Spring 2025
CS 645 – Security and Privacy in Computer Systems

Section: 002
Instructor: Cong Shi
Email: cong.shi@njit.edu
Course website: https://canvas.njit.edu/
Instructor website: https://njit.webex.com/meet/cs638

Office hours: Friday 2-3 pm. Also, by appointment via email.

Prerequisites:
Students are expected to enter this course with a basic knowledge of operating systems, networking, algorithms, and data structures.
Also, students should be able to program in Java and C for the programming component of the projects.

Textbook:
"Introduction to Computer Security", by M. Goodrich and R. Tamassia,
Addison Wesley, 2010, ISBN: 978-0321512949.

In addition, course material will include research articles from electronic databases such as: ACM Digital Library (http://dl.acm.org), IEEE Xplore (http://ieeexplore.ieee.org), and Science Direct (http://www.sciencedirect.com)

Description:
The course covers fundamental principles of building secure systems and techniques to protect data privacy. Topics include access control mechanisms, operating systems security, malicious code threats and software security, trusted computing, content protection, and database security. The course will also study existing technical approaches to protecting privacy, including Web anonymizers and anti-censorship tools, as well as policy and legal aspects of privacy.

A tentative list of topics includes:

- Introduction (security goals, overview of course topics, overview of attacks)
- Crypto crash course
- Access control mechanisms
- Operating systems security
- Software security, Secure Programming
- Web security
- Malicious code, Malware, Rootkits
- Trusted computing
- Introduction to security of networked systems
- Privacy and anonymity on the Web
- Content protection, Software obfuscation, Digital rights management
- Database security

- Security of electronic voting
- Computer crime - laws and ethics, Security & privacy policy (Sarbanes Oxley, HIPAA)
- Miscellaneous topics: side-channel attacks, gaming security, information assurance (common criteria), risk analysis

Grading:

3 Projects:	45% (each project has 15%)
Midterm exam:	25%
Final exam:	30%

Extra credit will be given for active participation in discussions during the class (up to 5%). The quizzes and exams are closed book unless specified otherwise.

Learning Outcomes:

After completing the course, students will be able to:

- Describe the main types of attacks that may occur in computer systems and networks.
- Describe the various models to evaluate the security of computer systems and interpret security guarantees.
- Describe the various security goals for communication over an insecure network.
- Identify the appropriate types of cryptographic primitives that should be used to achieve various goals, and describe the advantages and limitations of using symmetric-key versus public-key cryptography.
- Get familiar with various types of authentication mechanisms in computer systems and networks.
- Describe the role of physical security in securing computer systems and networks.
- Become familiar with mechanisms used to secure major operating systems and file systems.
- Describe the main types of attacks against computer programs and become familiar with the principles of secure programming.
- Describe the main mechanisms to secure the communication between computer systems at various network layers.
- Describe the main types of attacks against web-based systems and become familiar with the principles of building secure and private web-based systems.
- Design and implement new security frameworks in order to achieve security guarantees for a diverse set of real-world scenarios.
- Apply theoretical concepts in practice by using a programming or scripting language to implement attacks and defenses against web-based systems.
- Critically analyze a scientific article.

Honor Code:

Academic Integrity is the cornerstone of higher education and is central to the ideals of this course and the university. Cheating is strictly prohibited and devalues the degree that you are working on. As a member of the NJIT community, it is your responsibility to

protect your educational investment by knowing and following the academic code of integrity policy that is found at:
http://www5.njit.edu/policies/sites/policies/files/academic-integrity-code.pdf.

Please note that it is my professional obligation and responsibility to report any academic misconduct to the Dean of Students Office. ***Any student found in violation of the code by cheating, plagiarizing or using any online software inappropriately will result in disciplinary action. This may include a failing grade of F, and/or suspension or dismissal from the university.*** *If you have any questions about the code of Academic Integrity, please contact the Dean of Students Office at dos@njit.edu*

Note in particular that cheating on exams, copying homework assignments and exam papers, and plagiarizing (in full or in part) someone else's work is forbidden.

Collaboration of any kind is PROHIBITED in the exams. As part of projects, students must turn in code or work that has fully been written by him/her and no-one else. Any submitted text or code (even few lines) obtained through the Internet or otherwise, or is product of someone else's work, risks severe punishment, as outlined by the University; all parties of such interaction receive automatically 0 and grade is lowered by one or two levels. Likewise for Exams, if applicable. The work you submit must be the result of your own mental effort and you must safeguard it from other parties; if you can't protect your home computer, use a Lab (AFS) machine.

Modifications to Syllabus:
The syllabus may be modified at the discretion of the instructor or in the event of extenuating circumstances. Students will be notified in class of any changes to the syllabus.