interaction model supported by choosing to create a recreational game.

6.4 Reaching New Audiences

Interestingly, 2 of the 14 educators who used Control-Alt-Hack in their classrooms reported that they would not have covered similar security material in any other format. An additional educator gave this response, but was teaching a computer security course (E12-classroom), so this response may have been in error or a misinterpretation of our intention when posing the question (*If you had not used Control-Alt-Hack, would you still have covered the material?*); it is also possible that the educator intended to convey that they would not have covered topics included in the game such as physical security or cyber-physical security. We are conservative and count this response as an error. If the educators in the remaining contexts would not have covered

	Participant quote	Goal Mappings
A	"Slightly. I was aware that active testing and debugging are needed to improve security + add to innovation, but the reminder was helpful. The game led me to think about some aspects of modern life I don't usually consider."	Awareness #2: Breadth of Technologies
B	"I have to be honest and say that I've never heard of a "white hat" hacker before. I've always associated hackers with a negative term. Computer security consists of a lot more tasks than I had at first thought it had. Computer security applies to a lot of areas, like cars and phone apps, which I hadn't thought of."†	Awareness #2: Breadth of Technologies
C	---	
D	---	
E	"Not much. There was stuff such as not leaving laptops or usb drives out where others can get at them that I had known about but never gave much thought to before."	Awareness #3: Creativity of Adversaries
F	"Little bit w/ thinking of different scenarios like the small level computer hacking. In general I think of bigger hacking crimes when I think of hacking."	Awareness #1: Importance/Impact of Security* Awareness #2: Breadth of Technologies*
G	"No except that hacking might be fun – to use the knowledge to help solve a problem."	Perception #2: Professional Opportunities*
L	---	
M	"Yes. I didn't give much thought to it before or how many different ways it could be approached."	Awareness #3: Creativity of Adversaries*
N	"No, except that its [sic] very complicated."	Awareness #3: Creativity of Adversaries*
O	"Certainly lightens the mood for my outlook on C.S. and sheds some light for understanding reality of tasks involved."	Perception #1: Counter-Stereotype Awareness #3: Creativity of Adversaries*

†This was actually in response to the question: *Now that you've performed the activity, what do you think of when you think of computer security? (This may or may not have changed.)*

*These goals are only potentially implicated in the response. We invite the reader to perform personal interpretations.

Table 6. User responses and mappings to our design goals. Participants with no quotes did not provide evidence indicating that their awareness or perception of computer security changed. Project goals are fully articulated in Section 2.1.

comparable security material, however, then these classrooms represent instances where the game can serve to increase security awareness, presumably precisely because of its non-traditional format:

- E6-classroom: 75 high school students in a Computer Science course with some prior informal security experience.
- E9-classroom: 60 high school students in a Computers and Information Technology course with prior educational security experience.

This exposure of individuals in our Primary Audience (Section 2.3) to more security content than they might otherwise have been exposed is an indication of success.

7. USER STUDY RESULTS

With the educator surveys—the primary evaluation method of Control-Alt-Hack in this study—we gained the valuable perspectives of informed and expert individuals, as well as secondhand access to a large population of students. We also, however, wished to more directly study individuals' experiences with the game, and therefore performed a supplementary user study. We primarily simulated the experience of individuals of varying backgrounds picking up and playing the game in a non-classroom-setting. Section 5.2 provides background on the participants.

In performing the user study, we received participant responses that indicated that—at least in the short term—we are increasing or reinforcing participants' awareness and/or improving their perception of computer security and computer science, as per our Awareness and Perception Goals articulated in Section 2.1.

Table 6 presents participant quotes in response to the prompt on the post-gameplay questionnaire:

> *After performing the activity, some people say that their perception of computer security has changed, while others don't feel that it has changed much at all. Would you say that your perception of computer security has changed? If so, how?*

8 of the 11 participants provided responses which gave some indication that their awareness of computer security issues increased or their perceptions about the field were changed. Interestingly, even though some of these participants responded that their perception of computer security had not changed (2 out of the 8), they proceeded to elaborate and provide qualitative evidence that they were engaged with one of our learning goals. For the remaining 3 participants, none of their responses suggested that their awareness had increased or that their perceptions had changed. Some participants (3/11) supplied critiques on the game; however, the sentiments in those critiques are covered by the educators' critiques (Section 6.2), and we do not discuss them further here.

There is a range of participant responses present even in our small sample size. The Goal Mappings column provides a loose mapping from the participant's response to our project goals; the process is subjective, and we invite readers to interpret different mappings from participant responses to project goals.

The project goals are fully articulated in Section 2.1, but they might be paraphrased and shortened as follows:

- Awareness Goal #1: Importance/Impact of Security;
- Awareness Goal #2: Breadth of Technologies;
- Awareness Goal #3: Creativity of Adversaries;
- Perception Goal #1: Counter-Stereotype; and
- Perception Goal #2: Professional Opportunities.

All of the goals appear at least once in Table 6, suggesting that we have had some success in crafting the game to touch upon the issues in question.

8. REFLECTIONS

We take this opportunity to discuss some of our reflections from going through the process of creating, distributing, and evaluating a computer security-themed tabletop card game for the purpose of promoting computer security awareness and education.

Physical Games in Security Education. There is a long history of using games in education (Section 9), and our work further attests to the benefits and value of using a game—and in our case, a physical game—in educational settings. Such games do not always match the needs of the relevant educators, but when they do match, they can provide valuable catalysts for engaging students and achieving certain learning objectives—in our case, our Awareness and Perception goals.

Game Mechanics Tradeoffs. Our main observations concern the selection of game mechanics. Overall, working with pre-existing mechanics was a positive experience, especially given our lack of expertise in the area. We wish to re-emphasize, however, the fact that mechanics directly dictate or heavily influence gameplay properties, including: how long it takes to learn to play a game; how long games take to play; the replay value of a game; and the ability to form diverse strategies. Additionally, we were particularly interested in how much textual content could be inserted into the game. These variables, which ultimately contribute to an (unclearly defined) function that dictates gameplay enjoyment, are somewhat interdependent. For example, the replay value of a game is somewhat dictated by how much the game facilitates strategizing; a game's available strategies, in turn, have some relationship with the complexity of the game's rules, which directly affects the amount of time that it takes to learn a game, and partially affects the amount of time that it takes to play a game.

While these gameplay properties do not have clean-cut direct or inverse relationships, they nonetheless impact one another. When choosing or creating gameplay mechanics, sometimes tradeoffs will be necessary. It is critical to prioritize these properties in order to attempt to achieve an optimal fit.

Communication and Representation. One of our takeaways from the educator surveys was the relative importance of communicating to educators the exact nature of the game that we were distributing. While we did distribute cover letters with shipped games, they were insufficiently precise regarding the nature of the game. We never intended to design a game to teach penetration testing methods. Educators have a number of responsibilities, and may be too busy to fully vet a game before its use; it is therefore critical to provide as much information as possible regarding the nature of a game and its intended usage scenarios.

Graphic Design and Illustration. While we did not attempt to directly measure the contribution of the aesthetics of the game to achieving our goals, we do not wish to suggest its irrelevance by eliminating it from the discussion. From observation, we can comment that the graphic design, illustration, and production quality of the game seem to have a large effect at least on its initial reception. Perhaps the most poignant repeated comment that we have received upon presenting the game to others is, "It's like a real game!" The difference between these individuals' apparent expectations and their reaction to Control-Alt-Hack is an implicit commentary on their expectations regarding "educational games." Further study could help place the relevance of game aesthetics in the context of overall success.

9. RELATED WORK

We separate our discussion of related work into work on commercial games and games created more as research endeavors.

9.1 Commercial Games

Previous commercial tabletop card games dealing with computer security include games such as Fantasy Flight Games' *Android: Netrunner*, published in 2012, and Steve Jackson Game's *Hacker*, published in 1992 (now out of print). We believe that our contribution is distinct in several ways. First, we take many opportunities to ground our card contents in a variety of current technologies and actual attack threats (see Section A.1 and Table 7 in Appendix). While this means that Control-Alt-Hack is at risk of becoming outdated, this also means that it is particularly topical. Second, while these games undoubtedly helped—and continue to help—attract people to computer science and computer security, they portray hacking—and hackers—in the style of a particular niche (although compelling) subculture. We chose, primarily via graphic design and illustration choices, to embrace a more non-traditional hacker "tone" in the hopes of connecting with a slightly different audience. Third, since we created our card game specifically with awareness goals in mind, we are also contributing an evaluation of our game in education contexts.

9.2 Games in Research

Gondree et al. [11] gives an overview of some of the benefits of using casual games to impart modest security information; they reference Klopfer et al.'s [14] five freedoms essential to play, and reinterpret those freedoms as mapping to the adversarial, exploratory aspects of computer security.

[d0x3d!] is a tabletop board game designed to casually introduce a wide audience to some of the terminology and adversarial thinking that is involved in network security [8]. *Exploit!* is a card game that is primarily intended for entertainment for the security audience, not education [5]. *Elevation of Privilege* [18, 27], *Protection Poker* [33], and *OWASP Cornucopia* [20] are meant to help train and augment threat modeling and risk assessment in software development.

CyberCIEGE [4] and CyberProtect [30] are electronic games that have players act as network administrators who must utilize limited resources to manage overall network risk.

There are a variety of Capture-the-Flag competitions (e.g., [6, 21]), which are competitive and engaging ways to promote or simulate offensive security. There are also some defensive competitions, such as the Collegiate Cyber Defense Competition [19].

Educational research communities have looked at a variety of aspects of using games in education: for example, making educational games adapt to skill level [1], using game development as a vehicle for programming assignments [24], using games to teach specific topics such as computer ethics [2], or using games to teach how to detect phishing emails [25]. We stress, however, that educational games are used to teach a variety of topics beyond computer science or computer security, such as mathematical fractions (e.g., [3]) or algebra (e.g., [31]).

In the context of security education research, but not in the context of games, there have been numerous explorations of

methods for helping students learn the technical skills necessary to protect computer systems against attackers (e.g., [17, 32]).

10. CONCLUSION

In this paper we presented the design and evaluation of Control-Alt-Hack, a card game for increasing computer security awareness. Our goal was to generate awareness of security issues and improve the accuracy of people's perception of computer security as a discipline and career choice. Critically, we traded some technical complexity in the topics discussed in exchange for increased engagement: put another way, we set out to create a game that players could find inherently fun, from which they might learn incidentally in the course of enjoying the gameplay.

Our evaluation of the game, primarily derived from the experiences of 22 educators representing over 450 students, suggests that we accomplished our goals. Educators who used the game in their classrooms overwhelmingly indicated that they would suggest the game to others, while the majority reported both that they would use the game again and that students enjoyed the game and experienced increased security awareness. 2 educators teaching non-security computer science courses would not have taught the material without the game. A supplementary evaluation with 11 users suggested that even among a small number of participants, their reactions are aligned with a number of our goals in creating the game.

We view these results as a strong signal suggesting that our game represents an effective model for disseminating ideas and encouraging interest in computer security. We hope that our process for selecting mechanics, designing content, and evaluating our effectiveness is informative to those wishing to undertake similar endeavors, and we hope that further research will explore the usage of educational or awareness-raising games to engage and inspire.

11. ACKNOWLEDGMENTS

This work was supported in part by Intel Labs, an Intel PhD Fellowship, the ACM Special Interest Group on Computer Science Education, and the US National Science Foundation (NSF) under awards CNS-0846065 and CNS-1247216. Any opinions, findings, and conclusions or recommendations expressed in this article are the authors' and don't necessarily reflect the views of the funding agencies.

Tamara Denning and Tadayoshi Kohno are founders and equity owners of RGB Hats, LLC, a private, for-profit company which has licensed the subject technology from the University of Washington. This research is subject to the conditions of a financial conflict of interest management plan established by the University of Washington.

We thank everyone who playtested, provided feedback, or otherwise helped improve the game. We thank those who graciously lent us their names and biographic details: Deborah Alterman, Mike Clarke, Alexei Czeskis, Karla Danson, Iva Dermendjieva, Miro Enev, Roxana Geambasu, Sidhant Gupta, Dan Halperin, Melody Kadenko, Karl Koscher, Gabe Maganis, Cynthia Matuszek, Temitope Oluwafemi, Franzi Roesner. We thank Steve Jackson for licensing his game and providing feedback, and Deborah Alterman and Mike Clarke at the University of Washington's Center for Commercialization for helping obtain the license. We also thank and acknowledge the following people: Gravity Creative (Graphic Design), Rob Kelly (Character Illustrations), Web Design / Development (Thomas Winegarden), Juliet Fiss (Product Photos), and Tina Wegner (Production Manager).

12. REFERENCES

[1] E. Andersen. Optimizing Adaptivity in Educational Games. Foundations of Digital Games, 2012.

[2] B. Brinkman. The Heart of a Whistle-blower: A Corporate Decision-Making Game for Computer Ethics Classes. SIGCSE Technical Symposium, 2009.

[3] Center for Game Science. Refraction. http://centerforgamescience.org/portfolio/refraction/.

[4] The Center for Information Systems Security Studies and Research, Naval Postgraduate School. CyberCIEGE. http://cisr.nps.edu/cyberciege/.

[5] Core Impact. Exploit! http://www.coresecurity.com.

[6] DEF CON. DEF CON Capture the Flag. https://www.defcon.org/html/links/dc-ctf.html.

[7] T. Denning, C. Matuszek, K. Koscher, J. R. Smith, and T. Kohno. A Spotlight on Security and Privacy Risks with Future Household Robots: Attacks and Lessons. Ubicomp, 2009.

[8] [d0x3d!]. http://www.d0x3d.com.

[9] S. Drimer and S. J. Murdoch. Keep Your Enemies Close: Distance Bounding Against Smartcard Relay Attacks. USENIX Security, 2007.

[10] A. J. Feldman, J. A. Halderman, and E. W. Felten. Security Analysis of the Diebold AccuVote-TS Voting Machine. Electronic Voting Technology Workshop, 2007.

[11] M. Gondree, Z. N.J. Peterson, and T. Denning. Security through Play. *IEEE Security & Privacy*, 11(3), 2013.

[12] G. Gu, J. Zhang, and W. Lee. BotSniffer: Detecting Botnet Command and Control Channels in Network Traffic. Network and Distributed System Security Symposium (NDSS), 2008.

[13] M. Hicks, M. Finnicum, S.T. King, M. Martin, J.M. Smith. Overcoming an Untrusted Computing Base: Detecting and Removing Malicious Hardware Automatically. IEEE Symposium on Security and Privacy, 2010.

[14] E. Klopfer, S. Osterweil, and K. Salen, Moving Learning Games Forward: Obstacles, Opportunities, and Openness. The Education Arcade, 2009.

[15] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage. Experimental Security Analysis of a Modern Automobile. IEEE Symposium on Security and Privacy, 2010.

[16] C. Li, A. Raghunathan, N.K. Jha. Hijacking an Insulin Pump: Security Attacks and Defenses for a Diabetes Therapy System. Healthcom, 2011.

[17] P. Mateti. A Laboratory-Based Course on Internet Security. SIGCSE Technical Symposium, 2009.

[18] Microsoft. Elevation of Privilege. http://www.microsoft.com/security/sdl/adopt/eop.aspx.

[19] National Collegiate Cyber Defense Competition. http://www.nationalccdc.org/.

[20] OWASP. OWASP Cornucopia Ecommerce Website Edition. https://www.owasp.org/index.php/OWASP_Cornucopia.

[21] PlaidCTF. http://play.plaidctf.com.

[22] A. Rabkin. Personal Knowledge Questions for Fallback Authentication: Security Questions in the Era of Facebook. Symposium On Usable Privacy and Security (SOUPS), 2008.

[23] F. Roesner, T. Kohno, and D. Wetherall. Detecting and Defending Against Third-Party Tracking on the Web. USENIX Symposium on Networked Systems Design and Implementation (NDSI), 2012.

[24] K. Seaborn, M. S. El-Nasr, D. Milam, and D. Yung. Programming, PWNed: Using Digital Game Development to Enhance Learners' Competency and Self-Efficacy in a High School Computing Science Course. SIGCSE Technical Symposium, 2012.

[25] S. Sheng, B. Magnien, P. Kumaraguru, A. Acquisti, L.F. Cranor, J.Hong, and E. Nunge. Anti-Phishing Phil: The Design and Evaluation of a Game That Teaches People Not to Fall for Phish. Symposium on Usable Privacy and Security (SOUPS), 2007.

[26] B. Shimanovsky, J. Feng, and M. Potkonjak. Hiding Data in DNA. Information Hiding, 2002.

[27] A. Shostack. Elevation of Privilege: Drawing Developers into Threat Modeling. Microsoft Technical Paper, 2012.

[28] Steve Jackson Games. http://www.sjgames.com.

[29] L. Sweeney. Weaving Technology and Policy Together to Maintain Confidentiality. *Journal of Law, Medicine & Ethics*, 25(2-3), 1997.

[30] US Department of Defense. CyberProtect. http://iase.disa.mil/eta/cyber-protect/launchpage.htm.

[31] WeWantToKnow. DragonBox. http://www.dragonboxapp.com/.

[32] G. White and G. Nordstrom. Security Across the Curriculum: Using Computer Security to Teach Computer Science Principles. National Information Systems Security Conference, 1996.

[33] L. Williams, A. Meneely, and G. Shipley. Protection Poker: The New Software Security "Game." *IEEE Security & Privacy*, 8(3), 2010.

[34] E. Wustrow, S. Wolchok, I. Goldberg, and J. A. Halderman Telex: Anticensorship in the Network Infrastructure. USENIX Security, 2011.

A. APPENDIX

A.1 Card Topics and Research Papers

Table 7 gives some examples of Mission cards that were inspired by research results. These examples list one relevant research project per Mission; we acknowledge that other examples exist and that this is not a comprehensive list.

A.2 Educator Survey Contents

The questions asked in the online survey distributed to educators are given below:

1. How did you use Control-Alt-Hack®? Please describe the activity.
2. How long did the activity take?
3. Were there any written or oral components that students turned in or presented as part of the activity? If so, please describe.
4. Did you present or assign any supplementary materials? If so, please describe.
5. What, if anything, worked well with the activity?
6. What, if anything, would you do differently if you were to do the activity again?
7. How would you describe students' level of enjoyment and/or engagement with the activity?
8. How would you describe students' level of learning with the activity? On what particular topics was their learning focused?
9. Why did you choose to use Control-Alt-Hack® in your classroom?
10. Would you use Control-Alt-Hack® again in your classroom?
11. Why or why not?
12. Would you suggest Control-Alt-Hack® to others?
13. Why or why not?
14. If you had not used Control-Alt-Hack®, would you still have covered the material?
15. Did you cover the material using another (additional) method?
16. If applicable: What additional method did you use to cover the material?
17. If applicable: How would you compare these two methods (Control-Alt-Hack® and the additional method) of covering the material? What are the pros of each? What are the cons?
18. If applicable: If you had not used Control-Alt-Hack®, what alternative method would you have used to cover the material?
19. If applicable: How would you compare these two methods (Control-Alt-Hack® and the alternative method) of covering the material? What are the pros of each? What are the cons?

Card Title	Card Topic	Example Inspirational Research
[CENSORED]	Working on steganographic anti-censorship software	[34]
A Healthy Dose of Security	Consulting to improve the security of an insulin pump	[16]
A Rash Decision	Cross-correlating data sources to de-anonymize medical records	[29]
Cookie-Blocked	Writing a web browser extension to circumvent tracking cookies	[23]
Crash Test Dummy	Hacking an automobile	[15]
E. coli Cryptography	Implementing cryptography via synthetic biology	[26]
Hay Baby, Hay Baby, Hay	Demonstrating that a dating site has insecure password recovery questions	[22]
Here's Looking at You, Kid	Analyzing the security of a WiFi-enabled, webcam-equipped toy robot	[7]
I'd Tap That	Pen testing the security of a contactless payment system	[9]
Mr. Botneto	Measuring a botnet's growth, then reverse engineering the C&C algorithm	[12]
One Hacker, Won Vote	Pen testing an electronic voting machine	[10]
Trojan Protection	Looking for backdoors in the outsourced production of hardware	[13]

Table 7. Example Mission card titles, topics, and example research that inspired them.

20. What is the subject of your class?
21. What is the class format (e.g., MWF 50-min 10-week course, 2-hour training seminar, etc.)?
22. How many students participated in the activity?
23. What is the level of the students in your class?
24. What is the (approximate) level of student experience with computer science and/or computer security?
25. Is there anything else that you would like to add that we have not addressed?

A.3 Educator Survey Coding Disagreements

We include all 11 cases where the primary coder's and the secondary coder's coding results did not agree. The examples are given below, along with the quotes from the survey which were primarily responsible for the distinction between the coding results.

As mentioned in Section 5.1, except for one case in which the secondary coder misread the data and coded an error (Case 6), the primary coder's results—the results reported in the paper—always represent the stricter of the two viewpoints. That is, in the Results Section we report the upper bound on our interpretation of the critiques to the game and the lower bound on the game's role in engagement and awareness.

A.3.1 Positive Role

Below we provide information on the cases where the primary and reliability coder disagreed when coding the positive role(s) that the game performed. In all cases, the reliability coder coded the game as playing the role, while the primary coder did not. Quotes that led the reliability coder to code the game as "Social / Engagement" or "Awareness" are given below.

Social / Engagement:

- Case 1 (E11-checkout). *"It was a 7/10. the students enjoyed it but the word did not spread around and ignite students."*
- Case 2 (E12-classroom). *"Students reported that they enjoyed the game, but that the hour twenty was pushing the limit."*
- Case 3 (E16-classroom). *"The kids were all engaged with the game and playing it through." "Would rate it 8/10."*
- Case 4 (E22-vetting). *"They seemed engaged, although not so much that I would expect they would play it for fun."*

Awareness:

- Case 5 (E21-lunch). *"Brought up some terminology that staff and IT had not heard before. "pwned" :-)"*

A.3.2 Critiques and Tradeoffs

Below we provide information on the cases where the primary and reliability coder disagreed when coding critiques made to the game. In all cases except one (Case 6, coded in error), the primary coder coded the educator as offering that critique, while the reliability coder did not. Quotes that led primary coder to code the critique are given below.

Takes a long time to learn:

- Case 6 (E10-classroom): The disagreement was due to the reliability coder misreading the response. The reference to the presentation and the gameplay taking too long together was a reference to instructor's syllabus content, not the video introducing the game's rules.

Takes a long time to play:

- Case 7 (E1-classroom): [*Q: What, if anything, would you do differently if you were to do the activity again?*] *"have more play time during the topic"*

Not enough fun:

- Case 8 (E22-vetting): *"They seemed engaged, though not so much that I would expect them to play it for fun"*

Not enough educational value:

- Case 9 (E2-ACM): *"Learning was not so much learned throughout the game, but it did pose interesting questions that the students were curious about"*
- Case 10 (E3-vetting): *"I worry the card game will seem like a card game"*
- Case 11 (E12-classroom): *"Most students reported a low level of learning, the topics that were reported positively were presenting the students with real world context for what they were learning"*

A.4 Control-Alt-Hack-themed Assignments

5 of the 14 educators who used Control-Alt-Hack in the classroom reported using a custom assignment in concert with the game, as described below:

E4-classroom (12 undergraduate students with little or no prior security experience): Students were asked to identify at least three tasks from Mission cards that seemed interesting. A follow-up exercise may be to have them research real-life situations where the theme of one of the tasks is involved.

E7-classrooom (56 undergraduate students in a Cyber-Security and Information Assurance course, with little or no prior security experience): Students were asked to take a scenario from a card and craft a research paper inspired by the scenario.

E10-classroom (65 high school students in a Game Design course with little or no security background): Students were required to answer essay questions about the game and how it is put together. Optional questions asked about the game's relation to the IT industry and hacker culture.

E12-classroom (22 undergraduates in a Computer Security Course with prior educational security experience): Students wrote one to two paragraphs discussing the activity.

E18-classroom (30 undergraduate students in a Fundamentals of Information Security course with a variety of security backgrounds). Two questions were asked before the game: (1) *What does information security mean to you?*; and (2) *What skills are required in white-hat hacking?* Two questions were asked after the game: (1) *Did your answers to the previous questions change as a result of the game—and if so, how?*; and (2) *As a result of the game, did you discover any threats you hadn't considered—and if so, what?*

While some of the above assignments are similar to activities we propose on our web site (http://www.controlalthack.com), some of the assignments are original and demonstrate an interesting integration of the game into existing course plans and practices.