

SIGCSE 2014 Poster

Proposers: Wingyan Chung¹, Albert Chan², Daniel Plante¹, Ray Villalobos³, Joseph Woodside¹

¹ Stetson University
421 N. Woodland Blvd.
DeLand, FL 32723
386-822-7002 (office)
386-822-7407 (fax)
{wchung, dplante, joe.woodside}@stetson.edu

² Fayetteville State University
achan@uncfsu.edu

³ Seminole State College
planetoftheweb@gmail.com

SIGCSE 2014 Poster Proposal

Statement of Topic: Intelligence and Security Informatics: Developing Curricular Modules in Context

Significance and Relevance:

Intelligence and Security Informatics (ISI) is a cross-disciplinary field defined as the development of advanced information technologies, systems, algorithms, and databases for international, national and homeland security related applications, through an integrated technological, organizational, and policy-based approach. Despite significant research developments over the past decade, little work is found on preparing undergraduate students to enter the growing ISI profession. The “Computing in Context” project, funded by National Science Foundation (DUE-1141209), aims to develop, disseminate, and evaluate course materials and teaching modules that use active learning pedagogies and that put the learning of computing in real-world context. One of the project’s sub-groups focuses on teaching modules and pedagogical development that use active-learning in an ISI context. Supported by the Center for Business Intelligence and Analytics at Stetson University (<http://cbia.stetson.edu/cic>), the group convened for its first workshop in August 2013 and developed five exemplar teaching modules, as summarized below.

Database Design and Development for Cybercrime Investigation

Law enforcement agencies develop databases to support storage and access of data about cybercrime cases and suspects. In this module, students learn database design and development in the context of cybercrime investigation. Students learn about data structure in identifying cybercrime data attributes, collaborate in groups to define an entity relationship model, develop the database using a small-scale database management system, and create a professional presentation of the database. In-class discussions surrounding selection of database attributes and data structure, creation of attribute relationship, and effective communication of the end product serve to engage students in active learning. We assess the module effectiveness by measuring students’ performance in the exercises.

Securing Private Data on the Internet

Using online search tools, cybercriminals can write programs to scrape sensitive data (e.g., PDF or Excel files containing “ssn”, “password”) from targeted bank or company web sites. In this module, students learn to use PHP, Curl, and the Google Advanced Search API to scrape benign content from web pages (e.g., ISBN numbers from Amazon) to illustrate the methods. Students also will gain experience designing modular code and using Software-as-a-Service (SaaS) by accessing the RESTful search API. In-class activities involve programming such scrapers, discussing the ethics of acquiring data that is sensitive and unintentionally made public, and company policies and training that can help prevent such problems. Module assessment will focus on students’ acquisition of skill and knowledge.

Using Data Visualization to Understand Privacy Sentiment

To understand the effect and the moods, sentiments and trends of online privacy, the students can use open source and readily available tools to map out this data in a visual format. In this module, the students will learn how to read, parse and visualize data from

twitter that is related to privacy information and moods. They will use modern visualization tools such as Gephi and the d3 JavaScript library to create dynamic visualization of sentiment data related to privacy and security. The module will be implemented in a computer science class in which we will assess the module by a survey.

Mobile Security Intelligence

Mobility of computing devices can invite unwanted access to such private data as contacts, texts, calls, email, calendars, internal systems, credit card information, and personal data. Increases in breaches can be tied to regulation requirements, automation increases, social media development, and human errors. This module and associated learning outcomes include risk, event, use monitoring, and security analysis. In an applied activity, students collaborate in groups to solve security issues with bring your own device (BYOD) in business and present their findings and receive feedback through classroom discussions.

Computer Program Design and Development for Digital Forensics

Digital forensics professionals often need specific software tools to support investigation. This module targets students taking a second-semester programming course (traditionally known as CS2). We introduce a scenario of digital forensics and designed a series of labs to guide students through all stages of object-oriented programming design and development. Deployed as in-class activities, the labs cover such topics as using objects, creating classes, text files handling, inheritance, data structures, and recursion. A submission mechanism will be provided to track students' participation to support statistical analysis of the labs' effectiveness. We have deployed some of the labs to a CS2 class and will use the students' final grade in the course to evaluate the module.

Our poster presentation aims to connect with scholars who use active-learning or inquiry-based learning in teaching ISI topics or who are interested in connecting computing with the ISI discipline through teaching partnerships. We will extend our reach to the broader audiences who care about interdisciplinary computing education and who will likely adopt our modules in their teaching, thus helping to disseminate the materials to a wider community of learners.

Content of Poster: The poster will have four main areas: a summary of project goals, a description of inquiry-based learning in ISI, the five ISI modules developed, and an invitation to participate in evaluating and disseminating the course materials.

Abstract: Intelligence and Security Informatics (ISI) is a cross-disciplinary field that connects advanced information technologies, systems, algorithms, and databases with international, national and homeland security related applications. Our NSF-funded project, titled Computing in Context, has a focus of developing new teaching modules and pedagogies for the ISI discipline at the undergraduate level. In this poster, we present five exemplar modules that we developed for the ISI discipline: database design for cybercrime investigation, securing private data on the Internet, data visualization for understanding privacy sentiment, security intelligence for healthcare mobility, and program design for digital forensics. Our materials are designed for inquiry-based learning and for active engagement of students through discussion, hands-on practices, and various exercises.