Computer System Security (LINGI 2347)

Ramin Sadre

Three attributes of a secure system

- **Confidentiality**
  - Attacker cannot read/steal protected data
- **Integrity**
  - Attacker cannot modify protected data
- **Availability**
  - Attacker cannot disturb access to data

- We will see examples (attacks+defense mechanisms) for all three attributes in this course

What Is This Course About?

- Introduction to the security of computer systems

- Topics covered:

  - Network security: Attacks (DoS, Botnets,…) and defenses (Firewalls, NATs,…)

  - Software security: Buffer overflows

  - Web security: Cross site scripting, SQL injection,…

  - Using cryptography to secure communication

Prerequisites

- General knowledge of computer architectures and networks required (bachelor level) on:
  - C programming: Needed for lecture and exercises on buffer overflows
  - IP Networking
  - Basics of computer architectures: How does virtual memory work?

- If you don't remember how a TCP/IP packet looks like or how to manipulate strings in C, it is strongly recommended that you take a look at the respective bachelor course

Material

- Material will be posted on Moodle

    http://moodleucl.uclouvain.be

- We will have
    - Slides
    - Exercises
    - Links to relevant publications, websites, etc.
- Important information + announcements only on Moodle!

Assessment

- There will be an exam about the topics addressed in the lectures, counting for 65% of the final grade
- Two small projects: 35% of the final grade
  - Write code + report

- Exercises will not be assessed, but they will prepare you for the projects and the exam

Warning

- Some of the attacks that we will see in this course are very easy to execute (e.g. port scans)
- Check the rules of your ISP (including UCLouvain) to see what is allowed and what not