Teaching Cybersecurity to Wide Audiences with Table-Top Games

Tadhg Fendt
Department of Mathematical Sciences
Lewis & Clark College
tfendt@lclark.edu

Jens Mache
Department of Mathematical Sciences
Lewis & Clark College
jmache@lclark.edu

Abstract

Cybersecurity is a field of growing importance. A particular challenge is that there is an ever-growing base of technology that needs securing, coupled with a shortage of security specialists. This creates an important role for security education. Security education is considered difficult, especially with non-technical students, because the field is so broad. Table-top gaming has been suggested as an educational starting point to make a wide audience aware of the issues and to foster curiosity and enthusiasm for the field. In this paper we examine two such games, *Control-Alt Hack* and *[d0x3d!]*, compare their strengths and weaknesses and feasibility in the undergraduate classroom. In conclusion, *[d0x3d!]* seems preferable for use in the classroom.

1 Introduction

Given the challenges that accompany security education, we believe that more tools and activities are needed for instructors to effectively teach it. Table-top games provide a learning experience that is appropriately non-technical as a starting point and for students without much computer science background, yet still hands-on and thought provoking. In this paper, we examine two games, *Control-Alt Hack*, and *[d0x3d!]*. We review the basic mechanics and logistics of both games as well as the security concepts and the methods used to introduce them. Particular differences of interest to us are: the use of reading and language in the games, competitive vs. cooperative game-play, and the use of dynamic modeling. We discuss these differences, strengths and weaknesses of the games as well as their feasibility in an undergraduate class.

1.1 Motivation

This paper is directly motivated by a growing need for conceptually rich, non-technical resources for students without much computer science background. During the 2014-2015 school year, Lewis & Clark College will be offering an interdisciplinary perspectives in cybersecurity class in collaboration with the International Affairs department. As time in the classroom is at a premium, we want to be sure that if we decided to use one or both of these games that we could do so effectively and efficiently.

2 Background

Control-Alt Hack and *[d0x3d!]* have the same basic driving principle behind them: exposing “non-experts” to concepts in security with the aim of increasing awareness [1,2]. The designers readily admit that the games do not provide in-depth or technical instruction of security. However, they make the convincing argument that this is not necessary for the stated goals of outreach and exposure [1,2].

In *Control-Alt Hack* [1] each player becomes a white-hat hacker in a security consulting firm. Players have character cards that give them a certain set of skills to help them complete security audits and other missions. Players compete to gain the most "hacker cred" and the most successful hacker eventually becomes CEO of their own security firm.

In *[d0x3d!]* [2], the players work as a team to recover personal data that has been stolen and hidden on a computer network. The players take on different roles (i.e. wardriver, cryptanalyst, etc.) that give them special abilities to complete the mission. The team must infiltrate the network and recover the stolen data, all while the administrators patch, decommission, and possibly detect intrusions.. Both games are turn-based, card-driven games though *Control-Alt Hack* additionally uses dice rolls to resolve mission attempts.

3 Reading and Language

The vernacular of a game being used for educational purposes is a very important consideration for that game's effectiveness. This may seem rather strange at first because after all, you don't read games, you play them. But it turns out that it actually depends to a large degree on the type of game, which brings us to the first big difference between the two: *Control-Alt Hack* is much more text dependent than *[d0x3d!]*. The driving game mechanism in *Control-Alt Hack* is the mission card. The cards have a title, a description of the overall task, and lastly several sub components to the mission that are specific to one or more of the "hacker skills." In short, there is a lot of writing and it is used as the main way in which information is conveyed to the players. On the other hand in *[d0x3d!]* the cards make much better use of pictures and any writing is usually one or two words.

In a game that uses text as the main conduit for information, the clarity and efficiency of the words becomes even more important. Unfortunately, in addition to being more text-heavy overall, we feel that *Control-Alt Hack's* use of language is less effective in communicating security concepts for three reasons.

Firstly, it seems that *Control-Alt Hack* is attempting to get as much information into the game as possible. In one sense, this is good because it shows just how broad the field is and also breaks down the stereotype of security people as always feverishly typing on the command line. The downside, however, is that too much information can overwhelm students and not really stick with them. If you have one hour to play a game in class, less information can mean more focus.

Secondly, the vocabulary itself is sometimes quite vague. Mission cards address topics such as: wireless connection protocols, weaponized exploits, and software vulnerabilities. For teaching non-computer science students, it seems that these words are less effective than the more specific ones found in *d0x3d!*: honeypot, integer overflow, logic bomb, etc. The latter group of short, specific terms can be easily looked up and researched independently and later incorporated into class.

Finally, we also find several of the missions and much of the text to be superfluous and of questionable relevance to any computer security curriculum. In many cases, it seems these are included for humor which is certainly not a detraction in games generally. However, many of the jokes and comedic situations are only funny to those with knowledge of computer science or the tech industry and thus of little value to many students.

However, we think that *Control-Alt Hack* was successful with its use of language in the implementation of the "hacker skills" system. In the game, almost all mission are resolved under one or more of the five abilities the designers consider to be essential: hardware hacking, software wizardry, network ninja, social engineering, and cryptanalysis. While these terms are still somewhat vague, they subtly and effectively inject a very important question into the entire game: what is cybersecurity? It is actually a fairly hard question to answer. Security is a broad and multifaceted topic and these categories get that idea across.

This categorization also struck us as a good mental exercise for instructors in relation to curriculum design and for time allocation. Assuming that we agree with the rough categories, which of them should we be focusing on in our teaching efforts? In our security class for computer science students this past year, we focused roughly 40% each on software issues and network skills while the remaining time split between social engineering, crypto and hardware. Whether this is an optimal mix is certainly a pending question. There are many factors that contribute to what the syllabus will ultimately look like for a security course, including available tools, infrastructure and resources but in any case this provides interesting food for thought for those endeavoring to teach security.

4 Competitive vs. Cooperative Game-play

Another difference worthy of note is the nature of play in both games. *Control-Alt Hack* is a competitive game with players vying for the top CEO spot, whereas [*d0x3d!*] has all players cooperatively trying to recover the stolen data. Does a game being either competitive or cooperative make a difference for its educational outcomes? There are reasonable arguments on both sides. Competitive games are often seen as being more fun because there is the possibility of being a unique winner. Games that are more fun might be more readily played by students. On the other hand, some research has shown that women, relative to men, are less likely to want to play a competitive game [2]. This suggests that cooperative games may be more inclusive and can even help combat the severe gender gap in computer security. Further studies have shown cooperative games result in higher levels of interaction between players [3]. This could potentially lead to greater inter-player discussion and analysis as students review their play and adjust strategy together. On balance, we give the nod to the cooperative game because while it may not maximize fun, it certainly does not preclude it, and many other benefits can be conferred in an educational setting.

5 Games as Models

In general, games are usually trying to model something and the better the model, the better the game. Models are also a very good way of teaching. This is because they allow for the abstraction of complex systems so they can be examined and conceptually understood without the overhead and information overload. *Control-Alt Hack* and *d0x3d!* are no exception to this rule, and both attempt to model a different aspect of security with varying success.

D0x3d! takes the approach of actually modeling a computer network on which stolen data is hidden. The various pieces of infrastructure that make up the network are represented by tiles that the players can compromise and move through. This is also a dynamic model because of the actions of the system administrators, which are built into the game with pseudo-random card draws. These “patch” card draws can lead to the securing or decommission of compromised network infrastructure, constraining the players by changing their environment. In addition to being dynamic during the course of a single game, *d0x3d!* also allows for changes to be made and thus encourages experimentation and playing the game many times. At the beginning of the game, the players are free to "configure" the network topology however they want. This allows players to incorporate their own ideas and learning into the game to make play more interesting or challenging. Most importantly, with a few simple rules this model exposes players to the concept of navigating computer networks -- a real-world task that is a significant part of security from our experience with competitions such as CCDC [4] -- all without having to master details of secure shell, protocols or port numbers. Students could play the game first and then actually attempt some of the network traversal they were doing on a local lab or in the cloud.

Control-Alt Hack alternatively models the much more general concept of working as a security professional. Players are given a character with various skills that can be improved over time. The characters carry out what can be described as contracts to elevate their career until such a point that they can win the game by being the top hacker. This model too is dynamic because the players can interact in the game and take actions that affect one another. We feel that this model is less successful because the system it tries to emulate is complex and inexact relative to a simple computer network. It would also be hard to try to make direct links from actions in the game to activities students could actually attempt. A mission card that has the player complete a security audit would be hard to relate to for a non-expert.

6 Classroom Feasibility

When evaluating something like a game for use in class, it is important to consider certain logistical aspects of implementation. From experience, it may be unrealistic to have all the students play the game outside of class. This means playing the game in-class, heightening the need for efficiency and ease of use. While both games have supporting websites that offer suggestions to educators planning on using the game, we find that [*d0x3d!*] has two additional aspects that make a difference. First, the *[d0xed!]* website includes videos that concisely and effectively explain the rules of the game. While it may be unreasonable to expect students to play the game outside of class, given them a ten-minute online video to watch before coming to class is pretty low cost to even the least enthused students. Second, [*d0x3d!*] is open source and everything needed to play the game can be retrieved online and printed out for free.

7 Conclusions

In this paper we have reviewed the strengths and weaknesses of two table-top games, *Control-Alt Hack* and *[d0x3d!],* as well as their viability as teaching tools in the undergraduate classroom. We discussed in particular the role of language, competitive vs. cooperative game-play and the role of dynamic modeling. We conclude that *[d0x3d!]* is preferable as an educational tool to be used in-class and we will be attempting to use it in a perspectives course that includes non-computer science students during the 2014-2015 school year. Future work includes observations and results from the use of the table-top games in undergraduate courses.

8 Acknowledgements

This work is partially supported by NSF grant DUE-1141314, by the John S. Rogers Science Research Program of Lewis & Clark College, and by the James F. and Marion L. Miller Foundation. We would like to thank Richard Weiss for useful discussions. We further thank Alicia Kirkland, Miles Crabhill, Jon Poley, James Josephson, Christian Dicker, Sam Kelly and John Sibandze for their feedback and play-testing.

9. References

[1] Tamara Denning, Tadayoshi Kohno, and Adam Shostack, Control-Alt-Hack: A Card Game for Computer Security Outreach, Education, and Fun, Technical Report UW-CSE-12-07-01, University of Washington, 2012.

[2] Mark Gondree and Zachary N.J. Peterson, Valuing Security by Getting [d0x3d!]: Experiences with a Network Security Board Game, Proceedings of the 6th Workshop on Cyber Security Experimentation and Test (CSET), 2013.

[3] Zagal, J. P., Rick, J., and Hsi, I. Collaborative games: Lessons learned from board games. *Simulation and Gaming* 37, 1 (March, 2006).

[4] Cyber Security Defense Competition, http://www.nationalccdc.org/, accessed 6/10/14