System and Software Security
CS 5590 / ECE 5590
CS is the Home Department

I. Catalog Description

Secure software design, memory and file system security, operating system security for various platforms. Program classification, anomaly detection, malware detection and analysis. Technical challenges and problems in securing operating systems and software. Classic and modern algorithms, models, principles, and tools for system and application software security. Actual security examples. Pre: 5560/ECE 5560 (3H, 3C)

Course Number: 5590/ECE 5590

ADP Title: System and Software Security

II. Learning Objectives

Having successfully completed this course, students will be able to:

- Identify classes of security problems in computer systems and programs.
- Model threats, risks, attacks, and security goals.
- Identify causes of system and application vulnerabilities.
- Describe classic and modern security approaches and techniques.
- Compare pros and cons of various security solutions in terms of their security guarantees.
- Design and implement solutions for achieving secure operating systems, mobile applications, and software.
- Evaluate the security, robustness, usability, and efficiency of security tools.

III. Justification

Security problems represent an enormous challenge to the usability and safety of modern computing systems. Cyber security is critical to a broad array of societal concerns, including personal privacy, financial accountability and national security. Many career paths open to computer science and engineering graduates require them to have a good understanding of challenges arising in the context of system and software security and the methods used to improve the security of computing

systems (including personal computers, high-end computing clusters, mobile devices, as well as the applications running on them). This course is part of a set of three new courses and one revised course in cybersecurity from the departments of Computer Science (CS) and Electrical and Computer Engineering (ECE). The revised course is CS/ECE 5560 (new title, "Fundamentals of Information Security"), which provides necessary background in cybersecurity principles and techniques. The proposed CS/ECE 5590 focuses on more advanced security issues in the context of operating systems and application software.

The course will be taught at the 5000-level because it requires advanced knowledge of computer science and engineering topics (e.g., software development and operating systems) as provided by an undergraduate degree in computer science or computer engineering, and because it requires an appropriate background in cybersecurity as provided by CS/ECE 5560.

IV. Prerequisites and Corequisites

5560/ECE 5560

V. Texts and Special Teaching Aids

Required Texts: None. There is no single textbook that captures the topics covered in this rapidly changing field. Lecture notes combined with freely available readings and documentation provide the material needed by all students.

Recommended readings: Operating System Security. Trent Jaeger. Synthesis Lectures on Information Security, Privacy, and Trust. 2008, 218 pages. Morgan & Claypool.

Supplemental materials, including research on relevant topics, will be provided in class. Representative examples include:

Fred Cohen, "Computer Viruses Theory and Experiments," *Journal of Virology*, 1984.

R. Sekar, M. Bendre, P. Bollineni, and D. Dhurjati. "A fast automaton-based method for detecting anomalous program behaviors," In *Proceedings of the 2001 IEEE Symposium on Security and Privacy,* 2001, pp 144-155.

Eugene H. Spafford, "The Internet Worm Program: An Analysis," Purdue University Technical Report CSD-TR-823, 1988.

C. Warrender, S. Forrest, and B. Pearlmutter, "Detecting intrusions using system calls: Alternative data models," In *Proceedings of the 1999 IEEE Symposium on Security and Privacy*, Los Alamitos, CA, IEEE Computer Society, 1999, pp 133-145.

Lee Wenke, Salvatore J. Stolfo, Kui W. Mok, "A Data Mining Framework for Building Intrusion Detection Models," *IEEE Symposium on Security and Privacy*, 1999, pp 120-132.

VI. Syllabus

Course Topics	Percent of Course
1. Overview	15%
2. Operating system design and security	20%
3. Software vulnerabilities	15%
4. Mobile application security	10%
5. Anomaly detection	15%
6. Browser security	15%
7. Distributed system security	10%
TOTAL	100%