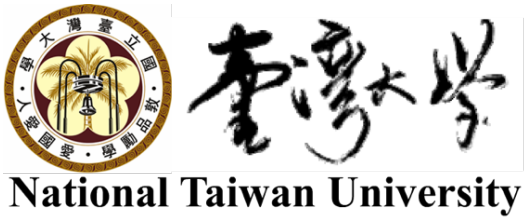
Course Information

CSIE 7190 Cryptography and Network Security, Spring 2019

https://ceiba.ntu.edu.tw/1072csie_cns

cns@csie.ntu.edu.tw

Hsu-Chun Hsiao



密碼學與資訊安全
(Cryptography and Network Security)

(14:20-17:10) Tuesdays 789 Location: R102

https://ceiba.ntu.edu.tw/1072csie_cns

Email: cns@csie.ntu.edu.tw

Agenda

1. 教學團隊和聯絡方式
2. 加簽原則
3. 課程大綱
4. 成績計算方式
5. 資訊安全倫理

Teaching Team & Office Hours

	Time	Location
蕭旭君	Tuesdays 11:00-12:00	511
毛偉倫	TBD	307
蕭乙蓁	TBD	307
江緯璿	TBD	307

聯絡方式：cns@csie.ntu.edu.tw

重要事項助教會寄信至@ntu.edu.tw信箱，並在課程網站上公告

加簽原則

上限：依教室狀況決定

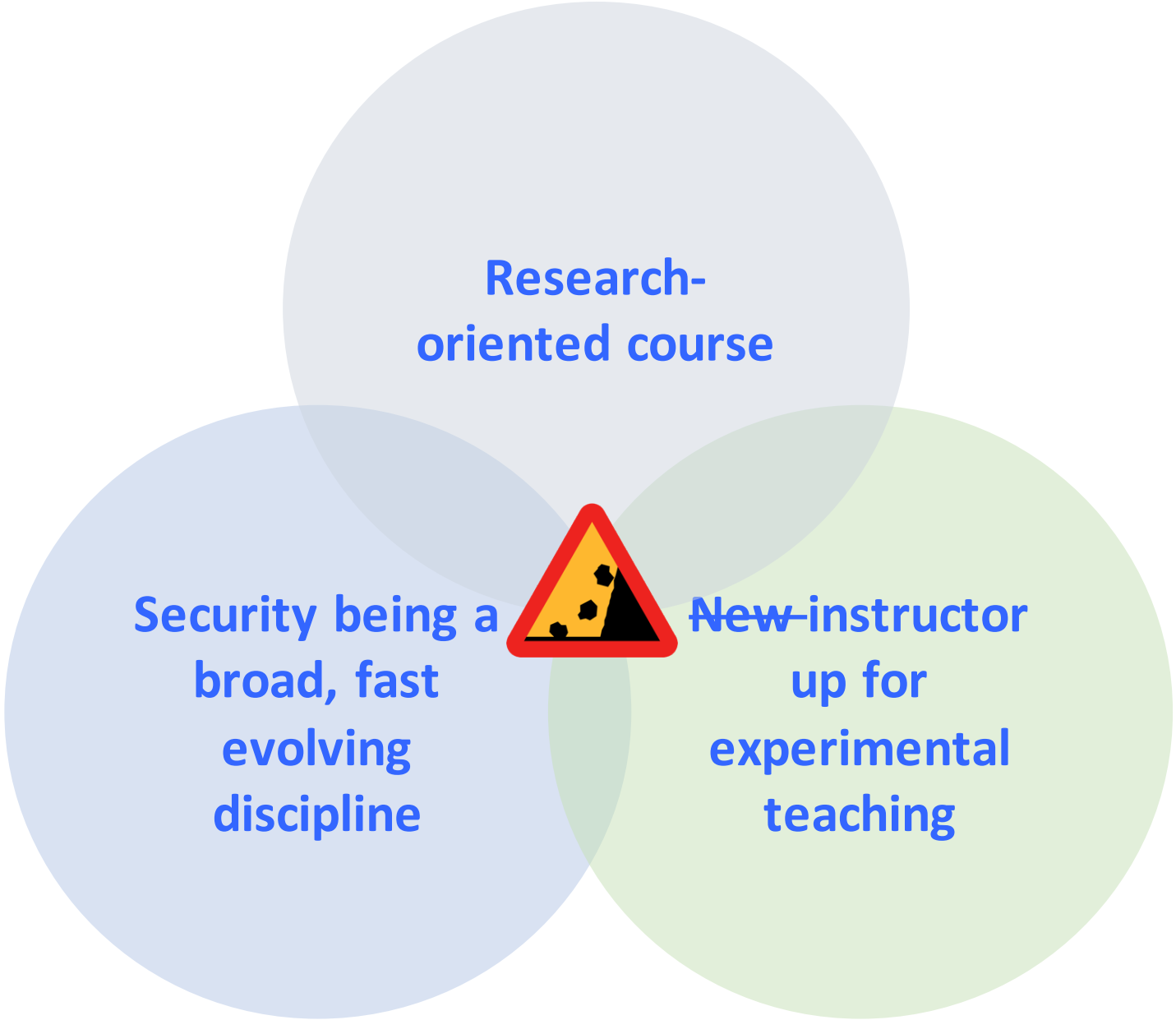
Write a paper critique (will show it later)

- Format: Text only, 1 page
- Deadline: 2/24 (Sun.) noon
- 加簽表單：https://goo.gl/forms/vtJxlVjEiMrr1OTF2

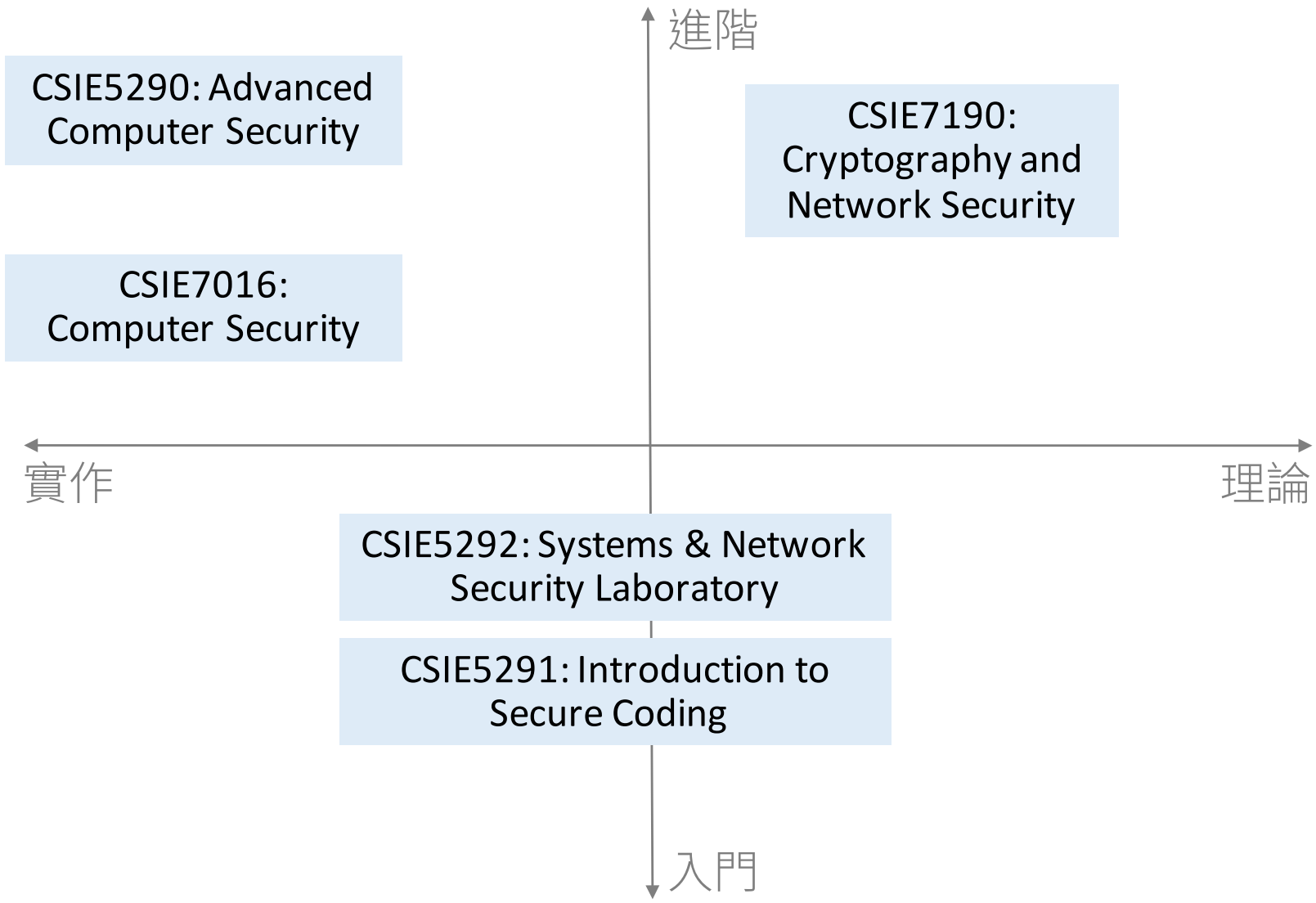
加簽順序：依成績而定，相同順位則抽籤決定

名單確定後助教會於下週上課前寄送授權碼

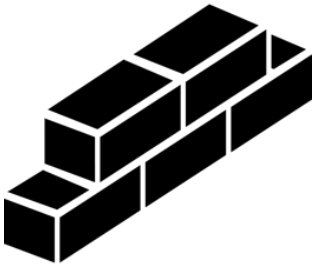
Course “features”



Are you in the right class?



Landscape of Security Research



密碼學
Encryption
Digital signature
Hash
MAC
PRNG
Block ciphers
…

安全協定/機制
Entity authentication
Anonymous routing
Public key infrastructures
Broadcast authentication
Key management
Secure e-voting
Encrypted email
…

安全實作
Type-safe language
Control flow integrity
Obfuscation
Sandboxing
Run-time enforcement
Trusted computing
…

弱點偵測
Penetration testing
Reserve engineering
Binary analysis
Dynamic taint analysis
…

This course

Course overview

Crypto Primitives

- Crypto Hash
- Encryption
- Message Authentication Codes
- Digital Signature

Cryptographic Protocols

- Authentication
- Key Exchange
- Public Key Infrastructure
- Anonymous Comm.
- Secure voting

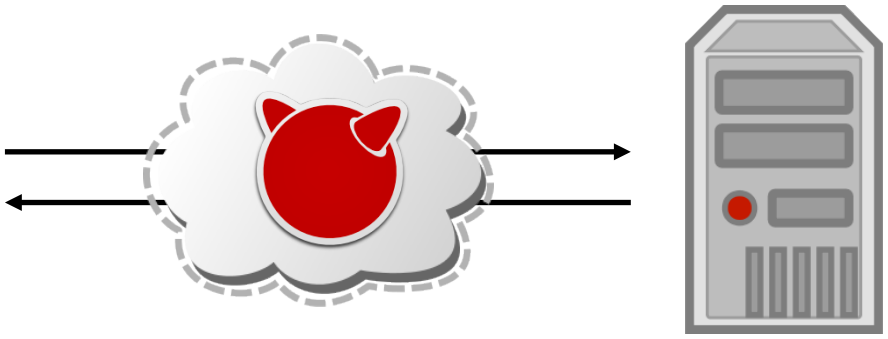
Network Security

- TCP, DNS, routing, WiFi
- Transport Layer Security
- Denial of Service
- Blockchain & Cryptocurrencies
- Other security topics: Web, software, systems

Example

Ensure program or system works correctly even in the face of attack

- Is it the right website? Is it really the owner of the account?
- Is the transaction content correct?
- Can anyone see my account information?
- Is the service available?



Topics we probably won't have time to cover

Firewall, IDS, IPS

Malware, virus

Formal verification

Trusted computing

Side-channel attacks

Physical security

Mobile security

AI/ML security

Cloud security

SDN security

VANET security

Wireless security

IoT security

Software security

Web security

…

課程目標

By finishing this course, you should be able to answer the following questions:

1. Describe important security concepts
2. Identify security threats & potential countermeasures
3. Build simple protection mechanisms
4. Analyze and reason whether real-world security systems achieve their desired goals

課程目標

How to accomplish these objectives

- We will practice the “security mindset” – thinking like an attacker & thinking about how things can be made to fail
- We will learn a variety of attack and defense techniques

This course covers important concepts in security but is not meant to be comprehensive

You’re expected to think and learn by yourself in this graduate-level course

Tentative class schedule

Wk.	Date	Topic
1	Feb 19	Introduction
2	Feb 26	Security & Crypto Overview
3	Mar 05	Cryptographic Hash Functions
4	Mar 12	Symmetric Cryptography
5	Mar 19	Asymmetric Cryptography and Public key Infrastructures
6	Mar 26	Authentication
7	Apr 02	No Class (Spring Break)
8	Apr 09	Anonymity and Privacy
9	Apr 16	1st midterm exam

Tentative class schedule

Wk.	Date	Topic
10	Apr 23	Insecurity of TCP/IP, BGP, DNS, WiFi
11	Apr 30	(D)DoS
12	May 07	Transport Layer Security
13	May 14	Selected Topics: Software, Web, Systems Security
14	May 21	Selected Topics: Guest Lecture
15	May 28	Selected Topics: Blockchain, Cryptocurrencies, secure voting
16	Jun 04	2nd Midterm Exam
17	Jun 11	Group presentation - I
18	Jun 18	Group presentation - II

Optional textbooks (Mostly available online)

Dan Boneh and Victor Shoup (book in progress). ***Graduate Course in Applied Cryptography.***

http://toc.cryptobook.us

Menezes, van Oorschot, and Vanstone. 1997. **Handbook of Applied Cryptography**. CRC Press.

http://cacr.uwaterloo.ca/hac

Jonathan Katz and Yehuda Lindell. 2007. ***Introduction to Modern Cryptography***. Chapman & Hall/CRC.

E-book available via NTU library

Ross J. Anderson. 2008. ***Security Engineering: A Guide to Building Dependable Distributed Systems*** (2 ed.). Wiley Publishing.

http://www.cl.cam.ac.uk/~rja14/book.html

William Stallings. 2013. **Cryptography and network security: principles and practice** (6 ed.). Pearson Publishing.

Grading components

Homework (30%)

Reading critiques (10% + 5% bonus)

Group project (25%)

- Proposal (5%)
- Final presentation (10%)
- Final report (10%)

Midterm exams (30%)

Class participation (5%)

Final grade: criteria

百分數		等第	定義	等第績分
90-100	95	A+	All goals achieved beyond expectation 所有目標皆達成且超越期望	4.3
85-89	87	A	All goals achieved 所有目標皆達成	4.0
80-84	82	A-	All goals achieved, but need some polish 所有目標皆達成，但需一些精進	3.7
77-79	78	B+	Some goals well achieved 達成部分目標，且品質佳	3.3
73-76	75	B	Some goals adequately achieved 達成部分目標，但品質普通	3.0
70-72	70	B-	Some goals achieved with minor flaws 達成部分目標，但有些缺失	2.7
67-69	68	C+	Minimum goals achieved 達成最低目標	2.3
63-66	65	C	Minimum goals achieved with minor flaws 達成最低目標，但有些缺失	2.0
60-62	60	C-	Minimum goals achieved with major flaws 達成最低目標但有重大缺失	1.7
≦ 59	50	F	No goals achieved 所有目標皆未達成	0
0	0	X	Not graded due to unexcused absences or other reasons 因故不核予成績	0

Failing grade for grad students

Failing grade for undergrads

Warning: final grade is non-negotiable

http://www.oia.ntu.edu.tw/upload/files/20150616223619.pdf

Grading component 1: Homework

Three homework assignments

- Half writing, half programming
- Late policy: 10% penalty per day, up to two days
- Upload to CEIBA

Plan (subject to change)

	Release Date	Deadline	Scope
HW1	Mar 12	Apr 2	Crypto (weeks 2-5)
HW2	Apr 13	May 14	Network (weeks 6-11)
HW3	May 21	Jun 11	Selected topics (weeks 12-15)

Grading component 2: Reading Critiques

10 reading critiques (10% + 5% bonus)

- Purpose: preview; learn how to do research
- Due before lecture; no credit for late submission
- Text only, one page. Be concise!
- Upload to CEIBA

之前曾經出過的reading可參考：

https://www.csie.ntu.edu.tw/~hchsiao/courses/cns19.html#sample-reading

Reading critique format

Your critique **MUST** contain the following:

1. **Summary** – answering these four questions in your own words:
   - What problem is the paper trying to solve?
   - Why does the problem matter?
   - What is the approach used to solve the problem?
   - What is the conclusion drawn from this work?
2. **Strength(s) of the paper**
3. **Weakness(es) of the paper**
4. **Your own reflection**, which can include but not limited to:
   - What did you learn from this paper?
   - How would you improve or extend the work if you were the author?
   - What are the unsolved questions that you want to investigate?
   - What are the broader impacts of this proposed technology?

Tip: Pay attention to assumptions and threat models.

Grading component 3: Group project

4人一組

時程

- 四月初繳交分組名單和題目
- 五月初繳交提案 （proposal）
- 6/11和6/18期末報告，每一組約15~20分鐘
- 六月底前繳交期末書面報告

詳細時程、報告形式、和評分標準會再公佈

之前修課同學的題目可參考：

https://www.csie.ntu.edu.tw/~hchsiao/courses/cns19.html#past-projects

Graduate students: Highly encourage to bring security thoughts to your current research

Undergrad students: Highly encourage to attend 專題成果展

Grading component 4: Midterm exams

Apr 16: 1st midterm

Jun 04: 2nd midterm

The format of exam questions is usually similar to the handwriting part of the homework assignments

Grading component 5: Class participation

Ask questions during or after the class

Give opinion during class discussion

Go to the TAs' or professor's office hours

Spot errors on the slides

Suggestions on how to improve this course

Course policies

In-class policy

- 大原則：不要打擾別人或影響老師上課

Late submission policy

- Critiques: no late submission is allowed
- Labs: 10% penalty per day, up to two days
- Project proposal and report: no late submission is allowed

Collaboration policy

- Discussion is encouraged, but you must acknowledge
- Copying solutions without proper acknowledgment constitutes cheating and will lead to a failing grade

Ethics of hacking

任何實務的操作練習皆應獲得明確的許可

修習這門課不構成任意存取別人的系統或資料的藉口

最重要的是要保護好自己，不要觸犯法律

Any attempt to cheat or attack others (including the teaching team) may lead to a failing grade

刑法第36章妨害電腦使用罪

第 358 條	無故輸入他人帳號密碼、破解使用電腦之保護措施或利用電腦系統之漏洞，而入侵他人之電腦或其相關設備者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。
第 359 條	無故取得、刪除或變更他人電腦或其相關設備之電磁紀錄，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。
第 360 條	無故以電腦程式或其他電磁方式干擾他人電腦或其相關設備，致生損害於公眾或他人者，處三年以下有期徒刑、拘役或科或併科十萬元以下罰金。
第 361 條	對於公務機關之電腦或其相關設備犯前三條之罪者，加重其刑至二分之一。
第 362 條	製作專供犯本章之罪之電腦程式，而供自己或他人犯本章之罪，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。

Reading critique #1

Write a critique on one of the following: (Note that the last one has two papers)

- M. Sharif, S. Bhagavatula, L. Bauer, M. K. Reiter, "Accessorize to a crime: Real and stealthy attacks on state-of-the-art face recognition, " in ACM Conference on Computer and Communications Security, 2016.
- M. R. Clarkson, S. Chong and A. C. Myers, "Civitas: Toward a Secure Voting System," in IEEE Symposium on Security and Privacy, 2008.
- G. Wurster and P. C. van Oorschot, "The developer is the enemy," in workshop on New security paradigms, 2008. & M. Green and M. Smith, "Developers are Not the Enemy! The Need for Usable Security APIs," IEEE Secur. Priv., vol. 14, no. 5, pp. 40–46, 2016.

Text only, one page

Reading critique #1

已選上的同學：

- Due: Tuesday 2/26 14:00
- 上傳至ceiba

要加簽的同學：

- Due: Sunday 2/24 noon
- 上傳至 https://goo.gl/forms/vtJxlVjEiMrr1OTF2
- 請記得寫姓名跟學號

Please clearly mark **Summary**, **Strengths**, **Weaknesses**, and **Reflections**

Remember to put proper attributions

Don't know where to find papers? Try Google Scholar

Questions?

Course website: https://ceiba.ntu.edu.tw/1072csie_cns
Email: cns@csie.ntu.edu.tw
重要事項助教會寄信至@ntu.edu.tw信箱，並在課程網站上公告