CNT5410: Computer Network Security, Fall 2018

Instructor: Prof. Vincent Bindschaedler (vbindschadler (at) ufl (dot) edu)

Location: NEB 0102

Meeting Times: MWF 12:50pm - 1:40pm

Credits: 3

Office Hours: Mondays 1:40pm - 2:40pm in CSE E406

Course Description:

This course is an introduction to computer and network security. Topics covered include cryptography, applied cryptography, public-key infrastructure, network security, firewalls, secure communications, web security, authentication, passwords, malware, botnets, denial of service, anonymity / mix networks and Tor, cloud computing, side channel threats, and other timely topics (as time permits).

This course aims to provide students with basic skills in computer security research as well as the tools to read, understand and analyze academic computer security research. Reading material will mostly consist of major papers from the research literature. Links to all reading materials will be provided.

Evaluation breakdown:

- Course research project (35%)
- Assignments (10%)
- Midterm (20%)
- Final Exam (30%)
- Participation (5%)

Attendance policy

Attendance will not be checked. However, it is **strongly encouraged** that students attend the lecture. The midterm and final exam will cover material from both assigned readings **and** lectures. Note: topics discussed in class may not fully overlap with the readings.

Assignments and late assignment policy

Students will be assigned written, hands-on and other tasks related to the course topics and course project. The assignments will be announced in class and will be handled through the E-learning platform (elearning.ufl.edu).

Assignments are **always** due before the start of class. Any assignment turned in late will incur a lateness penalty of 20% per day, up to a maximum of 3 days (after which the grade will be 0). If an extension is required for a legitimate reason, students must contact the instructor and (if possible) provide justification a **few days ahead** of the assignment due date.

Class participation

To encourage interaction, participation will be assessed and count for 5% of the grade. Students will be expected to have done the reading **before** class and actively participate during the lecture (e.g., by asking questions). This is critical to do well in this course.

Online students can demonstrate participation by interaction on the E-learning platform, via Email, and/or Skype.

Academic Integrity Policy

Students are required to follow the university guidelines on academic conduct at all times. Students failing to meet these standards will be reported to the Dean of Students, which can result in the student receiving an 'E' for the semester. Note that students are explicitly forbidden from copying anything off of the Internet (e.g., source code, text, slides), using anything from an answer guide, or copying code/answers from each other for the purposes of completing any assignment or a course project.

Ethics Statement

This course covers topics concerning the security of many systems that are widely deployed and potentially critical. As part of this course, we will investigate methods, tools and techniques whose use may negatively impact the rights, property and lives of others. As security professionals, we rely upon the ethical use of the above technologies to perform research. However, it is easy to use such tools in an unethical manner. Unethical use includes the circumvention of existing security or privacy measurements for any purpose, or the dissemination, promotion, or exploitation of vulnerabilities of these services.

This is **NOT** a class on hacking. Any activity outside of the spirit of these guidelines will be reported to the proper authorities both within and outside of UF and may result in dismissal from the class and the University. Exceptions to these guidelines may occur in the process of reporting vulnerabilities through the proper channels; however, students with any doubt should consult Professor Bindschaedler for advice. **DO NOT** conduct any action which could be perceived as technology misuse anywhere or under any circumstances unless you have received explicit permission from Professor Bindschaedler.