CSE 565: Computer Security, Fall 2014

Lecture Hours: Tu Th 8:00 am - 9:20 am (114 Hochstetter)
Instructor and E-mail address: Dr. Shambhu J. Upadhyaya; shambhu@buffalo.edu
Office Hours: Tuesdays 9:30 am – 11:00 am
Teaching Assistants:

1. Hayreddin Ceker, Tue. 5:00 pm - 6:00 pm, Wed. 5:00 pm - 6:00 pm, Near 302 Davis Hall (TA space)
2. Chaowen Guan, Mon. 3:30 pm - 4:30 pm, Wed. 3:30 pm - 4:30 pm, Near 302 Davis Hall (TA space)

Text Book:

- W. Stallings, Cryptography & Network Security, Principles & Practices, Pearson, 6th Edition, 2014.

Recommended Books:

- C.P. Pfleeger and S.L. Pfleeger, Security in Computing, 4th Edition, Prentice Hall, 2007.
- W. Trappe and L. Washington, Introduction to Cryptography with Coding Theory (2nd Edition), Prentice Hall, 2006.
- C. Kaufman, R. Perlman and M. Speciner, Network Security, Private Communication in a Public World, Prentice Hall, 1995.

Course Description: This course is intended to give you an in-depth understanding of computer system security. Security has become one of the major concerns in DoD, commercial organizations and home users. Security encompasses malware injection, hacker challenges, malicious break-ins and insider threats. Course topics include: Basic Encryption and Decryption – Symmetric Ciphers, Public Key Encryption such as Rivest-Shamir-Adelman (RSA) algorithm, El Gamal and Digital Signature Algorithms, Hash Algorithms; Network Security – Authentication, Email Security, IP Security, Web Security; System Security – Intrusions, Intrusion Detection, Malicious Software, Covert Channels, Firewalls.

Course Organization and Projects: Classroom lectures will be given using chalkboard style, assisted by prepared slides. Students are expected to have a copy of the slides prior to the lectures.

Several projects will be set up. These may be in the area of encryption/decryption, vulnerability analysis, intrusion detection and may involve programming. There may be both simulation based and real experiments in a security lab. More details will be provided at a later stage.

Student Background: Computer networks, probability theory, basic mathematics, algorithms.

Grading Policy: Missed classes will be a burden for the student, the TAs and the instructor. So, class attendance is strongly encouraged. There will be homeworks (graded for completeness only), projects, quizzes (unannounced) and three midterms. The tentative weights are as follows: Quiz - 20%, Midterm 1 - 15% (to be given on October 2nd), Midterm 2 - 20% (to be given on November 6th), Midterm 3 - 15% (to be given on December 2nd), Homeworks - 5%, Projects - 25%.

Learning Outcomes: One of the intents of this course is to enable you to understand the fundamental principles of the security field.

Academic Integrity: The value of our courses, grades, degrees and research findings are dependent upon adherence to standards of ethical conduct. Plagiarism and inappropriate collaboration will not be tolerated. In this course we will adhere to the departmental standard for academic integrity. For more details, refer to the class webpage.