CIS 755: Advanced Computer and Information Security

Summary:
The goal of this class is to give an overview, state of the art security tools and best practices, arm you with the knowledge of where and how to find tools we don't cover in class, and prepare you to use these tools and reason about the effectiveness and correctness of the way you integrate security into your future projects. We will cover a small amount of theory, but focus on more advanced practical topics in areas such as distributed system security, trustworthy computing, applied cryptography, privacy and anonymity, and advanced access control. After this course, you will be able to not only apply the solutions you learned to different problems, but find other existing theoretical and practical solutions, and also combine and extend existing solutions to create new ones. We will emphasize thorough understanding of key concepts, so we will do a lot of reading and critical reasoning, individually and as a group. The class requires only a minimum of background knowledge: CIS 553 or CIS 551 or instructor permission.

Knowledge and Skills Acquired:

- **Mastery of:**
  - Key concepts in computer security and applied cryptography
  - Past security successes and mistakes; common pitfalls
  - Security evaluation of new and existing systems and protocols
  - Thinking like an adversary

- **Familiarity with:**
  - Finding, reading, summarizing, and understanding modern computer security research literature
  - Number theory and cryptography
  - Proofs of security properties
  - Composability of existing security tools
  - Design of new security tools

Class meeting time: Thursdays 5:30PM – 7:00PM via teleconference
My office hours (Nichols 316A): Mondays 3PM – 4:30PM and Thursdays 2:30 PM – 4:00PM, or by appointment
Email: eyv (at) ksu (dot) edu
Phone: 785.532.7944
(A clarification on the nature of "office hours" [PDF])

Prerequisites: CIS 551/751 or CIS 553/753 or instructor permission.

**Evaluation:** 20% class participation and short quizzes, 25% exams I, 25% exam II, 30% final exam. Distance students must locate an exam proctor.

**Class participation:** come to class; be prepared to discuss and the material assigned for that day and ask questions. This may also include short written responses to assigned reading or questions about the day's discussion.

**Quizzes:** will be announced in advance, and will be short — at most 15 minutes. There will be a mix of true/false, multiple-choice, and fill-in-the-blank questions.

**Exams:** will be about one hour long, and consist of true/false, multiple-choice, fill-in-
the-blank, and short answer questions. These will be designed to test the limits of your knowledge, and no one is expected to get 100%.

Student Performance Expectations
The bulk of class time will consist of discussion of assigned reading material to ensure thorough understanding. I will supplement reading material with slides or explanations and clarification. After each class you should be able to clearly explain the material in the reading assignment, and potentially give examples of real-world applications of theoretical concepts. Don't worry if something is unclear; instead bring it up in class so we can all discuss it — it will help later, in this class and in the "real world". Please read all required material before coming to class, and be prepared to discuss and/or ask questions. It's not unusual to read something more than once to understand it completely, especially an academic paper. Sometimes true understanding requires reading some related material as well; sometimes group discussion is needed. This class will provide an environment to facilitate such discussion. When I can, I will point out when additional reading would help understand the assigned material, or when something is particularly challenging. Even when I do not, I still encourage you to do extra reading on your own. Be sure to let me know what else you read, and what you learned (or did not learn).

Required texts:


Recommended texts:

- Security Engineering by Ross Anderson. The second edition is out, but the first edition is now available for free online here: http://www.cl.cam.ac.uk/~rja14/book.html

Academic Honesty
Kansas State University has an Honor System and Integrity based on personal integrity, which is presumed to be sufficient assurance that, in academic matters, one's work is performed honestly and without unauthorized assistance. Undergraduate and graduate students, by registration, acknowledge the jurisdiction of the Honor and Integrity System. The policies and procedures of the Honor and Integrity System apply to all full and part-time students enrolled in undergraduate and graduate courses on-campus, off-campus, and via distance learning. The honor system website can be reached via the following URL: http://www.ksu.edu/honor. A component vital to the Honor and Integrity System is the inclusion of the Honor Pledge which applies to all assignments, examinations, or other course work undertaken by students. The Honor Pledge is implied, whether or not it is stated: "On my honor, as a student, I have neither given nor received unauthorized aid on this academic work." A grade of XF can result from a breach of academic honesty. The F indicates failure in the course; the X indicates the reason is an Honor Pledge violation.
The default in this class is that ALL work will be accomplished individually, UNLESS
my permission is given in advance of an assignment/quiz/exam/take-home exam/final. If you are in doubt, please ask.

Academic Accommodations for Students with Disabilities
Any student with a disability who needs a classroom accommodation, access to technology or other academic assistance in this course should contact Disability Support Services (dss@k-state.edu) and/or the instructor. DSS serves students with a wide range of disabilities including, but not limited to, physical disabilities, sensory impairments, learning disabilities, attention deficit disorder, depression, and anxiety. You can find more information on the Disability Support Services web page.

Expectations for Classroom Conduct
All student activities in the University, including this course, are governed by the Student Judicial Conduct Code as outlined in the Student Governing Association By Laws, Article VI, Section 3, number 2. Students who engage in behavior that disrupts the learning environment may be asked to leave the class. The bylaws for recent years can be found here.