CS 4351 - Computer Security

Spring 2022 Course Syllabus

Course Description: General concepts and applied methods of computer security, especially as they relate to confidentiality, integrity, and availability of information assets. Topics include system security analysis, access control and various security models, identification and authentication, protection against external and internal threats, communication protocols and internet security.

Course Goals: With the multiplication of tasks that are performed on computers and the advent of globalisation of computing in general, the topic of computer security becomes more and more important. We see in this course what is computer security, especially as it relates to the protection of information stored on the computers and exchanged between computers. Topics include: system security analysis, access control and various security models, identification and authentication, security in UNIX and Windows, communication security, cryptography, internet security, e-commerce security protocols.

Textbook: "Computer Security", by Dieter Gollmann, 3rd edition, Wiley, 2011. (ISBN 9780470741153)

Optional reference books:
``Computer Security: A Hands-on Approach", by Wenliang Du, 2019. (ISBN 154836794X) or
``Computer Security & Internet Security: A Hands-on Approach", by Wenliang Du, 2017. (ISBN 978-1-73300390-3-2)

Exams and Grades: The following percentages will be used in formulating the final grade:

- Two tests 25%
- Quizzes and class exercises 5%
- Final exam 35%
- Assignments 35%

Standards of Conduct: Students are expected to conduct themselves in a professional and courteous manner, as prescribed by the Standards of Conduct. Students may discuss work assignments and programming exercises in a general way with other students, but the solutions must be done independently. Similarly, groups may discuss group project assignments with other groups, but the solutions must be done by the group itself. Graded work should be unmistakably your own. You may not transcribe or copy a solution taken from another person, book, or other source, e.g., a web page. Professors are required to -- and will -- report academic dishonesty and any other violation of the Standards of Conduct to the Dean of Students.

Academic Dishonesty: Cheating is defined as submitting work under your name that was not done entirely by you for individual assignments or by your team for team assignments. (This includes taking programs from the web or cutting text from web pages and pasting them into documents, even if the source is cited). Cheating will not be tolerated – those caught cheating will be reported to the Dean of Students. You should be aware of the Standards of Conduct posted at http://www.utep.edu/vpfa/student_affairs/student/studindex/htm.

Disabilities: If you have a disability and need classroom accommodations, please contact The Center for Accommodations and Support Services (CASS) at 747-5148, or by email to cass@utep.edu, or visit their office located in UTEP Union East, Room 106. For additional information, please visit the CASS website at www.sa.utep.edu/cass.

Faculty Information: Professor: Luc Longpré Office Hours: TR 3-4PM. See https://www.utep.edu/cs/people

/longpre.html, expand "student appointments" for instructions on how to make appointments at other times.

Course outcomes:

Knowledge and Comprehension

1. Describe the functioning of various types of malicious code, such as viruses, worms, trapdoors.
2. Enumerate programming techniques that enhance security.
3. Explain the various controls available for protection against internet attacks, including authentication, integrity check, firewalls, intruder detection systems.
4. Describe the different ways of providing authentication of a user or program.
5. Describe the mechanisms used to provide security in programs, operating systems, databases and networks.
6. Describe the background, history and properties of widely-used encryption algorithms.
7. Describe legal, privacy and ethical issues in computer security.
8. List and explain the typical set of tasks required of a information security professional.
9. Describe the principles of steganography and watermarking

Application and Analysis

1. Compare different access control, file protection or authentication mechanisms.
2. Set up file protections in a Unix or Windows file system to achieve a given purpose.
3. Incorporate encryption, integrity check and/or authentication into a given program or algorithm.

Synthesis and Evaluation

1. Appraise a given code fragment for vulnerabilities.
2. Appraise a given protocol for security flaws.
3. Assess risk for a given network system using publicly available tools and techniques.