Control-Alt-Hack™: A Card Game for Computer Security Outreach, Education, and Fun

Department of Computer Science and Engineering
University of Washington
Technical Report UW-CSE-12-07-01
July 12, 2012

Tamara Denning
tdenning@cs.washington.edu

Tadayoshi Kohno
yoshi@cs.washington.edu

Adam Shostack
adam@homeport.org

ABSTRACT

A general lack of awareness about computer security contributes to the insecurity of new consumer technologies. We seek to increase people's prioritization of computer security and their understanding of the variety of attacks and technologies that can be vulnerable to compromise. We work towards this goal via fun: more specifically, via a recreational tabletop card game where people play as white hat hackers. In this paper, we describe our goals and experiences in creating this card game. We licensed a game mechanic from a hobbyist game company, worked with graphic designers and illustrators, and rewrote card text to make the game about working as a computer security professional. We discuss the possibilities for expanding the educational benefits of this game, both in and out of the classroom. We conclude by inviting others to engage in this outreach space by creating games or other enticing and novel artifacts to increase awareness and appreciation of the complexities and impact of computer security on people's daily lives.

1. INTRODUCTION

Working in computer security and privacy is, in many ways, a Sisyphean task. Consumer products repeatedly enter the market with little or no attention paid to computer security. While some domains—such as desktop operating systems and email—have registered in the public consciousness as areas that require active security intervention, many aspects of technology escape serious security scrutiny. That is part of the reason why new technologies frequently re-visit familiar security problems; for example, researchers have compared the security in today's embedded systems to the security of desktop machines in the mid-1990s, before the desktop computing industry began to systematically analyze and mitigate security risks [3]. We argue that this situation is due at least in part to a lack of security awareness.

Part of this problem is the insufficient security knowledge within the technology workforce. Technology creators—developers, engineers, designers, and managers—will always outnumber security specialists. Unless these people are explicitly exposed to security training during their academic education or on-the-job-training, they may not have the skills to implement secure systems or the foresight to consult an expert.

Another cause of technology insecurity is a lack of appropriate incentives and market pressure. Users do not always hold security as a priority, and therefore may not make tradeoffs to improve their security practices or purchase more secure products. Even when consumers do place a premium on being secure, they are generally not aware that computer security risks apply to all computing technologies—not just laptops, desktops, and the Web. An increased user demand for security would give businesses stronger reasons to invest in security policies, mechanisms, and personnel.

Given the benefit that would be offered by an increased awareness of computer security, we argue that a valuable and important goal is to develop new methods for increasing awareness and understanding of important issues in security: namely, (a) an appreciation for the role of computer security in technology; (b) an understanding of the breadth of technologies that might be affected by computer security risks beyond just laptops, desktops, and Web servers; and (c) the diversity and creativity of ways in which attackers might try to compromise systems.

In the spirit of these goals, we propose leveraging fun and entertainment to help spread security awareness; more specifically, we propose leveraging games. We describe here one such game: *Control-Alt-Hack*™, a tabletop card game where 3–6 people play as white hat hackers in a security consulting company. Our goal is explicitly not to create an educational game in the traditional sense of a game with a pedagogic goal; instead, we created a game that prioritizes fun and engaging gameplay over educational messages. To this end, we licensed a game mechanic from Steve Jackson Games [9] and re-skinned the cards' textual content, illustrations, and graphic design to touch upon the variety of scenarios and technologies implicated in breaches of computer security. Our hope is that, by playing and sharing this game, a diverse audience of people might gain an increased awareness of—and appreciation for—computer security needs and challenges.

More broadly, we hope that this work also serves as a broader call for additional work on increasing security

awareness, with the ultimate goal of helping improve the security of technologies entering the marketplace.

2. GOALS

We now describe our concrete objectives for increasing the awareness of security issues among non-experts. We also describe our additional outreach and educational goals.

2.1 Target Audience

In order to articulate our goals, it is necessary to establish the target audience whom we wish to reach. While we would ideally like a game that strongly appeals to everyone—and hence would help impart security awareness on a very large audience—it is more manageable (and more realistic) to focus on targeting a specific demographic. Below, we define our primary and secondary outreach targets.

Primary Audience. Our primary target audience is people with an affinity for computer science and engineering but without 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 Audience. To the extent that it is possible, we also try to make our game as appealing and educational as possible to a broader demographic, including: high school and undergraduate students generally interested in Science, Technology, Engineering, and Math (STEM subjects), but not necessarily computer science; more experienced computer scientists later in their careers; and the broader public. Sometimes catering to one demographic means placing less emphasis on another. For example, some game content might be funny and enjoyable to 20-year-olds but have less meaning to 55-year-olds.

The Security Audience. We have a third, specialized audience: computer security researchers and practitioners. These people will likely have little to learn from our game. Nevertheless, we hypothesize that if they find the game entertaining and value its educational properties they might then become evangelists for the game and help with further dissemination. In any case, we have to ensure that our game is technically correct and found up-to-standard by the computer security community.

2.2 Outreach Goals

Having articulated the audience whom we wish to reach with our card game, we now describe our computer security awareness and education outreach goals.

Awareness Goals. 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 objective includes the below sub-goals:

1. To impart an understanding of the importance of computer security, and the potential risks with inadequate security safeguards.
2. To convey 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 consumer technologies and cyber-physical systems.
3. To highlight the diversity of potential threats that security designers must consider, the creativity of attackers, and the challenging nature of building secure systems.

Technology innovations bring many positive benefits and we believe that it is important for security risks not to overshadow those benefits. Our fourth primary goal is:

4. To disseminate the idea that technologies can have both benefit and risks.

Secondary Goals: Perception Goals. Since the game will hopefully be played by people outside of the core computer science discipline (our Secondary Audience from Section 2.1), we also view this game as an opportunity to help address gender imbalance issues and negative stereotypes sometimes associated with computer science and computer security. This objective includes the below sub-goals:

1. To work against negative or dissuasive stereotypes about people in these fields, and to allow all players to associate with one or more of the characters, and envision themselves in the field
2. To highlight the variety of professional and personal opportunities available to people with these skills.

We also seek to use the game as an opportunity to clarify public perceptions of computer security, including:

1. To help reclaim the connotation of the word "hack" as a creative and exploratory activity, rather than a destructive one.

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.

3. GAME DESIGN

Our outreach goals, defined in Section 2, led us to make a number of decisions about the basic format of our game. First, due to the Exposure Goal, we decided to focus on creating a game that is fun to play and that has incidental educational value, in the hopes of exposing a large number of people to a modest amount of information. This is in contrast to *educational games*, which are more explicitly focused on teaching a topic and therefore deliver a larger amount of information to a more captive audience.

Second, we decided to create a physical, tabletop card game instead of an electronic game. This was to accommodate the playing of the game in social settings, which is intended to increase game enjoyment and encourage discussion among players; group discussion facilitates cooperative learning.

3.1 Choosing Mechanics

Since we are not experts in designing game mechanics, we chose to license game mechanics from a pre-existing game and re-skin all game content. Doing so also allowed us to

Figure 1. From left to right: (a) a Hacker character card with skills, special abilities, and personal description; (b) a Mission card based on security for cars—broadly deployed platforms with extensive embedded hardware; (c) a Mission card incorporating network intrusion and humor; (d) a Mission card on misconceptions about hacking.

forgo the otherwise necessary step of playtesting the mechanics—a time-consuming process that would otherwise be necessary to ensure that the game mechanics are balanced. We did playtesting to review our contributions to the game, which we discuss in Section 3.4.

We explored the rules and mechanics of a number of games available for sale in gaming stores. Although this selection does exclude some mass-market games, we judged that the hobby game market offered a larger selection of games with sufficient complexity to support our desired goals.

We licensed the *Ninja Burger* mechanic from Steve Jackson Games [9], which is best known for the *Munchkin* card game and the *GURPS* roleplaying system. We describe the re-skinned game premise in the next subsection.

3.2 Brief Overview of Game

The following is the game premise as described in our instruction manual:

You and your fellow players work for Hackers, Inc.: a small, elite computer security company of ethical, white hat hackers that perform security audits and provide consultation services. Their motto? "You Pay Us to Hack You."

Figure 1, Figure 2, and Figure 3 show examples from the game's 156 cards. There are four card decks: Hacker cards, Mission cards, Entropy cards (which include Bag of Tricks cards and Lightning Strikes cards), and Attendance Cards.

Each player is given a Hacker card. Gameplay is centered around Missions—a variety of audit jobs and pro bono work that require the selective application of hacker skills: Hardware Hacking, Software Wizardry, Social Engineering, Network Ninja, Cryptanalysis, Forensics, and others. The character's skill levels and player's dice rolls determine whether the player succeeds or fails at a mission. Players can increase their skill levels by purchasing useful items (Bag of Tricks); opponents can hinder player's efforts to complete a mission by playing Lightning Strikes on them. Mission successes and failures lead to the gain and loss of Hacker Cred. Players win the game by accruing enough Hacker Cred and becoming the CEO of their own consulting company. The Attendance Cards have a more minor role in game play, and we do not describe them further here.

3.3 Incorporating Goals

During the design process, we needed to re-design both textual and visual game components. In the following subsections we describe our process for incorporating our outreach goals (Section 2) into the game design.

3.3.1 Text

One of our first actions in writing new text was to create a list of the content that we wanted to cover in the cards, in order to meet our Awareness Goals and convey the range and depth of computer security issues. Table 1 lists some of the attack techniques and technologies that we decided to include as topics in the game; we also brainstormed lists of industry sectors, attacker types, and the range of human assets that can be impacted by system breaches. We incorporated these items as much as possible into the game, given other considerations and restrictions.

Figure 2. From left to right: (a) a Mission demonstrating the usage of technical skills for artistic purposes; (b) a Mission describing a social engineering attack on a traditional attack target; (c) a Bag of Tricks card illustrating a particular attack threat (dumpster diving); and (d) a Lightning Strikes card that demonstrates fun technologies.

Other Considerations. Above all, we needed to match card topics to the original game mechanics. For example, consider the "Lights, Camera, Hack!" card shown in Figure 1(d). In the original Ninja Burger game, this was the "Anime Convention" card, which required Disguise and Customer Service skill checks:

Breathe deeply and think of the good karma you acquire by letting these people live.
Disguise at +3: It is only necessary not to look like a REAL ninja. Everything else is simple.
Customer Service: You must not laugh.

When we did a 1:1 mapping from the Ninja Burger skills to our skill set (Hardware Hacking, Software Wizardry, etc.), this card became a blank card that required Cryptanalysis and Social Engineering tasks. The flavor text on this card—as with the rest of the deck—needed to match the given mechanics, and eventually was written as the "Lights, Camera, Hack!" card.

Additionally, given our target audience (Section 2.1), 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. Similarly, we aimed to make card content humorous and enjoyable. We particularly wished to avoid having the cards feel like classroom lectures or academic textbooks.

We partially addressed the Perception and Exposure Goals by incorporating some non-security and non-technical topics into the game. For example, the "eTextiles" card in Figure 2(a) does not deal with a security topic at all, but instead demonstrates the usage of technical skills for an artistic activity. Similarly, the "Hot Tub" Bag of Tricks card (not pictured) gives a Software Wizardry bonus as a result of relaxation: *It may have been expensive at the time, but every time you sit back in your new hot tub and admire the stars, creative inspiration strikes.*

We chose terminology—like calling the characters Hackers and having them win Hacker Cred—to address our last Perception Goal. We similarly designed some cards—such as the "Lights, Camera, Hack!" card from Figure 1(d)—to help clarify common misconceptions about computer security.

3.3.2 Visuals

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

When creating the portrait illustrations, we also addressed the Perception and Exposure Goals by balancing the

Table 1. Examples of some of the (non-mutually-exclusive) attack techniques and technologies that we incorporated into the game content.

Example Attack Techniques	Example Technologies
Cross-correlating data sources	Botnets
Disinformation	Censorship / Anti-censorship
Distractions	Consumer home technologies
Denial of service	Cyber-physical systems
Exploiting unpatched software	Financial systems
Exploiting weak passwords	Medical devices
Inside information	Military systems
Insider threat	Mobile phones
Physical compromises	RFID
Reverse engineering	SCADA / Infrastructure
Sniffing unencrypted data streams	Standards
Social engineering	Tracking / Tracking circumvention
Special equipment	

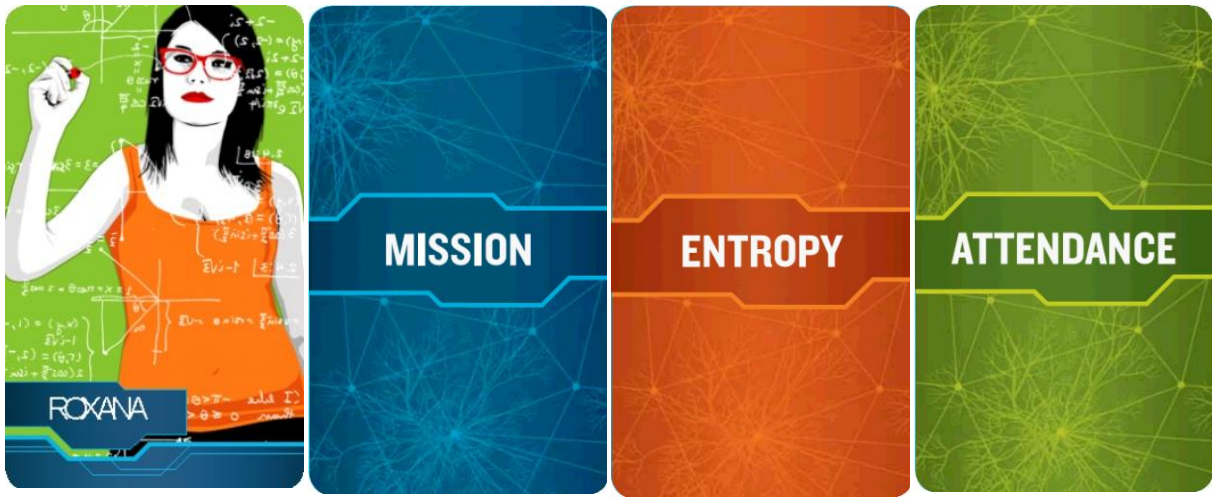

Figure 3. From left to right: (a) the portrait for the Roxana Hacker card (other side shown in Figure 1); (b) the back of the Mission deck; (c) the back of the Entropy deck (the Bag of Tricks and Lightning Strikes cards are part of the Entropy deck); and (d) the back of the Attendance deck.

characters' genders and ethnicities. We took care to show the characters engaging in a variety of hobbies and activities such as dancing, napping, rock climbing, traveling, and cooking, in addition to technical pursuits such as soldering and solving equations.

3.4 Feedback Process

We gathered feedback on iterations of the card deck in order to assess the feasibility of our goals and to gather suggestions for improvements to the game. 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 teacher of high school computer science, now an undergraduate lecturer (n=1); outreach officers (n=3); and assorted non-experts (n=14). These sessions have given us increased confidence that the game has the potential to meet our outreach goals.

4. DISCUSSION

Our focus to date has primarily been on designing, producing, and distributing a card game that meets our awareness and outreach goals for our target audiences. There are, however, a number of ways that we can augment the game itself to expand its educational impact.

Web Site. We are planning to create an accompanying Web site for the game that houses additional material. For example, many of the card contents are based off of actual attacks that have been in the news or academic papers published in conferences. These references—along with accompanying commentary—could be posted on individual Web pages dedicated to cards in the deck; this would help ground the game content in reality. Additionally, the site could provide links to security resources such as best practices for users and developers. Although harder to maintain and moderate, the site could also provide a forum for players to discuss topics with each other. We had additionally explored putting QR codes—with links to the relevant Web pages—on each card but chose not to do so due to space restrictions.

Incorporating into the Classroom. While our focus in designing the game was not on creating a classroom tool, the game could provide value if adopted in the classroom. We envision a number of ways in which the game could be integrated into classroom lessons via accompanying assignments. For example, the instructor might ask students to play the game outside of class. Students would then be asked to pick a particularly interesting technology or threat that arose during game play and research the topic further; our supporting Web site would serve as a good start for information. As another example, after a round of play, an instructor could circulate the entire deck of Mission cards and ask the classroom to pick three Mission cards—and their content—for deeper study.

As additional evidence that our game may be of potential interest to educators, we note that it deals with a number of the Big Ideas and Key Concepts from *Computer Science: Principles*, a proposed high school AP computer science course with broad support [4]. Specifically, we believe that the game touches on Big Idea 1: Creativity (Key Concepts A and B), Big Idea 3: Data (Key Concepts A, B, and C), Big Idea 6: Internet (Key Concept C), and Big Idea 7: Impact (Key Concepts A, B, C, and D).

Crowdsourcing and Community Involvement. We not only believe that our goals are important; we also believe that there is ample opportunity for future innovation addressing those goals. We further believe that games are an excellent vehicle for performing this computer security outreach. In addition to encouraging additional, independent efforts in this space, we also suggest there could be value in crowdsourced efforts around our game. For example, there is an opportunity for community involvement through contributing resources to the Web site or designing

educational exercises centered around the game. There is an even bigger opportunity for community collaboration, however, in the re-skinning of the game's expansion pack: we re-skinned the original game, but there remain 72 additional cards in the *Ninja Burger* expansion deck that have not been re-skinned. The security community could contribute topics for cards or card text, then vote on which cards are the most pertinent or appropriate for an expansion printing.

5. RELATED WORK

There is a body of related work that features security-themed games and educational techniques.

Core Impact's *Exploit!* is a card game that, similar to *Control-Alt-Hack*™, is based off of a hobbyist gaming mechanic and intended for entertainment, not education [5].

Microsoft's *Elevation of Privilege* (*EoP*) card game incorporates more technically advanced content and is meant to augment threat modeling training in industry [8]. Its target demographic is thus both more specialized and in many cases older than our Primary Audience. *EoP* is based off of the Hearts/Spades family of card games, but uses attack threat categories as suits: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege.

CyberCIEGE, from The Center for Information Systems Security Studies and Research at the Naval Postgraduate School, is an educational computer game (not card game) meant to teach IT and network security concepts [2]; players purchase and configure enterprise equipment while under attack from outside threats.

Off the topic of games—but on the topic of uncommon educational techniques—is the use of science fiction prototyping in computer security courses. Science fiction prototyping is a method for using creative writing to encourage students to envision and think deeply about the larger societal and contextual issues surrounding technology deployments and computer security [7].

At a high level, this paper aims to improve computer security for consumer technologies by focusing on computer security outreach. Another clear route to improving the status quo is by integrating computer security education early and deeply into the computer science curriculum. While this game could be incorporated into the classroom, this paper is not focused on education, and is orthogonal to a large body of research on computer security education (e.g., [1], [6], [10]).

6. CONCLUSION AND FUTURE DIRECTIONS

We introduce *Control-Alt-Hack*™, a 3–6 person recreational tabletop card game. We designed the game to be fun to play, but with the underlying motivation of raising security awareness and understanding among those who play it. The game—which involves white hat Hackers using their skills to complete Missions—offers numerous learning opportunities. Each Mission exposes players to a different technology that might be vulnerable to compromise, a creative and possibly surprising attack technique, or an exciting way to use technology or technical skills. Similarly, players may utilize Bag of Tricks cards to augment their skills or play Lightning Strikes cards on other players as part of competitive gameplay; each of these cards can also help the player learn more about the breadth of computer security and the challenges with anticipating adversary actions.

Control-Alt-Hack™ is explicitly not a replacement for rigorous education in computer security, whether in academia or on-the-job. Rather, the central goal is to increase the level of understanding (Awareness Goals) regarding security issues among as broad a collection of people as possible (Exposure Goal). We describe all of our goals and our design strategy for achieving these goals in this paper.

Stepping back, we argue that tabletop games can be a valuable resource in attempting to educate a broad audience about computer security topics. We also argue that there is significant value in raising awareness of computer security issues among technology designers—who might not otherwise receive formal security education—and among consumers, who must make decisions about the purchase and use of these technologies. We believe that both of these outreach areas are very fertile and wish to encourage further work in these spaces.

7. ACKNOWLEDGMENTS

This project was support in part by a gift from Intel Labs, a grant from the ACM Special Interest Group on Computer Science Education, and NSF grant CNS-0846065. We thank Steve Jackson and Elisabeth Zakes from Steve Jackson Games for all their help and assistance, and we thank Steve Jackson Games for letting us license the *Ninja Burger* mechanics. We thank Deborah Alterman at UW C4C for negotiating the *Ninja Burger* license for UW, and we thank Deborah, Matt Barker, and Sarah Hopkins for all their help and assistance throughout this project. We thank Barbara Combs and Huy Cao from Gravity Creative for the graphic designs, and Rob Kelly for the illustrations. We thank Tina Wegner for helping oversee the production of the game. We thank Jordan Weisman and Ray Wehrs for invaluable feedback and guidance during the genesis of this project. And we thank everyone who play tested the game and provided feedback.

8. REFERENCES

[1] S. Azadegan, M. Lavine, M. O'Leary, A. Wijesinha, and M. Zimand. An Undergraduate Track in Computer Security. In *Proceedings of the 8th Annual Conference on Innovation and Technology in Computer Science Education* (ITiCSE '03), 2003.

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

[3] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno. Comprehensive Experimental Analyses of Automotive Attack Surfaces. In *Proceedings of USENIX Security* (USENIX '11), 2011.

[4] Computer Science: Principles. http://www.cs.principles.org.

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

[6] C. E. Irvine, S-K. Chin, and D. Frincke. Integrating Security into the Curriculum. *Computer* 31, 12 (December 1998), 25-30.

[7] T. Kohno and B.D. Johnson. Science Fiction Prototyping and Security Education: Cultivating Contextual and Societal Thinking in Computer Security Education and Beyond. In *Proceedings of the ACM Technical Symposium on Computer Science Education* (SIGCSE '11), 2011.

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

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

[10] B. Taylor and S. Azadegan. Moving Beyond Security Tracks: Integrating Security in CS0 and CS1. *SIGCSE Bull.* 40, 1 (March 2008), 320-324.