Welcome to
CS5321 Network Security
- 2022/23 Sem 2 -

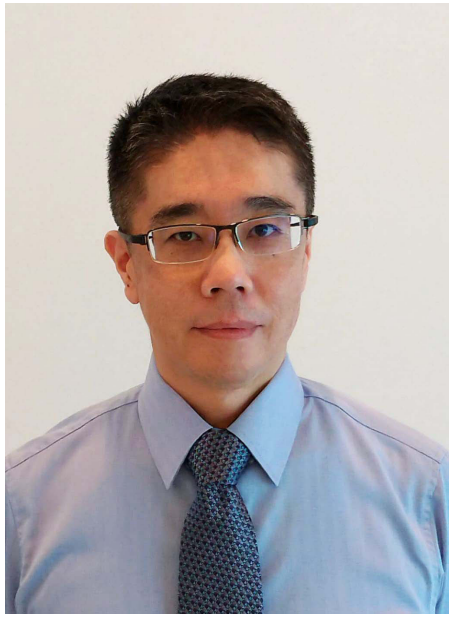
Daisuke MASHIMA

Email: mashima@comp.nus.edu.sg

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

Instructor Bio

Experience



Principal Research Scientist at Advanced Digital Sciences Center (ADSC) and Research Affiliate at University of Illinois

- Research interest includes cybersecurity, cyber-physical systems security, critical infrastructure security, etc.

Formerly research scientist at Fujitsu Laboratories of America

- Smart energy and smart home IoT systems
- Security and privacy in smart metering
- OpenADR2.0 standardization

Education

PhD in Computer Science from Georgia Institute of Technology (USA) in 2012

- Security and privacy in Electronic Healthcare Records

Contact Info

- Email: mashima@comp.nus.edu.sg

Why do we need Cybersecurity R&D?

Singapore firms fined $75,000 for personal data lapses affecting over 600,000 people

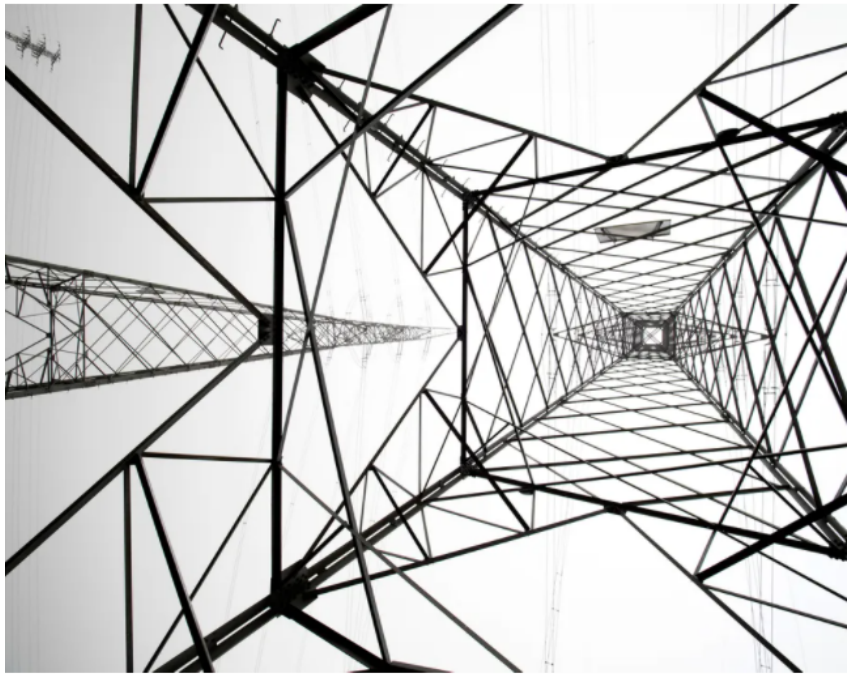
Hacker

New Research Shows Cyberattacks Affect Stock Prices

BY GILLIAN SWENY | MAY 5, 2021 | UNCATEGORIZED | 0 COMMENTS

Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid

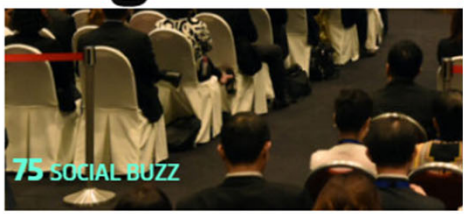
The hack on Ukraine's power grid was a first-of-its-kind attack that sets an ominous precedent for the security of power grids everywhere.



JOSE A. BERNAT BACET/GETTY IMAGES

Why do we want to study Cybersecurity?

Massive cybersecurity ski shortage in ASEA



By **Rebecca Oi** | 2 December, 2021

ZDNET tomorrow belongs to those who embrace it today

/ innovation

Home / Innovation / Security

APAC faces 2.1M shortage in cybersecurity professionals

Asia-Pacific region sees greatest growth in cybersecurity workforce, but still struggles to fill a gap of more than 2.16 million with 60% of organisations reporting a significant shortage in security staff, according to a study released by ISC2.

Written by **Eileen Yu,** Senior Contributing Editor

on Oct. 25, 2022

Wanted: Millions of cybersecurity pros. Salary: Whatever you want

By Clare Duffy, CNN Business

Updated 1948 GMT (0348 HKT) May 28, 2021

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: LT18
- Online discussion: **Canvas** 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.
- Physical Office: **CREATE Tower #14-02 in UTown**
  - Requires appointment in advance

Administrative Issues (2)

- Course slides
  - Final slides will be uploaded to **Canvas** after each lecture
    - Will provide a **draft** version before each lecture for preview.

- 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
  - 2 take-home exams [50%]
    - Exam 1 (25%), Exam 2 (25%)
  - Quizzes [25%]
    - 6 online quizzes (bi-weekly) using **Canvas**
    - The lowest score (including 0) will be removed. Remaining 5 scores are averaged. Fraction is rounded up.
  - Mini Project [20%]
    - Individual work
  - Participation [5%]
    - Attendance (QR Code shown break time and after lecture)
    - In-class and forum discussion
    - Volunteer for in-class paper summary presentation

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 7th quiz only for these people

Supplementary Readings

- For each week, 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

1. *Category*: What type of paper is this? A measurement paper? An analysis of an existing system? A description of a research prototype?

2. *Context*: Which other papers is it related to? Which theoretical bases were used to analyze the problem?

3. *Correctness*: Do the assumptions appear to be valid?

4. *Contributions*: What are the paper's main contributions?

5. *Clarity*: Is the paper well written?

    - For Cybersecurity papers, you should pay attention to:
      - Attacker / Threat model
      - Security assumptions

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	Take-home Exams	Quiz	Project
1	09-01-2023	Course Intro + Basic Crypto			
2	16-01-2023	Basic Crypto			
3	23-01-2023 [CNY]	Authentication / Secure communication Basics		Quiz 1	Announced
4	30-01-2023	PKI Security			
5	06-02-2023	TCP/IP Security		Quiz 2	
6	13-02-2023	Honeypot and threat intelligence	Exam 1 Out		
Recess	20-02-2023				
7	27-02-2023	Routing Security	Exam 1 Due	Quiz 3	
8	06-03-2023	DoS Attacks			
9	13-03-2023	DNS Security		Quiz 4	
10	20-03-2023	Anonymous Communication			
11	27-03-2023	Anti-censorship		Quiz 5	
12	03-04-2023	Blockchain	Exam 2 Out		
13	10-04-2023	Selected Topic		Quiz 6	Due
Reading	17-04-2022		Exam 2 Due		
Exam	24-04-2022				

Questions?