Editors: Cynthia Irvine, irvine@nps.edu | Alec Yasinsac, yasinsac@southalabama.edu

Security through Play

Mark Gondree and Zachary N.J. Peterson | US Naval Postgraduate School
Tamara Denning | University of Washington

Precollege classrooms have neither the support nor the room to explore computer security topics. At best, students are the targets of in-school safety campaigns, absorbing rules and best practices that only hint at the rich landscape of security problems. How to expose young students to cybersecurity outside the classroom—to computer security technology, concepts, and careers—is a challenge. Unfortunately, popular media might give more visibility to cyber careers, albeit in the form of outlandish movie-plot cyber capers, than any precollege STEM (science, technology, engineering, and mathematics) program does.

Here, we describe some opportunities for exposing young audiences to cybersecurity via informal lessons, leveraging play for education and outreach. The US Naval Postgraduate School (NPS) and University of Washington (UW) each independently developed informal security-themed tabletop games. [d0x3d!] is a board game about network security, designed by Zachary Peterson and Mark Gondree at NPS. Control-Alt-Hack is a card game about computer security, designed by Tamara Denning, Tadayoshi Kohno, and Adam Shostack at UW.

Play as Part of Security Education

Others have claimed success in encoding basic computer science principles in simple games.[1,2] Likewise, we hypothesize games might be able to encode skills essential in reasoning about security. Eric Klopfer and his colleagues identified five freedoms essential to *play*:[3]

- the freedom to experiment,
- the freedom to fail,
- the freedom to fashion identities,
- the freedom of interpretation, and
- the freedom of autonomous effort.

These might be rephrased as

- the freedom to test hypotheses against an adversary,
- the freedom to observe and learn from adversarial strategy,
- the freedom to adopt the identity and explore the motivations of an adversary,
- the freedom to experience and interpret a system from multiple perspectives, and
- the freedom to engage in or disengage from attacks strategically or arbitrarily.

Games inspire players to challenge the limits of play by exploring the meaning and interpretation of rules. Similarly, rule testing, rule interpretation, and rule breaking are prerequisite Red Team skills. We argue that such adversarial thinking is foundational to both strategic games and security engineering. Put another way, many cybersecurity concepts are game concepts. So, games are natural vectors for teaching the subject matter.

Of course, you can leverage play to motivate lessons in many ways. The games Protection Poker[4] and Elevation of Privilege (www.microsoft.com/security/sdl/adopt/eop.aspx) "gamify" an otherwise onerous and technical software development process. Turn by turn, players model security risk, using cards and points to motivate a larger conversation about system vulnerabilities. The University of New Mexico uses an online version of the parlor game The Werewolves of Miller's Hollow to explore information flow policy.[5] "Werewolves" exploit covert channels in a multiuser system to communicate with one another about their next victim, while avoiding detection by other players. Here, the in-game narrative and strategy are much more tightly aligned with the behaviors of secure-systems adversaries.

Serious Games in Security Education

The serious-games movement is associated with military-inspired training games that employ simulation to provide a captive audience with a narrow skill set. The military adopts these games in the contexts of flight simulation, conflict simulation, and emergency-scenario role-playing. Quite naturally, the

Copublished by the IEEE Computer and Reliability Societies

computer security domain has adapted wargaming.

Capture-the-flag (CTF) games are a type of full-simulation cyber wargame. Examples include DEF CON's CTF; iCTF at the University of California, Santa Barbara; and the US National Security Agency's CDX (Cyber Defense Exercise). These games' mechanics, time scale, and technical skills simulate the real world. For example, mechanically, an attack against SSL (Secure Sockets Layer) in a CTF exercise differs little from one on the Internet. (Of course, such an attack differs dramatically in other respects, such as legal and ethical consequences.) Full-simulation cybersecurity exercises are technically demanding for organizers and participants alike.

In contrast, partial-simulation games require far less technical expertise on the player's part. These games use a simpler set of mechanics than those in the real world. Examples are the NPS's CyberCIEGE (http://cisr.nps.edu/cyberciege),[6] the US Department of Defense's CyberProtect (http://iase.disa.mil/eta/online-catalog.html), and the US Defense Information Systems Agency's CyberOps: NetWarrior. Each differs in the expressiveness and fidelity of its simulation. However, all use artificial mechanics, speeded-up time frames, and simplified representations of security tools to let players with little technical skill play the network administrator's role.

Informal Security Games

Unlike simulation-based games, we aim to expose students to security through more informal games with modest pedagogical goals. We feel that using informal games in security has been relatively unexplored. Serious games tend to sacrifice many freedoms of play in the name of technical reality or simulation faithfulness. In contrast, our games' primary goals are to be engaging and fun. They seek to be social, challenging, dynamic, rewarding, and unconfusing—games you might want to play outside the classroom. Informal security games should be simple to learn, be accessible, require no special equipment, and be attractive to a variety of students (not just those with a predilection for computers or digital games). They can be an outreach tool, with the potential to foster interest in audiences otherwise underrepresented in computer science. The games should expose this audience to new ideas, raise awareness of new career opportunities, and stimulate continued study.

Why Tabletop Games?

We developed tabletop games—that is, card and board games—quite intentionally, finding they have a few advantages over their digital counterparts.

They're Accessible

They have the potential to engage students with low computer literacy and low "computer confidence."

They're Social

Social play is important for demonstrating security as an interactive field, despite popular misconceptions of computer science as a solitary or isolating pursuit. These games are more faithful to player expectations for social interaction, compared to interfaces in multiuser digital games.

They're Unobtrusive

The cost of maintaining a computer lab in a school is high and can be prohibitive; relocating a class to a lab is equally costly from the perspective of classroom time management. Also, most classroom computers are constrained in what software is permitted or can be run: even willing teachers might not be able to install or use some education software. In contrast, tabletop games are quick to set up, easy to store, and require no maintenance between use.

They're Modest

The game Operation doesn't yield a medical degree on completion, and Monopoly doesn't impact your tax status. Tabletop games make no pretense of presenting reality. So, they avoid the possibility of either being mistaken for a training game or leaving a player feeling "trained." Tabletop games are transparent about their limitations while still daring to reflect real-world phenomena.

They're Modifiable

They invite adaptation by players—for example, by using "house rules." Such interaction lets players engage both critically and personally with the medium, exercising a level of experimentation beyond that of typical digital games.

[d0x3d!]

In [d0x3d!] (see Figure 1), players collaborate as white-hat hackers. They must infiltrate and navigate an adversarial network, retrieve a set of valuable digital assets, and escape. The adversary is encoded in the game's mechanics, as the network periodically adjusts its state, either patching or decommissioning servers for forensic investigation. If time runs out, the adversary posts the players' assets on the Internet ("d0x3d" is hacker slang for intentionally releasing personally identifiable information on the Web to embarrass someone). Players thus struggle against the game itself, either winning together or losing together.

The game provides an artificial context for discussing real ideas in network security. When designing it, we made sure to introduce and use appropriate security terminology—for example, "administrators," "intrusion detection," "compromise," "patch," "0-day," and

Figure 1. [d0x3d!] being played at the 2013 US National Science Foundation's Scholarship for Service Symposium. Players collaborate as white-hat hackers, tasked to retrieve a set of valuable digital assets held by an adversarial network.

Figure 2. The contents of Control-Alt-Hack, including three of the game's Hacker character cards. Players use dice rolls and their character's level in certain hacker skills to attempt a variety of penetration-testing missions.

"forensics"—in ways consistent with their real-world interpretations. The game also encourages students to role-play, adopting hacker personas, each with a unique skill. For example, the Botmaster leverages his or her botnet for high-throughput content delivery, whereas the Insider leverages physical access to compromise machines more easily.

Control-Alt-Hack

In Control-Alt-Hack (see Figure 2), three to six players act as white-hat hackers at a security consulting company. Taking turns, they use dice rolls and their character's level in certain hacker skills—such as Network Ninja, Hardware Hacking, Software Wizardry, Social Engineering, and Cryptanalysis—to attempt a variety of penetration-testing missions, each with its own narrative. Successful missions gain players Hacker Cred, which gets them closer to being the company's next CEO.

Control-Alt-Hack is intended to raise players' awareness of a variety of issues: the creativity of motivated adversaries, the breadth of technologies—particularly embedded and cyberphysical systems—that are impacted by computer security, the different ways successful attacks can impact human assets, and the potential things you can do with computer security skills.

Playing Together

Here, we highlight some of our experiences in playing our games with different audiences.

One idea in [d0x3d!] is the value of digital property. In one play session, middle-school students collaborated to personalize the game's content. For example, instead of using the generically named pieces, they 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" (personally identifiable information). This small, introspective task caused students to map their values to the in-game narrative, leading to a student-driven discussion about online safety.

In another play session, after undergraduates played [d0x3d!] with a default, randomized network, they reconfigured the network to make winning as challenging as possible and then replayed the game. This demonstrates the type of perspective shift and strategic thinking needed to design, build, and defend distributed systems in the face of network attacks. We see it as a major success in engaging players to think like a security professional through play.

Formal evaluation of Control-Alt-Hack is still underway; initial feedback has been primarily positive, with high school, undergraduate-level, and graduate-level educators requesting free copies. The game has been invited to play sessions at the US National Science Foundation's Scholarship for Service Symposium and at a company's internal security training.

Some students have expressed interest in playing [d0x3d!] with their parents. Likewise, adults have shown interest in playing both [d0x3d!] and Control-Alt-Hack with their children (and spouses) to "finally explain what mom does at work." Managers have expressed interest in [d0x3d!] as an icebreaker with employees before talking about local IT policies.

Assessment Challenges

Although our initial experiences in playing these games have yielded positive feedback, much work remains to assess tabletop security games' impact and utility. The formal assessment of any security game as a pedagogical tool is difficult, and the current state of evaluation needs improvement. Some games lack the basic context prerequisite for assessment; for example, the CTF literature fails to enumerate specific learning objectives. To date, security game assessment has focused on a limited set of metrics: whether players "won," how long they took, how they performed in postgame summative assessments, and so on. Questions remain as to these tools' effectiveness in terms of

- their translation into real-world knowledge, skills, and abilities;

- lesson retention;
- identifying and correcting misunderstandings; and
- their generalizability outside their case studies.

Our games inherit those challenges, which are faced by any novel approach to security education. Drawing from previous research in educational-game evaluation,[7,8] we're designing exercises with well-defined learning objectives[9] against which these games can be assessed.

The abilities to affect student attitudes toward cybersecurity in STEM and act as an outreach tool necessarily require longer-term, longitudinal studies. We're pursuing inclusion in an after-school STEM program that's equipped to perform such impact assessments. However, STEM program participants tend to self-select on the basis of preexisting interest in STEM, and, ultimately, those programs might be inappropriate crucibles for assessing cybersecurity outreach.

The assessment of informal games appears to be complicated and somewhat different from that of serious games, which target more restricted and directly assessable outcomes. Regardless, a place exists for a variety of informal games that encode security concepts. Games are fun, and the security profession would benefit from broader awareness through an accessible dialogue.

For information on obtaining [d0x3d!] and Control-Alt-Hack, see the sidebar. ■

Acknowledgments

The US National Science Foundation (NSF) provided partial support for [d0x3d!] under award 1140561 and for Control-Alt-Hack under award 0846065. Any opinions, findings, and conclusions or recommendations expressed in this article are the authors' and don't necessarily reflect the NSF's views. Intel Labs and the ACM Special Interest Group on Computer Science Education provided additional funding for Control-Alt-Hack. [d0x3d!] is inspired by Forbidden Island, which was created by Matt Leacock and published by Gamewright. All rights reserved. Control-Alt-Hack © 2012 by the University of Washington. All rights reserved. "Control-Alt-Hack" and the logo are trademarks of the University of Washington. The game mechanics are based on the game Ninja Burger, © 2009 by Steve Jackson Games; used under license.

References

1. I. Bezáková, J.E. Heliotis, and S.P. Strout, "Board Game Strategies in Introductory Computer Science," *Proc. 44th ACM Technical Symp. Computer Science Education* (SIGCSE 13), ACM, 2013, pp. 17–22.
2. M. Berland and V.R. Lee, "Collaborative Strategic Board Games as a Site for Distributed Computational Thinking," *Int'l J. Game-Based Learning*, vol. 1, no. 2, 2011, pp. 65–81.
3. E. Klopfer, S. Osterweil, and K. Salen, *Moving Learning Games Forward: Obstacles, Opportunities, and Openness*, The Education Arcade, MIT, 2009.
4. L. Williams, A. Meneely, and G. Shipley, "Protection Poker: The New Software Security 'Game'," *IEEE Security & Privacy*, vol. 8, no. 3, 2010, pp. 14–20.
5. R. Ensafi, M. Jacobi, and J.R. Crandall, "Students Who Don't Understand Information Flow Should Be Eaten: An Experience Paper," *Proc. 5th Usenix Conf. Cyber Security Experimentation and Test* (CSET 12), Usenix, 2012, p. 10.
6. C. Irvine, M. Thompson, and K. Allen, "CyberCIEGE: Gaming for Information Assurance," *IEEE Security & Privacy*, vol. 3, no. 3, 2005, pp. 61–64.
7. L. Annetta and S. Bronack, eds., *Serious Educational Game Assessment: Practical Methods and Models for Educational Games, Simulations and Virtual Worlds*, Sense Publishers, 2010.
8. D. Ifenthaler, D. Eseryel, and X. Ge, eds., *Assessment in Game-Based Learning: Foundations, Innovations, and Perspectives*, Springer, 2012.
9. G. Wiggins, *Educative Assessment: Designing Assessments to Inform and Improve Student Performance*, Jossey-Bass, 1998.

Game Availability

[d0x3d!] is released under an open source content license allowing free distribution and adaptation. It's available for print-and-play or as an assembled game via an on-demand print service; for details, visit www.d0x3d.com.

Control-Alt-Hack is available free to US educators while supplies last; for details, see www.controlalthack.com. It's also available for purchase at Amazon.com via RGB Hats LLC, founded by Tamara Denning and Tadayoshi Kohno. International shipping is available from Ada's Technical Books (seattletechnicalbooks.com).

Mark Gondree is a research associate professor in the Naval Postgraduate School's Computer Science Department. Contact him at mgondree@nps.edu.

Zachary N.J. Peterson is an assistant professor in the Naval Postgraduate School's Computer Science Department. Contact him at znpeters@nps.edu.

Tamara Denning is a PhD student in the University of Washington's Computer Science and Engineering department. Contact her at tdenning@cs.washington.edu.