Auction Hero: The Design of a Game to Learn and Teach about Computer Security

Sonia Chiasson
Carleton University
Ottawa Canada
chiasson@scs.carleton.ca

Manas Modi
Indian Institute of Technology
Guwahati, India
manasmodi@gmail.com

Robert Biddle
Carleton University
Ottawa, Canada
robert_biddle@carleton.ca

Abstract: Although computer security is a concern for online users, many have difficulty making effective security decisions. Auction Hero is a simulation game modeling life online that aims to improve users' mental models of computer security and help users make more secure decisions. It attempts to simulate real life by making security a secondary consideration that requires vigilance but that may not always be the user's main priority. We present our design, the first prototype of the game, and the results of a cognitive walkthrough evaluation.

Introduction

With increased reliance on online systems, computer security and privacy are a significant concern for many institutions and individuals. Attackers manipulate users and systems to their advantage and we must address this problem from a technological perspective as much as possible. However, we should also aim to equip users with the knowledge to make informed decisions when their input is required. In this work, we aim to familiarize users with common online attacks, help them recognize the attacks, and teach them how to protect themselves. In particular, we want to help users build better mental models of online computer security.

The work includes building a computer game to model life online and reflecting the behavioural setting and pressures that make computer security so challenging. E-commerce buying and selling is the principal motif and the game mechanic includes making profitable transactions while avoiding various computer security attacks. We propose that learning about computer security should be a secondary task so that users can become accustomed to applying the peripheral awareness and continuous vigilance required with computer security while distracted by other tasks. We present the initial design of the game, describe the first prototype, and discuss results of a cognitive walkthrough evaluation that will inform later work.

Background

Improving security and privacy is challenging because of several unique characteristics. For example, users typically focus on primary tasks (Whitten & Tygar, 1999), leaving security as a secondary concern. They may concentrate on some aspects of strong security but undermine their efforts by neglecting other aspects, and they may act insecurely without realizing that this can have later ramifications. Existing user interfaces are often difficult for users to understand, or they impose unreasonable expectations on users, which further increases chances of security compromises. Accepted human-computer interaction (HCI) design principles may not apply because of the adversarial nature of security: attackers will actively try to breach the system, will leverage interface cues available to legitimate users, and will deceive users by spoofing trusted indicators.

A key element emerging from several human factors studies of security (Whitten & Tygar, 1999; Chiasson, van Oorschot, & Biddle, 2006) is that users typically have poor mental models of security threats. Users seldom understand the nature of good defence or how to adapt as technological threats evolve. Camp

Publication: S. Chiasson, M. Modi, R. Biddle (2011). AuctionHero: The Design of a Game to Learn and Teach about Computer Security. AACE World Conference on E-Learning in Corporate, Government, Healthcare & Higher Education (E-LEARN), October 2011. (Brief paper, 6 pages)

(2009) suggests using mental models as an explanatory device for understanding user behaviour. Our current work extends this idea by also aiming to directly influence users' mental models of security. Our research suggests that better mental models of the threats and defences will be helpful, and that it is possible to persuasively influence users towards more secure attitudes and behaviour.

The idea of mental models was introduced by Craik (Craik, 1943) almost 70 years ago, suggesting that humans translate external events into internal models used for reasoning. More recently, Young (1983) suggested that mental models are users' mental representation of their interaction with complex devices. Johnson-Laird (Johnson-Laird, 1986) postulated that mental models include only the minimum functionality required to understand the subject, and that people make assumptions to compensate for lack of knowledge. Norman's user-centered system design (Norman, 1986) has been very influential in HCI work on mental models, emphasizing that users form mental models based on interaction with a system, so designers must carefully design the system to convey the appropriate image.

Serious games (Bogost, 2007) have a primary purpose other than entertainment and allow people to interact with content in an engaging and immersive way. CyberCIEGE (Cone, Irvine, Thompson, & Nguyen, 2007), a simulation game to teach network security administration, has been used in university computer networking courses. Anti-Phishing Phil (Sheng et al., 2007) is a short game to teach people how to identify phishing websites (i.e., malicious websites posing as legitimate sites, intended to trick users into revealing their credentials). Smokescreen (Six to Start, 2011) is an elaborate, immersive game to teach teenagers about the risks of social networking. OnGuardOnline.gov (Federal Trade Commission, 2011) is a US government website offering video tutorials and multiple choice quiz games about various topics of online security.

In Bogost's approach to persuasion (2007), he posits that the interactive nature of computer games affords a new approach to rhetoric. He suggests that interactive software now affords a kind of "procedural rhetoric", whereby the software includes logic that embodies the rhetorical appeal. The nature of the appeal is not explicitly or directly communicated, but rather is discovered by the player through the exploratory nature of game play. The essential characteristic of aligning the game mechanic with procedural rhetoric is that success at the game must include appreciation the rhetorical appeal.

Game Design

The overall research goals of the project are using principles of usable security, mental models and serious games to develop the game, seeing how well the game increases understanding of security, and evaluating its impact on security and privacy behaviour in real life. The initial target audience is young adults in post-secondary institutions who are transitioning to an adult life where they have increasing responsibilities that require them to make security-related decisions. We anticipate that the framework will also be useful in the future for hosting modules created or adapted for other audiences such as office workers, teens, or children.

The game mechanic accounts for some of the engagement potential, but there is also a need for more affective elements. In particular, the game should use affective design (Johnson & Wiles, 2003), especially humour, to engage and immerse users, and keep them committed to the "magic circle" (Castronova, 2005). The idea of the magic circle is keeping users focused on the game world, and suspending their disbelief about the pretend environment. Moreover, this same mechanism will allow us to supply users with primary tasks, relegating computer security to a secondary task, just as happens in the real world.

Premise

The user takes on the role of an online auction trader who earns a living by building and selling robots, ultimately trying to earn enough money and reputation points to become an "Auction Hero" (a pun on "action hero"). Each robot is composed of five parts (head, body, two arms, and feet/base). The user must purchase all required parts before being able to assemble a robot and put it up for auction. As in real life, the trader must also be vigilant about computer security risks: phishing emails attempt to steal credentials to gain access to the trader's money, a weak account password may be cracked in a guessing attack (giving access to money and inventory), and the computer system may become vulnerable to malware if the antivirus is allowed to become out-dated (giving access to money and inventory, and making the system behave unreliably).

The main game is divided into 5 missions, each progressively more difficult, with post-mission quizzes inserted between missions. A screenshot of the main user interface is available in Figure 1. The top panel includes the user’s score (funds and reputation) and a navigation bar indicating the user’s progress through the game. The left-middle pane is the robot assembly area containing the blueprint for construction. The right-middle pane shows the user’s current inventory of robot parts. Several tabs (Inbox, Bank Account, Buy, and Sell) allow the user to manage email, bank transactions, and auctions. The bottom pane includes a System Status console which includes the antivirus status and a newsfeed of updates from the in-game world.

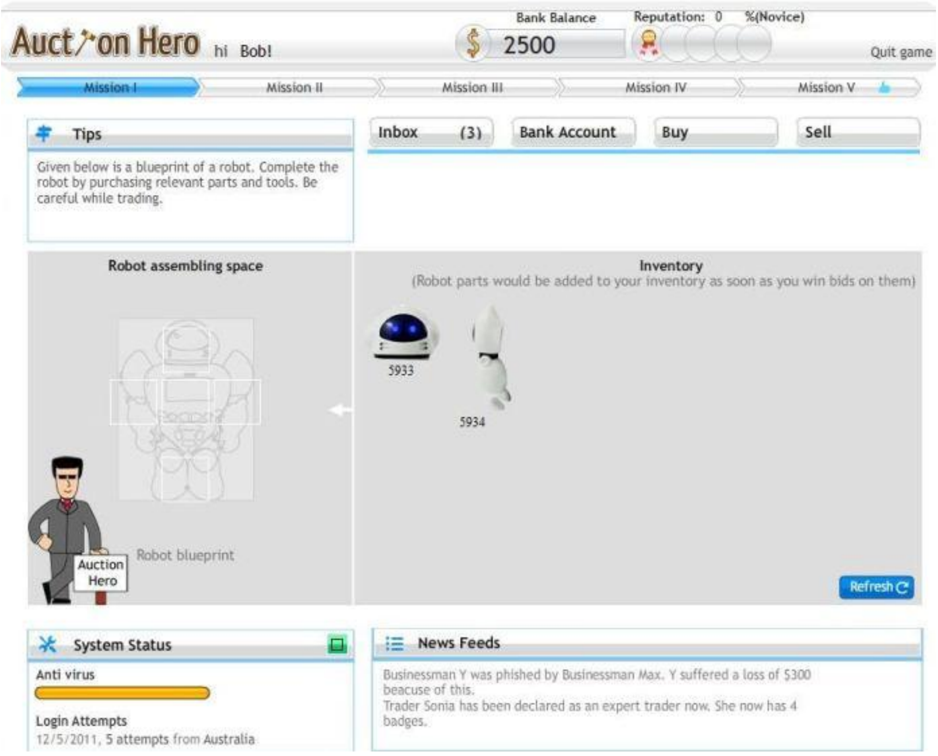
Learning objectives

The intention of the game is to use it as a platform for teaching about a variety of online security threats. The game is organized as a series of missions. Each mission has game goals such as earning money, but also pedagogical goals such as learning about phishing. While we initially focus on two specific threats, the intent is to develop further missions to teach about other online threats (such as password attacks).

Phishing: Phishing is a form of social engineering where users are tricked into entering their credentials on an illegitimate website, often designed to mimic an authentic site or otherwise appear legitimate (James, 2006). Typically, users receive email prompting them to visit a given website where they are asked to log in or provide other credentials that are then used by attackers to impersonate the user.

While playing the game, users will learn that this type of attack is possible, common characteristics of phishing scams in order to better detect them, potential consequences of falling victim to phishing, and how to handle phishing attacks. Users will receive phishing emails within the game, some mimicking legitimate system emails (for example, saying that they have won an auction, but for an item on which they never bid), others containing “too-good-to-be-true” offers (for example, offering deeply discounted items for sale). The emails will contain links to websites asking for some of their in-game credentials. If users fall for the phishing scam, their money, reputation, and/or inventory will suffer as an attacker breaks into their account. In case of a successful attack, an explanatory warning will be displayed. The post-mission quizzes will test users’ knowledge of phishing, awarding money or reputation points for correct responses and offering further instruction when users answer incorrectly.

Antivirus Management: Antivirus software is intended to detect, prevent, and remove malware (malicious software) from a user’s computer. Malware may include viruses, trojans, worms, spyware, and other threats. An antivirus should be installed and always running on a computer, but it must also be regularly updated because threats are continually evolving. New threats appear and old threats morph to avoid detection.



Bank Balance: 2500

Reputation: 0 %(Novice)

Given below is a blueprint of a robot. Complete the robot by purchasing relevant parts and tools. Be careful while trading.

(Robot parts would be added to your inventory as soon as you win bids on them)

12/5/2011, 5 attempts from Australia

Businessman Y was phished by Businessman Max. Y suffered a loss of $300 beacuse of this.
Trader Sonia has been declared as an expert trader now. She now has 4 badges.

Figure 1: A screenshot of the AuctionHero prototype 1.

A computer infected with malware can be compromised in several ways, including secretly recording and transmitting user input, stealing stored data, or altering the functionality of existing software or data.

The learning goal within the game is to inform users of the necessity of an antivirus, show potential consequences of letting its subscription lapse, and teach how to maintain the antivirus. The Auction Hero console includes an antivirus indicator which decreases over time. If users allow their antivirus to get too out-dated, then the risk of infection increases. As a result, a user's money or reputation may be decreased, items in inventory may disappear, items may be placed on auction with low minimum bids, or high bids may be placed on auction items without the user's knowledge.

Implementation

A web-based client-server architecture allows for easy distribution to a wide population. The user interface is built as a Flash application embedded in a web page. The Flash application controls all aspects of the user interaction. It is supported server-side by PHP scripts and a mySQL database.

Algorithms for handling all decision-making within the game are written in PHP. This includes all auction processing (bidding and selling), email generation (including phishing emails), transaction processing, funds and reputation maintenance, and quiz managing processed server-side based on requests from Flash. The decision to decouple the Flash interface from the decision-making allows for greater flexibility in the game. We can change the prevalence of phishing emails or the algorithms for auction processing (e.g., a higher reputation increases the likelihood of winning an auction or an unreasonably high minimum bid reduces chances that a user's item will be sold) without requiring modifications to the user interface.

Prototype 1

Based on several iterations of sketches and low-fidelity prototypes, we developed the first functional prototype of the game. It included the introductory segments and the first two missions. The first mission was comprised of buying parts to build a single robot. The second mission included assembling the robot and successfully selling it. Throughout both missions, users had to monitor the antivirus to ensure that it did not get out-dated and had to avoid falling for phishing and scam emails that appeared in the inbox.

Cognitive Walkthrough

A cognitive walkthrough is a usability evaluation inspection technique often used in the early stages of development that focuses on the learnability of a user interface (Wharton, Bradford, Jeffries, & Franzke, 1992). It is conducted in-person by a group of experts and assesses the potential for exploratory learning by simulating the cognitive activities of a user, usually represented as a persona, who is learning to perform key tasks with the system through exploration.

We conducted a 2-hour cognitive walkthrough with seven experienced HCI researchers, including some with expertise in usable security and serious game design. The session was video and audio recorded and was summarized by a note taker. Two personas were defined and assigned to specific individuals who were especially responsible for considering the tasks from their persona's point of view. The first persona, Alice, is a first year university student with a new computer. She knows that there are dangers online but is not sure what they are. She has just been told that there is a cool new security game and is going to try it out. The second persona, Bob, is a high school student in a computer class using a school computer. His teacher has just assigned his class the task of playing this computer game.

Several tasks were identified for evaluation during the cognitive walkthrough. Each task was divided into smaller sub-tasks, including security related sub-tasks such as updating the antivirus and avoiding phishing emails. The goal was to evaluate the introduction to the game and the first two missions.

The recordings of the cognitive walkthrough session were carefully reviewed and analyzed. One major suggestion was to reposition the role of the avatar (shown in figure 1), making him a trusted advisor and introducing a new ``trainee" character to represent the player, who will gradually change appearance to become an Auction Hero, Other suggestions included adding an activation process triggered by email before purchased items become available in inventory to encourage users to monitor their email, and reorganizing the 5 missions with respect to the security threats they address. To support building of mental models, the advisor should summarize what happened in the mission, going over the successful attacks and cases where the user's quick thinking avoided attack.

After our cognitive walkthrough had served to identify the specific issues we described above, we then reflected on the more general lessons. The emerging pattern involved the relationships between several conceptual frameworks inherent in our project. We identified the importance of clarity and simplicity for the auction interface and interaction because we would need the interplay between the security issues and the auction to be evident. The usability, therefore, needed to even better than a real auction site, but fortunately the complexity of the auction could be simplified. Similarly for the depiction of attacks, we needed this to be very clear lest the user not even notice the way they worked or how they related to their engagement with the auction process. The following structure emerged: we needed to foreground the auction, keep the security issues in the background, simplify both, but keep their essential elements intact. As with many applications of computing to pedagogy, the advantage is a kind of scaffolding. The scaffolding works by simplifying or eliminating less important details while exposing the critical learning topics. In our case, the involvement of both primary and secondary tasks means the scaffolding needs to be applied to both, and this only became apparent after interpreting what happened in the cognitive walkthrough.

Discussion and Conclusion

In real life, users tend to focus on their primary tasks, sometimes completely ignoring the secondary task of computer security. Primary tasks often require the user's full attention and concentration, and paying attention to a secondary task inevitably detracts from their primary activity (Wickens, Kramer, Vanasse, & Donchin, 1983). Considered in this light, it is unsurprising that security is ignored, especially given that security can be a significant burden. Security may be time-consuming, may be confusing, or may hinder progress towards the primary tasks. Unfortunately, attackers will leverage these high-cognitive-load, primary task situations as opportune moments to attack exactly because users' attention is focused elsewhere. For example, a phishing attack may rely on the fact that users will be focused on the tasks of checking their email and responding to an urgent request to verify their account information, rather than examining the URL of the requesting website or otherwise questioning the legitimacy of the request (Dhamija, Tygar, & Hearst, 2006).

We suggest that *learning about security* is also a secondary task for most users. It can easily be set aside or given only minimal attention as other tasks demand the user's attention. As such, traditional methods of education users about security tend to have limited success. Furthermore, bringing computer security to the foreground during the education process may teach users about security and may help them master certain skills but it does not provide training or practice in applying those skills while distracted by primary tasks.

Our approach of embedding security as a secondary task within the Auction Hero game offers a different approach to teaching about computer security. It provides learning in a context similar to those faced in real life, with similar pressures and demands on the user's attention. The game offers an exploratory platform where tradeoffs and consequences of security decisions can be observed because they have a direct effect on the user's success within the game. To succeed, users have to master both the skills needed for selling and buying robots and skills needed to avoid security threats when they are presented as secondary tasks. This mirrors real-life, where users similarly need continuous peripheral awareness of security while focusing on their primary tasks. The challenge in building Auction Hero is offering a simplified world that exposes the interplay between the primary and secondary tasks while still allowing users to experience the tension between the two.

In this paper, we explored the motivation and design for Auction Hero, a computer game to teach about online computer security and improve users' mental models of security. The cognitive walkthrough evaluation of our first prototype revealed general enthusiasm for the game, but also identified several areas for improvement for the next iteration. We are currently working on a second prototype which will allow user testing and evaluation of the learning effects.

Acknowledgements

This work is funded by the National Institute of Standards and Technology (NIST), an agency of the United States Department of Commerce. Funding from the Canadian GRAND Network Centres of Excellence is also acknowledged.

References

Bogost, I. (2007). *Persuasive games: The expressive power of videogames*. MIT Press.

Camp, J. (2009). Mental models of privacy and security. *IEEE Tech. and Society*, *28*(3).

Chiasson, S., van Oorschot, P., & Biddle, R. (2006). A usability study and critique of two password managers. In *15th USENIX Security Symposium.*

Cone, B., Irvine, C., Thompson, M., & Nguyen, T. (2007). A video game for cyber security training and awareness. *Computers & Security*, *26*.

Craik, K. (1943). *The nature of explanation*. Cambridge University Press.

Dhamija, R., Tygar, J., & Hearst, M. (2006). Why phishing works. In *ACM Conference on Human Factors in Computing Systems (CHI).*

Federal Trade Commission. (2011). *Onguardonline.gov*. http://www.onguardonline.gov/.

James, L. (2006). *Phishing exposed*. Syngress.

Johnson, D., & Wiles, J. (2003). Effective affective user interface design in games. *Ergonomics*, *46*, 1332-1345.

Johnson-Laird, P. (1986). *Mental models*. Harvard University Press.

Norman, D. (1986). Cognitive Engineering. In D. Norman & S. Draper (Eds.), *User Centered System Design: New perspectives on Human-Computer Interaction* (p. 31-62). Lawrence Erlbaum Associates.

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L., Hong, J., et al. (2007). Anti-phishing Phil: The design and evaluation of a game that teaches people not to fall for phish. In *ACM Symposium On Usable Privacy and Security (SOUPS).*

Six to Start. (2011). *Smokescreen*. http://www.sixtostart.com/smokescreen/.

Wharton, C., Bradford, J., Jeffries, R., & Franzke, M. (1992). Applying cognitive walkthroughs to more complex user interfaces: Experiences, issues, and recommendations. In *ACM Conference on Human Factors in Computing Systems (CHI).*

Wharton, C., Rieman, J., Lewis, C., & Polson, P. (1994). Usability inspection methods. In J. Nielsen & R. Mack (Eds.), (p. 105-140). John Wiley & Sons, Inc.

Whitten, A., & Tygar, J. (1999). Why Johnny can’t encrypt: A usability evaluation of PGP 5.0. In *8th USENIX Security Symposium.*

Wickens, C., Kramer, A., Vanasse, L., & Donchin, E. (1983). Performance of concurrent tasks: A psychophysiological analysis of the reciprocity of information-processing resources. *Science, 221*(4615).

Young, R. (1983). Surrogates and Mappings: Two kinds of conceptual models for interactive devices. In *Mental Models*, D. Gentner & A. Stevens (Eds.), (p. 35-52). Lawrence Erlbaum Associates.