Network Nightmares: Using Games to Teach Networks and Security

William Ryan
Ithaca College, Department of Strategic Communications
953 Danby Road
Ithaca, NY 14850
wryan@ithaca.edu

Jennifer Stewart
IUPUI, School of Informatics
535 W. Michigan St.
Indianpolis, IN 46202
jekstewa@iupui.edu

Dean Verleger
Dreamfed Games
200 South Rangeline Road
Suite 207D
Carmel, IN 46032
deanverleger@gmail.com

Jackie Crofts
Dreamfed Games
535 W. Michigan St.
Indianpolis, IN 46202
pollensaltas@gmail.com

ABSTRACT

We have created a game called *Network Nightmares* using an abstracted representation and simple game mechanics to introduce novice computer scientists to concepts in networks and computer security. The player plays from the perspective of a computer cracker looking for vulnerabilities in computer networks. This game uses an Angry-Birds-style interface where participants aim at and hit nodes within a computer network. This game is part of a larger research context to design simple media to extend the learning interface for an introductory computer science course outside of class hours by providing games, videos, and other media for students to engage with.

Categories and Subject Descriptors

K.3. [**Computing Milieux**]: Computers and Education

Keywords

Serious games, computer networks, computer security, education, abstraction

1. INTRODUCTION

Games are widely becoming a popular medium to teach instructional concepts in serious settings. They are useful for engaging students who are turning off to other forms of knowledge transmission as a way to keep students entertained and immersed in material they need to know to become effective professionals. [6] have demonstrated the efficacy of serious game in terms of knowledge gained and engagement when compared to a comparable text-based description of concepts for a university course on physiology. We have designed such a serious game teaching fundamentals of networks and security to an introductory

computer science course based as part of a series of media to be engaged with outside of the course and supplemental to the course lectures. This game, called *Network Nightmares*, is found at http://www.williamryanonline.net/nightmares/ and requires Flash Player 6.0 or higher to play. This game has been tested to work on Firefox and Chrome web browsers.

So far, games have been utilized in the field of computer science as a way to teach programming skills [1, 4]. We have taken the approach of building simple games, supporting smaller concepts and domains. As our game has been built to introduce networks and security, similar other games could deal with other high-level concepts such as data structures, computer architecture, operating systems, algorithms, and so forth. The key to this game design is keeping the development low-cost by having relatively simple learning objectives. While this game does not deal with any concept in the complexity or depth as [1, 4], it does provide an approach for building knowledge, supporting application, and developing strategy in using the concepts introduced to students.

As this was a simple game and was meant to be played on a student's own time, we wanted to explore games allowing a more abstracted nature to the content being learned in lectures. [3] explored content integration in serious games. He used the metaphor of chocolate-covered broccoli to describe games that do not integrate learning content and fun content well enough together. He explored two similar, though vastly differently represented games to help students learn division. The first game used intrinsic representations that displayed numbers on enemies' chests, corresponding to weapons that could be used to vanquish them. The second game used extrinsic representation that displayed weapons that could vanquish the enemy on the chest, followed by a series of division problems dealt with implicitly in the previous stage. [3] found very little evidence to suggest intrinsic integration was more effective from an instructional standpoint than extrinsic integration. He found no difference from the standpoint of time-on-task. He found the most convincing evidence intrinsic was better than extrinsic integration for less familiar (far) transfer tasks—where the nature of two independently performed task changes greatly—and not as a good for more familiar (near) transfer task—where the nature of the tasks are mostly the same. He did find, however, strong evidence of the motivational power of intrinsic integration in serious game design supporting games that are more abstracted in nature.

Two other games submitted to last year's FDG 2012 game festival demonstrated this idea of abstraction to instruct or teach. [5] designed a game to help those dealing with depression or those who have loved ones dealing with depression to experience and understand the cycles involved in depression. The game accomplished this by taking control away from player and forcing them into undesirable locations, even as the player tries to elude those locations. It uses metaphor to create an overwhelmingly hopeless experience meant to be a learning experience for players. [2] created a series of games for vocabulary improvement. In the first of the games described, the authors detailed Code Invaders where the game presented vocabulary the player was learning and relied on the meaning of the words to help the player navigate a maze to complete the game.

In all of these abstract games, the content to be learned is integrated into the mechanics and objective of the game as opposed to being separate from it. Our approach has taken a similar tact. We leverage game mechanics to convey meaning and importance of the learning concepts. In the next section, we present this game as it has been designed and how the representation accomplishes goals of helping players learn about computer networks and security. In the following section, we describe a plan for evaluating the efficacy of this approach. Finally, we conclude with future iterations to improve engagement and complexity of content dealt with in the game.

2. GAME DESIGN

The serious game designed leverages a more abstracted representation of content. The game is meant to instruct players on the basics of networks as well as the very basics of network security. The core concepts we represent in the game included the following from networks and security are described in Table 1.

Table 1. Serious game concepts

Concept	*Concept Description*	*Representation*
Network	Series of nodes and edges	Series of circles with connections
Node	An endpoint within a network	Circles fitted for viruses
Edge	Connection between two nodes	Lines connecting circles
Hub	Node connected to more than two other nodes	Circle connected multiple other nodes
Infection	A computer affected by a virus	Red instead of blue circles and lines
Port	A channel for communicating on a computer network	Separate networks connected by a lock
Virus	A dangerous computer program that does malicious deeds	Hazardous material symbol
Network Administration	An agent who maintains security for computer systems/networks.	An AI agent who sweeps the networks looking to clean up/block infections.

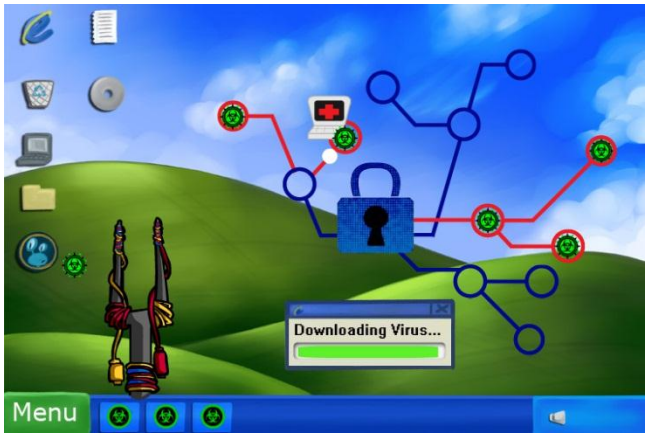

Figure 1. *Network Nightmares* first stage. Virus is being aimed and is ready to launch.

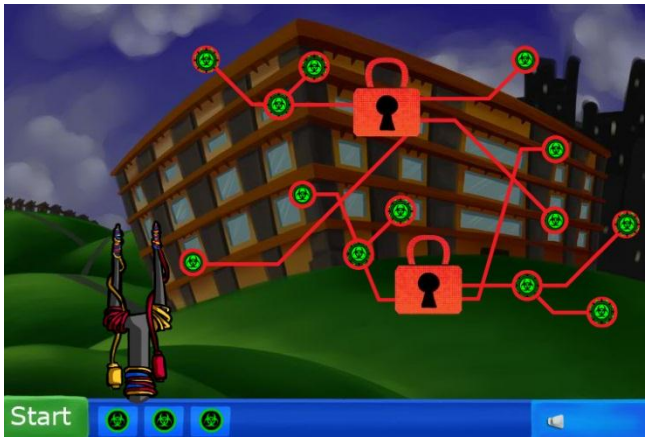

Figure 2. Completed second level.

For this game, the player takes on the role of computer cracker, releasing viruses on unsuspecting, though vigilantly guarded computer networks. We think this perspective provides insight into understanding the weaknesses of networks at a high level that network administrators face. It also provides a high-level way to address network concepts.

We use an Angry Bird game mechanic, where players attempted to launch viruses at the computer network. This launching mechanic gave players some control over what happens to the virus, but also relied somewhat on chance as to where the virus would land and infect exactly.

The number of viruses the player can unleash is limited to three, but the virus stock regenerates as long as there are infected nodes in the network.

At the same time the player is trying to infect the network, the network administrators are trying to heal infected nodes within the network. If an entire sub-network (as controlled by the port the player is infecting) is infected, the network administrator is shut out of the network and cannot fix it anymore. Each level is completed when all ports in the level have been fully infected as demonstrated in Figure 2.

2.1 Effective Learning Strategies

The conceptions of networks and security we wanted students to take away are embedded in the gameplay and abstraction of the representation of the game. They include:

1. Infect hubs for maximum damage.

This strategy draws out the importance of relationships within networks. We want players to walk away understanding that hubs are crucial to the power of networks. If their play leverages hubs, they will be more successful against network administrators. Hubs are also important from a network security perspective. Hubs become some of the most vulnerable aspects of a computer network when attacked. Denial of Service attacks frequently target hubs to affect the largest area of a network. Viruses/worms also leverage network structure, finding hubs to do the most damage.

2. Aim for areas furthest from administrators' current locations.

Networks are complex for automated systems to traverse. Although these administrators sense when and where an infection is occurring, networks are often vast with many sub-networks that must be scanned and monitored. From a network security standpoint, this means the most hidden and least scanned areas (or the areas furthest from the network administrators' current location in the game) are most vulnerable to immediate attack.

3. Focus on one port at a time.

Divide and conquer is a core algorithm and approach to network traversal (with its equivalent breadth-first search). In the game, it is wiser to deal with one port in its entirety first and then move on to other ports, than trying to take down all ports simultaneously. The reason is that each port has its own network administrator. We also want players to be cognizant of the role individual ports play in network security and how individual ports become vulnerable based on traffic coming in.

3. GAME EVALUATION

We have not had opportunities yet to test the efficacy of the game, but we do have a plan to use pre- and post-test structure to assess learning gains, learning strategy used, ability to apply concepts, and player engagement. We would like to compare this medium of serious games to other media such as video and text description against these metrics.

The evaluation plan will group students into one of four groups: control group; group reading a text description including definitions of concepts above and a brief description of computer security; group watching a short video describing computer networks and protocols; and the serious game group. All students will first complete a set of 16 Likert-scale questions demonstrating competency with the concepts above (2 for each concept). The control group will finish after this evaluation. Each of the other three groups will then be given their media to read, view, or play respectively. After they are finished with the media, they will complete the same 16 Likert-scale questions as before. They will also all answer the following two questions about their engagement:

1. On a scale with 1 being completely disagree and 5 being completely agree, the (text you just read, video you just watched, game you just played) was enjoyable.

2. On a scale with 1 being completely disagree and 5 being completely agree, the (text you just read, video you just watched, game you just played) held your attention.

They will also answer the following free response questions:

1. How can you apply what you learned to making computer networks secure?

2. How can you apply what you learned to using computer networks?

Finally, the participants playing the game will be asked a question about the strategies they used to successfully play the game.

These evaluations will allow us to compare learning gains in the game, learning gains as compared to other media, engagement with the various media, ability to apply knowledge between media, and whether student strategies match the effective learning strategies we have identified above.

4. FUTURE WORK

Future work for the game itself includes providing alternate modes and game mechanics to provide more challenges, but also convey real world concepts. The first proposed change would be to create a new game mode where player and AI switch roles. Now, the player plays the network administrator and needs to keep the network safe based on knowledge of network structures. Second, we'd like to add network nodes the player must protect at

higher levels. This would require a different strategy than just flinging the viruses everywhere, requiring more precision. Finally, we would like to experiment with different network models that provide even more complex relationships within networks that players must take account of as well as different kinds of computer attacks (e.g., Trojan horses, varying levels of vulnerabilities).

5. CONCLUSION

This paper describes our attempt to use serious games to supplement coursework in Computer Science dealing with networks and computer security. *Network Nightmares* uses abstracted representations to encourage learning of not just knowledge, but also strategies and approaches important for dealing with networks and security. We have purposefully relied on low-cost development and also simple game design to allow the opportunity for this game to be used as part of a more comprehensive media package including other games, scenarios, videos, and media. Our research plan calls for an extensive evaluation of this game in relation to other media to compare not just how effectively learning takes place, but also how engaging the media is. While evaluations have not yet taken place, we believe this game is an effective tool for introductory computer science courses.

6. ACKNOWLEDGEMENTS

We would like to thank the IUPUI Center for Teaching and Learning Curricular Enhancement Grant for funding this project and the IUPUI School of Informatics Technical Staff for helping to support our work, particularly David Phelps and Geoff Coryell.

7. REFERENCES

[1] Cohelo, A., Kato, E., Xavier, J., & Gonçlaves, R. (2011). Serious game for introductory programming, *LNCS, 6944*, 61-71.

[2] Bachhuber, J., & Saulnier, T. (2012). Wordplay games: Three game modules to improve student vocabulary knowledge. *FDG 2012,* 258-260.

[3] Habgood, M. P. J. (2007). *The Effective Integration of Digital Games and Learning Content*. (Unpublished doctoral dissertation). University of Nottingham, Nottingham, UK.

[4] Muratet, M., Torguet, P., Jessel, J., & Viallet, F. (2009). Toward a serious game to help students learn computer programming. *Int. Jour. Comp. Games Tech., 3*, 1-12.

[5] Rusch, D. (2012). Elude—Designing depression. *FDG 2012*, 245-257.

[6] Wong, W.L., Shen, C., Nocera, L., Carriazo, E., Tang, F., Bugga, S., Narayanan, H., Wang, H., & Ritterfeld, U. (2007). Serious video game effectiveness. *ACE 2007*.49-55.