CS 492: Computer Security

1. Course number and name: CS 492: Computer Security

2. Credits and contact hours: 3.000 Credit Hours, 3.000 Lecture hours

3. Instructor or course coordinator: Ewa Syta

4. Text book, title, author, and year


   a. other supplemental materials
      - The course uses Blackboard/Vista for homework assignments, handouts, grade book, and lecture notes.

5. Specific course information

   a. brief description of the content of the course (Catalog Description):
      This is an introduction to computer security for computer scientists. Topics include classical and modern techniques of conventional encryption; algorithms; public-key encryption, and hash functions; network security, with regard to e-mail, IP, and the Web; and system security intruders, viruses, worms, and firewalls. The fundamentals of network security issues are also explored.

   b. prerequisites or co-requisites: CS 253 and CS 254
   c. indicate whether a required, elective, or selected elective course in the program: Elective

6. Specific goals for the course

   a. specific outcomes of instruction, ex. The student will be able to explain the significance of current research about a particular topic.

   **Course objective 1: Cryptology**
   **Objective 1.1:** Understand the basics of classic cryptography and cryptanalysis, and provide examples of classic ciphers and attacks;
   **Objective 1.2:** Be able to explain the general design principles of symmetric key and public key cryptosystems, and provide specific examples of such systems;
   **Objective 1.3:** Apply basic number theory concepts and abstract algebra to cryptosystems.

   **Course objective 2: Access Control**
   **Objective 2.1:** Give a clear explanation of the authentication process, identify different authentication methods and factors, and provide examples of simple authentication protocols;
Objective 2.2: Describe the differences between authentication and authorization, and comprehend basic, multilevel and multilateral security models;  
Objective 2.3: Understand the importance of security planning and risk analysis.

Course objective 3: Network Security
Objective 3.1: Identify and categorize common threats and attacks in networks;  
Objective 3.2: Analyze in depth network security controls;  
Objective 3.3: Describe the most common internet security and e-mail weaknesses, and explain how they can facilitate different types of attacks;  
Objective 3.4: Explain the general architecture and functionality of the Kerberos authentication protocol, and the Secure Socket Layer (SSL) and IPSec communication protocols.

Course objective 4: Software Security
Objective 4.1: Describe the most common software based attacks, and identify the differences between non-malicious program errors, viruses and other malicious code;  
Objective 4.2: Understand and apply secure software development principles;  
Objective 4.3: Define the concepts and applications of digital rights management and software reverse engineering;  
Objective 4.4: Understand the basics of operating systems security and define their security functions, and understand the basic design principles of trusted operating systems.

b. explicitly indicate which of the student outcomes listed in Criterion 3 or any other outcomes are addressed by the course.

Outcome (a): An ability to apply knowledge of computing and mathematics appropriate to the discipline.  
Outcome (b): An ability to analyze a problem, and identify and define the computing requirements appropriate to its solution.  
Outcome (f): An ability to communicate effectively.  
Outcome (g): An ability to analyze the impact of computing on individuals, organizations, and society, including ethical, legal, security, and global policy issues.  
Outcome (h): Recognition of the need for and an ability to engage in continuing professional development.

7. Brief list of topics covered

1) Classic & Modern Cryptography and Cryptanalysis (Symmetric and Public Key Cryptography and Cryptanalysis)  
2) Hash Functions, Secret Sharing and Information Hiding  
3) Authentication & Authorization  
4) Real-World Security Protocols  
5) Software Security  
6) Operating Systems and Security  
7) Security in Networks  
8) Computer Forensics

8. Expected Performance Criteria
Students will demonstrate their understanding of covered material through homework assignments and two exams (midterm and final) which will include practical and theoretical problems. Students’ ability to critically examine new concepts and report on a problem will be evaluated based on their 20-30 minute oral presentation to a group of around 20 people. Final research project will check their ability to identify proper research topic, write a project proposal, conduct a research project and write a research paper. All assignments will ensure that students are able to understand the broad field of computer security and to use this understanding to pursue specific topics as needed.