# SEC 530
# Malware Analysis and Detection

Dr. Orçun Çetin

# Course Information

- https://sucourse.sabanciuniv.edu/plus/
  - All class materials will be uploaded to sucourse
  - You are responsible to check your e-mails and sucourse for announcements
- Instructor: Dr. Orçun Çetin
  - office: FENS L015
  - e-mails: orcun.cetin@sabanciuniv.edu
- Lectures: Thursday 10:30-13:30
- Useful Books:
  - Michael Sikorski and Andrew Honig, Practical Malware Analysis Handbook

# Course Information

Tentative Grading

- 30% Project
    - 1 project
        - Typically, group projects
        - Compose of multiple parts
- 30% labs & assignments (Not a group work)
    - Lab (simple malware)
    - Assignments (Optional) (More complex malware)
- 40% final

# Labs & Assignment

- Composed of instructions that serve as hands-on exercises on course topics.
  - most of the samples are from books and training courses.
  - only few samples will be real malware samples.
  - done under the supervision of the instructor.
- Students are required to submit their lab results via sucourse.

# Exam and Project

- Exam
  - No mid-term
  - There will be a only one Final exam
- Project
  - Typically includes coding and collecting data from samples
  - Compose of multiple parts

# Ethics and Cheating

- Plagiarism is not tolerated, homeworks are to be done personally
  - cooperation is not an excuse;
    - if you do not know how to cooperate, don’t do it.
- Students are assumed to agree that they will not use the knowledge they gain in this class to perform cybercrime.

# Tentative Syllabus

- Introduction to Malware Analysis
  - Classification of Malware
  - Environment Setup for Safe Analysis
  - Malware Analysis in Virtual Machines
- Basic Analysis
  - Basic Static analysis
  - Basic Dynamic analysis
- Advanced Static Analysis (Reverse engineering basics)
  - Review of x86 assembly
  - Disassembly with IDA Pro & other tools
  - Recognizing C Code Constructs in Assembly
  - Analyzing Malicious Windows Programs
- Advanced Dynamic Analysis
  - Debugging with OllyDbg & x32dbg
- More hands on malware analysis practice
  - Analyzing Java Binaries and Malware
  - Analyzing .NET Malware
  - Malware Analysis with Ghidra
- Malware Functionality
  - Malware Behavior & Covert Malware Launching
  - Malware Obfuscation
- Malicious document analysis
  - PDF, docs, macros