18-630 / 19-631 / 95-830: Introduction to Security and Policy

Instructors: Adrian Perrig (office hour Friday 4-5pm in CIC 2107)  
TAs: Hsu-Chun Hsiao and Tiffany Hyun-Jin Kim (office hours Wednesday and Thursday 4-5pm in CIC 2214).
We will meet Monday and Wednesday in Wean Hall 5403 10:30am-11:50am.  
Email to instructors should be sent only to 18630-f10-instructors (at) lists.andrew.cmu.edu

Course Description:
The growing importance of networks and distributed systems, and their use to support safety-critical applications, has made computer and communications security a central issue for systems today. This course will introduce students to the technical and policy foundations of computer and communications security. These foundations will be illustrated using deployed systems as case studies. The course will assume a basic working knowledge of computers and networks, but will not assume any prior exposure to topics in computer or communications security. Graduate standing or permission of the instructor is required.

Syllabus

Required Textbook:  

Suggested Textbooks (optional):  
Introduction to Cryptography with Coding Theory by Trappe and Washington, 2nd revision.  
Cryptography - a very short introduction by Piper and Murphy.  
Security Engineering by Ross Anderson (online version).

Great software tool to learn more about cryptographic algorithms: CrypTool.

Late Policy:  
The deadline for any assignment can be extended with a 10% penalty per day. No deadline can be extended by more than two days. so assignments will NOT be accepted 48 hours after the due date.

Collaboration Policy:  
Students are encouraged to talk to each other, to the TAs, to the instructor, or to anyone else about any of the assignments. Any assistance, though, must be limited to discussion of the problem and sketching general approaches to a solution. Each student must write out his or her own solutions to the homeworks. Consulting another student's or group's solution is prohibited, and submitted solutions may not be copied from any source. These and any other form of collaboration on assignments constitute cheating. If you have any question about whether some activity would constitute cheating, please feel free to ask.

Grading:  
Your final grade for the course will be based on the following weights for the individual assignments:

- 25% Homeworks
- 25% Midterm
- 40% Final Exam
- 10% Participation
The Midterm and Final Exams will be closed-book.