An Experiential Learning Approach to Building a Cyber Range: A Maritime Supply Chain Focus

Rafael Diaz, PhD
Graduate Program Director
School of Cybersecurity, Old Dominion University
rdiaz@odu.edu

Liuwang Kang, PhD
Project Scientist
Virginia Modeling, Analysis, and Simulation Center
Old Dominion University
lkang@odu.edu

Gregory Wilson
SFS Scholar
School of Cybersecurity, Old Dominion University
gwils006@odu.edu

Abstract

The emergence of cyber-physical systems (CPSs) and extensive use of Operations Technology (OT) across different sectors of our society inexorably increases operational complexity and cyberattack exposure. Cybersecurity protection of critical infrastructure systems requires a systemic approach to evaluate their vulnerability, cyber threats, and countermeasures. A highly qualified workforce is imperative to the protection of these CPSs. This short paper presents initial endeavors in building a cyber range to provide students with experiential learning opportunities using a maritime port terminal as an environment.

Introduction

Experiential learning is an education process characterized by hands-on experiences, active participation, and reflection (Gentry, 1990; Kolb, 1984; Wurdinger & Carlson, 2009). It stresses that people learn best by doing and reflecting on their experiences. Learners participate in tasks replicating real-world situations and are encouraged to ponder the learnings from those experiences.

Experiential learning has been identified as a critical learning component in higher education (Budhai, 2017; Retallick & Steiner, 2009). Notably, it is vital to learning computer science and information systems (Allen, 2021; Manolis et al., 2013). Likewise, cybersecurity education may benefit further from these environments (Rege, 2015) and is expected to catalyze a highly qualified workforce. The deployment of a cyber range fits well to provide learners with an experiential learning platform to learn cybersecurity techniques to harden cyber-physical systems. In these computational environments, participants can replicate real-world cyber-attacks and defense scenarios. Cyber ranges that mirror participants' surroundings (e.g., maritime ports in large metropolitan coastal communities) can effectively engage learners further. Researchers can also examine cybersecurity vulnerabilities, anomaly detection, and mitigation methods (e.g., Smith et al. (2021)).

This short paper describes the initial efforts in building a CPS-based Cyber range focused on the Port of VA. The cyber range comprises the building and integration of several environments that include: 1. Virtual driving environment, 2. Physical environment, 3. CPS Integration. The following sections focus on step (1), or the virtual environment, and identify potential training exercises that can be associated with

different courses composed of Cybersecurity Curricula of undergraduate and graduate programs at Old Dominion University.

1. Virtual Driving environment simulation using SUMO

To recreate the Port of VA operational land side, we must develop and simulate vehicle driving environments in a port. We applied SUMO (Simulation of Urban MObility) since it allows real-time modeling of traffic lights, road networks, and vehicle driving behaviors. To simulate it, we first extracted the port's road networks and obtained historical traffic data of the port. Then, we input the historical driving data into SUMO so that SUMO can accurately simulate the traffic condition of the road network and how these vehicles drive on the road in real-time.

Fig. 1. Map of Virginia International Gateway (VIG)

a. Road network extraction

We extracted a SUMO road network from OpenstreetMap to indicate the road information of a port. The SUMO Road network belongs to a directed graph and describes the traffic-related part of a map Specifically, the SUMO road network contains edges, nodes, and additional parts. Additional parts have road components (e.g., stop signs). We extracted its SUMO road network from OpenstreetMap (Figure 2).

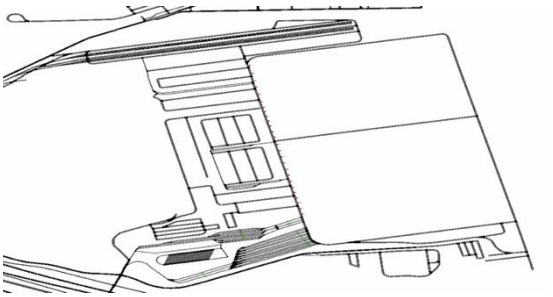


Fig. 2. SUMO road network extracted

b. Traffic route generation

We first gathered the port's historical traffic data and then applied them to generate vehicle driving routes for driving environment simulation. Here, the historical traffic data includes the number of containers needed to be shipped, the number of vehicles arriving at the port, and the number of vehicles leaving from the port at each period in a day. For VIG, we obtained its historical traffic data for total 30 days and input these data into SUMO route network to simulate vehicle driving environments of VIG. Here, we randomly selected one day's traffic data and added them in Figure 3 to show how the number of shipped containers and the number of vehicles change at different periods. In Figure 3, we see that the container terminal in VIG usually has other containers needed to be shipped.

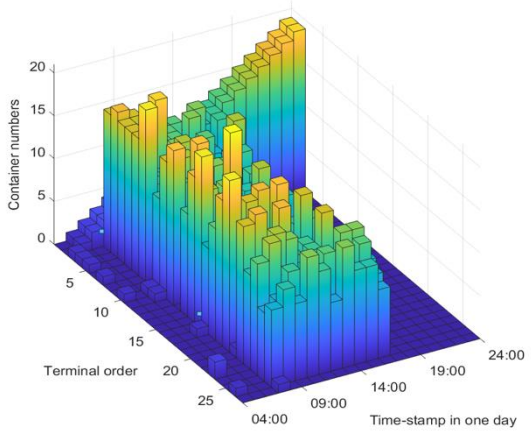
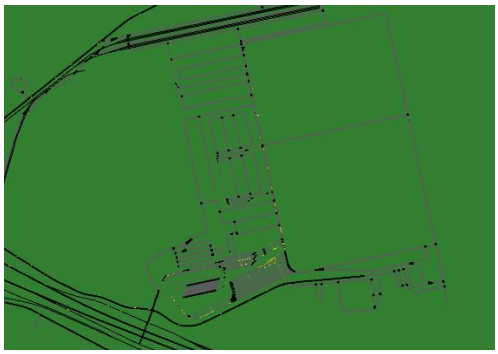
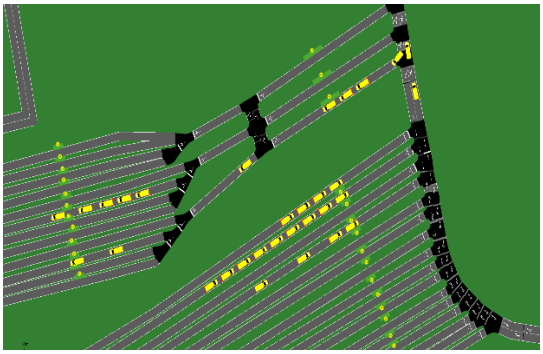


Fig 3. Shipped containers in one day for VIG

Based on the historical traffic data, we generated vehicle driving trips for vehicles in a port through our proposed trip generation algorithm so that the port has enough vehicles to satisfy the requirement of container terminals and the containers in the container terminals can be shipped in time. Each vehicle driving trip defines the road lines where a vehicle should drive, gates which a vehicle passes through, and a specific container terminal where a vehicle should drive to ship or pick up its container. We can generate vehicle-driving trips for VIG to ship containers in each container terminal. We see that the container terminal in VIG has different numbers of vehicles driving trips in one day. The maximum value reaches around 200 trips/day, while the minimum equals 1 trip/day. Figures 4(a) and 4(b) show VIG's traffic environment simulation result. Table 1 shows the cybersecurity issues to be studied in the proposed experiential learning environment, including the course numbers to be connected.



4a. The simulation of the whole part



4 b. The simulation of a small part area

Cybersecurity Issue	Proposed Training/Tool	Specific Tool/Course
Terminology of equipment used when trucks pass through gates and checkpoints.	Within the Cyber range, photos of equipment can be used have student use OSINT to discover equipment name and use. This method will allow the student to make a connection with the technology being used.	CYSE301– Cybersecurity Techniques and Operations Linux VM with ExifTool, Steghide, or similar. CYSE270-Linux System for Cybersecurity
RFID Cloning **RF protocol exposure/ capture-replay attacks**	Students build an RFID cloning rig. Once cloned, students can use the access card to further study RFID frequencies and learn more about the technology by unlocking a box with an SDR (software-defined radio) located inside to learn about radio frequencies.	CYSE250-Basic Cybersecurity Programming and Networking Rig – Raspberry Pi pico, bread board, jumper wires, RFID card, RFID-RC522 module, power supply/battery, Python code RTL-SDR or similar connected to Linux Vm running GNU radio and GNU radio companion
Knowledge of software used when trucks move through a port.	Simulation of how the software works can be hidden within a Linux operating system for the student to find and then use the video simulation to answer questions or to research common vulnerabilities to the software.	CYSE301- Cybersecurity Techniques and Operations ECE419-Cyber Physical System Security
Fraudulent movement of a truck or a truck tractor.	Students perform penetration testing to identify and address security weaknesses and ensure compliance with regulatory requirements. *Focal techniques:* • Metasploit: An exploitation framework that helps penetration testers identify and exploit vulnerabilities in target systems on Nmap • Burp Suite: A web application security testing tool that intercepts, modifies, and replays web traffic. • Nessus: A vulnerability scanner that can identify vulnerabilities and misconfigurations in systems	CYSE450- Ethical Hacking and Penetration Testing 5g Testbed and SUMO simulation to capture-replay movement of a tractor in a defined path
Phishing emails that represent ProPass	Students are exposed to what this Phishing emails look like in a port operational environment, how the port deal to combat these types of emails, and how they are constructed all can be utilized within the cyber range	CYSE450- Ethical Hacking and Penetration Testing
Wi-Fi/Cellular/Mesh Networks issues in a maritime environment.	This attack surface could be taught from many different approaches, even down to analyzing the packet information using Wireshark or similar network analyzation tools.	IT315-Introduction to Networking and Security CS462 -Cybersecurity Fundamentals CYSE301- Cybersecurity Techniques and Operations ECE419-Cyber Physical System Security

Table 1. Cybersecurity issues to be studied in the Cyber Range

Conclusion and Future Directions

In this paper, we presented the development of a virtual environment to simulate a CPS-based cyber range that uses the operational setting of the port of VA as a theme. By itself, SUMO cannot replicate the communication between vehicles and test how vehicles respond because of vehicle communication loss resulting from a cyber-attack. To handle this, in the next stage, we propose to simulate vehicle driving behaviors of vehicles using robots by considering that robots have similar working mechanisms as vehicles and can be controlled remotely through wireless communication. We introduced a set of robots to simulate

vehicle driving behaviors controlled remotely through wireless communication. Since we are interested in how a vehicle responds when driving on the road or passing through a gate in a port, we will build physical gates and road lanes and integrate them with the virtual environment. As a future step in completing the simulation, we will analyze how we can purposively implement cybersecurity tools to analyze vulnerabilities and identify mitigation actions to harden the systems, as presented in Table 1.

References

Allen, G. I. (2021). Experiential learning in data science: Developing an interdisciplinary, client-sponsored capstone program. Proceedings of the 52nd ACM Technical Symposium on Computer Science Education,

Budhai, S. S. (2017). *Best practices in engaging online learners through active and experiential learning strategies*. Routledge.

Gentry, J. W. (1990). What is experiential learning. *Guide to business gaming and experiential learning*, *9*, 20.

Kolb, D. A. (1984). Experience as the source of learning and development. *Upper Sadle River: Prentice Hall*.

Manolis, C., Burns, D. J., Assudani, R., & Chinta, R. (2013). Assessing experiential learning styles: A methodological reconstruction and validation of the Kolb Learning Style Inventory. *Learning and individual differences*, *23*, 44-52.

Rege, A. (2015). Multidisciplinary experiential learning for holistic cybersecurity education, research and evaluation. *USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 15)*.

Retallick, M. S., & Steiner, C. (2009). A model for implementing a college-wide experiential learning program in higher education. *Nacta Journal*, 2-6.

Smith, K., Diaz, R., Shen, Y., & Longo, F. (2021). *Conceptual Development of a Probabilistic Graphical Framework for Assessing Port Resilience* 23rd International Conference on Harbor, Maritime and Multimodal Logistic Modeling & Simulation, Poland.

Wurdinger, S. D., & Carlson, J. A. (2009). *Teaching for experiential learning: Five approaches that work*. R&L Education.