Welcome to
CS5321 Network Security
- 2020/21 Sem 2 -

Daisuke MASHIMA

Email: mashima@comp.nus.edu.sg

http://www.mashima.us/daisuke/index.html

Learning outcomes

- This module aims to prepare undergrad/grad students for ***research and development* in network security** by studying basics and literature as well as investigating research problems in ***network and distributed systems***.

- At the end of the module, students will be able to:
  - ***understand*** the ***security challenges and opportunities*** of various emerging network and distributed systems;
  - ***critique*** state-of-the-art ***attack/defense mechanisms*** and ***identify*** possible ***gaps*** that could be addressed by future work.

Administrative Issues (1)

- Class: Mon 6:30 pm – 8:30 pm
- Venue: Zoom (Link is announced on **LumiNUS**)
- Online discussion: **LumiNUS** forum

- (Virtual) Office hour: on Tue-Thu at 6 pm – 7 pm
  - Make use of office hours for clarifications, course feedback, etc.
  - On **Zoom**
    - Make an appointment on the day before via email. Link will be provided then.
  - Office: **CREATE Tower #14-02 in UTown** or COM2-02-44 (also requires appointment in advance)

Administrative Issues (2)

- Course slides
  - Final slides will be uploaded to **LumiNUS** after each lecture
    - Will provide a draft version before each lecture
- Lecture videos
  - Zoom recording will be uploaded after each lecture
- No required textbook
  - Suggested (optional) textbooks
    - "Introduction to Modern Cryptography" by Jonathan Katz and Yehuda Lindell
    - "Network Security: Private Communication in a Public World" by Kaufman, Perlman, and Speciner

Administrative Issues (3)

- Assessment/Grading
  - 3 Exams [50%]
    - Exam 1 (10%), Exam 2 (20%), Exam 3 (20%)
  - Quizzes [20%]
    - 3 quizzes
    - The lowest score (including 0) will be removed from total
      - e.g., Score of 3 quizzes (0,8,9) => Will get total 17 (out of 20).
  - Mini Project [20%]
    - Involves programming as well as hands-on experiment using virtualized environment. Detail will be announced in Week 10
    - Individual work
  - Participation [10%]
    - In-class participation (5%) and Forum participation (5%)

Administrative Issues (4)

- Quiz (20%): In-class, 15 min
  - Multiple-choice questions on LimiNUS
  - Quiz 1: Lecture and reading in Weeks 4 - 6
  - Quiz 2: Lecture and reading in Weeks 7 – 9
  - Quiz 3: Lecture and reading in Weeks 10 - 12

- Exam 1 (10%): Take-home (Out in Week 3)
  - Will cover the basic notions of cryptographic primitives taught in Week 1 - 3
- Exam 2 (20%): Take-home (Out in Week 7)
  - Will cover the topics covered in Week 4 - 7
- Exam 3 (20%): In-class, open-book (Week 13)
  - Will cover the topics covered in Week 8 - 12

Administrative Issues (5)

- Policy on exams: if you *"have to miss"* exams, let me know *in advance with a proof* (e.g., military exercises, business travels)
  - We will provide a make-up exam (with similar difficulty)
- Policy on quizzes:
  - You can miss one quiz without any penalty; thus, no make-up quizzes
  - Missing two or more quizzes due to work?
    - This should be very unusual
    - If this happens, we can consider having a 4th quiz only for these people

Supplementary Readings

- In some weeks, research papers will be assigned
  - Announced at or before the preceding lecture
  - 1 – 2 papers for each time
  - Haven't read research papers?
    - https://web.stanford.edu/class/ee384m/Handouts/HowtoReadPaper.pdf

Prerequisites

- **CS 3235** Computer Security
  - Students who didn't take the class but still are interested in taking the course may be able to enroll subject to **waiver approval**. Please consult Prof. Seth Gilbert (seth.gilbert@comp.nus.edu.sg)
- Basic knowledge
  - Computer networks; e.g., TCP/IP, routing, naming, Internet architecture.
  - Computer security; e.g., basic cryptography
- Basic cryptography will be covered in the first two lectures
- Domain knowledge will be covered in every lecture
- If you have concerns about this, please contact me immediately.

Tentative Course Schedule

Week	Date	Tentative Subject	Exams	Quiz	Project
1	1/11/2021	Course Intro + Basic Crypto			
2	1/18/2021	Basic Crypto			
3	1/25/2021	Authentication / Secure communication Basics	Exam1 (Take-home)		
4	2/1/2021	PKI	Exam 1 Due		
5	2/8/2021	TCP/IP Security			
6	2/15/2021	Routing Security		Quiz 1	
Recess	2/22/2021				
7	3/1/2021	DNS Security	Exam 2 (Take-home)		
8	3/8/2021	DOS attacks	Exam 2 Due		
9	3/15/2021	Intrusion Detection Systems		Quiz 2	
10	3/22/2021	CPS/ICS security			Announced
11	3/29/2021	Cloud Security			
12	4/5/2021	Blockchain		Quiz 3	
13	4/12/2021	Selected topic	Exam 3 (in class)		
Reading					Due