

Syllabus of CS 6803

Syllabus

Revised 8/10

Course Description and objectives

The primary goal of this course is to present a system and management view of information security: what it is, what drives the requirements for information security, how to integrate it into the systems design process, and life cycle security management of information systems. A second goal is to cover basic federal government information security policies and methodologies. Topics covered include information security risk management, security policies, security in the systems engineering process, laws related to information security, and management of deployed systems.

This course will not be about the technologies of information security, but how those technologies are integrated into a system and managed. A broad (but not detailed) knowledge of information security technologies is assumed: cryptography (public key and symmetric key), firewalls, IDS, viruses/virus detection, access control, etc. The prerequisites from the Poly curriculum are Computer Security (CS392, CS681, CS6813, or equivalent) and Network Security (CS393, CS682, CS6823, or equivalent). The full depth of these courses is not needed, and a single basic course in computer and network security from another university is sufficient. Note that students who do not have the prerequisites in the past have often struggled to earn a grade of C.

This course, combined with the courses in computer security and network security technology, provide the qualifications for the US government "NSTISSI-4011 - INFOSEC Professionals, National Training Standard" certification, and the "CNSSI-4013 National Information Assurance Training Standard For System Administrators (SA)." Students who have taken all required courses will be certified by Polytechnic University. In addition, the material for the "CNSSI 4016 National Information Assurance Training Standard For Risk Analysts" is covered in this and

related technology courses, and Polytechnic is in the process for getting approval to grant this certification.

Policies and Grading

Course policies, grading, contact information, etc. are in the “Policies and Grading” section in the General Course Information area on the course web site. All students are responsible to understand the contents of that document and follow the policies laid out there. That document describes a term project to be performed by student in teams. This syllabus includes class sessions in which the student teams will present reports on their projects to the class for discussion by the class and suggestions from the instructor.

Week by week list of course topics

- Introduction: Course motivation and overview. Information security in the system life cycle. Term project approach goals, teaming, and expectations. Introduce a case study to be built on through most lectures, and a second case study for students to build on in homework assignments.
- Risk I: Risk Analysis. Identifying and categorizing risks: assets at risk, threats. And vulnerabilities.
- Risk II: Risk Management. Approaches to managing risks: reduction, mitigation transfer, and acceptance. Formal risk analysis and management processes such as at NIST, and OCTAVE.
- System Security Engineering (SSE): Integrating security into a systems engineering process.
- SSE continued. Balancing conflicting requirements, “trade studies”; More details on the Team Projects
- Security Policy. Purpose of security policies. Approaches to developing policies. Examples of policies.
- Legal issues: How laws impact information security requirements. Laws examined include Sarbanes-Oxley, HIPPA, Gramm-Leach-Bliley, and CA SB 1386 (California Breach Law).
- Term Project Preliminary Design Review: each team will present their preliminary (high level) project design for class discussion and instructor feedback and guidance.

- Evaluation and assurance: General principals, DoD Orange book methodology, Common criteria. The architecture of DoD classified systems. DoD Certification and Accreditation of information systems.
- Security management of deployed systems: The ongoing management of the security of deployed systems as part of the system security life cycle in the context of ISO 17799: acquisition, change management, policy enforcement, security monitoring, patch management, decommission, etc. The role of the Information System Security Officer
- Contingency planning: Incident response planning for the immediate response to a security incident, including containment, preserving evidence, restoration, legal actions, and incident review/lessons learned. B. Business Continuity Planning: making sure the organization can continue functioning after a security incident.
- TEMPEST and related topics: Emissions Security (EMSEC) and protection (TEMPEST), Transmission Security (TRANSEC). and Operational Security (OPSEC).
- Remaining DoD topics: Physical security Federal government key management policies and procedures. B. Information security audit.
- Term project Critical Design Review: each team will present their final (detailed) project design for class discussion and instructor feedback and guidance. This review is essentially an outline of the project final report.
- Complete Term Project Report Due finals week

Textbooks:

Textbooks: There is no textbook that covers even most of the material in this course in a complete manor. Two books are useful for both the material in this course, and as valuable references for security professionals. Reading assignments will be made in each of these books, and other references will be found on the web.

Management of Information Security by Michael E. Whitman and Herbert

J. Mattord, first or second edition, ISBN 978-1423901303

- A good, general reference for risk analysis, policy, standard security management processes
- In my view, does not properly reflect the system view

- Either the first or second (new) edition of this book can be used, and page reference for both will be given in reading assignments. Feel free to buy the first edition as a used book.

Security Engineering, Ross Anderson, ISBN 978-0470068526

- Excellent book on many aspects of security
- More oriented toward technology than management
- Great examples of the results of good security engineering in the real world, including system flaws
- In my view, reflects a system view of the security, but does not reflect a systems engineering process view of how to get there
- Either the first or second (new) edition of this book can be used, and page reference for both will be given in reading assignments.
- The old (first) edition available as a free download at

<http://www.cl.cam.ac.uk/~rja14/book.html>

Other References:

Additional web sites for each lecture are in the on-line “webliography” for each topic course. The webliography is a list of links with brief descriptions of what the link is about if it is not obvious from the link name. Two topics (risks, lectures 2 and 3; and system security engineering, lectures 4 and 5) span two lectures, and the webliography for both lectures is with the first for that topic. **Be sure to look over the webliography entries for each lecture.** They provide material that is not in the textbooks (particularly for government related topics and for the lecture on security related laws, which have changed significantly since the texts were published. Some of the entries are listed as specific reading assignments, others are references to be used as needed, both in this course and in the future. The entire text of all the webliography entries for each week is *not* required reading. But you should be aware of the references,

Related background works that are useful for the application of this course in professional environment. These are not specifically referenced in the course, but are worth being aware familiar with.

Schenier, Bruce, "Secrets and Lies: Digital Security in a Networked World", John Wiley and Sons, 2000. A non-technical book about why technology alone does not provide security written by a noted expert in security technology.

Schenier, Bruce, "Cryptogram" Newsletter, free monthly newsletter with articles and essays on security and security technology, with insightful commentary on the implications of various news stories. Sign up at <http://www.schneier.com/>

A description of the newsletter from that web site:

Crypto-Gram is a **free** monthly e-mail newsletter from security expert Bruce Schneier, with over 100,000 readers. In its seven years of regular publication, Crypto-Gram has become one of the most widely read forums for free-wheeling discussions, pointed critiques, and serious debate about security. As head curmudgeon at the table, Schneier explains, debunks, and draws lessons from security stories that make the news.

comp.risks newsgroup available from your favorite netnews source. The "ACM FORUM ON RISKS TO THE PUBLIC IN COMPUTERS AND RELATED SYSTEMS" Discussions of all kinds of risks from the use of computers, including security breaches, system failures, poor design, user misuse, etc. and the implications to users, innocent bystanders, and society in general. Some government agencies have been known to ask job interviewees if they read this regularly and are happy when they do.