Issues in Information Systems
Volume 17, Issue IV, pp. 120-126, 2016

WAR GAMES: SIMULATION VS. VIRTUAL MACHINES IN CYBERSECURITY EDUCATION

Matthew North, Utah Valley University, mnorth@uvu.edu

ABSTRACT

The use of both simulations and virtual environments have been used in education for many years. This study examines the results of the use of these techniques in a cybersecurity course. Four graduate-level course sections were used two examine the effectiveness of simulations versus virtual machines (VM) in learning a number of different cybersecurity topics. Two sections used simulation while the other two used VM. Course content and learning objectives for all four sections were the same. Student performance was assessed using the same rubrics and standards for all students. Results show that students working in virtual environments consistently achieved a higher degree of mastery of the cybersecurity concepts than their counterparts who used simulations. Students also reported greater degrees of trust and enjoyment in the VM course sections.

Keywords: Cybersecurity, Education, Virtual Machines, Simulations

INTRODUCTION

Educators have long striven to create authentic learning experiences for their students. Among the many techniques employed to create realistic and hands-on learning experiences, simulations and virtual machines (VM) have emerged as popular options in information systems and technology programs (Pusey & Sudera, 2012). This is largely due to the ability of these techniques to emulate real-life scenarios that graduates from technology-related programs are likely to encounter in the professional world (Hoffman, Burley and Toregas, 2012; Conklin, Kline and Roosa, 2014). By providing a realistic framework to experiment with cybersecurity issues such as malware, intrusion detection and prevention, and monitoring, students can better prepare for the legitimate concerns and challenges faced by the organizations that will employ them (Hoffman, Rosenberg, Dodge & Ragsdale, 2005; Pittman, 2013). Simulation and virtual environments both offer opportunities to create such realistic scenarios for learning, in a safe environment (Zahir, Pak, Singh, Palwick & Zhu, 2015).

In this paper we examine the effectiveness of simulation versus virtual environment for teaching cybersecurity techniques. Using four sections of a graduate-level cybersecurity class, we developed exercises and assessments for common cybersecurity lessons, then employed a simulation environments for students in two course sections to complete the exercises, while using virtual machines for the same exercises in the other two course sections. Student performance was assessed by the same instructor across all four sections using the same evaluation instruments, and the results were then tested for statistically significant differences, which were found. Additionally qualitative data were gathered from students to further inform the results of the experiment.

LITERATURE REVIEW

Authentic learning experiences have long been important components of effective instructional design (Mirkovic & Benzel, 2008). Simulation and virtual environments are two of many options, and improvements in both performance of, and access to, computing resources has fueled, even enabled a more extensive adoption of these modes of educational delivery (Ross, 2015). While fully acknowledging that these instructional tools are not new—simulators were largely pioneered in the aviation and aerospace industries more than five decades ago—universities have seen an extensive expansion of their use in more recent years (Schneider, 2013). Particularly in disciplines that involve computing technology, the adoption of simulations and VM have seen a recent, rapid increase in adoption (Mirkovic, Dark, Du, Vigna & Denning, 2015).

Cybersecurity is among the most optimal topics to teach using artificial environments (McGettrick, 2013). There are two primary reasons for this. First, cybersecurity, by necessity, touches potentially dangerous and risky topics including malware (viruses, worms, etc.), network vulnerabilities, and design flaws (Dark, 2014; Patel, 2014). To allow students of cybersecurity to experience these very real risks in a real computing environment could put that environment at risk for actual compromise, exposing the system's owner to unnecessary risk. This may also expose students to liability. Simply put, using a real computing environment to teach learners about cybersecurity is not a good idea (Patel, 2014). Additionally, artificial environments such as simulations and VM provide safe spaces for students to actually intentionally unleash potential cyber-problems, in order to observe, intervene and repair in ways that will not harm operational and mission-critical systems (Bergin, 2015; Dark, 2014). Rather than simply learning *about* cyberthreats, students can examine them first-hand, in ways that better prepare them for real-world security needs (Shumba, 2006).

Although these techniques can facilitate a desirable environment for testing and teaching, some continue to express concern over such detailed instruction—instruction that could enable a learner to engage in unethical or even illegal behaviors (Cormack, 2015; Dipert, 2010; Radziwill, Romano, Shorter & Benton, 2015). In some instances, even students have expressed reticence at the prospect of unleashing a virus on a computer or network, or probing a web application for possible vulnerabilities (Cheolho, Jae-Won, & Kim, 2012; Furman, Theofanos, Choong & Stanton; 2012). Despite such hesitations, most experts agree that the best way to prepare ethical and capable security professionals is to ensure that they have the best possible understanding of threats and techniques employed by so-called black hat hackers (Heckman, Stech, Schmoker & Thomas, 2015). Furthermore, advocates of authentic educational experiences in cybersecurity argue that simulation and VM have now become essential in preparing new generations of ethical cybersecurity professionals (Quigley, Burms & Stallard, 2015).

With the need established for competent cybersecurity specialists, we recognize the importance of education within a safe environment. Some experts have advocated specifically for simulations to be used in cybersecurity (Mahoney & Ghandi, 2011); while others favor and promote VM solutions (Babiceanu & Seker, 2016; Locasto, Ghosh, Jajodia & Stavrou, 2011). The difference between the two is subtle, but important: In simulations, only a specific, pre-defined set of options and outcomes is possible, while in VM, all of the full capabilities of a system (albeit an artificial system) are available to the user. Thus, the level of authenticity is raised in VM versus simulation, but so is the level of risk (Yoo & Shon, 2016). Virtual machines infected with malware, for example, can be deleted with no harm done, so long as they are not able to share resources with their host systems. A simulation can demonstrate what such an infection might be like, but only to the extent that the simulation is configured to illustrate the infection—it's only as good as its defined scope in its ability to teach, but this also guarantees that it won't *actually* infect anything (Vassilev & Celi, 2014; Williams & Krueger, 2005). Much debate continues on the tradeoff between higher authenticity and higher safety (Adams, Hitefield, Hoy, Folwer & Clancy, 2013; Burley, Eisenberg & Goodman, 2014; Dark & Mirkovic, 2015; McDuffie & Piotrowski, 2014; Paus-Hasebrink, Wijnen & Jadin, 2010).

With this debate in mind, and a desire to understand if one method is preferable over the other, this study was undertaken.

RESEARCH METHODOLOGY

The methodology for this study was designed to address two research questions:

1. Is there a difference in student learning on cybersecurity topics when using simulations versus virtual machines for instruction?
2. Will students indicate a preference for learning via simulation versus virtual machine?

The first question can be stated as a hypothesis and tested empirically:

H_1: Graduate students in cybersecurity will demonstrate the same level of mastery whether topics are taught via simulation or virtual machine.

The second question is answered qualitatively through surveys of students. Since students in the study were not exposed to both simulation and VM, they were not asked to compare the two educational delivery techniques, but rather, to simply provide feedback about their experience, preferences and likes/dislikes of the systems.

Four sections of a graduate-level course on cybersecurity at a large national university were selected for this study. The course covers topics that include malware infection, SQL injection, network monitoring and defense, and incident response. All students involved in the classes are required to take it, and all are pursuing master's degrees in either Cybersecurity or Information Technology. Two sections were taught in the fall semester, and two more were taught in the spring semester. In all, 42 students were enrolled in the two course sections that completed exercises via virtual machines, and 47 students were enrolled in the two sections that used simulations. Students completed three exercises using the selected delivery modalities: malware detection and mitigation, SQL Injection, and network monitoring. Student performance was evaluated using a common rubric and then scores across the four sections were compared for statistical difference using a standard *t*-test. Further evaluation of student experience was then conducted by surveying the students and asking about their opinions regarding the simulation or virtual machine.

RESULTS

Since the study participants were graduate students with advanced standing (more than half way to completion of their master's degrees), it was not surprising to see high completion rates on all three of the assignments that were used. In fact, 100% of students completed all three exercises in all four sections. Using student performance data on the three assignments, we were able to use *t*-tests to determine if statistically significant differences occurred between simulation and virtual machine modes of delivery.

Table 1. *t*-test P Values for Three Cybersecurity Assignments

Malware Assignment	SQL Injection Assignment	Network Monitoring Assignment
.00648	.676	.00027

With an alpha level of .05, we can reject the null hypothesis for the Malware and Network Monitoring assignments—there is a statistically significant difference between student performance scores. Post-hoc analysis shows that in both instances, student scores were higher in the VM environment than in the simulation environment. With regard to the SQL Injection Assignment, we fail to reject the null hypothesis. There is no statistical evidence on this assignment that students benefit from use of a virtual machine as opposed to a simulation.

With these results in hand, we turn to qualitative survey data to answer the second part of our research question: do students prefer one modality over the other. A selection of student comments is telling.

Simulation comments:

- "Do not use the SIM. The SIM requires work. The cause and effect of changes is impossible to see. The results do not make any sense."
- "I had high hopes for the simulation but it disappointed. It was not realistic and there were little decisions for us to actually make. I expected it to be more interactive and like a real-world environment."
- "The capstone simulator needs some more work to become more realistic and match user guide. The controls and impacts some controls had did not make logical sense."
- "The simulator, while a good idea in theory, is ineffective in practice. The simulator does not supply enough information about events and incidents to give students the feedback necessary to make informed decisions."

VM Comments:

- "I love the hands-on approach. Getting to actually contain a virus, spot an unattended port, etc. helped me learn the concepts better."

- "Using actual software and monitoring tools enhanced my learning. This is so much better than just reading about it in a book."
- "I got frustrated when the lab manual didn't explain why I got the results I did. Then I googled a little about what I was seeing in the VM and I found out Windows Server has a log file that records some network activity. I learned way more than I even had to for the lab."

These comments are reflective of an overall trend in student comments on the surveys. Students did not know that other sections were using a different delivery mode, so there was no comparing being done by the students; they were simply reacting to what they experienced. Almost unanimously, students in the VM sections reported positive experience and appreciating the 'real-world' feel to the experience, while students in the simulator sections regularly reported feeling frustrated by a lack of understanding of how the simulator worked and determined its responses. Further, students expressed a desire to do more in the simulator environment than that environment would allow.

SUMMARY

Based on the results of this experiment, it is clear that students enjoy getting their hands on the computer and being able to control the environment they're working in. In two out of three instances, student performance in a virtual machine environment was demonstrably better than in a simulator environment. While students did perform well on all of the assignments used to test our hypothesis, use of the VM never proved to be worse than the simulator in terms of student outcomes.

Student reaction to both environments included appreciation for a hands on approach, however appreciation for the VM delivery was more positively received. The ability to deviate from the planned assignment requirements, to explore misunderstood or unexpected results was seen as a positive by students in the VM course sections. In contrast, students in the simulation sections felt constrained by their assignment environment, and reported that their understanding of results in the simulator were unclear. Based upon their assignment scores, they were clearly able to complete the assignment, but less overall satisfaction or positive experience.

In the Literature Review section, we touched on the fact that experts in the area of cybersecurity education sometimes express trepidation about virtual machines due to an increased risk of crossover to real world systems; something that is virtually eliminated by the use of simulations. For these exercises, we used a VM that was fully quarantined from host systems so that no file or data transfer could occur between VM and host. The set up and configuration of this virtual environment was somewhat intensive, however it was not perceived to be overly burdensome, and not much more time consuming than setting up the simulations.

Overall, evidence in this study supports the use of VM delivery for authentic cybersecurity experiences. Students appreciate this modality, they perform well while completing relevant, real-world cybersecurity tasks, and demonstrate competency in skills that they will need as they enter the information technology workforce.

REFERENCES

Adams, M. D., Hitefield, S. D., Hoy, B., Fowler, M. C., & Clancy, T. C. (2013). Application of Cybernetics and Control Theory for a New Paradigm in Cybersecurity.

Babiceanu R, Seker R. Big Data and virtualization for manufacturing cyber-physical systems: A survey of the current status and future outlook. Computers in Industry [serial online]. February 29, 2016; Available from: ScienceDirect, Ipswich, MA.

Bergin, D. L. (2015). Cyber-attack and defense simulation framework. *Journal of Defense Modeling & Simulation, 12*(4), 383.

Burley, D. L., Eisenberg, J., & Goodman, S. E. (2014). Would Cybersecurity Professionalization Help Address the Cybersecurity Crisis? *Communications of the ACM, 57*(2), 24-27.

Cheolho Yoon, C., Jae-Won Hwang, H., & Kim, R. R. (2012). Exploring Factors That Influence Students' Behaviors in Information Security. *Journal of Information Systems Education, 23*(4), 407-415.

Cormack, A. (2015). Internet Vulnerability Scanning—Is It Lawful? *Journal of Internet Law, 18*(9), 3-6.

Conklin, W. A., Cline, R. E., & Roosa, T. (2014). Re-engineering Cybersecurity Education in the US: An Analysis of the Critical Factors. 2014 47th Hawaii International Conference on System Sciences, 2006.

Dark, M. (2014). Advancing Cybersecurity Education. IEEE Security & Privacy Magazine, 12(6), 79.

Dark, M., & Mirkovic, J. (2015). Evaluation Theory and Practice Applied to Cybersecurity Education. *IEEE Security & Privacy Magazine, 13*(2), 75.

Dipert, R. R. (2010). The Ethics of Cyberwarfare. *Journal of Military Ethics, 9*(4), 384-410.

Drew, E. (2009). Prototyping a Computer-Based Simulation of the Finance Sector. 2009 Cybersecurity Applications & Technology Conference for Homeland Security, 319.

Emami-Taba, M., Amoui, M., & Tahvildari, L. (2013). On the Road to Holistic Decision Making in Adaptive Security. *Technology Innovation Management Review*, 59.

Fonash, P. & Schneck, P. (2015). Cybersecurity: From Months to Milliseconds. *Computer, 48*(1), 42-50.

Furman, S., Theofanos, M. F., Choong, Y., & Stanton, B. (2012). Basing Cybersecurity Training on User Perceptions. *IEEE Security & Privacy Magazine, 10*(2), 40.

Heckman, K. E., Stech, F. J., Schmoker, B. S., & Thomas, R. K. (2015). Denial and Deception in Cyber Defense. *Computer, 48*(4), 36-44.

Hoffman, L., Burley, D., & Toregas, C. (2012). Holistically Building the Cybersecurity Workforce. *IEEE Security & Privacy Magazine, 10*(2), 33.

Hoffman, L., Rosenberg, T., Dodge, R., & Ragsdale, D. (2005). Exploring a national cybersecurity exercise for universities. *IEEE Security & Privacy Magazine, 3*(5), 27.

Kott, A., Alberts, D. S., & Wang, C. (2015). Will Cybersecurity Dictate the Outcome of Future Wars? *Computer, 48*(12), 98-101.

Kumar, R. L., Park, S., & Subramaniam, C. (2008). Understanding the Value of Countermeasure Portfolios in Information Systems Security. *Journal of Management Information Systems, 25*(2), 241-279.

Locasto, M. E., Ghosh, A. K., Jajodia, S., & Stavrou, A. (2011). Virtual Extension the Ephemeral Legion: Producing an Expert Cyber-Security Work Force from Thin Air. *Communications of the ACM, 54*(1), 129-131.

Mahoney, W., & Gandhi, R. A. (2011). An integrated framework for control system simulation and regulatory compliance monitoring. *International Journal of Critical Infrastructure Protection*, 441-53.

McDuffie, E. L., & Piotrowski, V. P. (2014). The Future of Cybersecurity Education. *Computer, 47*(8), 67-69.

McGettrick, A. (2013). Toward Effective Cybersecurity Education. *IEEE Security & Privacy Magazine, 11*(6), 66.

Mirkovic, J., & Benzel, T. (2012). Teaching Cybersecurity with DeterLab. *IEEE Security & Privacy Magazine, 10*(1), 73.

Mirkovic, J., Dark, M., Du, W., Vigna, G., & Denning, T. (2015). Evaluating Cybersecurity Education Interventions: Three Case Studies. *IEEE Security & Privacy Magazine, 13*(3), 63.

Niu, H., & Jagannathan, S. (2015). Optimal defense and control of dynamic systems modeled as cyber-physical systems. *Journal of Defense Modeling & Simulation, 12*(4), 423.

Pastrana, S., Tapiador, J. E., Orfila, A., & Peris-Lopez, P. (2015). DEFIDNET: A framework for optimal allocation of cyberdefenses in Intrusion Detection Networks. *Computer Networks*, 8066-8088.

Patel, P. (2014). Defense against the dark arts (of Cyberspace) universities are offering graduate degrees in cybersecurity. *IEEE Spectrum, 51*(6), 26.

Paus-Hasebrink, I., Wijnen, C. W., & Jadin, T. (2010). Opportunities of Web 2.0: Potentials of learning. *International Journal of Media & Cultural Politics, 6*(1), 45-62.

Peretti, K. K., Swire, P., Waite, J. M., & Wool, J. R. (2015). New Export Requirements on the Horizon for Cybersecurity Products and Technologies. *Intellectual Property & Technology Law Journal, 27*(9), 23-27.

Pittman, J. (2013). Understanding System Utilization as a Limitation Associated with Cybersecurity Laboratories--A Literature Analysis. *Journal of Information Technology Education: Research*, 12363-378.

Pusey, P., & Sadera, W. A. (2012). Cyberethics, Cybersafety, and Cybersecurity: Preservice Teacher Knowledge, Preparedness, and the Need for Teacher Education to Make a Difference. *Journal of Digital Learning in Teacher Education, 28*(2), 82-88.

Quigley, K., Burns, C., & Stallard, K. (2015). 'Cyber Gurus': A rhetorical analysis of the language of cybersecurity specialists and the implications for security policy and critical infrastructure protection. *Government Information Quarterly, 32*(2), 108-117.

Radziwill N, Romano J, Shorter D, Benton M. The Ethics of Hacking: Should It Be Taught? [serial online]. December 8, 2015; Available from: arXiv, Ipswich, MA.

Ross, C. (2015). Educational Paradigm Change to Dissect to Prosect or to Game (Simulation) That Is the Question? *College Quarterly, 18*(1).

Schneider, F. B. (2013). Cybersecurity Education in Universities. *IEEE Security & Privacy Magazine, 11*(4), 3.

Shumba, R. (2006). Teaching Hands-On Linux Host Computer Security. *Journal on Educational Resources in Computing, 6*(3).

Sterbenz, J., Çetinkaya, E., Hameed, M., Jabbar, A., Qian, S., & Rohrer, J. (2013). Evaluation of network resilience, survivability, and disruption tolerance: analysis, topology generation, simulation, and experimentation. *Telecommunication Systems, 52*(2), 705-736.

Thierer, A. (2013). The Pursuit of Privacy in a World where Information Control is Failing. *Harvard Journal of Law & Public Policy, 36*(2), 409.

Vassilev, A., & Celi, C. (2014). Avoiding Cyberspace Catastrophes through Smarter Testing. *Computer, 47*(10), 102-106.

Williams, C. S., & Krueger, K. R. (2005). Is Your Network Safe? *T.H.E. Journal, 33*(4), 36-41.

Yoo, H., & Shon, T. (2016). Challenges and research directions for heterogeneous cyber–physical system based on IEC 61850: Vulnerabilities, security requirements, and security architecture. *Future Generation Computer Systems*, 61128-136.

Zahir S, Pak J, Singh J, Pawlick J, Zhu Q. Protection and Deception: Discovering Game Theory and Cyber Literacy through a Novel Board Game Experience. [serial online]. May 20, 2015; Available from: arXiv, Ipswich, MA.