System and Network Security: Course Plan

Prof. Ankit Gangwal
Assistant Professor, IIIT-H, India
email: *gangwal@iiit.ac.in*
Web: *CiaoAnkit.github.io*

- *"Welcome! Before we begin, let's sort a couple of things."*

Table of contents

Particulars

- Credits: 4
- Coverage: State-of-the-art of systems and network security
- Language: Content delivery, exams, etc. will be in English
- Schedule: Spring semester (Tuesday & Friday 10:00-11:30)
- Webpage: *https://ciaoankit.github.io/teaching.html*

Course contents

- Concepts of systems and network security
  - Fundamentals of cryptography
  - Operating system security
  - Network attacks and defenses
  - Web security models
  - Smartphone security architectures
  - Microarchitecture security
  - Sandboxing
  - Vulnerabilities analysis techniques
  - Privacy and censorship
  - Social engineering attacks

PS: Course contents may vary depending on the interest and response from the students

Projects and assignments

- Students are expected to work on multiple learning-oriented projects and assignments
  - Paper review: Research-oriented **group** project
  - Mini project: Programming-oriented **group** project
  - Individual assignments (if any)

- Group information
  - Team information via Office Forms (get your **group's ID**)
    - https://forms.office.com/r/YaNzTN213W
    - Deadline: **January 31, 2022**
  - Project information via Office Forms
    - https://forms.office.com/r/pmmdNamGvL
    - Deadline: **February 28, 2022**

Projects and assignments

- Paper review
  - Select a paper related to systems and/or network security
    - Published in the last **two** years from a **top** security conference
  - Prepare
    A. A LaTeX **report** (single-column, 10pts)
       1. A summary of the paper (max 2 pages)
       2. Major critiques on assumptions, technical approach, analysis, and/or results (no page limit)
       3. Suggestions for improvements/extensions (no page limit)

    B. A **self-explanatory** Beamer **presentation** (max 20 slides)
  - Final submission format: *pdf*
    - Named as *GroupID_RollNoA_RollNoB_..._RollNoZ.pdf*

Projects and assignments

- Paper review
  - Report submission via **TurnItIn**
    - ClassID: **32833759**
    - Enrollment Key: **2122_SNS_KT**
    - Deadline: **March 10, 2022**
    - Plagiarism must be **< 30%** | Else complete disqualification
  - Presentation submission via **Dropbox** file request
    - https://www.dropbox.com/request/GVJB3bAo2h6xiiqYAUzV
    - Deadline: **March 10, 2022**

Projects and assignments

- Mini project
  - Implement a security vulnerability/exploit/attack (e.g., SQLi, XSS)
    - Update code to defend against implemented attack
  - Or, a demo of an exploit against a real application is also accepted
    - Provided that its fix is furnished
  - Submit
    A. Source code
    B. Screenshots of execution
    C. Clear instructions (in *README.txt*) to set up environment (if any) and execute the code
  - Final submission format: *zip*
    - Named as *GroupID_RollNoA_RollNoB_..._RollNoZ.zip*

Projects and assignments

- Mini project
  - Project submission via **Dropbox** file request
    - https://www.dropbox.com/request/jhIxMXeueX7ySrgUwgNP
    - Deadline: **March 31, 2022**
  - Paper presentation and project demo
    - Everyone gets ready before **April 01, 2022**
    - Random calls, 5 groups per day
      - **April 01, 05, 08, 12, 19** (and **May 04, 05, 06** reserved)

Grading, examinations, and policies

- Grading
  - Relative grading
  - Final grade set: {A, A-, B, B-, C, C-, D, F} | No ‘P’ grade possible

- Examinations & marks distributions
  - Assignments, projects : 50%
  - Mid-term exams, quizzes : 20%
  - End-term exam : 30%

- Policies
  - Do and submit your own original work
  - Cheating, plagiarism, and academic dishonesty will carry consequences

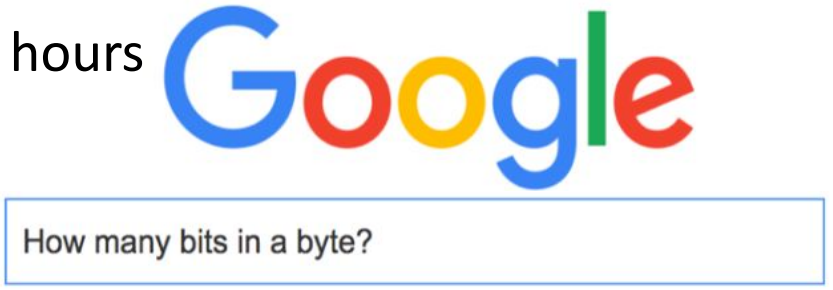
Textbooks and references

- There is no single textbook that can cover entire course material, some good references to start are given below (most of them are available on the Internet)

1. J. R. Vacca. "Network and System Security."
2. B. Menezes. "Network Security and Cryptography."
3. W. Stallings. "Cryptography and Network Security: Principles and Practice."
4. Research papers.

Setting expectations

- Don’t expect 24x7 answers
  - Instructors are not on duty 24x7
    - Don’t expect response before next business day
    - Queries over weekend should never expect fast responses
      - Be happy with something before Monday
- Try to figure out yourself
  - Students should answer each other; start your assignments early!
- Forums are not for debugging
  - Utilize right venue: Go to TA office hours
  - Send detailed Q’s/bug reports
    - Not *“no idea what’s wrong”*



- *"Finally, prioritize things!"*

Good luck.

Thank you!