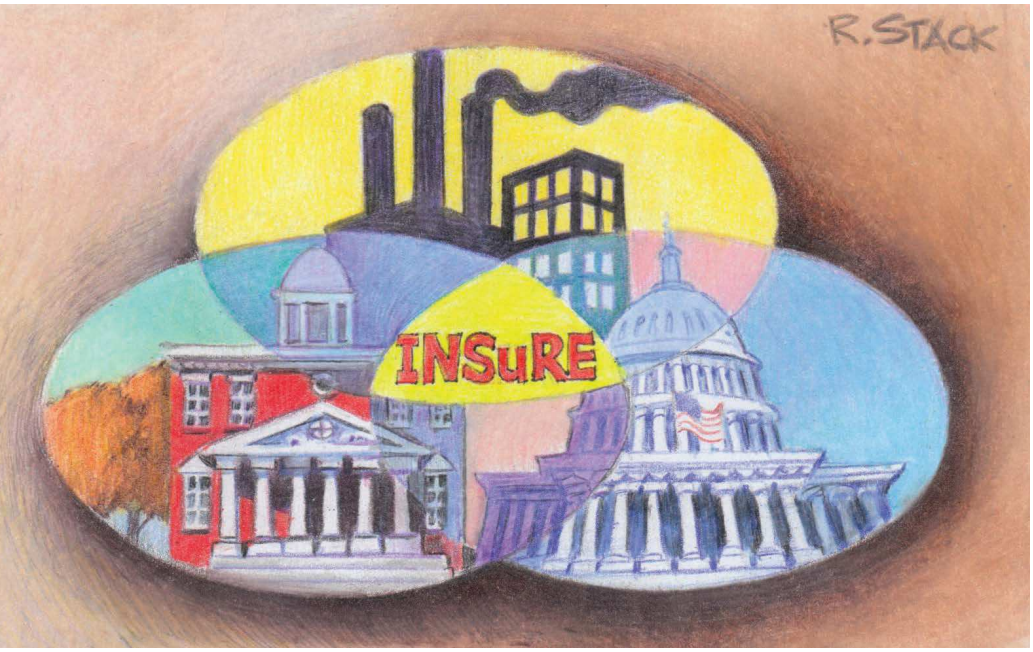
Editors: Melissa Dark, dark@purdue.edu | Jelena Mirkovic, mirkovic@isi.edu | Bill Newhouse, william.newhouse@nist.gov

INSuRE: Collaborating Centers of Academic Excellence Engage Students in Cybersecurity Research

Alan Sherman | University of Maryland, Baltimore County
Melissa Dark | Purdue University
Agnes Chan | Northeastern University
Rylan Chong | Purdue University
Thomas Morris | University of Alabama in Huntsville
Linda Oliva | University of Maryland, Baltimore County
John Springer | Purdue University
Bhavani Thuraisingham | University of Texas at Dallas
Christopher Vatcher | University of Maryland, Baltimore County
Rakesh Verma | University of Houston
Susanne Wetzel | Stevens Institute of Technology



The Information Security Research and Education (INSuRE) collaborative is a network of National Centers of Academic Excellence in Cyber Defense Research (CAE-R) universities that cooperate to engage students in solving applied cybersecurity research problems.[1] Begun in fall 2012 by Melissa Dark, professor of computer technology at Purdue University, and Mark Loepker, NSA Security Education Academic Liaison for Purdue, INSuRE has fielded a multi-institutional cybersecurity research course in which small groups of undergraduate and graduate students work to solve unclassified problems proposed by NSA, other US government agencies, and private organizations and laboratories.

The approximately 80 CAE-R universities include a significant collection of cybersecurity students, educators, and researchers.[2] Although the individual universities were "nodes of excellence," these nodes weren't purposefully constellated into a research network. The INSuRE project created an educational and research network of CAE-Rs. As such, INSuRE is a self-organizing, multidisciplinary, multi-institutional, and multilevel collaborative organization.

In this article, we describe our experiences with the INSuRE course, including examples of student projects and lessons learned. More detailed information on

 Copublished by the IEEE Computer and Reliability Societies

INSuRE Participants

The first Information Security Research and Education (INSuRE) course took place in the fall of 2012 at Purdue University with five students who formed two groups supported by three technical directors. With funding from the US National Science Foundation, the project soon added three more schools: University of California, Davis; Mississippi State; and University of Maryland, Baltimore County (UMBC). Many of the INSuRE students at all universities were also CyberCorps: Scholarship for Service scholars.

In the following years, the course expanded to include a total of

- *13 universities*—Carnegie Mellon University; Dakota State University; Iowa State University; Mississippi State; Northeastern University; Purdue University; Stevens Institute of Technology; University of Alabama in Huntsville; University of California, Davis; University of Houston; UMBC; University of Texas at Dallas; and University of Texas at San Antonio;
- *five national labs*—Argonne National Labs, NIST, Oak Ridge National Labs, Pacific Northwest National Labs, and Sandia National Labs;
- *three government organizations and federally funded centers*—Johns Hopkins University Applied Physics Lab, NSA, and Naval Surface Warfare Center Crane Division; and
- *two state organizations*—Indiana Office of Technology and New Jersey Office of Homeland Security and Preparedness.

A small number of private companies also participated some years. For example, the spring 2014 edition included a private defense contractor, Assured Information Security, located in UMBC's research park. Each partner organization suggested research problems.

INSuRE can be found in previous publications.[3–6]

The INSuRE Course

The INSuRE project's central activity is its cybersecurity research course, in which students form small groups that work on problems of national interest. The NSA and other organizations contribute suggested problems and provide technical directors (TDs) to mentor student groups. The geographically diverse participants connect and collaborate using various conferencing and data-sharing technologies (for more on INSuRE's participants, see the sidebar).

Table 1 summarizes the growth of the INSuRE course from its start in 2012 through spring 2017.

Every semester, a rotating subset of the collaborating universities offers a section of the course at their schools. Doing so enables each university to participate at a frequency that suits its needs while fostering a diverse set of relationships among the schools.

To facilitate collaboration, the project uses the Purdue University Research Repository (purr.purdue.edu), Purdue's instantiation of the open source software platform HUBzero (hubzero.org). Users can share files, publish datasets and computational tools with DOIs, and participate asynchronously in discussion groups across multiple institutions. Individuals and groups participate synchronously in periodic community meetings using WebEx conferencing software, supplemented by an audio bridge. INSuRE instructors share experiences and develop common syllabi, handouts, and grading rubrics.

All class activities revolve around student projects. TDs present their suggested problems, and then students submit bids and form groups (typically three to five students each). In some schools, instructors assign groups; in others, students self-select groups. Each group prepares a proposal, including a literature review, specific aims, and a research plan. Formal group presentations to the INSuRE community include progress reports and final reports.

Throughout the course, students interact with their TDs, who can follow their groups through a "dashboard" slide summarizing the group's progress. Most groups work on problems suggested by the TDs; some propose their own custom projects or variations of suggested problems. Organizations sometimes propose the same or a similar project in multiple semesters. Student groups can continue projects completed in previous terms or, in some cases, revisit a problem addressed before by others.

Once a semester, key faculty and student members from each participating school meet in person, together with some of the TDs, to review outcomes, discuss possible improvements, nurture relationships, and plan ahead.

In summer 2016, the project initiated INSuRECon (sites.google.com/a/uah.edu/insurecon16), an annual student-organized research conference featuring five competitively selected project presentations from the INSuRE course.

Project Examples

To illustrate the type of research carried out in the INSuRE course,

we briefly describe the suggested problem lists and three representative student projects.

Problem Lists

Partner organizations provide lists of suggested problems covering a wide range of topics, including

- policy-based stored information management, protection, and access control;
- software assurance, including machine-assisted semantic understanding of code;
- cloud computing, including cleanup of data spillage in Hadoop clouds;
- forensics, including cloud forensics and mobility forensics in the Internet of Things;
- derivation of intelligence from encrypted VPN streams;
- protocol analysis and verification;
- botnets;
- machine learning for malware classification;
- vehicular data bus security; and
- incident-response capabilities assessment.

TD Trent Pitsenbarger of NSA explained, "The tasks we place on our INSuRE task list represent areas where the organization needs greater insight and past tasks have helped us." These areas include understanding new technologies (for example, Fast Identity Online [FIDO] authentication), tool development (for example, control flow integrity), and validation of guidance (for example, guidance on cleaning up sensitive data spillage in clouds).

Project 1: Moving-Target Defense

A three-student team from University of Texas at Dallas, working together with Argonne National Labs, developed a moving-target defense (MTD) to protect against probing attacks on webservers.[7] At random bounded intervals between 15 and 60 seconds, the system switched the webserver between Apache and Nginx. Dynamically updated IP tables redirected web traffic to the active server. This deception aimed to hinder attacks by constantly changing the target.

To test the system's effectiveness, the team launched simulated attacks against the web service with and without MTD protection. With MTD protection, a WordPress application ran normally 76 percent of the time, experienced lag 14 percent of the time, and was down 10 percent of the time. By contrast, without MTD, the application ran normally 13 percent of the time, experienced lag 7 percent of the time, and was down 80 percent of the time. This work suggests that MTD is a practical and effective defense against web service probing attacks.

Project 2: Analysis of Fast Identity Online

In three separate terms, teams from University of Maryland, Baltimore County (UMBC), Purdue, and Stevens Institute of Technology analyzed the FIDO authentication protocol under development by the FIDO Alliance (fidoalliance.org). In spring 2014, a team from UMBC studied the new FIDO protocol, assessing its goals, strengths, and weaknesses. This team's work complemented that of another concurrent UMBC team studying the Pico authentication system (mypico.org). FIDO and Pico offer different approaches to the eventual replacement of passwords.

Building on the initial UMBC work, in fall 2014, a team from Purdue evaluated the FIDO-ready Samsung Galaxy S5 fingerprint reader's vulnerability to a particular spoofing attack.[8] Discovered by a German security research lab, this attack lifted a latent fingerprint. The Purdue team couldn't successfully replicate the attack, although they did produce a fingerprint by lifting a latent fingerprint.

In spring 2015, a team from Stevens continued this work by studying two attacks on each of four different fingerprint scanners: two FIDO-compliant devices (Samsung Galaxy S5 and iPhone S5) and two non-FIDO-compliant devices (Hamster Area Scanner and Validity Swipe Sensor). For each device category, one device had a swipe sensor and one had an area sensor. One attack created a "fake finger," and the other produced a latent fingerprint. The team successfully performed each attack on the Galaxy S5 and on both non-FIDO-compliant devices. Differences between FIDO- and non-FIDO-compliant devices were not due to the FIDO protocol but rather to differences in the component authenticators' strengths. Subsequently, NSA removed the problem from the INSuRE set because the three student teams had resolved all the questions.

Project 3: Detecting Intrusions on Supervisory Control and Data Acquisition Systems

A two-student team from Mississippi State University studied machine-learning techniques for detecting cyberattacks against industrial control systems. The team worked from a dataset of cyberattacks and normal behavior from an electricity transmission system. The dataset included alteration and injection attacks against protection relays and energy management system (EMS) software. The injection attacks sent illicit network packets to protection relays to cause the relays to operate and open a circuit breaker. The alteration attacks used a man-in-the-middle to alter voltage and current sensor data sent from phasor measurement units to the EMS software. The dataset also included instances of single line-to-ground faults at random locations

Table 1. Growth of the Information Security Research and Education (INSuRE) course from fall 2012 through spring 2017.

Term	No. of universities	No. of students	No. of technical directors (NSA + other)	No. of student groups
2012 fall	1	5	3 + 0	1
2013 summer	1	1	0	1
2014 spring	3	33	7 + 0	13
2014 summer	1	1	0	1
2014 fall	4	22	7 + 1	8
2015 spring	8	52	7 + 3	21
2015 fall	7	42	8 + 8	14
2016 spring	6	72	6 + 9	27
2016 fall	8	64	5 + 6	25
2017 spring	7	54	6 + 15	22

in the simulated transmission system, and changes in system load at random times.

First, the team extracted features from the dataset and applied clustering techniques to learn event classes. Second, they built a classifier using the Mamdani fuzzy inference system. Inputs to the classifier comprised a heterogeneous collection of voltage, current, frequency, Snort log, and protection relay log information from one time stamp.

The team validated their work by comparing results to similar classifiers developed from K-means and fuzzy C-means clustering algorithms. Their approach outperformed K-means and fuzzy C-means intrusion detection systems.

Outcomes and Lessons Learned

From fall 2012 through fall 2016, the INSuRE class produced 140 project reports on 110 separate problems and taught 356 students (many of whom have since been hired by government organizations).

In addition to the works presented at INSuRECon, INSuRE projects resulted in refereed conference publications,[7–12] refereed posters, and published datasets.[6]

Takeaways for Educators

We summarize here some of the outcomes, lessons learned, and challenges from the perspective of educators.

Outcomes. To improve the course, faculty frequently discussed processes and outcomes. In May 2014, students submitted course feedback via an online survey administered through SurveyMonkey. Items included rank-order, Likert scale, and open-ended questions. The most highly rated elements included developing expertise in a specific cybersecurity topic, developing qualifications for a cybersecurity job, and working with a government or industry mentor. Students identified development of cybersecurity research skills as an important course outcome. Survey results also showed that students found limitations with the electronic communication methods used to interact with other institutions.

In fall 2016, Purdue conducted a pilot study investigating the INSuRE course's effect on student research self-efficacy, which is a self-judgement of one's ability to perform particular research tasks. Students (five undergraduate, 12 graduate) from eight universities completed pre- and postsurveys in which they rated their research self-efficacy using a 100-point Likert scale (where 0 denoted complete uncertainty, and 100 denoted complete certainty).

Given the small sample size and Likert scores' relative nature, the team analyzed the data using a nonparametric Wilcoxon test. Student research self-efficacy showed statistically significant improvements (pretest mean 73.56, median 76.33, interquartile range [65.38–83.54]; posttest mean 83.27, median 86.83, interquartile range [74.54—89.42]; $z = -2.58$, $p < 0.01$; Cronbach alpha 0.96 for each survey).

Students gained valuable experience carrying out research, presenting their work, writing proposals and reports, using tools (such as for software analysis),

working in groups, building relationships, and communicating succinctly and effectively with their TD. Because the problems touched a broad range of issues, students and faculty gained knowledge outside their focused areas of expertise. In addition, the course inspired students to tackle challenging problems. The INSuRE course has benefited from a significant number of female students.

For some students, this course was their first exposure to research and helped them learn to take the initiative and lead. Several INSuRE students continued their studies at the PhD level, citing the course as an important motivating factor. One university reported that its INSuRE course prompted a faculty member to add an INSuRE problem to his research area, increased the number of students completing capstone engineering projects in cybersecurity, and motivated local companies to engage in cybersecurity projects with the university.

Although the INSuRE research experience inspired most students, a few also learned that cybersecurity research wasn't a path they wanted to pursue.

Lessons learned. Many factors contributed to the groups' success. To begin, it was helpful to screen students (especially undergraduates) to make sure they were motivated and ready to engage in research. It was also important that each team had a student leader with strong organizational skills. TDs also contributed significantly through their enthusiasm, availability, and probing questions. Course alumni contributed to project success by enthusiastically functioning as course assistants, facilitators, and mentors.

In some terms, instructors required each group to provide periodic peer evaluations of a paired group. Doing so delivers additional feedback to the evaluated group and helps the evaluating group learn the research process. However, such peer evaluations come at the cost of student and faculty time and effort, and can be difficult to coordinate across diverse university schedules.

Some schools restricted enrollment to graduate students, while others permitted some undergraduates to participate. In mixed classes, graduate students were usually expected to take on greater leadership roles than were undergraduates. Many instructors found, however, that student performance typically had more to do with student capability and motivation than with degree level.

INSuRE's central activity is its cybersecurity research course, in which student groups work on problems of national interest.

Although most schools offered the INSuRE experience as a dedicated course, others enrolled students as independent study projects or as part of an existing course (for example, capstone). Faculty found the biannual in-person meetings very useful, helping participating universities improve the course by applying lessons learned. They also fostered the strong personal relationships necessary for effective collaboration.

Challenges. Challenges included dealing with different time zones and university schedules (for example, semester versus quarter systems). Also, although useful, the conferencing software yielded video displays that were limited in comparison to the rich interaction possible through in-person meetings. Significant instructor involvement is required to stay on top of all projects.

One semester is a short period of time to complete a research project, yet one year might be longer than many students are willing to invest. At many of the universities, grant support was essential to allow faculty members to teach a small, specialized research course that counted toward their official teaching duties. Teaching the INSuRE class often meant not teaching some other course, which might have been a larger required class.

Some centralized support was essential to organize the network, maintain a project repository, and manage the collaborative technologies. Financial resources were needed for this centralized support, hardware and software, in-person meetings, teaching assistant support if the class was large, and instructor time.

Takeaways for Government Policymakers

At modest investments, the INSuRE project produced a sizable return, especially in terms of recruiting highly qualified cybersecurity students into the government workforce. In addition, by funding a research network, government could support cybersecurity research without favoritism to particular universities.

Another benefit is that the INSuRE course enabled government organizations to stimulate research on projects that they lacked time to pursue.

Aspects of the INSuRE model can be applied to other settings. For instance, in 2016–2017, UMBC pioneered a new initiative to extend CyberCorps: Scholarship for Service (SFS; www.sfs.opm.gov) awards to nearby Montgomery

College and Prince George's Community College students who will complete their degrees at UMBC. While still at the community college level, these scholars help solve IT security problems for their county government.

Securing a sustainable funding model is a challenge. One option is a subscription model in which companies and organizations contribute in return for access to students and their work. Another option is a charity model in which sponsors (such as government) fund the program for the national good. We welcome the opportunity to explore future relationships with government, industry, foundations, and other groups to continue the outstanding student work nurtured by INSuRE.

The INSuRE project has inspired and educated numerous students, empowering them to work collaboratively on real-world problems and interact with experienced TDs. They also learn how to perform research, including how to produce fast and actionable results in team projects. The project has strengthened the CAE-R network and helped government organizations, not least of all by motivating students to pursue government service. University faculty have also benefited from the connections they build with other researchers, schools, and government organizations. The course is being offered again in fall 2017. INSuRE's continued success will depend on strong external support from government, industry, and foundations, and on internal support from universities. ■

References

1. "About Us," INSuRE Hub, 2017; insurehub.org/about-us.
2. "NSA/DHS National CAE in Cyber Defense Designated Institutions," Nat'l IA Education and Training Programs; www.iad.gov/NIETP/reports/cae_designated_institutions.cfm.
3. M. Dark, "Innovation in Graduate Cyber Education Project INSuRE," invited talk, *Nat'l Initiative for Cybersecurity Education Conf.* (NICE 14), 2014.
4. M. Dark and L. Stuart, "Innovation in Cybersecurity Research Traineeship in the INSuRE Project," *Proc. 7th Ann. Southeastern Cyber Security Conf.* (SCSS 15), 2015.
5. M. Dark et al., "Realism in Teaching Cybersecurity Research: The Agile Research Process," *Proc. 9th IFIP WG 11.8 World Conf.* (WISE 15), 2015, pp. 3–14.
6. A. Sherman et al., *The INSuRE Project: CAE-Rs Collaborate to Engage Students in Cybersecurity Research*, Cornell Univ. Library arXiv.org, 2017; arxiv.org/abs/1703.08859.
7. M. Thompson et al., "Dynamic Application Rotation Environment for Moving Target Defense," *Proc. Resilience Week* (RWS 16), 2016; doi.org/10.1109/RWEEK.2016.7573301.
8. R.C. Chong et al., "The FIDO INSuRE (Information Security Research Education) Project: An Agile Research Experience," *Proc. Colloquium for Information Systems Security Education* (CISSE 15), 2015, pp. 1–7.
9. T. Alabi et al., "Toward a Data Spillage Prevention Process in Hadoop Using Data Provenance," *Proc. Workshop Changing Landscape in HPC Security* (CLHS 15), 2015, pp. 9–13.
10. T. Alves, R. Das, and T. Morris, "Virtualization of Industrial Control System Testbeds for Cybersecurity," *Proc. 2nd Ann. Industrial Control System Security Workshop* (ICCS 16), 2016, pp. 10–14.
11. C. Falk, "A Model and Tool for Public Cloud Provider Risk Assessment," *Proc. 7th Ann. Southeastern Cyber Security Summit* (SCSS 15), 2015; insurehub.org/sites/default/files/Public%20Cloud%20Tool%20Paper%20-%20SCSS%20Submission%20Revised.pdf.
12. S. Nair, S. Mittal, and A. Joshi, "OBD_SecureAlert: An Anomaly Detection System for Vehicles," *Proc. IEEE Workshop Smart Service Systems* (SmartSys 16), 2016; ebiquity.umbc.edu/_file_directory_/papers/792.pdf.

Alan Sherman is a professor of computer science at University of Maryland, Baltimore County (UMBC). Contact him at sherman@umbc.edu.

Melissa Dark is a professor of computer technology at Purdue University. Contact her at dark@purdue.edu.

Agnes Chan is a professor of computer and information science and executive director of cybersecurity programs at Northeastern University. Contact her at ahchan@ccs.neu.edu.

Rylan Chong is a doctoral student in information security at Purdue University. Contact him at rchong@purdue.edu.

Thomas Morris is the director of the Center for Cybersecurity Research and Education, and an associate professor of electrical and computer engineering at University of Alabama in Huntsville. Contact him at tommy.morris@uah.edu.

Linda Oliva is an assistant professor of secondary education at UMBC. Contact her at oliva@umbc.edu.

John Springer is an associate professor of computer and information technology at Purdue University. Contact him at jaspring@purdue.edu.

Bhavani Thuraisingham is the Louis A. Beecherl Jr. Distinguished Professor of Computer Science and executive director of the Cyber Security Research Institute at University of Texas at Dallas. Contact her at bxt043000@utdallas.edu.

Christopher Vatcher is a doctoral student in computer science and electrical engineering at UMBC. Contact him at cn1@umbc.edu.

Rakesh Verma is a professor of computer science and director of the ReDAS Lab at the University of Houston. Contact him at rmverma6@gmail.com.

Susanne Wetzel is an associate professor of computer science at Stevens Institute of Technology. Contact her at swetzel@cs.stevens.edu.