CS2107 Review + Final Exam Tips

Teaching Mode

- **13** Lectures: including 2 guest lectures from industry & government
- **9** Tutorials
- Continual Assessment (50%):
  - 2 Assignments (25%): Do submit **A2** before its deadline
  - 1 Mid-term quiz (15%)
  - 1 Group presentation on open-ended topic (5%)
  - 1 LumiNUS online quiz assessment (5%)
- **Final Exam (50%)**: Open-book, Saturday 23 Nov, 09:00-11:00
  Please *double-check* the timing & venue with CORS again!

Module Description

Objective

This module serves as an introductory module on information security. It ***illustrates*** the ***fundamentals of how systems fail*** due to malicious activities ***and how they can be protected***. The module also places emphasis on the practices of secure programming and implementation. Topics covered include **classical/historical ciphers**, **introduction to modern ciphers** and cryptosystems, ethical, legal and organisational aspects, classic examples of direct attacks on computer systems such as **input validation vulnerability**, examples of other forms of attack such as **social engineering/phishing attacks**, and the **practice of secure programming**.

Outcomes

- Awareness of common and well-known attacks (e.g. phishing, XSS, SQLI, ...)
- Understand basic concepts of security (e.g. confidentiality, availability, ...)
- Understand basic mechanisms & practice of protections (e.g. crypto, PKI, access control, ...)
- Awareness of common pitfalls in implementation (Secure programming)

More Specific Intended Learning Outcome (ILO)

After completing the module, you will be expected to be able to:

1. Explain *the C-I-A security requirements* and recognize their breaches in recent security incident news
2. Describe *key concepts and basic mechanisms* of principal protection mechanisms in information security, such as encryption, authentication, and access control
3. Identify the *limitations* of classical cryptographic schemes, and recognize *well-known attacks* on vulnerable hosts, networks, and Web servers

More Specific Intended Learning Outcome

4. Utilize some *basic security tools* (e.g. OpenSSL, Wireshark) and security-related *Linux commands* to perform encryption, network traffic analysis, and file access control
5. Pinpoint flaws in programs due to common *insecure programming practices*, and suggest improvements using more secure practices instead

Some of the terminologies encountered in this modules

Secure channel, Alice, Bob, Eve, Encryption, Decryption, Key-space, Known-plaintext attack, Authenticity, Confidentiality, availability, Authentication protocol, man-in-the-middle, Passwords, Dictionary attack, random IV, Kerckhoff's principle.

Side-channel attack, timing attack, ATM skimmer, Social Engineering.

DDOS, Syn flood, WPA, SSL, Wireshark, Spoofing, Sniffing, Poisoning, Public Key Infrastructure, Digital Signature, RSA, Certificate, Tor.

Input validation, SQL injection, Secure Programming, buffer overflow, Stack smashing, Integer Overflow, TOCTOU, CVE.

Key-logger, virus, worm, rootkit, botnet.

Access Control List, Capability, rwx, superuser, root, Least Privileges, Privilege escalation, Reference Monitor.

Completed Lectures

Lecture 1: Encryption

Security requirements, encryption/cryptography, key length, IV, Kerckhoffs's principle

Lecture 2: Authentication (weak)

Password, 2FA, confidentiality $\not\Rightarrow$ integrity, phishing

Lecture 3: Authentication (strong)

PKC, hash, MAC, signature, birthday paradox, strong authentication

Lecture 4: PKI, SSL

PKI, signature, certificate, CA, authentication protocol, key exchange, SSL/TLS

Lecture 5: Network Security

Layering, naming issue (DNS attack), DDoS, firewall

Lecture 6: Access Control

Access control matrix, UNIX access control, privilege escalation

Lecture 7 : Secure Programming (I)

Background on computer architecture, call stack, format string vulnerability

Lecture 8 : Secure Programming (II)

Various pitfalls, data representation, buffer overflow, integer overflow

Lecture 9 : Secure Programming (III)

Android security, TOCTOU, problem with scripting languages, counter measures

Lecture 10: Web Security

Completed Tutorials

- **Tutorial 1: Introduction & encryption**

  Security requirement, key length requirement, tradeoff of usability & security
- **Tutorial 2: Encryption & password**

  Password, security questions, 2FA, role of IV
- **Tutorial 3: Data-origin authentication**

  Birthday attack, hash, secure random number generation, implementation issue on secret key generation (which illustrates that hash doesn't produce truly random sequence)
- **Tutorial 4: PKI, SSL and Birthday attack variant**

  PKI, proxy-re-encryption, limitation of PKI, variant of birthday attack
- **Tutorial 5: Security protocol - renegotiation attack on SSL/TLS**

  SSL/TLS, re-negotiation attack (which illustrates subtlety of protocol design)
- **Mid-term quiz discussion**
- **Tutorial 6: Network security + access control**

  Firewall design (2-firewall setting, DMZ), access control (using LumiNUS as an example)
- **Tutorial 7: Privilege escalation**

  SetUID, privilege escalation, how programming bug leads to security vulnerability
- **Tutorial 8: Software security**

  Format string & buffer overflow vulnerabilities, safe/unsafe C functions, integer overflow
- **Group presentations (2 sessions)**

Assignments: CTF Style

- For hacking-challenge ***gamification***: phased hint releases, possible task-completion dependency, etc.
- For **automated** challenge-submission **marking**: real-time and scalable checking of submission attempts, *mark scoreboard*
- Assignment 1:
  Cryptography, authentication
- Assignment 2:
  Network, software and web security
- Additional **online quiz assessment** via LumiNUS:
  for overall material review and final-exam practice

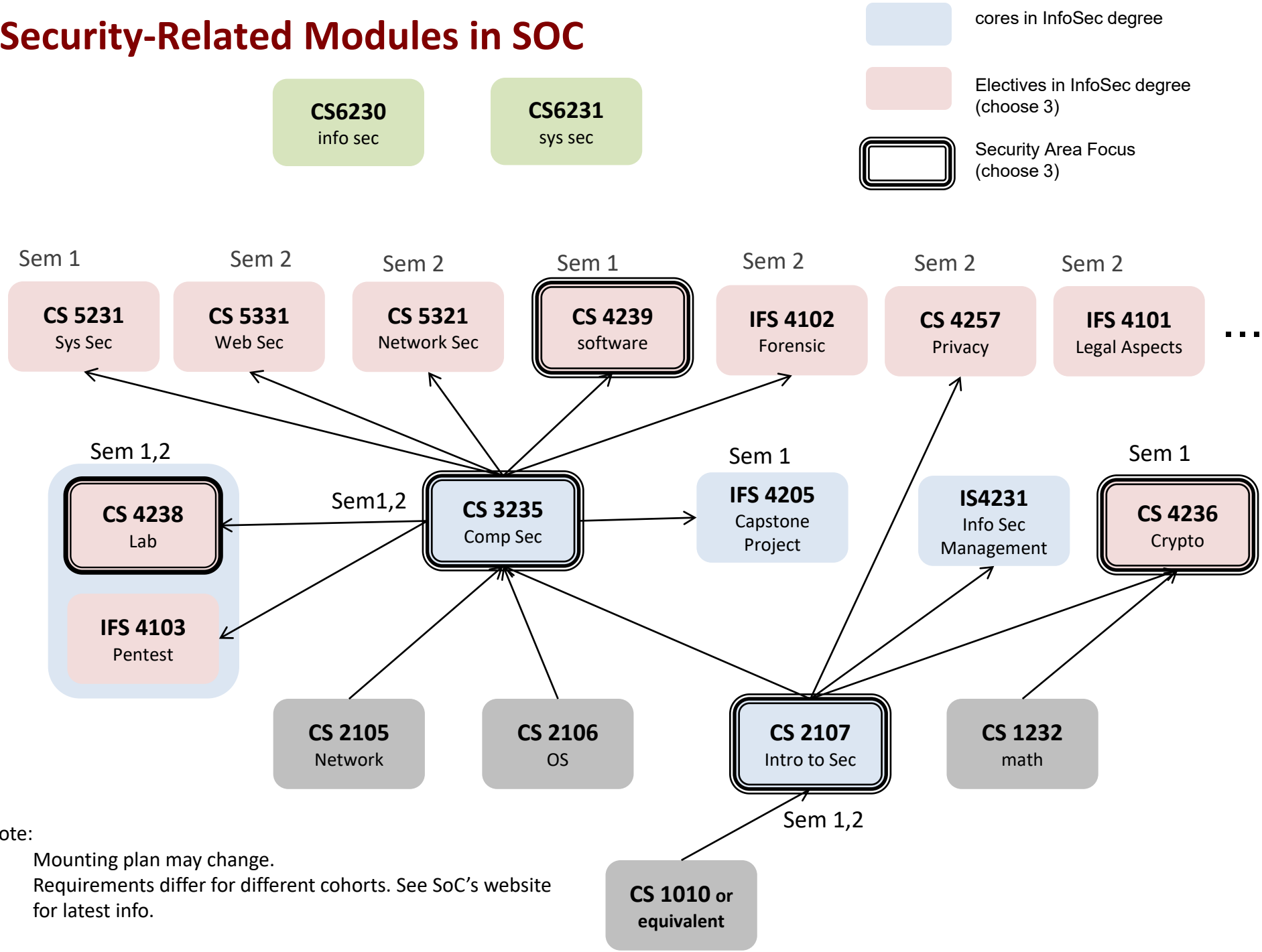
Ethical Use of Security Information

- We have discussed **vulnerabilities and attacks**
- Most vulnerabilities have been fixed, ***but***:
  - **Do not** assume that all systems are patched/fixed
  - **Some attacks** may still cause harm!
- Purpose of our security modules:
  - Learn to prevent malicious **attacks**
  - Use your knowledge for **good** purposes

Hacking: It's Fun, Don't Cross the Yellow Line

Next Steps

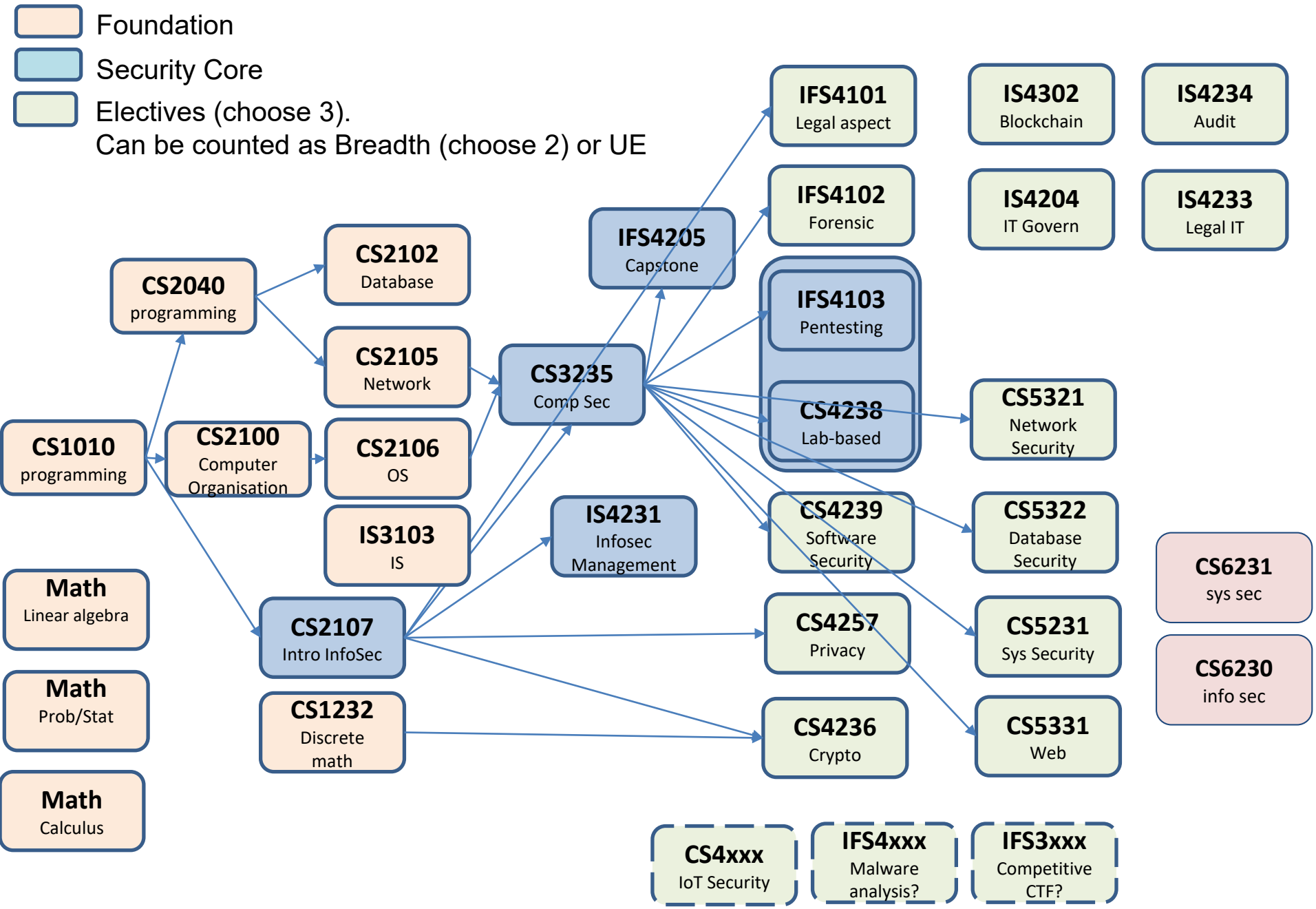
Security-Related Modules in SOC

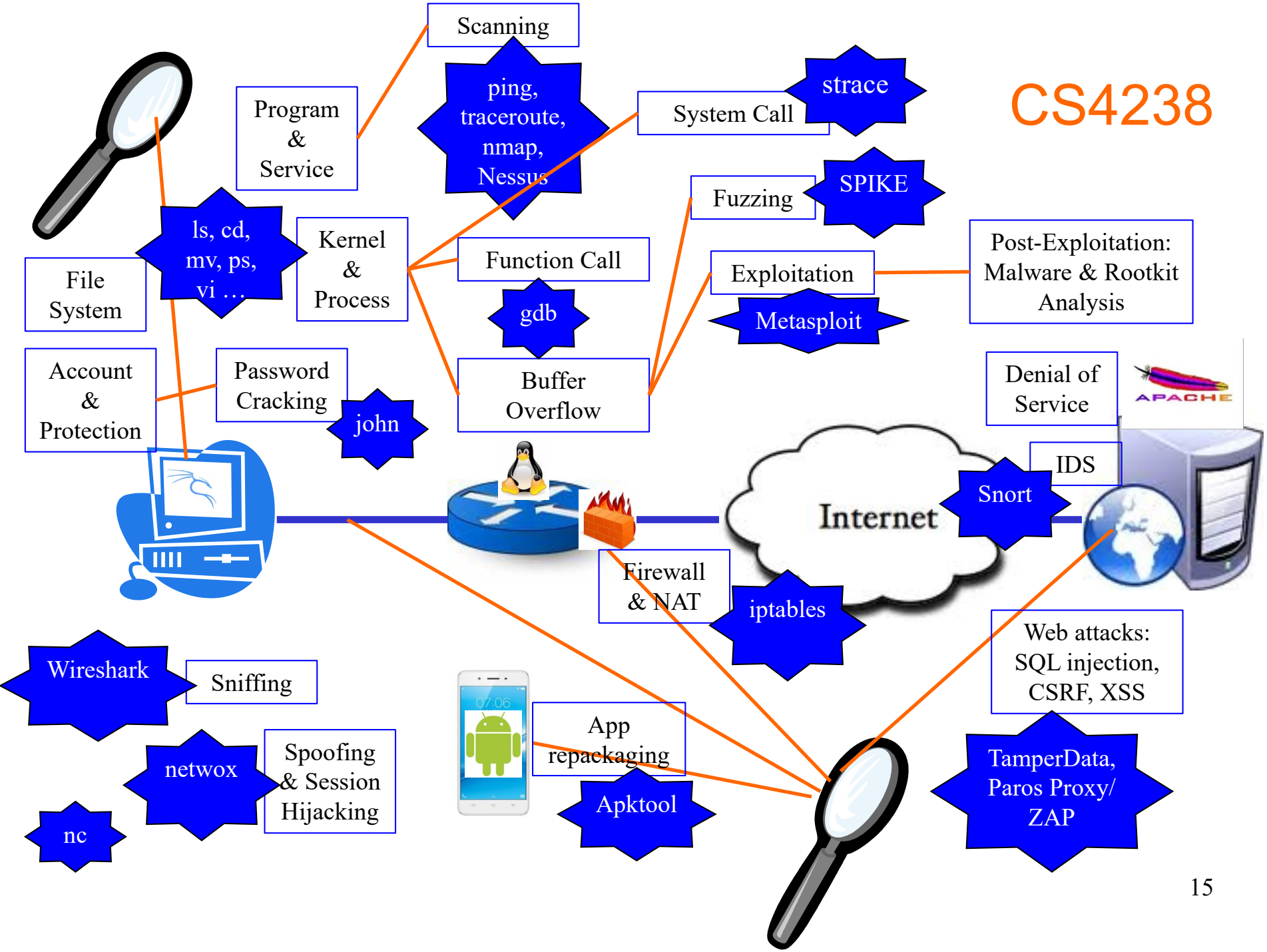


Note:

1. Mounting plan may change.
2. Requirements differ for different cohorts. See SoC's website for latest info.

Security-Related Modules and BCOMP InfoSec Requirements




CS4238
Scanning
ping, traceroute, nmap, Nessus
Program & Service
System Call
strace
Fuzzing
SPIKE
Post-Exploitation: Malware & Rootkit Analysis
File System
ls, cd, mv, ps, vi …
Kernel & Process
Function Call
gdb
Exploitation
Metasploit
Account & Protection
Password Cracking
john
Buffer Overflow
Denial of Service
APACHE
IDS
Snort
Internet
Firewall & NAT
iptables
Wireshark
Sniffing
Web attacks: SQL injection, CSRF, XSS
App repackaging
Apktool
netwox
Spoofing & Session Hijacking
nc
TamperData, Paros Proxy/ ZAP

Recent News Items (Oct 2016)

NUS, Singtel launch $43 million cyber security laboratory

The NUS-Singtel Cyber Security Research and Development Laboratory, hosted by the NUS School of Computing, is the 10th laboratory supported under the Laboratory@University scheme by the NRF. PHOTO: ST FILE

PUBLISHED 3 HOURS AGO | UPDATED 1 HOUR AGO

Irene Tham Tech Editor (mailto:itham@sph.com.sg)

The Straits Times, Oct 24, 2016

Recent News Items (2017)

www.channelnewsasia.com/news/singapore/singapore-to-set-up-new-defer

Menu

Singapore to set up new Defence Cyber Organisation

National servicemen could also be selected for cyberdefence vocations as the army seeks to bolster itself against infocomm threats.

Posted 03 Mar 2017 12:44 **Updated** 03 Mar 2017 22:32

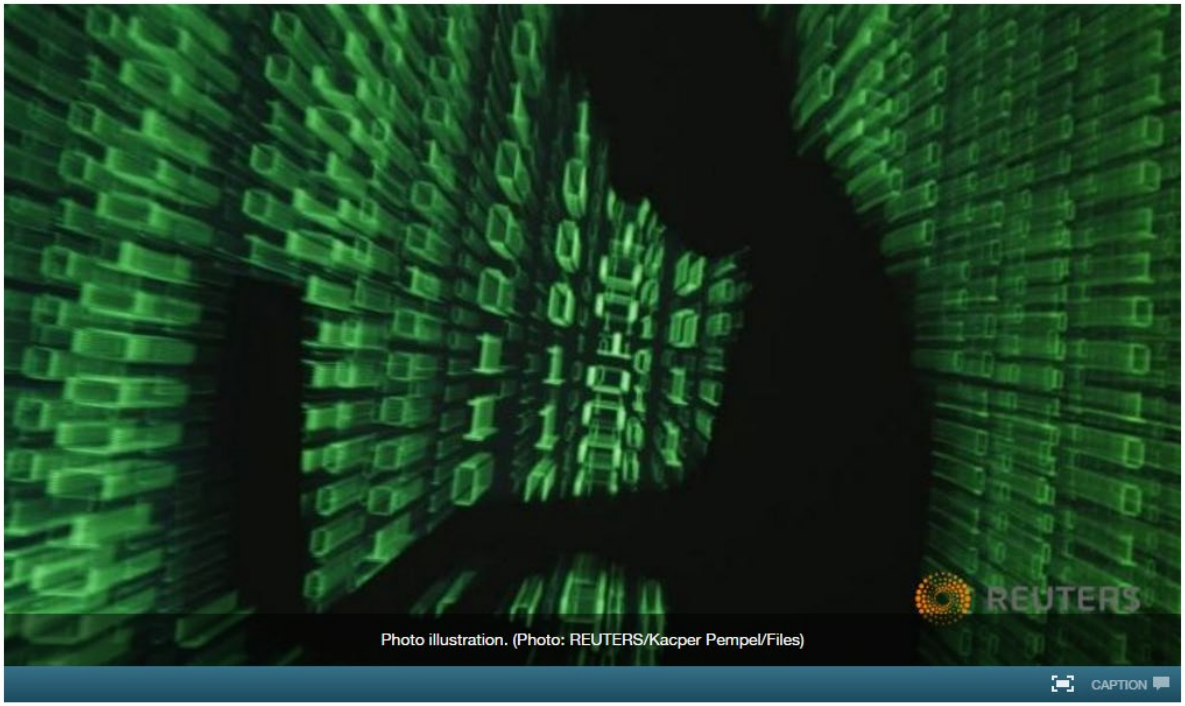


Photo illustration. (Photo: REUTERS/Kacper Pempel/Files)

CAPTION

1087 Email More A A

SINGAPORE: A new Defence Cyber Organisation (DCO) will be set up to monitor and defend the Singapore Armed Forces' (SAF) networks around-the-clock from cyberthreats, Defence Minister Ng Eng Hen announced in Parliament on Friday (Mar 3).

Channel News Asia, Mar 3, 2017

Recent News Items (2017)

www.channelnewsasia.com/news/singapore/singapore-to-set-up-new-defer

Menu

The Cyber Defence Group consists of a security monitoring unit, an incident response and audit unit as well as the Cyber Defence Test and Evaluation Centre (CyTEC). Opened in 2015, CyTEC facilitates network security testing and conducts training, among others.

WANTED: CYBERDEFENDERS

The SAF has also created a new cyberdefence vocation for both full-time and operationally ready national servicemen. Those who have demonstrated their abilities at cyber competitions, as well as those currently working in the cybersecurity industry, may also be selected and identified to be "cyberdefenders".

"Our cyberdefenders will need to possess a high level of skill given the increasing frequency and complexity of cyberattacks," said Second Minister for Defence Ong Ye Kung. "They will be entering a very selective and demanding vocation, comparable to the commandos or naval divers."

In their vocation, which will be implemented from August, they are expected to perform roles such as monitoring networks and systems, responding to incidents and forensic analysis. As a pilot project, they may also be deployed to support the Cyber Security Agency to defend critical information infrastructure supporting Singapore's key networks.

MINDEF also announced that the Headquarters Signals and Command Systems, which includes the SAF training institute for cyberdefence, will sign a memorandum of understanding with Singapore Technologies Electronics (Info-Security) and Nanyang Polytechnic this month.

- CNA/jo

1087 Email More

Channel News Asia, Mar 3, 2017

Recent News Items (Oct 2016)

THE STRAITS TIMES

Strengthening our cyber defences

Cyber security = job security for Singapore grads

From left: Mr Ang Yihan, 25, Mr Winwin Lim, 26, Mr Ian Yeo, 28, Mr Kelvin Tan, 28, and Mr Lee Wei Yan, 27, at the Kaspersky Lab headquarters in Moscow. The fresh graduates were in Russia for a one-year IT security attachment and training programme. PHOTO: KASPERSKY LAB

PUBLISHED OCT 23, 2016, 5:00 AM SGT

From Singapore to Moscow, such is the demand for professionals in this sector that the sky's the limit

The Straits Times, Oct 23, 2016

The Rest of the Semester:
Final Exam

Final Exam

- Open book, **2** hours, NUS approved calculators, total: **50** marks
- Saturday, 23 Nov morning (*please double-check time & venue again!*)
- **Format**:
  - Q1: Terminology (10 marks)
  - Q2: MCQs (10 marks)
  - Q3: Short answer questions (10 marks): answer in 2-3 sentences or with a diagram
  - Q4: Scenario-based questions (20 marks)
- **Covered materials**: all lectures and tutorials, which also include:
  - Cryptography
  - Authentication
  - Network security
  - Firewall design
  - Access control
  - Secure programming
  - Web security

NATIONAL UNIVERSITY OF SINGAPORE

CS2107 — INTRODUCTION TO INFORMATION SECURITY

(Semester 1: AY2019/20)

Time Allowed: 2 Hours

INSTRUCTIONS TO STUDENTS

1. Please write your Student Number only. Do not write your name.
2. This assessment paper contains **FOUR** questions and comprises **SIXTEEN** printed pages.
3. Answer **ALL** questions.
4. Write your answer within the given box in each question on this question paper.
5. This is an **OPEN BOOK** assessment.
6. You may use **NUS APPROVED CALCULATORS**.
   Nonetheless, you should be able to work out the answers without using a calculator.

Student Number: _ _ _ _ _ _ _ _ _

This portion is for examiner's use only:

Question	Full Marks	Marks	Remarks
Q1	10		
Q2	10		
Q3	10		
Q4	20		
Total	50		

Thanks!
(And Please Congratulate Yourself Too!)