Using Virtual Reality to Enforce Principles of Cybersecurity

Jinsil Hwaryoung Seo
Department of Visualization
Texas A&M University
College Station, Texas
hwaryoung@tamu.edu

Michael Bruner
Department of Visualization
Texas A&M University
College Station, Texas
michael.bruner3@tamu.edu

Austin Payne
Department of Visualization
Texas A&M University
College Station, Texas
payn4478@tamu.edu

Nathan Gober
Department of Electrical and Computer Engineering
Texas A&M University
College Station, Texas
ngober@tamu.edu

Donald "Rick" McMullen
High Performance Research Computing
Texas A&M University
College Station, Texas
mcmullen@tamu.edu

Dhruva K. Chakravorty
High Performance Research Computing
Texas A&M University
College Station, Texas
chakravorty@tamu.edu

ABSTRACT

The Cyberinfrastructure Security Education for Professionals and Students (CiSE-ProS) virtual reality environment is an exploratory project that uses engaging approaches to evaluate the impact of learning environments produced by augmented reality (AR) and virtual reality (VR) technologies for teaching cybersecurity concepts. The program is steeped in well-reviewed pedagogy; the refinement of the educational methods based on constant assessment is a critical factor that has contributed to its success. In its current implementation, the program supports undergraduate student education. The overarching goal is to develop the CiSE-ProS VR program for implementation at institutions with low cyberinfrastructure adoption where students may not have access to a physical data center to learn about the physical aspects of cybersecurity.

KEYWORDS

HPC training, summer camps, broadening participation, assessment strategies, best practices. diversity, high school students

1 INTRODUCTION

Cybersecurity is a constantly evolving landscape. It is critical to raise awareness of disruptive computing technologies that result in new threats that appear on extremely short timescales. A recent report on the state of CS curricula in Texas, entitled "Building the Texas Computer Science Pipeline" recommended that students be aware of prevalent threats to personal information, prevalence of cyber-bullying, the increasing need for confidentiality [9]. In an increasingly technological era, students must learn to be conscious of digital citizenship and cybersecurity at an early age. While the software aspects of cybersecurity get prominent attention, physical access control to a cybersystems remains a high-priority requirement. Poor physical security may be out of compliance with government regulations, but also presents an incredible risk to the integrity of the machines in question. For this reason, software cybersecurity is built on a foundation of good physical access control.

As such, any cybersecurity training program must have a cybersecurity training program that emphasizes the physical aspects of cybersecurity. However, existing cybersecurity programs do not offer much training in this area. Further, 2- and 4-year universities alike have struggled to support sufficient faculty in computer education [13, 17]. As a result, certifications have become a favored source of cybersecurity education. We have developed a system that utilizes the emerging technology of virtual reality to enhance cybersecurity education at the university level, particularly in the area of physical security. In this paper, we present the development of the CiSE-ProS virtual reality (VR) program and a pilot study with high school students at the Summer Computing Academy at Texas A&M University.

The rest of the paper is organized as follows. A brief survey of government standards and regulations, as well as existing training solutions, is presented in Section 2. The benefits and limitations regarding the use of advanced technologies, including virtual reality, is discussed in Section 3. We discuss the importance of advanced computing education in Section 4, and the program to facilitate learning is outlined in Section 5. The design of the CiSE-ProS system is discussed in Section 6, followed by an evaluation of the system's effectiveness, in Section 7.

2 PREVIOUS WORK

The National Security Administration and Department of Homeland Security consider system administration and, by extension, access control to be a core knowledge unit, essential to any 2- or 4-year cybersecurity education program [14]. The National Institute of Standards and Technology publishes standards for security of data centers in the United States, including security of physical access controls. Its National Initiative for Cybersecurity Education emphasizes that "a knowledgeable and skilled cybersecurity workforce is needed to address cybersecurity risks within an organization's overall risk management process" [16]. The latest standards require organizations to verify individual authorizations for access to the data center, to maintain audit logs of access, to escort visitors on the premises, and to change combinations and locks when they are

https://doi.org/10.22369/issn.2153-4136/10/1/13

compromised, among other standards. High-sensitivity locations are further required to demand physical access authorization to the data center that is different than access to the surrounding facilities [11]. However, these standards, while essential for organizations, do not inform the physical security aspects of our practitioner training. These standards establish organization-level expectations, which is useful for management, rather than individual-level expectations, which is useful for practitioners.

The Computer Technology Industry Association (CompTIA) is a vendor-neutral certification provider that offers many ANSI-accredited security practitioner certification programs that include topics on physical access. The CompTIA A+ exam, an entry-level exam, requires its participants to compare and contrast a variety of physical security methods [5]. The CompTIA Network+ and Security+ exams, both considered intermediate-level exams, both require a summarial knowledge of physical security controls [7, 8]. Also, the CompTIA Advanced Security Practitioner (CASP) exam requires participants to analyze security components, including physical access control systems [6]. This suggests that familiarity with physical access control is a desired skill in the IT industry. These exams range from 90 to 165 minutes in length and cost between $211 and $439.

Texas A&M University offers a 16-hour minor field of study for undergraduates in cybersecurity [20]. Students may select from courses such as "Advanced Network Systems and Security" and "Cybersecurity and Digital Ethics". Other institutions have also implemented programs in cybersecurity, with some emphasis made on physical security. One such program is the Master of Science in Information Assurance and Security program at Sam Houston State University in Huntsville, Texas [19]. The 36-hour degree requires coursework in principles of access control and physical approaches to data protection. Graduate-level programs, while comprehensive, require previous undergraduate work, as well as significant investments of time and money. These barriers to entry reduce the accessibility of the field of cybersecurity, and do little to resolve the diversity gap which exists in the professional computing environment.

The National Security Agency and Department of Homeland Security designate over 200 degree-granting institutions across the country as National Centers of Academic Excellence in Cyber Defense Education, of which Texas A&M University is one [15]. Institutions designated as CAE-CDE must provide degree programs that equip students in a specified selection of essential cybersecurity topics. Of these, physical security is required to be addressed in introductory IT Systems Components courses, a foundational knowledge unit, and physical security is an important aspect in Security Program Management courses, a non-technical core knowledge unit. Hardware and Firmware Security, which focuses primarily on physical threats, is an optional knowledge unit [14].

All fields of study evolve over time, but cybersecurity chiefly is marked by a rapidly changing nature, underscoring the need for young cybersecurity professionals to be prepared to identify and mitigate new threats in their daily routine. These educational programs and government standards demonstrate a desire amidst society at large to have a well-trained cohort of computing technology and cybersecurity professionals.

3 ADOPTING EMERGING TECHNOLOGIES

Virtual reality and augmented reality are participatory technologies that provide the means to achieve engagement while underscoring the role of computing in scientific discovery and research. VR systems have seen increased adoption across industries since 1999, when researcher Fred Brooks, having taken a survey of VR technologies, concluded that it "barely works" [4]. Recently, VR systems are used to replace expensive rapid prototyping systems, perform research on ergonomics, and communicate ideas (including the playing of video games) [1]. More than a decade and a half has passed since students were first described as "digital natives," [18] and technology has advanced even more rapidly in the 21st century than before. Indeed, the students of today are the children of the students that Prensky studied. Students today are not merely proficient in emerging technologies, it is indigenous to them.

One ongoing challenge with the emerging technology is locomotion within the simulation. The method of control and locomotion can have a significant impact on the immersion and positive affect on the part of the user [2]. Free movement in the VR environment is restricted by the detection range of the motion sensors and the range of the communication between the wearable technology and the simulator, even if this communication is wireless. Additionally, the simulation may include obstacles to movement that are difficult to replicate physically in any dynamic way. VR systems must overcome the dual challenges of preserving immersion while allowing the user to move through an environment larger than the dynamic range of the VR system. Any data center environment is likely to be larger than the free movement restrictions of a VR environment, so in our CiSE-ProS system there must be some capability for locomotion.

Existing solutions for VR locomotion are varied, and few have seen widespread adoption. Some solutions place the user within a large external motion capture system and allow the floor to move beneath them while they walk. These solutions cannot currently create an accurate feel of a floor space and do not recreate the internal feeling of walking [3, 12]. Other solutions implement motion in software, either by teleporting the user on their command or by guided motion, as if fixed on a track. Of these, the teleportation, both free and to fixed points, imparts significantly fewer feelings of motion sickness on the user, in addition to being fast and easy to operate [10].

4 ADVANCING KNOWLEDGE AND UNDERSTANDING IN COMPUTING

Computing is a constantly evolving landscape. Disruptive computing technologies result in new threats that appear on extremely short timescales. Today's computer education curriculum must equip students to use existing technology while preparing them to use emerging technologies. VR and AR are likely to play important roles in computing technology in the future, given their current trajectory of development, so using them as part of other training programs will accomplish both ends.

Advanced computing resources, including high performance computing, high capacity storage, and enterprise-scale network devices, have become common across all industries. The concept of a data center is increasingly familiar, so training on the needs of

a data center benefits all professions that may use these advanced computing resources.

Physical access control to a data center is a high-priority requirement. The National Institute of Standards and Technology Special publication 800-53 requires that any system of moderate-to-high security implement an access control scheme that "allow[s] only authorized accesses for users... which are necessary to accomplish assigned tasks" [11]. In addition to compliance to regulations, limiting physical access to data center devices reduces the number of possible attack vectors on those machines.

If physical access to a data center is compromised, many assumptions that software cybersecurity systems make may be violated, including the topology of the network, the presence of any given machine in the data center, or even that a peripheral device is not malicious. A physical attacker can introduce devices that deceive the system, delivering maliciously incorrect information to other parts of the system, causing undesired behavior. For this reason, software cybersecurity is built on a foundation of good physical access control. Future practitioners in STEM fields will require exposure to advanced computing resources in order to be effective.

To that end, our CiSE-ProS system will be used at Texas A&M University in education programs targeted at students who are on educational tracks towards careers in STEM fields. The purpose of these programs are to usher in the next generations of cyber-practitioners in the country through hands-on exercises and active learning opportunities. Modern computing and cybersecurity education, and indeed modern STEM education, cannot simply impart programming knowledge, but must seek to develop in its students a well-rounded view of the computing fields.

5 PEDAGOGY

The underpinning conceptual framework implemented for training incorporates elements of active learning such as exploratory learning via research projects where mentors provide guidance to help focus mentees activities in productive directions and group discussions in research seminars. Part of these guided activities includes the use of our CiSE-ProS system. The use of the VR system is an opportunity for the student to engage in the material being taught in an experiential way. Active learning has been shown among high-ability trainees to produce significantly higher levels of metacognitive activity than procedural training, leading to the development of higher adaptive transfer. In addition, the training provided through the surrounding program incorporates several elements of the experiential learning cycle in which:

- *New experiences:* Students are introduced to several aspects of cybersecurity
- *Processing ideas and taking ownership of ideas:* Skills developed in earlier guided practice are later revisited in exercises where students have opportunities to integrate and apply these skills to specific problems.
- *Opportunities to develop hypotheses to solve problems, and validate them:* Students must decide on which of their repertoire of skills to select and apply to problems.

With a view toward broadening the learning and understanding of students through further diversification of learning approaches, we designed the educational process using the backward design approach [21]. In this approach, the learning objectives are defined in advance, and techniques are designed to support them. Such an approach to learning mirrors typical engineering design processes, where the goals and parameters of a product are established prior to the design phase. This parallel marks our pedagogical process already as a proven and effective one. In addition, STEM students seeing the backward design approach in pedagogy may be further encouraged to use it in their own design decisions.

We first identified the learning objectives and competencies that participants were expected to learn and built each exercise around them. Throughout the development process of CiSE-ProS, the focus is on developing scenarios that facilitate learning in the user. To develop desired capabilities, the CiSE-ProS program focuses on the described attributes:

- *Defining desired capabilities:* Trainees using the CiSE-ProS system should be able to describe physical access security measures and use them easily.
- *Operationalizing learning outcomes:* The CiSE-ProS system should provide an immersive environment where the trainee can experience these security measures and respond effectively to them. Additionally, the trainees can be observed by other students, leading to collaborative discussions wherein the instructor can guide students towards a better solution than the one demonstrated.
- *Evaluating learner development:* The learner is evaluated at all times while in the simulations by an operator. The learner also completes a survey following the experience to determine short-term retention of the material.

6 CISE-PROS VR

The CiSE-ProS VR seeks to enable aspiring computer scientists, developers, and engineers in their pursuit of computing fields by offering cybertraining programs that focus on cybersecurity. This effort seeks to help prepare the next generation of cyber-practitioners in the United States. The overarching objectives of the program are to:

- Use research-based methods to develop a high-impact, high-immersion opportunity that introduces participants to concepts in computing including software, hardware, networking, cybersecurity and data management practices,
- Reinforce and develop further knowledge of cyber skill sets through exercises,
- Retain participant interest after the camp by offering access to series of free in-person and online cybertraining-themed short courses and seminars at Texas A&M.

The CiSE-ProS VR program was developed to support users to learn cybersecurity principles through immersive and embodied tasks in the virtual data center environment. It offers a blend of cybersecurity and interactive visualization technologies to students in an innovative learning environment. The CiSE-ProS VR program is designed on the principles of engagement, training, retention, and sustainability to promote cyberinfrastructure as a professional career path. Virtual reality technology enables embodied/interactive learning that allows high engagement while underscoring the role of computing in scientific discovery and research. Simultaneously,

Figure 1: The HTC Vive system, which contains a headset, two handheld controllers, and two motion tracking sensors.

the rapidly changing nature of the cybersecurity landscape underscores the need for young adults to be prepared to identify and mitigate new threats in their daily lives.

6.1 Hardware

To fully utilize the potential of virtual reality, we chose an HTC Vive (Figure 1) that allows embodied actions including selection, manipulation and navigation within the virtual data center in the program. The HTC Vive was chosen as the primary hardware target for running this application due to its popular use in both the consumer market and development space for virtual reality applications. For instance, Unity 2017, the game engine used for developing this program, offers a great amount of support for initializing and running the HTC Vive hardware in a short amount of time. As a result, more time was allocated in developing the user interaction and implementing crucial elements for simulating the data center seen here. While the hardware was able to ease development constraints, the HTC Vive has also proven to be a popular product within a good portion of the target audience, making the system more accessible and easy to use.

6.2 User Training Scenario in CiSE-ProS VR

The main user experience consists of four activities in the virtual data center: 1) tutorial, 2) entering/exiting the data center, 3) inspecting the data center, and 4) replacing hardware.

Tutorial Room. Although the users within the target audience have shown to have moderately high technology literacy in using this hardware, it is still crucial to provide guidelines and rules so that new users are able to use the application by themselves. To compensate for this, the program offers a quick tutorial for the users to learn about the functionality provided and the expectations of them to complete the provided simulation later in the program. For instance, the user learns about how objects can be picked up with the controllers, by holding the triggers on the back of the controllers. To help introduce the concept, the tutorial stage provides rubber balls for them to pick up and throw within the environment (Figure 2). While this may seem fairly straightforward to some users within this program, it is important for the tutorial stage to also

Figure 2: The first instruction monitor in the tutorial room. The red balls on the table are used as demonstrations to familiarize the user with object manipulation in the virtual environment.

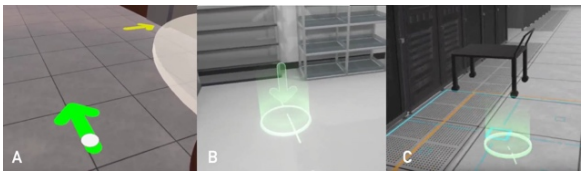

Figure 3: Iterations in the development of the locomotion tool, from the first iteration (A) to the current iteration (C).

account for those who may not be comfortable with the hardware just yet. As a result, this allows the user to interact with the given objects as much time as needed, before proceeding to the next on their own pace.

After completing the object interaction portion of the tutorial stage, users will learn how to navigate around the given space through the use of teleportation. This technique has already proven to be a popular navigational tool, and many iterations were created to achieve a better user experience as well as minimizing visual distractions throughout the data center (Figure 3). For instance, we used 2D arrows and 3D arrows as a navigational tool in the environment (Figure 3A). In this iteration, the user would simply point and click towards these objects above the ground and teleport the user to these points in space. When presenting this to users, there seemed to be frustration of not being able to see them clearly in the space, as well as not having enough feedback of where the controller was being pointed to. From these initial observations, it was decided that utilizing the SteamVR's teleportation tool was the better direction, in order to reduce these issues in a timely manner (Figure 3B). The next iteration of the teleportation tool used a grid on the ground for each teleportation point, allowing the user a larger degree of freedom of teleporting around the space (Figure 3C). In addition, the tool provided better visual feedback for the pointing and clicking portion of the program, as colors and trajectory of the cursor on the controllers were introduced. Although it showed

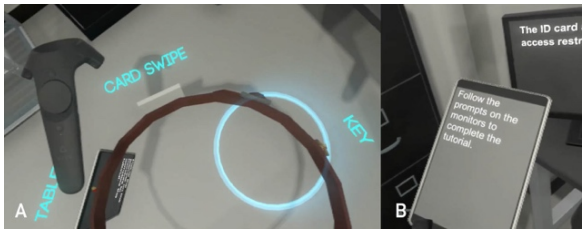

Figure 4: The user's tool belt in the VR simulation, containing (A, from left to right) a tablet, an ID card, and a rack key. (B) The tablet contains the last instructions given, so that the user can refer to it.

promises in improvement, the rendered grid for each teleportation point created more visual clutter in the data center. This also proved to be somewhat counter-intuitive for setting teleportation points, as tight corridor spaces created overlaps of these points, leading to less efficiency in navigating around the environment. As a result, the current iteration of this tool uses a similar approach with the arrows, but with better visual feedback through the use of colors and additional objects, such as having a circle below the arrow to show where exactly the point is located in the environment. In addition, the visual elements of the cursor was kept from the previous iteration, to prevent any recreation of the initial problems found earlier in the development process. With the combination of these elements in the tool, teleportation around the environment have shown to have better ease of navigation, based on a set of preliminary observations.

After users have learned how to use the locomotion tools, they make their way towards the other side of the room, where they pick up a tool belt before proceeding further into the level (Figure 4A). The tool belt is the most important aspect of the program, as users will need to be versatile and resourceful in completing tasks with the given items. The belt contains a card swipe and a regular key in this program, which are typical elements found in this type of profession. Users will need to use these items to gain access to secured areas, in a manner very much like how the average data center secures their resources and implements access control. In addition, the tool belt also features a tablet for the user to interact with. Since this type of tool is often used by those in this profession to understand the protocols of a particular data center, the tablet is used a guide for the users, in case they ever feel lost or confused about what needs to be completed next (Figure 4B). After the user has learned about the functionalities of all of the given items on their tool belt, they have successfully completed the tutorial stage and can proceed to the main areas of the data center to test their abilities.

Entering/Exiting Data Center. Users will next be brought into a lobby area, from where they can explore the data center. While in the lobby, users will receive instructions about the the main task at hand. The user will first need to navigate from the lobby area to the server room on the second floor of the building. To successfully accomplish this, they will need to gain control access of the elevator. In this virtual data center, access is granted by the use of a key card reader. The user can get access by swiping the card provided in the

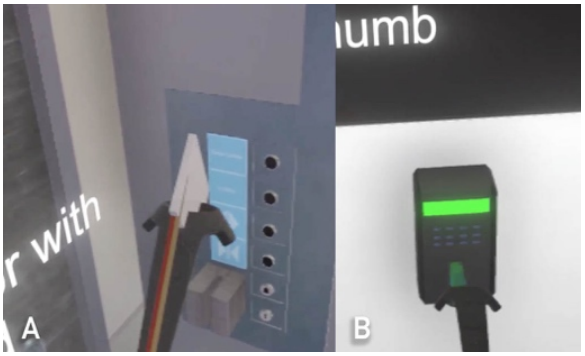

Figure 5: Tools to enter and exit the data center. (A) Using the ID card to operate the elevator. (B) Using the thumb scanner in the mantrap room.

Figure 6: Inspecting the data center. The rows of racks are lettered, and the positions within the rows are numbered. The user is instructed to navigate to rack B5.

tool belt (Figure 5A). Once the user has successfully passed the key card reader, he/she will be able to select buttons to move between different floors.

After selecting the "Data Center" button in the elevator, the elevator opens up to a "mantrap" room, a security clearance checkpoint before reaching the main server room. Here, users will approach the security guard behind the glass and scan his/her thumb on the thumb scanner in order to proceed to the main data center (Figure 5B).

Inspecting Racks. The user now can navigate the data center by teleporting to different areas of the room (Figure 6). While navigating, the user can find problematic nodes on the racks.

Replacing Hardware. One of the main tasks in this application is replacing a RAM on one of the server nodes within the area of the data center, while also following security protocols. To replace a RAM module, they will reach the main area of the program, where the broken node is located. Once they figure out its location, based on its given row number, they will start the process of removing and repairing a node.

First, they will need to remove the two cable attached in the front of the node (Figure 7). While it may vary on the amount of cables for certain data center, for the sake of this simulation, this

Figure 7: Removing Cables from the Node

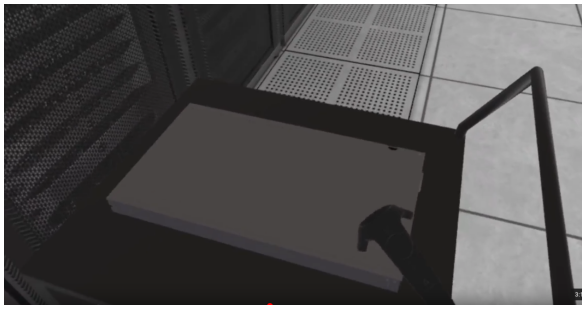

Figure 8: Placing the node on a cart for transport.

node only features two cables with their own distinct colors. Next, the node can be taken out, but it must be placed on the cart near the node (Figure 8). The reason for this is that these types of nodes are known to be extremely heavy, which is both difficult and not desirable to simulate accurately for this program. To help reinforce this idea, the program forces the user to place the node on a cart to transport it around the server room. After the node has been placed on the cart, they are able to move the cart into the workplace area to begin the repair process.

The repairment of the node begins with the user removing the top cover to view the computer parts and seeking for the broken RAM. For this program, the broken component is marked as red, while the rest of the computer parts are marked as green. The users will need to use their controllers to detach this part and replace it with the new RAM, which is provided on their workstation (Figure 9). Once they successfully replace the RAM, they will need to put the cover back on the node and return it to its server through cart transportation once more. From there, users will place the node back to its original spot, and reconnect the cables that were detached from earlier. After accomplishing this task, they will be able to exit the data center.

7 EVALUATIONS AND ASSESSMENTS

The earlier prototype of the CiSE-ProS VR simulator was demonstrated at the TAMU HPRC booth SuperComputing 17 Conference

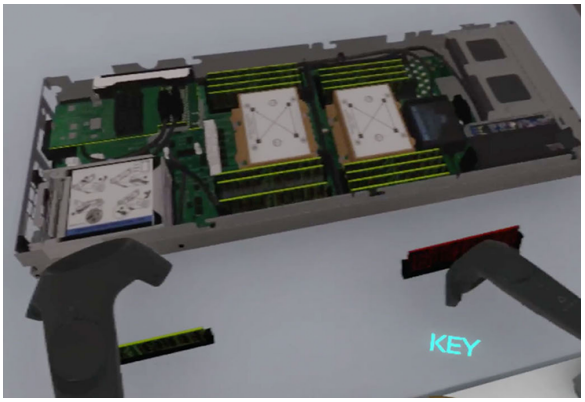

Figure 9: Replacing a defective RAM card.

in Denver, CO. The current version was tested with students who participate in the Summer Computing Academy at Texas A&M University. We collected participants' feedback using questionnaires. In addition, we collected background information to identify high-achieving or highly knowledgeable students who might need additional frameworks or scaffolds of instruction to be available. Evaluations and assessments are critical aspects of program refinement. Twenty-five students' virtual reality experiences were assessed using a post-experience survey. 80% of the participants had prior virtual reality experience: Google cardboard, HTC Vive, or Oculus Rift. They have used VR for mostly games and science education programs. They experienced the CiSE-ProS VR in a typical HTC Vive setting. Each student spent about 5 minutes in the program and filled out the survey afterwards. Their experiences with the CiSE-ProS VR application were very positive. 90% of students remembered the layers of data center physical security and the procedure of fixing a node with a broken RAM in the VR application. In addition, students acknowledged that virtual reality technology would be beneficial to education and were fascinated by interactive and immersive qualities of the virtual reality technology. The students' experiences were also assessed one week after the initial VR session. 80% of the participants still remembered the details of the data center security checkpoints and the procedure of replacing hardware in the node. Students acknowledged that virtual reality technology would be beneficial to education and were fascinated by interactivity, realistic simulation, and immersion. Some of their written responses include:

"VR is very interactive so it would be a good way to teach students that will keep them engaged," (ID03)

"It is very easy and fun to use and make, it's very easy to remember information." (ID05)

"You can explore places rather than read them in the text book." (ID18)

"Great for visual learners" (ID22)

8 CONCLUSION AND FUTURE DEVELOPMENT

Based on observations and feedback given on the current version of CiSE-ProS VR, we learn that embodied interaction in a virtual reality

training program can benefit students with short term and long term memories in engaging and playful ways. We also learn that there are a few elements that can be improved upon to help further build a more effective and engaging version of this application. For instance, during the tutorial stage, it appeared that some users were confused about how to use the controls, despite our efforts of using audio, text, and even visual cues on the controller to teach them this information. As a result, it is expected that visual graphics that vividly depict the motion and button presses in front of the user will have better results for users retaining and understanding this information. It also appeared that users weren't able to differentiate when to use the card swipe and key, based on the wording of the directions given to them. By establishing clear definitions and wording of these item's uses, this should be able to help mediate this problem.

In addition to improving these elements, the inclusion of new areas or components of this program is also being heavily considered as long-term goals. For instance, the current iteration of this program only focuses on one particular scenario. In the future, the implementation of more scenarios to choose from that tests either or both routine maintenance or emergency situations would make the program more applicable for others to utilize its potential in learning. To further build upon this mentality, it has also been suggested to allow users to customize the layout of a data center, security levels, and scenarios to mimic closely to a particular data center, to help better retain information in a similar environment. While this direction is tailored for those interested in expanding the learning potential, the cognitive effects of using this application is also being considered as well, as interests has been shown in analyzing the effectiveness and the outcomes of using this program, in comparison to other learning methods offered.

ACKNOWLEDGMENTS

The authors would like to thank staff, student workers and researchers at Texas A&M HPRC, Department of Visualization, the Laboratory for Molecular Simulation, TexGen, Division of Research and Provost IT for supporting the HPRC short course program at Texas A&M University. Portions of this research were conducted on the Ada and Terra clusters, and virtual machines provided by TAMU HPRC. We gratefully acknowledge support from the National Science Foundation Abstract 1730695 (https://www.nsf.gov/awardsearch/showAward?AWD_ID=1730695) "CyberTraining: CIP: CiSE-ProS: Cyberinfrastructure Security Education for Professionals and Students." We also appreciate Dell for providing VR laptops. Special thanks to the instructors of each course: Dylan Rodriguez, Michael Dickens, Rick McMullen, Lisa Perez, Mark Huang, Ping Luo, Jian Tao, Yang Liu, Marinus Pennings, Keith Jackson, Noushin Ghaffari, and Shichen Wang. We also gratefully acknowledge support from Francis Dang, Mark Huang and Jack Perdue for maintaining the clusters and virtual machines used in these efforts.

REFERENCES

[1] Leif P. Berg and Judy M. Vance. 2017. Industry Use of Virtual Reality in Product Design and Manufacturing: A Survey. *Virtual Reality* 21, 1 (2017), 1–17.

[2] Max Birk and Regan L. Mandryk. 2013. Control Your Game-self: Effects of Controller Type on Enjoyment, Motivation, and Personality in Game. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '13)*, Wendy E. Mackay, Patrick Baudisch, and Michel Beaudouin-Lafon (Eds.). ACM, Paris, France, 685–694. https://doi.org/10.1145/2470654.2470752

[3] Ian Bishop and Muhammad Rizwan Abid. 2018. Survey of Locomotion Systems in Virtual Reality. In *Proceedings of the 2nd International Conference on Information System and Data Mining (ICISDM '18)*. ACM, Lakeland, FL, USA, 151–154. https://doi.org/10.1145/3206098.3206108

[4] Frederick P. Brooks. 1999. What's Real About Virtual Reality? *IEEE Computer Graphics and Applications* 19, 6 (1999), 16–27.

[5] Computer Technology Industry Association. 2018. CompTIA A+ Certification Exam Objectives. https://certification.comptia.org/docs/default-source/exam-objectives/comptia-a-220-902-exam-objectives.pdf

[6] Computer Technology Industry Association. 2018. CompTIA Advanced Security Practitioner (CASP) Certification Exam Objectives. https://certification.comptia.org/docs/default-source/exam-objectives/comptia-casp-objectives-(cas-002).pdf

[7] Computer Technology Industry Association. 2018. CompTIA Network+ Certification Exam Objectives. https://certification.comptia.org/docs/default-source/exam-objectives/comptia-network-n10-007-v-3-0-exam-objectives.pdf

[8] Computer Technology Industry Association. 2018. CompTIA Security+ Certification Exam Objectives. https://certification.comptia.org/docs/default-source/exam-objectives/comptia-security-sy0-501-exam-objectives.pdf

[9] Carol L. Fletcher. 2014. *Building the Texas Computer Science Pipeline: Strategic Recommendations for Success.* Technical Report. Texas Regional Collaboratives. https://www.thetrc.org/web/assets/files/pdfs/Building-the-Texas-CS-Pipeline_Fletcher.pdf

[10] Julian Frommel, Sven Sonntag, and Michael Weber. 2017. Effects of Controller-Based Locomotion on Player Experience in a Virtual Reality Exploration Game. In *Proceedings of the 12th International Conference on the Foundations of Digital Games (FDG '17)*. ACM, Hyannis, Massachusetts, USA, 30.

[11] Joint Task Force Information Initiative. 2013. *Security and Privacy Controls for Federal Information Systems and Organizations.* Technical Report. National Institute of Standards and Technology. https://doi.org/10.6028/nist.sp.800-53r4

[12] William E. Marsh, Tim Hantel, Christoph Zetzsche, and Kerstin Schill. 2013. Is the User Trained? Assessing Performance and Cognitive Resource Demands in the Virtusphere. In *Proceedings of the 2013 IEEE Symposium on 3D User Interfaces (3DUI)*, Anatole Lécuyer, Frank Steinicke, and Mark Billinghurst (Eds.). IEEE Computer Society, Orlando, Florida, USA, 15–22. https://doi.org/10.1109/3DUI.2013.6550191

[13] National Academies of Sciences, Engineering, and Medicine. 2018. *Assessing and Responding to the Growth of Computer Science Undergraduate Enrollments.* The National Academies Press, Washington, DC. https://doi.org/10.17226/24926

[14] National IA Education and Training Programs. 2018. *Centers of Acadcemic Excellence in Cyber Defense 2019 Knowledge Units.* Technical Report. National Security Agency and Department of Homeland Security. https://www.iad.gov/NIETP/documents/Requirements/CAE-CD_2019_Knowledge_Units.pdf

[15] National Security Administration. 2018. Information Assurance Directorate at the NSA. https://www.iad.gov/NIETP/reports/cae_designated_institutions.cfm Retrieved December 12, 2018.

[16] William Newhouse, Stephanie Keith, Benjamin Scribner, and Greg Witte. 2017. *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework.* Technical Report. National Institute of Standards and Technology. https://doi.org/10.6028/nist.sp.800-181

[17] One Hundred Fifteenth Congress of the United States of America, First Session 2017. *Public-Private Solutions to Educating a Cyber Workforce: Joint Hearing Before the Subcommittee on Cybersecurity and Infrastructure Protection of the Committee on Homeland Security, House of Representatives and the Subcommittee on Higher Education and Workforce Development of the Committee on Education and the Workforce, House of Representatives.* One Hundred Fifteenth Congress of the United States of America, First Session, U.S. Government Publishing Office, Washington. http://purl.fdlp.gov/GPO/gpo90199 pp. 42-43,66.

[18] Marc Prensky. 2001. Digital Natives, Digital Immigrants Part 1. *On the Horizon* 9, 5 (2001), 1–6.

[19] Sam Houston State University. 2018. Academic Catalog 2018-2019. https://catalog.shsu.edu/

[20] Texas A&M University. 2018. Cybersecurity–Minor. http://catalog.tamu.edu/undergraduate/engineering/cybersecurity-minor/cybersecurity-minor.pdf

[21] Grant P. Wiggins and Jay McTighe. 2005. *Understanding by Design* (expanded 2nd ed.). ASCD, Alexandria, Virginia, USA.