Cybersecurity Assessment Tools Project MiniHackathon
1-4 pm, Tuesday, June 4, 2019
Meeting Room 2,1 Von Braun Conference Center, Huntsville, Alabama

Call for Participants

We seek your help in improving multiple-choice test items for the Cybersecurity Curriculum Assessment (CCA) tool that we are developing for graduates entering the workforce. Participants will discuss and provide feedback on approximately 30 draft questions. We seek 20 cybersecurity experts who are working in higher education, private industry, or government. Participants are expected to register for the 2019 National Cyber Summit. People interested in participating should contact Alan Sherman (email: sherman@umbc.edu).

Project Overview. Presently there is no rigorous, research-based method for measuring the quality of cybersecurity instruction. Validated assessment tools are needed so that cybersecurity educators have trusted methods for discerning whether efforts to improve student preparation are successful. The Cybersecurity Assessment Tools (CATS) Project provides two rigorous evidence-based instruments for assessing and evaluating educational practices: the CCA and the Cybersecurity Concept Inventory (CCI). This MiniHackathon will not involve the CCI, which targets students in any first course in cybersecurity.

Project Team. Alan T. Sherman, Linda Oliva, Dhananjay Phatak, Travis Schepnik, Enis Golaszewski (UMBC), Geoffrey Herman, Spencer Eliot (University of Illinois at Urbana-Champaign), Peter Peterson (University of Minnesota Duluth).

Workplan. After a brief introduction to the CATS Project, participants will take the draft CCA, discuss their reactions, and provide suggestions for possible improvements. In addition, each participant will be given an opportunity to suggest ideas for new scenarios and questions. Please bring a laptop.

An Overview of the CCA. Targeted at college graduates entering the workforce, the Cybersecurity Curriculum Assessment (CCA) will be a 50-min, 25-question multiple-choice test that assesses conceptual understanding of the following five core concepts in cybersecurity:

1. Identify vulnerabilities and failures.
2. Identify attacks against the CIA triad and authentication.
3. Devise a defense.
4. Identify the security goals.
5. Identify the potential targets and attackers.

Each test item comprises three parts: a scenario (possibly shared among more than one question), a stem (question/prompt), and five answer choices. Several items may share the same scenario but will have a unique stem and unique answer choices. Each stem focuses on one of the above targeted concepts. Each stem has exactly one best choice (and four distractors). Test items target timeless fundamental concepts, not merely factual information.

Benefits. Each accepted participant will: (1) Be helping to improve cybersecurity education. (2) Be given an opportunity for reimbursement (about $200) for one hotel night and one day of food per diem. (3) Be invited to dinner at 5pm after the MiniHackathon at the Pane E Vino pizzeria, 300 Church St., SW, about a 5 min walk from conference center.

Support for this event is provided in part by the National Science Foundation under SFS Capacity Grant 1819521 and by the 2019 National Cyber Summit.

---

1 Around the corner from the main exhibit entrance.