

Course proposal: CSC 214, “Computer and network security”

Department of Computer Science · November 22, 2013

The Department of Computer Science proposes to introduce a new course, “Computer and network security,” dealing with the security of computing systems and the networks over which they communicate, including tools and techniques for undermining or for reinforcing the reliability and usability of computer systems, the theoretical concepts that underlie those techniques, and the ways in which governments, corporations, interest groups, and individuals currently use them.

These topics are of increasing practical importance both to computing professionals and to citizens and activists. Our recent alumni and current students have frequently suggested the creation of such a course, and we have sought and now found an opportunity to adjust our curriculum to include it.

Here is a proposed outline and schedule of topics. The selection reflects the learning outcomes suggested under the headings “Human factors and security,” “Foundational concepts in security,” “Threats and attacks,” “Network security,” “Cryptography,” “Web security,” “Platform security,” “Security policy and governance,” “Security and protection,” “Privacy and civil liberties,” and “Security policies, laws, and computer crimes” in *Computing Curricula 2013* (<http://ai.stanford.edu/users/sahami/CS2013/>). Roman numerals refer to major divisions of the course. Arabic numerals enumerate the weekly class sessions.

I. Orientation

1. The symmetric goals of information security; the ethics of control and power; keeping and exposing secrets

II. Tools

2. Cryptography; random-number generation; symmetric-key systems
3. Hash functions; asymmetric (public-key) systems
4. Distributed systems; the economics of information; “big data”
5. Standards, protocols, and institutions for computer and network security; the roles of law, code, and social norms
6. Social engineering; exploiting human psychology and physiology
7. Formal risk analysis and threat assessment

III. Applications

8. Case studies: Confirming perfect data transfer; digital signatures; document encryption
9. Authentication systems; biometrics; multi-factor authentication systems
10. Case studies: Wikileaks; Anonymous; Secure Drop
11. E-commerce; Internet scams, phishing, spam, malware distribution; banking and bookkeeping; Bitcoin
12. Case studies: Digital restrictions management; copyright enforcement; watermarking
13. Intelligence and counterintelligence; surveillance; the history of the National Security Agency
14. Cyberterrorism and cyberwarfare

As a textbook for the course, we propose *Security engineering: a guide to building dependable distributed systems*, by Ross J. Anderson (Indianapolis: Wiley Publishing; second edition, 2007; ISBN 978-0-470-06852-6), supplemented by regular reading of several Web logs that address security events and issues of general interest in real time:

- Matthew Green, *A few thoughts on cryptography engineering*
<http://blog.cryptographyengineering.com/>
- Bruce Schneier, *Schneier on security*
<http://www.schneier.com/blog/>
- Ross J. Anderson *et al.*, *Light blue touchpaper*
<http://www.lightbluetouchpaper.org/>
- Brian Krebs, *Krebs on security*
<http://krebsonsecurity.com/>

We propose to offer the course for two credits. The class will meet once a week throughout the semester, each session lasting an hour and fifty minutes. Most class sessions will be primarily discussion, with frequent short oral presentations by students. We’ll assess students on the basis of their oral presentations and written papers.

This course will be an elective, open to both majors and non-majors, and is not intended to serve as a prerequisite for any other course.

This proposal forms part of a large package of curriculum changes that are neutral with respect to staffing, collectively requiring exactly as many staff lines for new and revised courses as for the cancelled and obsoleted courses they replace.