THE VCCLL COOKBOOK

Overview

The University of Southern Maine (USM), the University of Maine at Fort Kent (UMFK) and the York County Community College (YCCC) have completed a two year pilot of the project Virtual Cybersecurity Collaborative Learning Laboratory (VCCLL). The objective has been to determine the feasibility of implementing an inter-institutional virtual cyber security collaborative learning laboratory. This shared educational environment has allowed Maine students in different locations to gain practical collaborative experience in preventing and mitigating cyberattacks in real time. The original research design was developed to allow for the evaluation of the feasibility of implementing the inter-institutional laboratory simulations over three semesters each year of the grant, when students responded to Denial of Service and Data Exfiltration exploit scenarios. Evaluation research throughout the pilot has utilized a mixed-method approach, with an emphasis on interviews, surveys, observations, and usage data to assess faculty and student attitudes toward and use of the virtual cybersecurity laboratory, and the extent of cooperation among the three institutions in the implementation of the laboratory. Observational analysis of student performance has allowed for assessment of the promise of the virtual laboratory for achieving the expected learning outcomes related to Protect and Defend cyber security scenarios.

The VCCLL comprises the technical infrastructure, the pedagogical models, and the cross-team and within team interactions. The technological infrastructure which was developed during the first year of the grant has performed exceptionally from the first “setup day” and throughout all of the exercises during the two year pilot. This is a significant achievement given the complexities of working with University of Southern Maine, University of Maine Fort Kent, York County Community College and the University of Maine System IT and Network personnel. This project has accomplished a number of important “firsts”, not the least of which is the first time a high speed connection has been made from UMS to the Maine Community College system, which typically is operated by third parties at least to the perimeter systems.

As much as the technological infrastructure and scenarios are at the center of the VCCLL pilot project, the human factor surrounding collaboration and interpersonal communication emerges as one of the most critical aspects contributing to the student experience. The design of both the physical space and technological infrastructure being quite robust, 1) the students could speak (in person - non-electronic) with the local peers (within and across teams) in standard conversational modes, one to one or in the small groups; 2) they could use a “chat” application online; 3) they could use email; 4) they could use dedicated cell phones. All modes of communication were used but as expected individuals varied in terms of their primary choice of communication. Across all sites, there was much non-electronic in person conversation and mutual help and discussion.

The major goals of Maine Cyber Security Cluster’s Virtual Cybersecurity Collaborative Learning Laboratory (VCCLL) have been to:

- Pilot and evaluate the feasibility of an inter-institutional virtual cyber security collaborative learning laboratory that is designed to foster teamwork among undergraduate students across large distances.

VCCLL Cookbook Overview
• Collect and analyze data related to faculty and student attitudes toward and use of the virtual cybersecurity laboratory, and the extent of cooperation among the three institutions to address the implementation of the laboratory.

• Conduct a preliminary analysis of the impact of the virtual laboratory on cyber security learning outcomes.

• Assemble operational, technological and pedagogical materials to provide a replicable template for other higher education institutions to develop and implement a virtual environment platform and a collaborative learning laboratory.

The VCCLL Cyber Corp Cookbook has been compiled as a resource for cybersecurity and IT faculty and staff who are interested in following our approach to creating a cybersecurity collaboratory for students where they can be engaged in real-time, hands-on cybersecurity scenarios. The cookbook contents represent how we have approached creating such an environment, the choices that were made, what “ingredients” work together and lessons learned.

The nine units we have assembled here, encompass the primary areas for undertaking this kind of cybersecurity experiential learning lab. In this cookbook you will find discussions and explanations of key topics, each essential to a successful recipe. These units include the following; (1) Participant’s Guide, (2) Facilitator’s Guide, (3) Technology Operations, (4) Scenario Development (5) Range Management, (6) Management and Administration, (7) Partnering at a Distance, (8) Communication and Teambuilding and (9) Frequently Asked Questions (FAQ’s).

Organization of the Cookbook

There are several aspects to the organization used in the CC Cookbook we want to highlight. As mentioned earlier, the book is structured into nine units sequenced in the order you and your institution may need as you consider the development of a virtual collaborative experience. You may find that the facilitator's guide and the participant's guide are enough to help launch your collaboratory. For others, Partnering at a Distance is the place you begin as you consider working across geographic boundaries. Whether you decide to implement the virtual scenarios with one or multiple partners, these units are designed to provide you with the information needed for implementation as well as recommendations and insights gleaned from our own two-year experiences. The Cookbook is not designed to be a one-size-fits-all approach to creating a successful virtual collaborative learning experience for all students. Higher education institutions are all unique – different environments, different levels of student interest and capacity, different faculty and staff engagement – and how each institution implements the recommendations in the VCCLL Cookbook will vary.

Using the Cookbook

Each of the units is organized to give you background information, and the “whys” of our approach. These sections are not intended to tell you every step you must undertake but
instead represents what we believe to be the foundational information that is needed to undertake such an effort. Each of the units addresses a particular aspect of building the virtual collaborative learning experience and are designed to help you take what you have prepared and implement it.

We hope that the Cookbook provides you with all information you need to not only replicate but to build upon the work of our Cyber Corp pilot project. However, in the world of cybersecurity and virtual hands-on learning with students and colleagues, there is always something else to mention and that’s where the FAQ’s section comes in. It contains a number of questions and answers to some of the basic questions we have encountered over the life of the pilot project.

Acknowledgements

This has been a collaborative project and the Cookbook represents that partnership and collegial spirit. We want to thank our students across the three higher education institutions who joined us to experience BetaPort and the cybersecurity scenarios we challenged them with. Their insights and perspectives have helped create the document you see here. Our thanks as well to our home institutions, the University of Southern Maine, the University of Maine at Fort Kent and York County Community College for their institutional support throughout the project and to the National Science Foundation for the funding that enabled this work to occur. Each of us has put words on the page, but it is a team such as this one that has created this final product. We offer it to other higher education institutions looking to engage and excite students about how they can learn and develop skills in the virtual world of cybersecurity.

The VCCLL team includes:

Dahlia Lynn, Ph.D. PI NSF CyberCorp Grant
Raymond Albert, Ph.D. CO-PI NSF CyberCorp Grant
Mark Monin, CO-PI NSF CyberCorp Grant
Carl Blue, Ph.D. Department of Technology
Edward Sihler, Director of Technical Services, Maine Cyber Security Cluster
Lynn Lovewell, Director of Operations, Maine Cyber Security Cluster
James, Owens Senior Research Scholar, Maine Cyber Security Cluster
Daniel Light, Education Develop Center