2013

Valuing Security by Getting [d0x3d!] Experiences with a network security board game

Gondree, Mark; Peterson, Zachary N. J.

Valuing Security by Getting [d0x3d!]

Experiences with a network security board game

Mark Gondree
Naval Postgraduate School

Zachary N. J. Peterson
California Polytechnic State University

Abstract

We motivate using non-digital games to teach computer security concepts and describe the inspirations driving the design of our board game, [d0x3d!]. We describe our experiences in designing game mechanics that teach security principles and our observations in developing an open-source game product. We survey our experiences with playing the game with students and our plans for supporting the game in and out of the classroom.

1 Introduction

In this paper, we describe our experiences in developing [d0x3d!], a cooperative tabletop game that encodes modest pedagogical objectives intended to expose young people to topics in computer security. We describe our game's goals, the process of integrating mechanics and art design to support informal lessons, and our experiences in releasing [d0x3d!] as an open-source product. We believe [d0x3d!] has the potential to start a dialogue with young audiences about the value of data and to expose students to opportunities as computer security professionals. We have informally play tested [d0x3d!] with over a hundred students, across both secondary and post-secondary education, and report on those experiences.

1.1 Motivation

As a discipline, computer security goes largely ignored in the K-12 curriculum. Looking at computer science more generally, there only 14 states that include CS instruction as part of their education standards [26]. When computer science is taught, it is often as an elective course, in preparation for the advanced placement (AP) exam. The College Board, which develops and administers AP exams, reports that in 2011 a total of 3.4 million AP exams were given, of which only 20,000 were in CS [8]. This is particularly remarkable when compared to other STEM disciplines: over 150,000 AP Biology and 300,000 AP Calculus exams were administered in the same year. Indeed, Computer Science is the only AP exam that has seen a decline over the last ten years.

Perhaps even more troubling, access to a computer science curriculum is unequal, unrepresentative of the nation's demographics and tightly correlated with future careers in CS. Using the demographics of AP CS exam takers as an indicator, only 21% are women and 8% are a recognized minority. This is compared to 49% female and 58% minority across all AP exams [8]. The College Board reports that students enrolled in AP CS are eight times more likely to major in CS [21], while a 2010 Google employee survey showed that nearly all CS majors (98%) reported having exposure to CS prior to college, compared to less than half of non-CS majors (45%).

The US is failing to meet current demand for IT security professionals [24]. The 2011 Taulbee survey reports the production of BS degrees in computer science and computer engineering has decreased over the past decade, although the 2012 Taulbee survey shows recent improvement in these trends. Looking into the near future, the production of computing majors is falling behind projected job openings by a factor of five and a half [1]. If these trends continue, it will have a lasting, negative impact on the nation's economic future [7].

Cybersecurity education programs are finding it difficult to meet new and projected workforce demands [5]. While specialized programs and professional certificates may be an appropriate short-term strategies to satisfy the immediate need for qualified professionals [12], future demand needs to be addressed by curbing more systemic trends affecting CS education. Indeed, these feelings are reflected in the US CyberSpace Policy Review, a 2009 report commissioned by President Obama, which recommends the establishment of new K–12 educational programs for digital safety, ethics, and security, as well as

the expansion of university curricula in these topics.

Cybersecurity education is accompanied by its own unique challenges, which act as a barrier to adoption. While security issues permeate nearly all aspects of our day-to-day lives, the technical complexities and mundane subtleties of computer security do not easily lend themselves to a high school or underclass college curricula [4, 17]. Thus, a significant challenge in computer security pedagogy is in developing tools that teach security concepts to a wide audience (particularly non-STEM students) and that foster curiosity in security topics and that develop interest in CS and STEM disciplines.

Of course, we are not the first to recognize or attempt to rectify these curricular deficiencies. Efforts to inject CS topics into K-12 education generally follow one of two approaches: efforts to bring CS into the curriculum by modifying state and national standards, and efforts to form extra-curricular clubs and activities. Games are appropriate for use in both of these settings, and have strong potential for being used to teach cybersecurity topics to students at both secondary and post-secondary levels. We posit that finding new ways of bringing security topics into classrooms and clubs will have a positive effect on STEM education as a whole. We must cultivate a constellation of educational instruments able to stimulate interest in CS, with a high potential for engaging students without an inherent inclination for CS. We believe informal games can be an important part of the solution if we (as a community) understand both how to merge informal play with pedagogical objectives, and how to evaluate the effectiveness of games in the context of enhancing student understanding of cybersecurity and preventing misunderstandings. We share our experiences, as a step toward these goals.

2 Related Work

Digital games have been used in the context of teaching security concepts and developing security awareness, including CMU's *Anti-Phishing Phil* [23], the Naval Postgraduate School's *CyberCiege* [18], and the US Military Academy's *MAADNET* [15]. Whereas, the games *Protection Poker* [25] and *Elevation of Privilege* are non-digital games that "gamify" the practice of risk assessment for software development.

Full-simulation cybersecurity exercises engage players in a game that very closely simulates real-world attack and defense mechanics. Examples of these games include DEF CON's capture the flag contest, UCSB's International capture the flag (iCTF) competition, and NSA's Cyber Defense Exercise (CDX).

Similarly, some security coursework has used narrative and play in ways that more tightly align in-game strategy with its security lessons. For example, the Univ. of New Mexico uses a digital variant of the parlor game *Werewolf* to explore information flow policy in class [11].

More directly related to ours is the game *Control-Alt-Hack*, a re-skinning of Steve Jackson's *Ninja Burger* in the context of a security consulting firm [10]. The game has modest pedagogical goals, and is designed to expose the player to a variety of computer security terminology, careers and applications.

3 Design Goals

Several principles and goals guided [d0x3d!]'s design.

Fun. The intention was to design a social, challenging, dynamic, re-playable, rewarding, and un-confusing game—a game that one might play outside the classroom. We believe fun games can be an effective outreach tool, with the potential to expose players to new ideas and careers, and to stimulate continued study in the field. Games that are not fun do not engage students and, necessarily, will be ineffective at outreach.

Accessible. Tabletop games have the potential to engage students with low computer literacy and low "computer confidence." Our goal was to build a game that is simple to learn and play, requiring no technical background or familiarity with a computer. Further, tabletop games have no pretense of presenting a technical reality, simplifying and omitting technical details. This can be embraced, to make broad security themes (rather than technical details) accessible to wide populations.

Collaborative. Social play is important for demonstrating security as an interactive field, despite popular misconceptions of computer science as a solitary or isolating pursuit. Cooperative games are more faithful to player expectations for social interaction, compared to the headsets and interfaces of multi-user digital games. Collaborative games may be appropriate for classroom settings, where arguing and contentious interactions are avoided. In our game, we sought collaborative mechanics, allowing students to collectively strategize and problem solve.

Meaningful. Board games are finite, discrete, non-deterministic systems where humans act as the primary computational device. Bezáková *et al.* [3] observe that tabletop games provide a context in which students can reason about simple algorithms. Berland and Lee [2] observe that cooperative, strategic games allow students to engage in distributed, computational reasoning. Horn *et al.* [16] use board games to perform discrete simulations foundational to agent-based modeling. We believe games can leverage these observations, to support procedural and analytical reasoning about adversaries.

Unobtrusive. The direct and indirect costs of maintaining a computer lab are high; additionally, classroom computers are constrained in what software runs (even

willing teachers may not be able to install software of their choice). In contrast, our game should be quick to set up, easy to store, and require no special equipment to play. Further, it should be freely distributed online, so it can be printed and played at small cost.

Modifiable. One goal was to release the game under a license supporting modification. Making the game open to adaptation and re-mixing invites player-developed add-ons and variants. By developing new game pieces, mechanics, and rules, players engage critically and personally with the medium, exercising a level of experimentation beyond that of typical digital games.

Catalytic. The game should create the context for a broad security conversation, rather than reflect or embody some deeply-embedded, single lesson. This allows the game to be technically inaccurate, while still creating opportunities to contextualize and abstract complex security concepts in follow-on discussion.

4 Game Mechanics

[d0x3d!] is a cooperative board game in which players assume the role of white-hat hackers, tasked to retrieve a set of valuable digital assets held by an adversarial network. There are four digital assets in the game—Personally Identifiable Information (PII), Authentication Credentials, Financial Data and Intellectual Property (IP)—reflecting the idea that a variety of data is valued, and valued in different ways. The object of [d0x3d!] is to infiltrate and navigate the network, recover the four stolen assets, and successfully escape without detection. The adversary of the game (the network administrators) is encoded in its mechanics, as the network periodically adjusts its state, by either patching or decommissioning servers for forensic investigation. If time runs out, the adversary posts the players' assets to the Internet (the title 'd0x3d' is hacker slang for the practice of intentionally releasing PII on the web for the purpose of embarrassment). Players, thus, struggle against the game itself, either winning together or losing together. The game's mechanics are largely inspired by Matt Leacock's *Forbidden Island* [1].

The intention of [d0x3d!] is to create an artificial context for discussing real ideas in network security. As part of the design process, we made a conscious effort to introduce and use appropriate security terminology—*e.g.*, administrators, intrusion detection, compromise, patch, zero-day and forensics—in ways consistent with their real world interpretations. The game encourages students to role-play, by adopting hacker personas and viewing a network from the perspective of an attacker.

[1]For a more detailed explanation of game play, please see the game's website, `d0x3d.com`.

Before commenting how we relate the game's design to its security narrative or learning objectives, we briefly summarize the game's mechanics. Players must collect all four digital assets and then escape the network by using their abilities and exploiting network vulnerabilities. On a player's round, she spends from a per-turn allowance to take some number of actions: compromising a node, moving to another compromised node, and trading cards with other players. She then receives some digital *loot* cards, representing discovered knowledge about system vulnerabilities or data associated with the target assets. A player recovers a digital asset by discarding four cards picturing that asset, while occupying its corresponding *capture point*. At the end of the player's turn, the network adjusts itself: players follow rules to change the network's state based on pulling cards from a special *patch deck*. This represents the actions of a non-player character, the network admin, who impedes the progress of the players toward their goal.

4.1 Collaborative Games

Research has consistently found gender and social differences in player gratification and play preferences. In particular, many studies suggest women are less likely than men to choose to engage in competitive games or competitive situations [19, 20, 13, 9]. As it was our intention to develop a game appealing to and appropriate for mixed-gender audiences, we felt it was inappropriate to force players into competitive situations Instead, we sought to develop a cooperative game, where players collaborate socially to achieve a common goal.

In our game, each player has access to a special ability unique to their role. Zagal *et al.* [27] studied collaborative board games, finding unique roles increased interaction or bargaining during group coordination, even facilitating players to act selflessly in their actions for the group. Further, we believe collaborative games fit into a classroom well, as they mirror the type of goal-based social cooperation necessary in projects and group work. As in other collaborative board games, the source of game tension is not other players but, instead, a semi-random, in-game event affecting all players.

4.2 In-Game Security Terminology

Our pedagogical goals to communicate security terminology are modest: to use select, network security terms as appropriately as possible and to pique curiosity in the subject matter, without causing confusion or misunderstandings. We let our professional judgements guide our mapping of terms to game pieces and mechanics, rather than structure a game around the learning objectives of any particular curricula.

At a high level, generally, each game piece communicates some network or security terminology or idea. Admittedly, some mechanics are introduced purely for balance and the use of a security-themed narrative is opportunistic. For example, the mechanic in which four cards are combined (as part of collecting trophies needed to complete the game) are described in terms of key shares, combined according to a secret-sharing scheme to decrypt and collect the digital asset stored at a capture point. In the following sections, we describe some more essential design choices that support our security narrative and literacy goals.

4.3 Network Representation

The modularity of the [d0x3d!] board allows players to rearrange the layout and configuration of the "network" at the start of each game. While we suggest an initial topology for the network, players can explore new and interesting network topologies, adding to replayability. Each network node tile represents some common enterprise infrastructure, *e.g.* DNS servers, mail servers and single-sign-on servers. Some components, such as the Firewall and VPN Gateway, are "hardened," which require additional actions to compromise and, like their real-world counterparts, simulate an impediment to hacker movement through the network.

The iconography selected for each node both reinforces their meaning and adds additional learning opportunities. For example, we attempt to communicate the diversity of network clients using nodes that represent a laptop, desktop, tablet and mobile phone, showing their similarity in role by labeling each as a Client node.

We attempt to implement the capture point mechanic in a way that reinforces the roles of the infrastructure and the interpretation of the digital asset held there. For example, the capture points for the Personally Identifiable Information (PII) asset are an IMAP and SMTP server. The association helps to reinforce that email can hold PII, and may help students reflect on their experiences of sharing personal information in email.

4.4 Threat Representation

In [d0x3d!], the players and their actions are the basic source of threats against the game's network. The hacker roles reflect the diversity of threats faced by the network: malware, social engineering, insider threats, cryptanalysis, botnets, *etc.* Some player roles were ascribed mechanics to be illustrative of hacker threats; for example, the Botmaster's ability to leverage his botnet's throughput to communicate more data per turn. Other roles are merely evocative of an ability: the Cryptanalyst can move diagonally due to her ability to see problems "from a different angle."

Players occasionally draw *zero-day exploit* cards, which they can use later, to immediately compromise and occupy any network node, even hardened servers. The zero-days are each named after the software vulnerability being exploited at the target, such as a Buffer Overflow or an Integer Overflow. The ability to use these exploits at will against arbitrary targets may be unrealistic, but does serve to reinforce the idea that flaws are ubiquitous, that attacks can be relatively simple to deploy (*i.e.* canned exploits), and that making a service immune to compromise may be difficult or impossible in a large, diverse network. Additionally, the single-use nature of the cards reflect the knowledge disclosure and need for strategy typically associated with zero-days.

4.5 Defense Representation

The network under attack is represented by the board's dynamic state: nodes may be available, available but compromised, or decommissioned due to compromise. The per-round patch mechanic illustrates the challenges inherent to a "penetrate-and-patch" approach to security. Through these mechanics, players may recognize that patching allies temporary defects, does not prevent future attack and may, in fact, introduce new vulnerabilities. The reactionary nature of the penetrate-then-patch cycle is further captured through the *decommissioning* mechanic. If a hacker's footprint is noticed (if a player occupies the tile actively being patched), the player is ejected from the server and the node is removed from the game "for forensic investigation."

As in other cooperative games, the intensity of non-player game events are mediated by a meter, similar to the "terror track" in *Arkham Horror* and the "infection rate track" in *Pandemic*. Our meter has been opportunistically titled the Information Operations Condition (INFOCON) meter, following the DoD's network condition naming convention. The INFOCON meter reflects the magnitude of attention received by the network from its administrators and corresponds loosely to the perceived condition of a network under attack. Ultimately, the threat level may increase to the point where admins shut the network down, resulting in a loss for the players.

4.6 Limitations

Like all physical simulations of the digital world, we acknowledge that [d0x3d!] is imperfect. We believe students playing a game reflecting computer security ideas intuitively accept that the medium fails to reflect complete technical accuracy. We give some examples of mechanics we feel misrepresent the field, and remark that we are actively developing resources to identify and correct student misunderstanding after play.

Our game's characterization of digital assets is overly

Figure 1: Early designs for a compromised node: a physical "hole" in a greyed-out icon (top left), a negated color change (top right), an X and a negated color change (bottom left), and the final design (bottom right) using just a background color change.

simplistic. The four categories of valuable assets are arbitrary and overlapping. As a result, categorization of real-world assets in these terms may be challenging: a birth certificate may be PII or, at times, an authentication credential. Further, representing data using a token is flawed: once a trade secret is known or embarrassing photos are leaked, these may not be reclaimed in any meaningful fashion. More generally, the game's focus on confidential data fails to represent the variety of other valued properties, like availability or integrity.

The game's network representation is overly simplistic and does not reflect a sophisticated notion of network adjacency, even for a planar graph. Representing the player using a pawn leverages an inappropriate physical analogy, likening compromising a server to invading a contested space or burglary. This, of course, is flawed and misrepresents both the scale and automation enjoyed by attackers. More generally, the game fails to represent anything beyond a penetrate and patch approach to network security, precluding from its mechanics even the possibility of trusted systems, active defense mechanisms or adaptive security countermeasures.

5 Product Design and Development

We share some of our observations and lessons-learned in developing our game as a physical product.

5.1 Game Iconography

Research related to intuitive security iconography has been largely concerned with standardizing visualizations

Figure 2: Design for the Social Engineer: a stylized human figure (left) and the final weeble character (right).

of security policy or security status indicators. Our game has a different usability requirement: the iconography for a piece of technology in the game should lend some intuition about its role and purpose in a network. While some semi-standard iconography exists—like Cisco's network pictograms and Microsoft's network icons for Visio—there has been little usability research showing these to be effective in communicating an idea or imparting an intuition to a broad audience. Instead, for our game, we selected icons originally developed for customizing GUIs. Unlike network diagrams, these are representations which are intended to be consumed and understood by end-users as part of a user-interface.

The remainder of the game's graphic design was largely an exercise in selecting and adapting existing pictograms (chosen to be relatively intuitive), creating abstract but clear elements to reinforce mechanics, and double-coding representations for clarity. For example, a compromised node features a broken border, reinforcing the rule that hackers can enter this node or exit this node to any adjacent, compromised node (see Figure 1). We attempted to keep design elements relatively minimal, and removed or softened our reliance on physical analogies when we believed they might reinforce incorrect intuitions in the player.

5.2 Player Avatars

Nowak observes that players find anthropomorphic avatars more attractive and credible, and are more likely to choose those [22]. Thus, we targeted anthropomorphic figures, rather than objects or some generic representation of software. We were concerned, however, about player representation, due to a significant body of literature criticizing player avatar design in video games. While we developed artwork for detailed, human avatars with their own style and clothes, we rejected these based on the belief they might restrict player expression and undermined homophily. Heeter observes that games

girls invented were more likely to include customizable avatars than those boys invented [14]. Nowak observes that players strongly prefer to be represented by avatars that match their own gender [22]. In general, we felt the lessons learned from video game design informed us that players may be disappointed by representations whose clothing, accessories and gender were selected for them, may not align with their preference, and restricted their freedom of representation and ability to role play. Ultimately, we designed relatively androgynous, anthropomorphic avatars, resembling the pawns of the game (see Figure 2). We are aware that a gender bias may cause our androgynous characters to be interpreted as male: Bradshaw *et al.* [6] observe this in video games, although their findings suggest girls may be more likely to interpret an androgynous character as female. We leave open a more thorough player study, to see which iconography has promise to be a better outreach instrument.

5.3 Language Dependence

Text-heavy games are less accessible to students whose first language is not English. So too, games with too many "in jokes" and cultural references become exclusionary and work against our outreach goals. The website Board Game Geek suggests a 0–4 *language neutrality* rating to judge if a game is accessible to non-native speakers. A 0-neutrality game has few or no components with text, such as *Chess* or *UNO*. A 3-neutrality game poses a serious challenge for language conversion, as in Steve Jackson's *Munchkin* or *Chez Geek*. A 4-neutrality game is essentially unplayable by non-native speakers, such as *Scrabble* or *Trivial Pursuit*. [d0x3d!] ranks in the 0–1 range, as it may (at most) require a small cheat-sheet to play. While we have not studied the game with ESL populations formally, we find anecdotal evidence that the game imposes no serious language barrier. In particular, within the first week of our release, the game was forked for Polish and Chinese translation. We currently have over a dozen forks, mostly devoted to translation.

5.4 Open-Sourcing Board Games

One of our design goals was to develop a game that is free to use, free to adapt and free to remix. Several game designers have released their original work under such licenses: the strategy game *Sovereign* is released under a CC-BY-SA license and *Elevation of Privilege* is released under a CC-BY license. Far fewer games have transparently re-used open-source components. The board game *GiftTRAP*, a notable exception, used crowd-sourcing via Flickr to gather artwork: users licensed their submissions under a CC-BY license for inclusion in the game, and the resulting cards both carry attribution and are distributed online under a CC-BY-NC license.

Our game re-uses open-source icons, *e.g.*, those from the Open Security Alliance, Tango and others. We found that licenses associated with candidate icons posed an interesting challenge: some icon sets were incompatible with one another, and some even carried software licenses (generally agreed to be inappropriate for creative content). Certainly, combining incompatible licenses into a derivative work is not possible. However, it is unclear what is a derivative work in a board game. That is, it is unclear how to interpret "copyleft" in the context of physical games. We consider a game to be a collection of components, where each component is a work carrying its own license. We find this to be the only reasonable interpretation, as requiring a uniform license across all components quickly runs into problems. Does one consider all components actively in play during a game? All components ever produced? All expansion packs and boosters? If two game pieces are so functionally inseparable that one cannot be discarded and re-implemented in isolation, then we consider these to be a single functional component that must share a license; however, requiring a strictly uniform license across all components quickly becomes untenable for any open, re-mixable game.

6 Field Tests

Since Spring 2012, we have played [d0x3d!] with students in a variety of extracurricular settings, including:

CyberAdventurers, Salinas, CA. A week-long summer day camp designed to introduce middle school students to topics within computer science. Students had little to no experience with security concepts. We played with a mixed-gender group of 15-20 students, largely from populations underrepresented in CS.

Information Systems Security Association (ISSA) Triangle InfoSecCon, Raleigh, NC. An annual IT security event sponsored by the Raleigh ISSA Chapter that, as part of its mission, encourages local high-school students to participate. We played with a mixed-gender group of 15-20 high school students, largely from populations underrepresented in CS.

Hartnell Community College, Salinas, CA. On two different occasions we played the game with students enrolled in a network security course at a local community college. Each time, we played with a predominantly male group of 25-30 undergraduate students, each of whom were pursuing a major related to computer science and information systems.

Monterey Academy of Oceanographic Science (MAOS), Monterey, CA. A day-long outreach event serving MAOS, a STEM program at Monterey High School for high-achieving students. We played with a mixed-gender group of 65-70 high school students.

6.1 Observations

Much remains to assess our game's impact and its ability to meet its various learning objectives. We remark that assessment strategies for informal security games, like ours, have been largely unexplored in the academic literature. The task appears to be far more complicated than in the context of serious games, for which assessment (while still difficult) tends both to target a narrower set of learning outcomes and to explore these in a more explicit manner, *e.g.*, using a partial simulation game to teach and evaluate student ability to configure a firewall.

We have begun to formulate pre-test and post-test activities to gauge student understanding relative to our security terminology. For example, one of our play sessions featured a post-game instrument in the form of a worksheet, where students collaborated to associate a technical term featured in the game to its real-world definition, assisted by its in-game context. While most students completed this task successfully, without better pre-test evaluation, instrument factor analysis and a control group, our game's role in this outcome is unclear.

The observations that follow are a type of "action research" investigation to evaluate the effectiveness of the game; however, our results are too preliminary to draw meaningful conclusions.

6.1.1 Contextualizing Player Values

In one play session, students customized their digital assets before playing the game. For example, rather than use generically-named assets, one group played with 'my house alarm code' (authentication credential), 'grandma's recipe for arroz con gandules' (intellectual property), 'Elisa's mom's bank account number' (financial data), and 'Yasmine's address' (PII). We found this small task helped us check for student understanding related to these terms, by observing group discussions and the choices written on students' game pieces. Forcing students to map their personal values to the in-game narrative may also have been a factor in the spontaneous, student-driven group discussion about online safety that followed play. We now include a customizable digital asset mat as part of the staple game, and are developing a lesson plan to assist teachers in discussing digital assets before and after playing with students.

6.1.2 Exploring Network Layouts

In several play sessions, students elected to re-play the game, working as a group to intentionally configure the network with the goal of making the game as challenging as possible. This involved placing nodes holding the assets behind hardened nodes, with minimal connections to the network and far away from the starting positions of the hackers. Thus, high value nodes became harder to reach and hackers occupying these positions were more likely to be ejected from the network, should they be discovered during the patch round. Some students also began to explore "house rules" for the game, inventing variant mechanics such as combining two sets of games and making the goals competitive rather than cooperative. We feel these observations show students demonstrating the type of perspective shift and strategic thinking that must be employed in configuring real-life networks to withstand attack. We see this type of adversarial thinking as a major success in engaging players to think like a security professional through play.

6.2 Feedback

Generally, players have reported positive experiences playing the game. Some students have expressed interest in playing the game with their parents; likewise, adults have shown interest in using it with their children. One manager expressed interest in [d0x3d!] as an icebreaker with employees, before talking about local IT policies. While, we have received no reports of negative experiences, we have observed occasional low interest during game play or confusion with rules. One fear associated with cooperative games, in general, is that a dominant personality may inhibit collaboration, *i.e.* a bully can ruin the game for everyone. We presume this applies equally to our game, but we have not witnessed the phenomena during play sessions; we note that an adult presence at each session may contribute to the observed behavior of our players. More generally, we observe that cooperative play in our game encourages discussion about strategy and rule interpretation, and may play a larger role in starting a dialogue about the game's relationship to real-life phenomena.

7 Conclusions

We have summarized lessons learned and experiences with developing and playing [d0x3d!], motivating informal games as a promising tool for security lessons with modest educational objectives. This is largely work-in-progress, as much remains to evaluate the effectiveness of these games in meeting their goals. Our game inherits those challenges facing any game used in education: relevancy to curriculum, accessibility to and appropriateness for its audience, and difficulty in evaluation. We are actively working to collect feedback related to these issues, more directly and systematically.

We are actively developing lessons appropriate for direct use in the K-12 classroom, based on our observations of how student players tended to interact with the game (see Section 6). We are working with local K-12 teachers to adjust these lessons, to scaffold and reinforce existing curricular goals, using our game as the context for relevant follow-on activities: critical reading of essays, inter-

preting charts and graphs, and doing non-encyclopedia research. We are also working on ways to encourage players to re-mix and adapt the game. During initial play tests, players frequently tested the game's limits by imagining new rules and cards, often with suggestions along the lines of "wouldn't it be cool if there was a card that did *x*..." To encourage this, we are developing an online, customizable card creator, to more easily generate new characters, nodes and other game pieces.

[d0x3d!] is released under an open-source content license allowing free distribution and adaptation. It is available for print-and-play [2] or as an assembled game via an on-demand print service; for details, see its website: `http://www.d0x3d.com/`.

Acknowledgments

The authors would like to thank Ann Gallenson, Schipper Design and M. Sherwood Design for graphic design work; Sue Higgins, Joe Welsh and Kate Lockwood for help field testing; and the players who provided input during the design process. [d0x3d!] is inspired by Forbidden Island, which was created by Matt Leacock and published by Gamewright. All rights reserved. The US National Science Foundation (NSF) provided partial support for this work under award #1140561.

References

[1] AMERICAN COLLEGE TESTING PROGRAM. The condition of college and career readiness. `http://goo.gl/KoHvo`, July 2010.

[2] BERLAND, M., AND LEE, V. R. Collaborative strategic board games as a site for distributed computational thinking. *International Journal of Game-Based Learning 1*, 2 (2011), 65–81.

[3] BEZÁKOVÁ, I., HELIOTIS, J. E., AND STROUT, S. P. Board game strategies in introductory computer science. In *The ACM Technical Symposium on Computer Science Education* (2013).

[4] BISHOP, M. Computer security education: Training, scholarship, and research. *Security and Privacy 35*, 4 (2002).

[5] BOOZ ALLEN HAMILTON. Cyber IN-security: Strengthening the federal cybersecurity workforce. Whitepaper, July 2009.

[6] BRADSHAW, J., CLEGG, S., AND TRAYHURN, D. An Investigation into Gender Bias in Educational Software Used in English Primary Schools. *Gender and Education 7*, 2 (June 1995).

[7] COMMITTEE ON PROSPERING IN THE GLOBAL ECONOMY OF THE 21ST CENTURY. Rising above the gathering storm: Energizing and employing america for a brighter economic future. National Academies Press, 2007.

[8] COMPUTER SCIENCE TEACHERS ASSOCIATIONS. CSTA national secondary computer science survey. csta.acm.org, 2011.

[9] CROSON, R., AND GNEEZY, U. Gender differences in preferences. *J. of Economic Literature 47*, 2 (May 2009), 448–474.

[10] DENNING, T., KOHNO, T., AND SHOSTACK, A. Control-Alt-Hack: A card game for computer security outreach, education, and fun. Tech. Rep. UW-CSE-12-07-01, U. of Washington, 2012.

[2] At GitHub: `http://github.com/TableTopSecurity`

[11] ENSAFI, R., JACOBI, M., AND CRANDALL, J. R. Students Who Don't Understand Information Flow Should be Eaten: An Experience Paper. In *Proc. of the 5th USENIX conference on Cyber Security Experimentation and Test* (2012).

[12] EVANS, K., AND REEDER, F. A human capital crisis in cybersecurity: A report of the CSIS commission on cybersecurity for the 44th presidency. Whitepaper, Center for Strategic & International Studies, November 2010.

[13] HARTMANN, T., AND KLIMMT, C. Gender and computer games: Exploring females' dislikes. *Journal of Computer-Mediated Communication 11*, 4 (July 2006), 910–931.

[14] HEETER, C., EGIDIO, R., MISHRA, P., WINN, B., AND WINN, J. Alien games: Do girls prefer games designed by girls? *Games and Culture 4*, 1 (Dec. 2008), 74–100.

[15] HILL, J. M. D., SURDU, J. R., LATHROP, S. D., CONTI, G., AND CARVER JR, C. A. MAADNET: Toward a web-distributed tool for teaching networking and information assurance. In *Educational Multimedia, Hypermedia and Telecommunications* (2003).

[16] HORN, M. S., WEINTROP, D., BEHESHTI, E., AND OLSON, I. D. Spinners, dice, and pawns: Using board games to prepare for agent-based modeling activities. In *American Educational Research Association Annual Meeting* (2012).

[17] IRVINE, C. E., CHIN, S.-K., AND FRINCKE, D. Integrating security into the curriculum. *IEEE Computer 31*, 12 (1998), 25–30.

[18] IRVINE, C. E., THOMPSON, M. F., AND ALLEN, K. CyberCIEGE: An information assurance teaching tool for training and awareness. In *Federal Information Systems Security Educators' Association Conference* (2005).

[19] KAFAI, Y. B. Video game designs by girls and boys: variability and consistency of gender differences. In *From Barbie to Mortal Kombat: gender and computer games*, J. Cassell and H. Jenkins, Eds. 1998, pp. 90–114.

[20] LUCAS, K., AND SHERRY, J. Sex differences in video game play: a communication-based explanation. *Communication Research 31*, 5 (2004), 499–523.

[21] MATTERN, K. D., SHAW, E. J., AND EWING, M. Advanced placement exam participation: Is AP exam participation and performance related to choice of college major? `research.collegeboard.org`, October 2011.

[22] NOWAK, K. L., AND RAUH, C. The Influence of the Avatar on Online Perceptions of Anthropomorphism, Androgyny, Credibility, Homophily, and Attraction. *Journal of Computer-Mediated Communication 11*, 1 (Nov. 2005), 153–178.

[23] SHENG, S., MAGNIEN, B., KUMARAGURU, P., ACQUISTI, A., CRANOR, L. F., HONG, J., AND NUNGE, E. Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish. In *Proc. of the Symposium on Usable Privacy and Security* (2007).

[24] VIJAYAN, J. Demand for it security experts outstrips supply. `http://goo.gl/6wKfH`, Mar. 2013.

[25] WILLIAMS, L., GEGICK, M., AND MENEELY, A. Protection Poker: Structuring Software Security Risk Assessment and Knowledge Transfer. In *Proc. of the International Symposium on Engineering Secure Software and Systems* (Mar. 2009).

[26] WILSON, C., SUDOL, L. A., STEPHENSON, C., AND STEHLIK, M. Running on empty: The failure to teach K-12 computer science in the digital age. `http://goo.gl/unHPr`, 2010.

[27] ZAGAL, J. P., RICK, J., AND HSI, I. Collaborative games: Lessons learned from board games. *Simulation and Gaming 37*, 1 (Mar. 2006), 24–40.