JOHNS HOPKINS
WHITING SCHOOL
of ENGINEERING | Information Security Institute

# Developing and Disseminating Advanced Educational Materials on Cybersecurity Research Topics to Community Colleges

Anton Dahbura, Xiangyang Li, Joseph Carrigan and Christopher Venghaus

Johns Hopkins University Information Security Institute

Baltimore, MD

*Work conducted under DoD Grant S-004-2017 CAE Cybersecurity (CAE-C) “Investment in Expansion of CAE-C Education Programs”*

# Overview

- There is an urgent need to develop effective and current teaching materials and learning mechanisms to train cybersecurity faculty and students in the sizeable community college community.

- We are developing a course and accompanying materials to provide students at the community college level with an introduction to various topics on the forefront of cybersecurity research.

- The objective is to interest students in the field and motivate them to advance their education and careers in the field of cybersecurity.

- The project will seek the leverage of the already established partnership relationship with the Hagerstown Community College (HCC) to test and disseminate the outcomes.

# Approach

- We are developing a distributable course that will provide an introduction to advanced topics in cybersecurity, targeted at community college students and made available to community college faculty and staff.
- The size of the audience that we are trying to reach would preclude holding live lectures.
- Modeled on our past efforts with HCC- during a week, students will view a lecture from JHUISI faculty, staff, or graduate students and participate in classroom activities designed to reinforce the subject of the lecture.

# Project Advisory Panel

- The project will include an advisory panel of Subject Matter Experts (SME’s) from higher education institutions, government agencies, and industry practitioners.
- This panel will assist by providing input and feedback on cybersecurity topic selection, educational module design and delivery, and marketing and outreach efforts.

# Materials

- Videos

  JHUISI will select faculty and staff to develop video lectures that cover given topics in cybersecurity.  These videos will be professionally produced.  Each video lecture will cover one topic.  A lecture may be delivered as a single video or as multiple short videos.  The total video time for a lecture will be about an hour.

- Background Information

  Community College instructors may not be completely familiar with all the topics that we cover in the course.  Therefore, we will provide background information for each lecture.  The professors teaching the course will be able to review these materials prior to the introducing the students to the material.

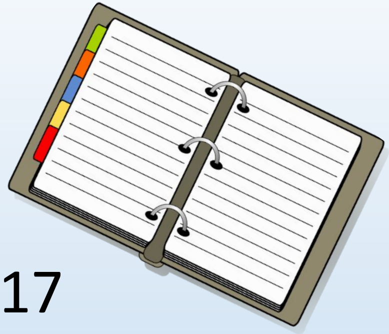
- Course Material

  JHUISI will develop multimodal materials for the course.  The instructors will be able to select the set of course materials that best suits the abilities of the students.  We envision providing three levels of materials of increasing depth on each topic.   The materials will include homework assignments and answer keys, unit tests and answer keys, a final exam and answer key, and hands-on laboratory exercises where applicable.

# Envisioned Use

- CC’s will offer the course as an introduction seminar series to Cybe
- The class should meet two times a week for 75 minutes.
- Each week, the instructors will review the background information in the kit to familiarize themselves with the topic of the week.
- During the first class meeting of the week the instructor and the students will watch the video or videos for that week.
- During the second class meeting, students will participate in an in-class activity designed to reinforce the lessons discussed in the video.  This in-class activity may be a discussion, a review of other research on the topic, or a hands-on activity.

# Schedule



- Develop Curriculum July 1, 2017 – August 30, 2017
- Develop Lectures September 1, 2017 – November 30, 2017
- Develop Assignments September 1, 2017 – January 31, 2018
- Produce Videos December 1, 2017 – April 30, 2018
- Distribute Packets May 1, 2018: The packets will be made available online on a website hosted by JHU.

# Course Structure

- Unit 1: Cyber-Defense (4 weeks)
  Module 1-1: Policies and Procedures
  Module 1-2: Network defense 1 (firewalls, anti-virus)
  Module 1-3: Network defense 2 (IDS, IPS)
  Module 1-4: People are the weakest link
- Unit 2: Penetration Testing (4 weeks)
  Module 2-1: Vulnerability Scanning
  Module 2-2: Social Engineering
  Module 2-3: Password Cracking
  Module 2-4: Compromising Wi-Fi networks
- Unit 3: Cryptography (3 weeks)
  Module 3-1:  Symmetric and Asymmetric Cryptography models
  Module 3-2:  Practical Cryptography
  Module 3-3:  Cryptanalysis
- Unit 4: Healthcare Security (4 weeks)
  Module 4-1: Patient Privacy and HIPAA
  Module 4-2: Security of Electronic Medical Records
  Module 4-3: Medical Device Security
  Module 4-4: New Research Topics in Health Care Security

# Requirements of a Participating Institution

- This course will be made available to any institutions that request it.
- Participating Community colleges will need to have the following:
  - A means to play the videos for a class of students
  - A means to reproduce the course materials as needed
  - A means of hosting virtual machines or
  - Physical machines capable of being used for the labs
  - An instructor that can understand the material well enough to teach the class