Applied Cybersecurity Research

Prerequisites: Students may come from computer science, computer engineering, information technology, or any related technical field (e.g., electrical engineering, information systems, math). Each student is expected to bring significant expertise, interest, and experience in at least one relevant technical area. Each student is expected to bring significant expertise, interest, and experience in at least one relevant technical area.

Length of Completion: 15 week semester plus 1 week of final exams.

Level of Instruction: Graduate or upper division undergraduate.

Learning Setting: In-class/face-to-face instruction.

***Course Description***

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 computer science 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 participate actively in class.

**Learning Outcomes:**

Upon completion of the course, students will be able to:

* + Identify a research problem
  + Search an electronic database for literature
  + Write a literature review
  + Formulate a research question
  + Design a research study
  + Collect data
  + Analyze data
  + Draw conclusion based on the analysis
  + Report the data effectively (e.g., developing charts, figures, and tables)
  + Write a research report
  + Orally present your research to other researchers
  + Collaborate with your mentor

**Materials:**

Required Books and Materials

No course materials are required for this section.

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).

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>
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-critical-infrastructure-protection/>

Information Technology-based Resources

Blackboard Learn - This course uses the Blackboard Learn learning management system (http://mycourses.purdue.edu). Class assignments to be handed in will be posted under Course Content > Assignments in Blackboard with assignment instructions and, when applicable, a due date.

Purdue University Research Repository (PURR) - This course uses PURR (http://purr.purdue.edu), 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 PURR. PURR also holds resources for preparing deliverables; you will be directed to these when they are needed.

**Technical Specifications:**

* Depends upon the research project.

**Grading:**

|  |  |
| --- | --- |
| Assessment Mechanism | Percentage |
| required reading reports | 5% |
| project bids | 5% |
| project proposal | 10% |
| literature review | 10% |
| knowledge and resource sharing plan | 5% |
| progress report | 15% |
| progress report presentation | 3.5% |
| final report | 25% |
| final report presentation and poster | 6.5% |
| assessment of team members | 5% |
| **Total:** | **100%** |

**Course Schedule**

|  |  |  |
| --- | --- | --- |
| Week | Lessons | Assignments due |
| 1 | * Introductions (10 min) * Orientation to INSuRE (vision, network, iterative/incremental, expectations) (20 min) * Interacting over conference call (5 min) * Bid process (10 min) * Article assignment * *How to Read a Paper* by Keshav * *The Protection of Information in Computer Systems* (section IA only) by Saltzer & Schroeder * *Why Information Security is Hard* by Anderson * TD Problem Overview Session I | Preliminary indication of interest in problems due in class  350-word EACH article reports due |
| 2 | * Discussion of articles * Locating/analyzing relevant literature (20 min) * Questions about preparing bids * Group activity: example & practice bid (build toward proposal) (20 min) * One article from your reference list that you will including in your bid and prepare a 5-minute presentation on the article to be delivered on September 16. * TD Problem Overview Session II | Article for 5 minute presentation identified |
| 3 | * 5 minute article presentations * Tutorial: presenting over teleconference * Group activity: how to propose work * TD Problem Overview Session III | 5 minute articles presentations due September 4  Bids due |
| 4 | * Notes on proposal drafts * How to read critically and write technically * In-class work session/office hours * 5 minute paper presentations by students * Group activity: managing tasks and data * In-class work session/office hours/TD calls if needed | 1st Draft proposal due |
| 5 | * Weekly dashboard: how to report incremental work & drive TD interaction * Assign weekly dashboard presentation * Notes on proposal lit review, expectations for expanded lit review * Data management (knowledge and resource sharing plan) session | Team proposal due |
| 6 | * Assign weekly dashboard presentation * Introduction of progress report assignment |  |
| 7 | * Deliver weekly dashboard update in class * Discuss progress reporting | Weekly dashboards start, due every Thursday |
| 8 | * Progress report draft presentations in class | Weekly dashboard due |
| 9 | * How to pass data, results, etc. (data management) * Practice presentation progress report * Progress report presentations | Progress reports due |
| 10 | * Progress report presentations | Weekly dashboard due |
| 11 | * Research Team Work | Weekly dashboard due |
| 12 | * Research Team Work | Weekly dashboard due  Knowledge and resource sharing plan due |
| 13 | * Final report expectations | Weekly dashboard due |
| 14 | * Final presentations practice * Final presentations |  |
| 16 | * Final presentations practice * Final presentations | Final report due |