CSCI 4250/6250 – Fall 2015 Computer and Network Security

Instructor: Prof. Roberto Perdisci
perdisci@cs.uga.edu

CSCI 4250/6250

‣ What is the purpose of this course?

  ‣ Combined Undergrad/Graduate Intro to Computer and Net Security

  ‣ Focuses on understanding security principles, protocols, and pitfalls:

    ‣ How do systems fail under attack?

    ‣ Defend yourself: best practices, design more secure systems

‣ What this course is not!

  ‣ This is **not a hacking course**

  ‣ While we will talk about vulnerabilities and attacks, we will not focus on how to write exploits

  ‣ Focus will be on analyzing security mechanisms, pitfalls, learn from past mistakes, and think about how to design more secure systems

▶

Course Topics

- Introduction: CIA, Design Principles, Crypto concepts
- Access Control and Security Models
- More crypto
  - confidentiality and integrity
  - Symmetric- and Public-key crypto
  - SSL / IPSec / DNSSEC
- OS and software security
- Malware, Botnets
- Web security
- Operational network security and privacy
  - Spoofing, Poisoning, Firewalls, IDS, Anonymity, etc…
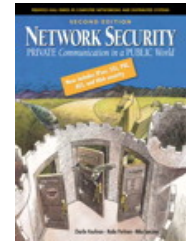- Physical Security (if time allows…)

Books

▸ **Textbook 1:** *Introduction to Computer Security*
  ▸ Michael T. Goodrich and Roberto Tamassia
  ▸ Addition Wesley

▸ **Textbook 2:** *Network Security: Private Communication in a Public World, 2/e*
  ▸ Charile Kaufman, Radia Perlman, Mike Speciner
  ▸ Prentice Hall

▸ **Recommended Readings:** *Introduction to Computer Security*
  ▸ Matt Bishop
  ▸ Addition Wesley

▸ See website for other recommended readings…
  ▸ http://www.cs.uga.edu/~perdisci/CSCIx250-F13/Syllabus.html

How will students be evaluated?

- Class participation: U,G=5%
- Paper Reviews: U=N/A, G=10%
- Development Projects and Assignments: U,G=25%
- Midterm Exam: U=35%, G=30%
- Final Exam: U=35%, G=30%

Overall Grade

- Weighted sum of all points

  - $S = 100*(0.10*c/C+0.25*a/A+0.10*p/P+0.30*m/M+0.30*f/F)$
    - S >= 90% = A   S >= 85% = A-
    - S >= 80% = B+   S >= 75% = B
    - S >= 70% = B-   S >= 65% = C+
    - S >= 60% = C   S >= 55% = C-
    - S >= 40% = D   S < 40% = F

  - c = number of classes attended (max: C)
  - a = overall assignments points (max: A)
  - p = overall paper presentation points (max: P)
  - m = midterm exam points (max: M = 100)
  - f = finale exam points (max: F = 100)

Class Participation (5%)

▶ Class participation is required
  ▶ Students will need to sign the attendance log at the beginning of sample lectures

▶ Not all topics discussed during lectures are covered in the textbooks

▶ Lectures will be interleaved with assignments/projects discussions

Paper Presentations (U=N/A, G=10%)

- Throughout the term, graduate students will be required to read a number of academic/technical papers

- For each paper, students will be required to prepare a presentation to be given to the entire class
  - Introduce problem
  - Summarize paper
  - Briefly describe proposed system/algorithms
  - Report most important experimental results
  - Live demonstration (when appropriate)
  - More detailed guidelines later…

- NOTE: Some of the topics discussed in the assigned papers may be part of the midterm and final exams for everybody!

Development Projects + Assignments (25%)

- Students will be required to complete a number of development projects
  - Development in C, Java, or Python
    - (other languages conditioned to my explicit approval)
  - Some projects must be conducted individually
  - Others may be conducted in pairs (I will indicate which ones), in which case the evaluation will be the same for both students
  - Most projects will be evaluated with a *binary criteria*
    - It works correctly => X points (X depends on project difficulty)
    - It does not work (does not compile, fails tests, etc.) => 0 points
    - I will announce possible exceptions to this rule for specific projects

  - Development Projects and Assignments under Linux
    - You will use a specific VM image (provided later…)

Development Projects + Assignments (25%)

- ▸ Other assignments will include
  - ▸ Pencil-and-paper homework
  - ▸ Hands-on network experiments / analysis

- ▸ Lateness Policy
  - ▸ Students will be allowed a maximum of **one** late submission
  - ▸ Max delay = 7 days
  - ▸ Past this threshold, all future late assignments will penalized 100%

Exams

▸ **Midterm Exam (U=35%, G=30%)**

 ▸ Will cover all topics discussed up to one week before the exam

▸ **Final Exam (U=35%, G=30%)**

 ▸ Can cover **all topics**

 ▸ Main focus on second part of the course

 ▸ Will include some questions about most important topics covered in the first part of the course

▸ **Both Midterm and Final may also contain some questions related to papers assigned for review**

Academic Integrity

▸ Every student must abide by UGA's **academic honesty policy**

▸ Dishonest behavior including cheating, copying, or forging experimental results **will not be tolerated** and will be reported according to UGA's policies

▸ **Always adopt an ethical conduct**
  ▸ **Never use what you learn to attack real systems!!!**

▸ Specific to Development Projects:
  ▸ You are *allowed* to search for examples and documentation
  ▸ You are *not allowed* to reuse other people's code (no cut and paste!)
    ▸ Use examples to understand how the code works and then **write your own code!**
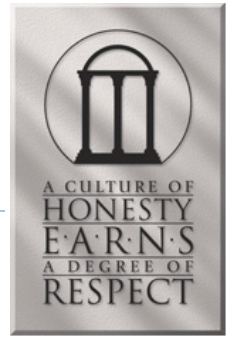
Logistics

‣ Course Website

 ‣ http://www.cs.uga.edu/~perdisci/CSCIx250-F15/

 ‣ I will post info on topics covered in class, assignments, projects, and related deadlines

‣ Mailing List

 ‣ CSCIx250-F15@listserv.uga.edu

 ‣ Assignment 0:

  ‣ See course calendar for instructions on how to subscribe to the list (only UGA.edu email addresses are allowed)

 ‣ Use mailing list to ask any questions about the course (avoid posting questions specific to your case on the list)

 ‣ You can also use the mailing list for discussion

 ‣ DO NOT expect me to answer to all questions. I will answer only to important questions/urgent issues, anything else can be addressed during last 5min of class

Logistics

‣ As a reminder… Classes are on
  ‣ Monday at 3:35-4:25pm, Boyd 306
  ‣ Tuesday and Thursday at 3:30-4:45pm, Boyd 306

‣ Office hours
  ‣ Thursdays, 1-3pm
  ‣ GSRC Room 423

‣ TA
  ‣ TBD < TBD [at] uga [dot] edu>

Questions?