Editors: Matt Bishop, bishop@cs.ucdavis.edu
Cynthia Irvine, irvine@nps.edu

Security Education Using Second Life

Jungwoo Ryoo, Angsana Techatassanasoontorn, and Dongwon Lee
Pennsylvania State University

Institutions of higher education, government agencies, and private organizations have been making sustained efforts to teach some information security skills more efficiently. In these efforts to improve security education, the dominant pedagogical approach has been to use security exercises in a lab setting. However, this approach might not deliver effective learning experiences for two reasons:

- *Narrow focus on technology.* Current laboratory exercises focus on security attacks and technical solutions, yet security management must also account for operations and people.[1] Failing to address any of them leaves systems vulnerable, so security education must equally emphasize technical security measures and safe online behaviors.
- *Decontextualized learning.* Most existing security labs teach abstract concepts that aren't situated in real-life contexts, such as simple message-sending scenarios between people, to teach security protocols and encryption methods.[2] However, a student who learns security concepts solely in a decontextualized setting might not be able to apply the necessary skills when facing real-life security threats.

Addressing these two shortcomings requires security education approaches built around real-world scenarios that actively engage students.[3] Just as a problem-based learning approach fosters a collaborative discovery process through solving authentic, real-world problems,[4] security education should be anchored in real-life problems that help develop technical security skills and promote safe online behaviors. Discovery learning is a paradigm that emphasizes students as active participants in the learning process as they interact with the environment and other students.

Sophisticated virtual environments that use 3D simulations are well-suited for such learning because they provide vicarious experiences and more realistic contexts than other technologies do. They not only make learning more enjoyable, but they also enable students with little knowledge about a problem domain to develop a greater understanding of it, better problem-solving skills, and higher-order thinking about issues and rationales to support their solutions. Second Life (www.secondlife.com), a 3D virtual immersive world that simulates everyday real-world activities, can serve as an ideal platform for incorporating both realistic scenarios and discovery learning into security education. Here, we share our experience in developing a scenario-based security education system using Second Life and implementing it in introductory courses on information security at Pennsylvania State University.

The Scenario

Our approach involves a learning module to help students obtain a basic understanding of how businesses and individuals can protect themselves against key security threats. At the end of the learning module, students should be able to

- appropriately configure a router and its built-in firewall to strengthen computer and network security;
- understand the implications of a router's weak security configuration;
- appropriately choose strong passwords;
- understand the implications of using weak passwords;
- appropriately choose Web sites that provide strong access control; and
- understand the implications of interacting with Web sites that don't provide strong access control.

We start by putting student teams in charge of opening a new virtual store in Second Life. Their main tasks are to purchase a router from an online store, install and configure it for their Second Life store, choose a type of product to sell, and stock the store with the products purchased from trustworthy online vendors. They must accomplish these tasks with a limited budget, but they have three team assets at the beginning of the module:

- an empty storefront on a Second Life island with the basic building structure and furniture provided;
- US$5,000 of cyber money to acquire the necessary computing equipment and products for the Second Life store; and
- an initial security readiness score of zero (using a Web-based tool, an instructor periodically evaluates and calculates security readiness scores as an average of the technical security readiness score and the online purchase behavior score).

Table 1. Technical security readiness score calculation.*

SCORE	SCORE CALCULATION
A router password setup	Zero through 100 points computed by a password strength test algorithm (based on the time it takes to crack a given password)
Firmware upgrade practices	100 points if a team upgrades router firmware when it becomes available; zero points otherwise
Firewall port settings	25 points if HTTP is enabled 25 points if SSH is enabled 25 points if FTP is disabled 25 points if Telnet is disabled

*The technical security readiness score is a weighted average of the router password setup (20%), firmware upgrade practices (30%), and firewall port settings (50%).

The technical security readiness score includes a router password setup (20 points), firmware upgrade practices (30 points), and firewall port settings (50 points); see Table 1. The online purchase behavior score depends on the choice of an online store, each of which has varying levels of access control, from none up to a maximum of four access control features. A team that buys something from an online store that has zero, one, two, three, or four access control features receives zero, 20, 40, 80, or 100 points, respectively. So, if a team makes all its purchases from two online stores, one with no access control and the other with two access control features, its online purchase behavior score would be 20 = (0 + 40)/2.

At the end of this learning module, the team that spends the least amount of money and has the highest security readiness score wins the game.

Virtual Stores and Scores

The virtual storefront in Second Life has shelving space to display products as well as a separate IT room to house the router and computers (see Figure 1a). Each store is also equipped with a message board (see Figure 1b) designed to engage students in various security attack scenarios. For example, in the aforementioned firmware upgrade scenario, the message board notifies students when new firmware is available: if they don't realize the message's significance and ignore it, the next message says that their router is compromised due to an exploit and must be reset. As a consequence of this oversight and lack of action, the team gets zero points for their firmware upgrade practices.

The message board can also show text messages generated either manually by an instructor or automatically by an attack engine. An XML/RPC method delivers messages to Second Life from an external Web-based interface for instructors. Separately from the message board, a scoreboard shows each team's overall security readiness score (see Figure 1c). The scores are updated every time students make security-relevant decisions, such as changing router passwords or firewall settings.

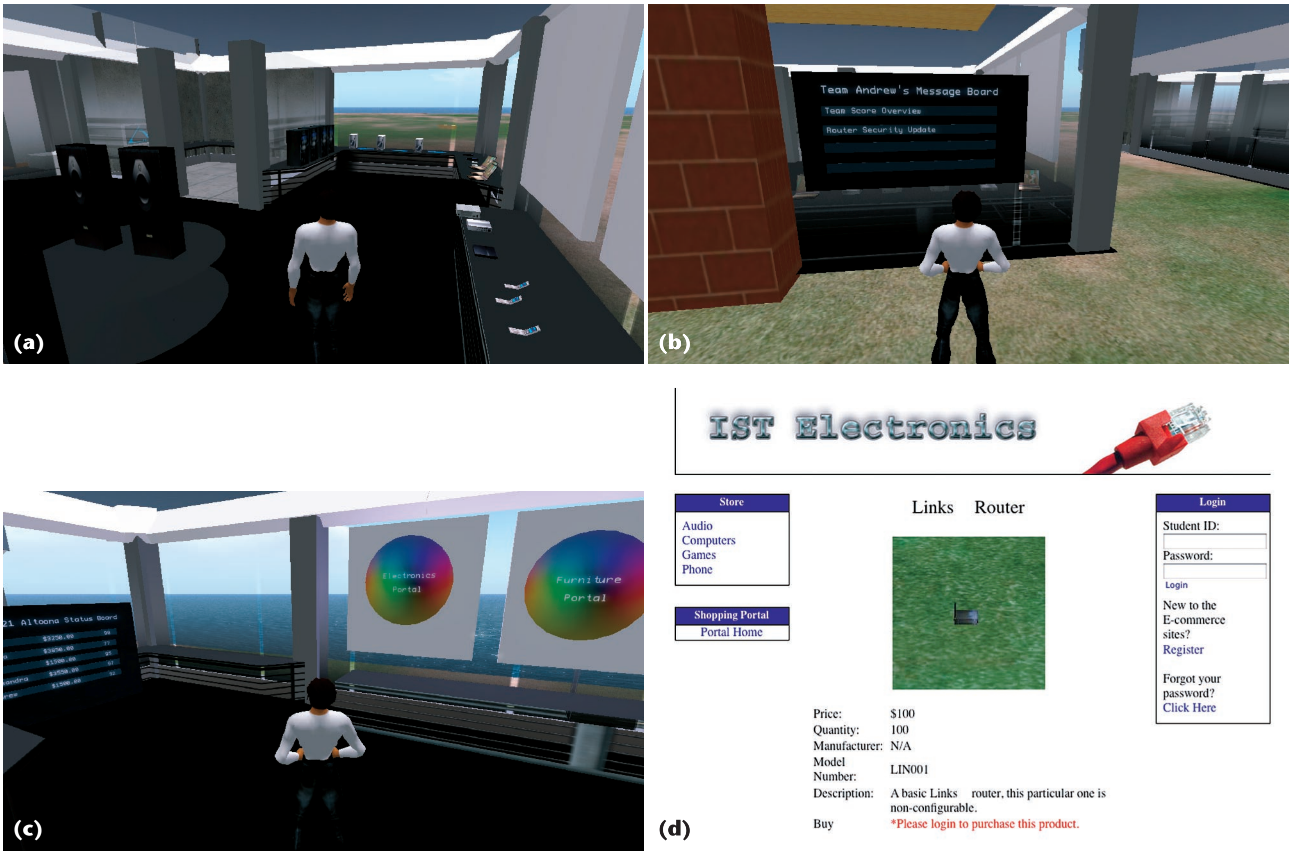
Online Stores

Our scenario provides eight online stores for furniture and electronics products that instructors created as stand-alone Web sites outside of Second Life (see Figure 1d). All the stores have similar site structures and navigation patterns and offer the same set of items, but the access controls vary among them—for example, the online stores use different combinations of access control methods. Some online stores might have zero access control features, whereas others might have one, two, three, or four.

Students first explore all the available online stores' security features (by trial and error or reading security and privacy statements) and then choose the one that they think is the most secure. This choice has a direct impact on their security readiness score. The team that picks the most secure e-commerce site receives the highest score. After deciding on an online store, a designated student team member registers and makes purchases that appear in the Second Life environment via an XML/RPC method.

Router Setup

The first item a student team is expected to buy is a router to protect their Second Life storefront from instructor-launched security attacks. When delivered to Second Life, the router, by default, has weak security settings, such as open ports, no password setup, and outdated firmware. Each team's task is to heighten its shop's security readiness level by properly configuring the router. As the team addresses the security problems one by one, the scoreboard reflects desirable behaviors by displaying a higher team score. Students configure their routers through a Web interface outside Second Life just as in a real-life situation.



Price:	$100
Quantity:	100
Manufacturer:	N/A
Model Number:	LIN001
Description:	A basic Links router, this particular one is non-configurable.
Buy	*Please login to purchase this product.

Figure 1. Virtual storefront and online shop. The student accomplishes his or her tasks by using (a) the virtual store, (b) the message board, (c) the scoreboard and portal, and (d) the online store.

Security Attacks

Once the stores are set up, the instructors launch random attacks against common information security vulnerabilities that users often overlook. To facilitate a fair evaluation, the instructors use the same set of attacks for all teams. For instance, each team's router password is tested for its strength. If a password recovery tool cracks it within a day, instructors change the router password the next day so that the affected student team members can no longer log on to their router. To reset the password, the team must pay a consulting fee ($500) to a teaching assistant posing as an IT consultant. Regaining access to the router is important because avoiding new attacks requires its reconfiguration. A firmware upgrade is a good example of this—unless upgraded to the latest version, the next attack (a new exploit capitalizing on the older firmware's weaknesses) will compromise the router again, forcing the students to resort to the consultant's help again for another $500. Teams are expected to proactively defend their Second Life shops from these attacks by adopting the best security practices. The evaluation focus isn't on what students do during or after an attack but is rather on the precautions they take before an attack.

Student Evaluation

We incorporated this security learning module into two Penn State "Introduction to Information Security" courses in 2008. Before their engagement with the module, we introduced the students to the virtual world in general and Second Life in particular through a class lecture, a short video clip, and a brief hands-on exercise.

Table 2 summarizes the module's evaluation on learning outcomes and overall enjoyment. A comparison of pre- and post-test understanding of security concepts shows that students significantly improved their comprehension. The evaluation of pre- and post-self-efficacy in technical security skills and safe online behaviors likewise shows improvement in students' confidence in their ability to use technical security measures and safe online behaviors in a real-life setting. Finally, students seemed to enjoy their learning through the Second Life module—one student specifically commented, "We were very impressed with the realistic router setup, the self-updating scoreboards, and the interaction between the Web pages and Second Life."

Table 2. Evaluation of the Second Life security module.*

MEASURES	PRE-LEARNING		POST-LEARNING	
	MEAN	STANDARD DEVIATION	MEAN	STANDARD DEVIATION
Conceptual security understanding (13 questions)	9.59	2.42	12.66	2.15
Technical security self-efficacy (7-point Likert scale)	5.88	1.31	6.27	1.15
Safe online behavior self-efficacy (7-point Likert scale)	5.98	1.26	6.28	1.21
Enjoyment (7-point Likert scale)			5.19	1.75

* Conceptual security understanding was measured by using multiple-choice questions that evaluate an understanding on a router setup, security threats, and appropriate access controls; technical security self-efficacy was measured by asking students to respond to the statement, "I feel confident that I can use technical security mechanisms to address security threats"; safe online behavior was measured by asking students to respond to the statement, "I feel confident that I can engage in safe online behaviors to effectively deal with various security threats"; enjoyment was measured by asking students to respond to the statement, "This activity was fun to do."

In building our first learning module in Second Life, our lack of expertise in its propriety programming language and in building 3D objects in general was often a hurdle. Nevertheless, the preliminary results from our evaluation of the Second Life–based security education approach are encouraging. In fact, we now have additional funding from the US National Science Foundation to develop additional security learning modules and broaden our implementation and assessment efforts. □

Acknowledgments

The ACM Special Interest Group on Computer Science Education special projects grant sponsored this research. We thank Anna Squicciarini for her help with the incorporation of the Second Life security learning module in the "Introduction to Information Security" course and Bart Purcel for his assistance with Second Life administration. We also thank three undergraduate students, Taylor Davenport, Cody Halbleib, and Johnny Chen, for their programming work and assistance with the evaluation of the learning module in classes.

References

1. W.V. Machonachy et al., "A Model for Information Assurance: An Integrated Approach," *Proc. 2001 IEEE Workshop on Information Assurance and Security*, IEEE CS Press, 2001, pp. 306–310.
2. L. Hamey, "Teaching Secure Communication Protocols Using a Game Representation," *Proc. Australasian Computing Education Conf.* (ACE 03), Australian Computer Society, 2003, pp. 187–196.
3. Nat'l Research Council, *Evaluation and Improving Undergraduate Teaching in Science, Technology, Engineering, and Mathematics*, Nat'l Academy Press, 2003.
4. H.S. Barrows, "A Taxonomy of Problem-Based Learning Methods," *Medical Education*, vol. 20, no. 6, 1986, pp. 481–486.

***Jungwoo Ryoo** is an assistant professor of Information Sciences and Technology at the Pennsylvania State University-Altoona. His technical interests include software security, software architecture, and security management. Ryoo has a PhD in computer science from the University of Kansas. Contact him at jryoo@psu.edu.*

***Angsana Techatassanasoontorn** is an assistant professor in the College of Information Sciences and Technology at the Pennsylvania State University. Her research interests include information security, virtual worlds, and IT-enabled social innovations. Techatassanasoontorn has a PhD in business administration in information systems from Carlson School of Management, University of Minnesota. Contact her at angsanat@ist.psu.edu.*

***Dongwon Lee** is an associate professor in the College of Information Sciences and Technology at the Pennsylvania State University. His technical interests include data management, data security, and the Web. Lee has a PhD in computer science from the University of California, Los Angeles. Contact him at dongwon@psu.edu.*