THE UNIVERSITY OF ARIZONA

SP26 SIE 472 / 572: Information Security and Research (INSuRE)

Course Syllabus

Instructor: Bill Hayes

Email: billhayes@arizona.edu
847-404-0136

Office Hours: *TBR via Zoom*

On Campus Offering: Mon, Wed, Fri 11:00 – 11:50am
Old Engineering, Room #301

Description of Course

This course engages students in diverse and varied national cybersecurity/information systems security problems, under an existing and very successful umbrella program called "INSuRE", that enables a collaboration across several universities, cyber professionals and cross-disciplined cyber related technologies. Led by Stevens Institute of Technology and made possible by a grant from the NSA and NSF, 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/or private organizations and laboratories. Students will learn how to apply research techniques, think clearly about these issues, formulate and analyze potential solutions, and communicate their results with sponsors and other participating universities.

Working in small groups under the mentorship of technical experts from government and industry, each student will formulate, carry out, and present original research on current cybersecurity / information assurance problems of interest to the nation. This course will be run in a synchronized distance fashion, coordinating activities with other INSuRE technical clients and sponsors, along with partnering universities which are all National Centers of Academic Excellence in Cyber Defense Research (CAE-R).

Examples of past research projects are noted below. These are *representative* of the types of projects that the various organizations have sponsored over prior semesters of the INSuRE program. ***The exact projects for any given semester are not provided until the start of the semester, and therefore the following list should be used as reference only.***

- **NSA:** The Impact of Known Vulnerabilities on Layered Cyber Defensive Solutions
- **NSA:** Cryptographic Protocol Analysis and Verification
- **NSA:** Emergent Security of Multi-Cloud Environments
- **NIST:** Black-Box Entropy Estimation
- **MITRE:** Detecting Malicious Activity in Operational Technology Telemetry
- **MITRE:** Robust TTP Detection Analytic Development
- **John Hopkins Applied Physics Lab:** Software Assurance: Defect Localization
- **MIT Lincoln Lab:** Abstract Algebra of Cyberspace
- **MIT Lincoln Lab:** Anonymized Network Analysis on the Edge
- **US DoD:** Infrastructure Cybersecurity in a Hybrid Cloud Environment

Course Prerequisites or Co-requisites

Students may come from computer science, software engineering, computer engineering, information technology, or any related technical field (e.g., electrical engineering, information systems, math). Each student is expected to bring expertise, interest, and exposure to at least one relevant cyber related technical area. (If you are uncertain whether you have the necessary technical background to participate in this course, coordinate with your advisor prior to enrolling.)

One of the following courses is required to insure an appropriate background in Cyber related technical areas: SIE 471 / 571 / 573, ECE 478/578, ECE 509, MIS 416/516 or related course.

(Other relevant coursework or professional work experience can also be used to fill the prerequisite requirements with the approval of the instructor.)

Course Format and Teaching Methods

This is predominately a research-oriented course. There will be lectures to help get teams of students acclimated to the format and structure of the course. Each team will be assigned to work with an outside research organization (such as the NSA, one of the National Labs, or other research institutions) and a Technical Director from that organization will be assigned to help facilitate the required research. There are periodic status reviews with other students from different universities across the country that are participating in the INSuRE program, along with many industry experts and the sponsors from the various research institutes. There will be in-class discussions and working sessions to help teams share and learn from one another.

Course Objectives

Upon completion of the course, students will have completed a selected research project with a participating sponsor / national laboratory of their choosing. Projects will be proposed by and introduced to the students at the beginning of the semester, and students will be given an opportunity to form teams and select projects that interest the team. Each team will submit 3 Project Bids in response to sponsor provided problem sets (that will ultimately become team projects), followed by a team generated Project Proposal to the assigned sponsor proposed research area. Additionally, there will be one interim review, other related assignments, and a Final Report and Final Report Outbrief that teams will use to share their research with their sponsors and others involved in INSuRE. Students will also be asked to individually write a final paper documenting their personal INSuRE Research Experience and Lessons Learned. As part of their Final Report, master's

level students will be required to write an additional proposal and a summary of recommended extensions for potential future research and analysis that the sponsoring organizations could consider for ongoing research and analysis.

Expected Learning Outcomes

Because the nature of the research projects varies from semester to semester, and across the different teams affiliated with the multi-university INSuRE program, specific learning outcomes will vary from project to project. Some projects will focus on various tools and methodologies related to preventing cyber-attacks, while other projects may focus on information security and networking. Some projects may focus on advances in cryptography and encryption/decryption schemes, where other projects may focus on Software Assurance, Social Engineering, Cyber policy and Law, or the Internet of Things (IoT). Students will have the opportunity to select and write a proposal in response to various sponsor provided topics. The field of cybersecurity is rich and diverse, and students will have the opportunity to be exposed to many different aspects of cyber that interest them. Once accepted by a sponsor, a technical director from that organization will be assigned to the team and they together will develop a plan for the approaches, technologies, and tools that will be used over the course of the semester to address that topic. However, upon the completion of this course, all students should be able to:

(1) Identify, formulate, and solve complex engineering problems in the diverse field of cybersecurity by applying multifaceted principles of engineering, science, and mathematics. [ABET Student Outcome 1]

(2) Communicate effectively, through both written technical reports and oral presentations, with a wide range of audiences, including faculty and students from other universities that are participating in the INSuRE program, and various professionals from prestigious National labs and research organizations such as the NSA, Argonne National Labs, and John Hopkins Applied Physics Lab (APL), among others. [ABET Student Outcome 3]

(3) Recognize and address both ethical and professional responsibilities in cyber policy and engineering, resulting in informed decisions and approaches that impact cyber research and solutions in global, economic, environmental, and societal contexts. [ABET Student Outcome 4]

(4) Work cooperatively as a multidisciplinary team, whose team members together provide leadership, create a collaborative and inclusive environment, establish goals, plan tasks, and meet objectives in solving cyber related problems/research. [ABET Student Outcome 5]

(5) Develop and conduct appropriate experimentation, analyze and interpret data, and use engineering judgement to draw conclusions and potential solutions / countermeasures to different real-world cyber threats and vulnerabilities. [ABET Student Outcome 6]

(6) Acquire and apply the knowledge gained from researching different cyber technologies and use appropriate learning strategies and partnerships with technical directors from the participating national labs and affiliations. [ABET Student Outcome 7]

(7) Exercise and demonstrate an ability to develop a proposal and recommendations for

potential future research and analysis that the sponsoring organizations may consider for ongoing efforts within their own organizations or in subsequent semesters of the INSuRE program. [Graduate students only]

Course Operation

This course is structured around weekly progress throughout the semester. The expected weekly progress is outlined in the course schedule which will be posted on D2L. Note the official **DUE DATES** for course deliverables are all posted on D2L.

INSuRE Required Work:

Working in teams, each student must complete a research project on a focused topic in cybersecurity. The project must aim to accomplish new, significant results (survey papers are not acceptable). Each student must communicate findings in an oral presentation to the class and in a written report in the format of a computing discipline technical report (about 10–20 pages). Every aspect of the project (including proposals, reviews, reports, and presentations) is intended to match the process that professional engineering researchers follow in carrying out original research.

Project topics come from lists of problems supplied by government or industrial partners. The main deliverables are a written technical report, a poster, and an oral presentation describing the team's new and significant findings (similar in form and length to those from technical research conferences such as USENIX Security). Each student is expected to attend and participate actively in class.

INSuRE Principles:

This course rests in part on the following principles:

1) Collaboration—including among industry, government, and different universities— can facilitate learning and the advancement of science and technology.
2) All course activities and deliverables model those of professional cybersecurity researchers.
3) Excellent research bridges both theory and practice.
4) All participants in the course are expected to conduct themselves in their speech, behaviors, and computer interactions with integrity and with respect for others.
5) A connected research network enables researchers of all experience and expertise levels to find solutions to real-world classified and unclassified cybersecurity problems.

Course Schedule / INSuRE Objectives

The Course Schedule is posted and maintained on the class D2L site. Note that the course schedule is subject to change and is dependent on coordination with other universities across the nation that are participating in the course. Official dates, objectives, and assignment due dates will be posted on D2L.

When appropriate, the instructor will provide feedback on course work that needs to be manually

graded (e.g., papers, assignments) within 72 hours of submission. You will be able to see results for automatically graded course work after the specified deadline.

D2L Course Management System:

This course uses the University of Arizona's D2L course management system. You are **required** to use D2L with this class and are encouraged to check our D2L class course space daily.

You are also encouraged to have D2L email forwarded to your primary University of Arizona email account. I will use D2L for course assignments, content distribution, and important announcements. The University of Arizona's D2L system is available at: http://D2L.arizona.edu.

INSuRE Hub – INSuRE's Collaboration Environment:

This course uses the INSuRE Hub, an online collaboration and data management platform, as a medium for exchanging materials with other institutions and problem sponsors. Some class assignments are also deliverables, and there may be other information you wish to make available to your technical director (TD); these should be uploaded to the INSuRE Hub. The INSuRE Hub also holds resources for preparing deliverables; you will be directed to these when they are needed.

Information on how to use the INSuRE Hub tools will be provided to all students at the beginning of the class.

Required Texts or Readings

There are no specific textbooks required for this class, however students are strongly encouraged to obtain any of the supplemental books and materials shown below as it relates to their selected research topic

Supplemental Books and Materials (Optional):

1. Anderson, Ross, Security Engineering: A Guide to Building Dependable Distributed Systems, Wiley (2008), second edition. ISBN 978-0-470-06852-6, QA76.9.A25A54 2008; http://www.cl.cam.ac.uk/~rja14/book.html
2. Bishop, Matt. Computer Security: Art and Science, Addison-Wesley (2003). ISBN 0201440997, QA76.9.A25B56 2003
3. Ferguson, Niels, Bruce Schneier, and Tadayoshi Kohno, Cryptography Engineering: Design Principles and Practical Applications, Wiley (Indianapolis, 2010). ISBN 978-0-470-47424-2, LC 2010920648
4. Stinson, Douglas R., Cryptography: Theory and Practice, Chapman & Hall/CRC (Boca Raton, 2006), third edition. ISBN 978-1-58488-508-5
5. John R. Vacca, ed, Computer and Information Security Handbook, Elsevier, 2013 (second edition).

Required or Special Materials

You will need a computer and the ability to remotely access a collaboration site that will be provided by the instructor for both the mid semester and final reviews with other universities and sponsors.

Information on how to do this will be provided by the head INSuRE coordinator from Stevens Institute of Technology.

Assignments and Examinations: Schedule/Due Dates

Assignments, progress reporting and other class deliverables are posted to the appropriate sections within the **class D2L** area. Due dates will be published in the course schedule which will be posted and maintained on D2L. Assigned dates and times for the progress reports with sponsors and other universities will be determined as a collaborative effort with the INSuRE program and dates may change, but advanced notice will be provided to all students and schedules posted to D2L as soon as they become available. For anything that is shared with your sponsors or other universities, you must follow the posted submission instructions, including file-naming conventions, the general rule for which is on the INSuRE Hub.

Some assignments are also project deliverables to your sponsors and should be uploaded to the INSuRE Hub; these will be clearly marked and the turn-in submittal will not be considered complete without the upload to the INSuRE Hub. Format and content specifications (in the form of a rubric and/or template) will be provided for via D2L.

Grades will be assigned as measures of performance on required activities.

The grading distribution for course assignments/homework, class participation, projects, and exams is as follows:

Narrated Intro, Literature review & Report:	5%
Project Bids:	5%
Project Proposal:	10%
Mid-Term Project Deliverables:	15%
Final Report:	20% **
Final Report Presentation:	15%
INSuRE Research Experience and Lessons Learned	10%
Confidential Team Member Evaluations:	15%*
Weekly Dashboard Updates	5%
Total	***100%***

Team member evaluations will be averaged across the individual team member inputs and used as a factored for the final score for each of the deliverables up to the point of that evaluation (there will be two evaluations throughout the semester).

***** The Final Report grade for Master's level students will adhere to a different rubric than for BS students. The MS Final Report Rubric will associate a portion of the Final Report grade to the Final Report presented to the INSuRE community and a portion to a separate paper written by each MS student on potential future extensions of the research that was conducted for the project. BS students will not be required to write this paper.***

The project will be evaluated on the basis of scientific merit, effective presentation, and appropriateness to the assigned project. Rubrics will be available for every assignment / deliverable.

Homework is due at the time that it is specified in the course schedule and/or D2L content pages (all homework assignments will be posted on D2L).

Late Work:

Late work is strongly discouraged, and only accepted when a schedule deviation is requested and approved by the instructor prior to the due date. Late work affects others. *Any late homework / assignments that have not received prior approval will not be accepted and will receive 0 points.*

Should you encounter an unanticipated or uncontrollable event that may prevent you from meeting a deadline, contact the instructor immediately to request an extension. Extensions are not automatic or guaranteed.

Peer review is an important aspect of the course, and peer review requires coordinating schedules, including among different universities. Some projects may depend on other projects. To complete the project by the end of the term, it is important to complete each milestone on time. Professional researchers often have deadlines to meet.

Quality of Work Expectations:

One of the program outcomes for this course is to communicate effectively with professional audiences of various types. This requires that one take personal pride in their work, and be held accountable for professional quality work. To this end, the following quality expectations are established for this course:

- Unless otherwise specified, homework and applied project assignments should be formatted as if they are being presented to non-technical business managers. Organization, conciseness, formatting, and style count -- make an impression!

- Unless otherwise specified, research papers must be formatted in one of the following two academic styles:
    - APA (recommended; used for most Purdue and College of Technology theses and directed projects).
    - IEEE (accepted)

- For all out-of-class work, organization, presentation style, grammar, and spelling will be weighted into the score. Spelling will be evaluated using the Microsoft *Word* Standard United States dictionary.

- Points will be lost for poorly organized or unprofessional work. This includes spelling and grammar errors, poor word choice, and poor sentence structure.

- Points will be lost for not following instructions.

- Students who have writing difficulties or deficiencies, and students for whom English is a foreign language should consider using the services provided for free through the University of Arizona Writing Laboratory

Feedback on Submitted Work

For purposes of this section, feedback refers to the scored assessment of learning on any given assignment, examination, project or paper. Scores are summed, categorized, and weighted to determine the final course grade. The following policies apply to scores:

- Feedback will be provided regularly by your instructor – as quickly as possible. Every instructor has multiple responsibilities beyond his/her courses. And each instructor has a unique way of providing feedback. If you believe you are not getting enough feedback, you are encouraged to contact your instructor and ask for more.

- The instructor will make every effort to grade assignments no later than one calendar weeks after the assignment due date.

- To comply with federal privacy law (specifically, FERPA), graded materials will never be passed around the classroom, or placed in any publicly accessible location, physical or online. Most scored work will be returned via D2L directly to the named student or student team.

- Any student wishing to appeal any given score must return his or her graded work with a written statement explaining the appeal. An appeal must be submitted no later than one calendar week after the original score is posted. Any work submitted for re-grading will be graded in its entirety.

Final Examination or Project

There are no mid-term or final exams in this course. The research project and mid-term and final reports are described in the section prior to this.

Grading Scale and Policies

The following scale will be used to award the final grades, for both 400 / 500 students:

Percentage	Letter Grade
90% – 100%	**A**
80% – 89%	**B**
70% – 79%	**C**
60% – 69%	**D**
<60%	**E**

A rubric will be made available on D2L for all deliverables for the course.

Graduate students will be required to write an additional paper related to their research topic. This

topic of this paper will be determined after the research topics and sponsoring agency are assigned. This paper will account for 30% of their Final Report grade.

Requests for incomplete (I) or withdrawal (W) must be made in accordance with University policies, which are available at http://catalog.arizona.edu/policy/grades-and-grading-system#incomplete and http://catalog.arizona.edu/policy/grades-and-grading-system#Withdrawal respectively.

Dispute of Grade Policy: Any disputes for a grade on one of the course deliverables must be made within 1 week of receiving the grade.

Scheduled Topics/Activities

The course schedule and due dates will be maintained online at D2L. Please refer to D2L often for any changes that may be made throughout the semester.

Bibliography

Selected Research Conferences (see the proceedings):

1. ACM Conference on Computer and Communications Security (typically held in November); http://www.sigsac.org/ccs/CCS2013/
2. IEEE Symposium on Security and Privacy (typically held in May); http://www.ieee-security.org/TC/SP2014/
3. USENIX Security (typically held in August); https://www.usenix.org/conference/usenixsecurity13
4. IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection; http://www.ifip1110.org/Conferences/
5. ACM Transactions on Information and System Security (TISSEC); http://dl.acm.org/pub.cfm?id=J789
CNIT/TECH 58100 Fall 2017
6. IEEE Transaction on Information, Forensics, and Security (TIFS); http://www.signalprocessingsociety.org/publications/periodicals/forensics/
7. IEEE Security & Privacy Magazine; http://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=8013
8. International Journal on Critical Infrastructure Protection (IJCIP); http://www.journals.elsevier.com/international-journal-of-criticalinfrastructure-protection/

Classroom Behavior Policy

To foster a positive learning environment, students and instructors have a shared responsibility. We want a safe, welcoming, and inclusive environment where all of us feel comfortable with each other and where we can challenge ourselves to succeed. To that end, our focus is on the tasks at hand and not on extraneous activities (e.g., texting, chatting, reading a newspaper, making phone calls, web surfing, etc.).

Students are asked to refrain from disruptive conversations with people sitting around them during lecture. Students observed engaging in disruptive activity will be asked to cease this behavior. Those who continue to disrupt the class will be asked to leave lecture or discussion and may be reported to

the Dean of Students.

Threatening Behavior Policy

The UA Threatening Behavior by Students Policy prohibits threats of physical harm to any member of the University community, including to oneself. See http://policy.arizona.edu/education-and-student-affairs/threatening-behavior-students.

Online Collaboration / Netiquette

In some of your coursework, you will primarily communicate with sponsors, other universities and peers virtually through a variety of tools such as discussion forums, email, and web conferencing. The following guidelines will enable everyone in the course to participate and collaborate in a productive, safe environment.

- Be professional, courteous, and respectful as you would in a physical classroom.
- Online communication lacks the nonverbal cues that provide much of the meaning and nuances in face- to-face conversations. Choose your words carefully, phrase your sentences clearly, and stay on topic.
- It is expected that students may disagree with the research presented or the opinions of their fellow classmates. To disagree is fine but to disparage others' views is unacceptable. All comments should be kept civil and thoughtful. Remember that this course abides by university policies regarding disruptive behavior: http://policy.arizona.edu/education-and-student-affairs/disruptive-behavior-instructional-setting
- Compose your messages and posts in a word processing tool, and check your spelling and grammar before submitting your post / email.

Accessibility and Accommodations

At the University of Arizona we strive to make learning experiences as accessible as possible. If you anticipate or experience physical or academic barriers based on disability or pregnancy, you are welcome to let me know so that we can discuss options. You are also encouraged to contact Disability Resources (520-621-3268) to explore reasonable accommodation.

If our class meets at a campus location: Please be aware that the accessible table and chairs in this room should remain available for students who find that standard classroom seating is not usable.

Code of Academic Integrity

Students are encouraged to share intellectual views and discuss freely the principles and applications of course materials. However, graded work/exercises must be the product of independent effort unless otherwise instructed. Students are expected to adhere to the UA Code of Academic Integrity as described in the UA General Catalog. See: http://deanofstudents.arizona.edu/academic-integrity/students/academic-integrity.

The University Libraries have some excellent tips for avoiding plagiarism, available at http://new.library.arizona.edu/research/citing/plagiarism. The instructor will be using online plagiarism detection tools that will indicate the total amount of material that is pulled from published resources. More than 10% on any given assignment will adversely impact your grade for the assignment and may result in a failing grade.

Selling class notes and/or other course materials to other students or to a third party for resale is not permitted without the instructor's express written consent. Violations to this and other course rules are subject to the Code of Academic Integrity and may result in course sanctions. Additionally, students who use D2L or UA e-mail to sell or buy these copyrighted materials are subject to Code of Conduct Violations for misuse of student e-mail addresses. This conduct may also constitute copyright infringement.

UA Nondiscrimination and Anti-harassment Policy

The University is committed to creating and maintaining an environment free of discrimination; see http://policy.arizona.edu/human-resources/nondiscrimination-and-anti-harassment-policy

Our classroom is a place where everyone is encouraged to express well-formed opinions and their reasons for those opinions. We also want to create a tolerant and open environment where such opinions can be expressed without resorting to bullying or discrimination of others.

Additional Resources for Students

UA Academic policies and procedures are available at http://catalog.arizona.edu/policies

Student Assistance and Advocacy information is available at http://deanofstudents.arizona.edu/student-assistance/students/student-assistance

Confidentiality of Student Records

http://www.registrar.arizona.edu/personal-information/family-educational-rights-and-privacy-act-1974-ferpa?topic=ferpa

Subject to Change Statement

Information contained in the course syllabus, other than the grade and absence policy, may be subject to change with advance notice, as deemed appropriate by the instructor.

- **Academic advising:** If you have questions about your academic progress this semester, or your chosen degree program, please note that advisors at the Advising Resource Center can guide you toward university resources to help you succeed.

- **Life challenges:** If you are experiencing unexpected barriers to your success in your courses, please note the Dean of Students Office is a central support resource for all students and may be helpful. The Dean of Students Office can be reached at 520-621-2057 or DOS-deanofstudents@email.arizona.edu.

- **Physical and mental-health challenges**: If you are facing physical or mental health challenges this semester, please note that Campus Health provides quality medical and mental health care. For medical appointments, call (520-621-9202. For After Hours care, call (520) 570-7898. For the Counseling & Psych Services (CAPS) 24/7 hotline, call (520) 621-3334.

- **Staying current:** You are required to complete all assignments and class participation activities on your own time to accomplish.

- **Remain flexible:** If pandemic conditions warrant, the University may require that we return to remote operations. If that is the case, we will notify you by D2L Announcement and email that we are moving to remote operations.

- **Class Recordings:**
    - For lecture recordings, students must access content in D2L only. Students may not modify content or re-use content for any purpose other than personal educational reasons. All recordings are subject to government and university regulations. Therefore, students accessing unauthorized recordings or using them in a manner inconsistent with University of Arizona values and educational policies are subject to suspension or civil action.