CS2107 Review, Singapore Cyber Landscape, and Final Exam Tips

Teaching Mode

- **13** Lectures
- **9** Tutorials (+ 2 sessions for Group presentation)
- **11** Self-exploration activities (self-exercised mini *labs*)

- Continual Assessment (55%):
  - 2 Assignments (25%): *Do submit **A2** before its deadline*
  - 1 Mid-term quiz (15%)
  - 1 Group presentation on open-ended topic (5%)
  - Tutorial attendance (5%)
  - 1 **LumiNUS Quiz** assessment (5%): *before its hard deadline*
- **Final E-exam (45%)**: Open-book, **Wednesday, 1 Dec 09:00-11:00**

  Please *double-check* the timing 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 secure channel
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 (ILO)

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

Some of the Terms Encountered in This Module

Alice, Bob, Eve, Encryption, Decryption, Key-space, Known-plaintext attack, Ciphertext-only attack, Confidentiality, Integrity, Availability, Authenticity, Passwords, Random IV, Multi-factor authentication, Kerckhoff's principle

Digital signature, RSA, Certificate, Public Key Infrastructure, Authentication protocol, Secure channel, SSL, HTTPS, WPA, Wireshark

Dictionary attack, Side-channel attack, Timing attack, Key logger, ATM skimmer, Social engineering attack, Man-in-the-middle attack

DDOS, Syn flood, Botnet, Spoofing, Sniffing, Poisoning

Access Control List, Capabilities, UNIX's rwx permission triplet, superuser, root, Least privilege, Privilege escalation, Reference monitor

Web cookies, Same-Origin Policy, Session ID

Virus, Worm, Rootkit, Cross Site Scripting attack, Cross Site Request Forgery

Input validation, SQL injection, Secure programming, Buffer overflow, Stack smashing, Integer overflow, CVE

Completed Lectures

Lecture 1: Encryption *(a big **multi-part** lecture)*

Security requirements, encryption/cryptography (classical ciphers, stream cipher, block ciphers) & attacks, key length, IV, Kerckhoffs' principle

Lecture 2: Authentication (Password/weak)

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

Lecture 3: Authenticity (MAC & Signature)

PKC, hash, MAC, signature, birthday paradox

Lecture 4: PKI + Channel Security

PKI, certificate, CA, hierarchical trust relationship

Lecture 5 : Secure Channel, TLS/SSL, Crypto Misc.

Strong authentication, key exchange & authenticated key exchange, SSL/TLS, authenticated encryption

Lecture 6: Network Security

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

Lecture 7: Access Control

Access control model, Linux/UNIX access control, privilege elevation

Lecture 8: Web Security

Web security issues & threat models, TLS/SSL issues, UI attacks, cookies & SOP, XSS, CSRF

Lecture 9 : Software Security

Background on computer architecture, call stack, integer overflow, data representation issue, buffer overflow, security problem with scripting languages, counter measures

Completed Tutorials

Tutorial 1: Introduction & Encryption

Security requirement, key length requirement, role of IV, tradeoff of usability & security

Tutorial 2: Encryption & Block Cipher

Block size, mode-of-operation, DES insecure usage, 3DES

Tutorial 3: Encryption & Password

Password, security questions, 2FA

Tutorial 4: 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 5: PKI, SSL and Birthday Attack Variant

PKI, proxy-re-encryption, limitation of PKI, variant of birthday attack

Mid-term quiz discussion

Tutorial 6: Security Protocol - TLS and Its Renegotiation Attack

SSL/TLS, re-negotiation attack (which illustrates subtlety of protocol design)

Tutorial 7: Network Security + Privilege Escalation

Firewall rules (2-firewall setting, DMZ), setUID, privilege escalation

Tutorial 8: Software Security

Buffer overflow vulnerabilities, safe/unsafe C functions, integer overflow

Group project presentations (last 2 sessions)

Shared Self-Exploration Activities

Activity 1: Introduction, Classical ciphers

A look at malicious-executable creation difficulty in practice, substitution cipher cracking scripts

Activity 2: Classical ciphers & attacks

Scripts that implement & attack Shift/Caesar cipher, Vigenere cipher, One-Time Pad

Activity 3: Block ciphers, Pseudo-random numbers

OpenSSL for encryptions using block ciphers & modes-of-operation, pseudorandom numbers in Linux/UNIX

Activity 4: Authentication (Password)

Password & shadow files, password cracking using John the Ripper

Activity 5 : Authenticity (MAC & Signature)

OpenSSL for hash & MAC, SHA-1 collision attacks, RSA encryption scheme

Activity 6: PKI

Browser-reported certificate problems, Openssl for public-key pair generation, certificate inspection, RSA

Activity 7: TLS/SSL

Openssl for TLS/SSL connection, TLS server configuration & certificate, TLS server & client check

Activity 8 : Network security

Wireshark, Nmap

Activity 9: Access Control

Linux access control

Activity 10: Web Security

OS command injection, SQL Injection, XSS, bypassing anti-XSS input-sanitization

Activity 11: Buffer Overflow Vulnerability & Exploitation

Assignments: CTF Style

- For ***gamification*** of hacking challenges: phased hint releases, possible task-completion dependency, etc.
- For **automated** challenge-submission **marking**:
  real-time & 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
- Remember again:
  Computer Misuse and Cybersecurity Act (CMCA)
- Please **observe the prevailing law**

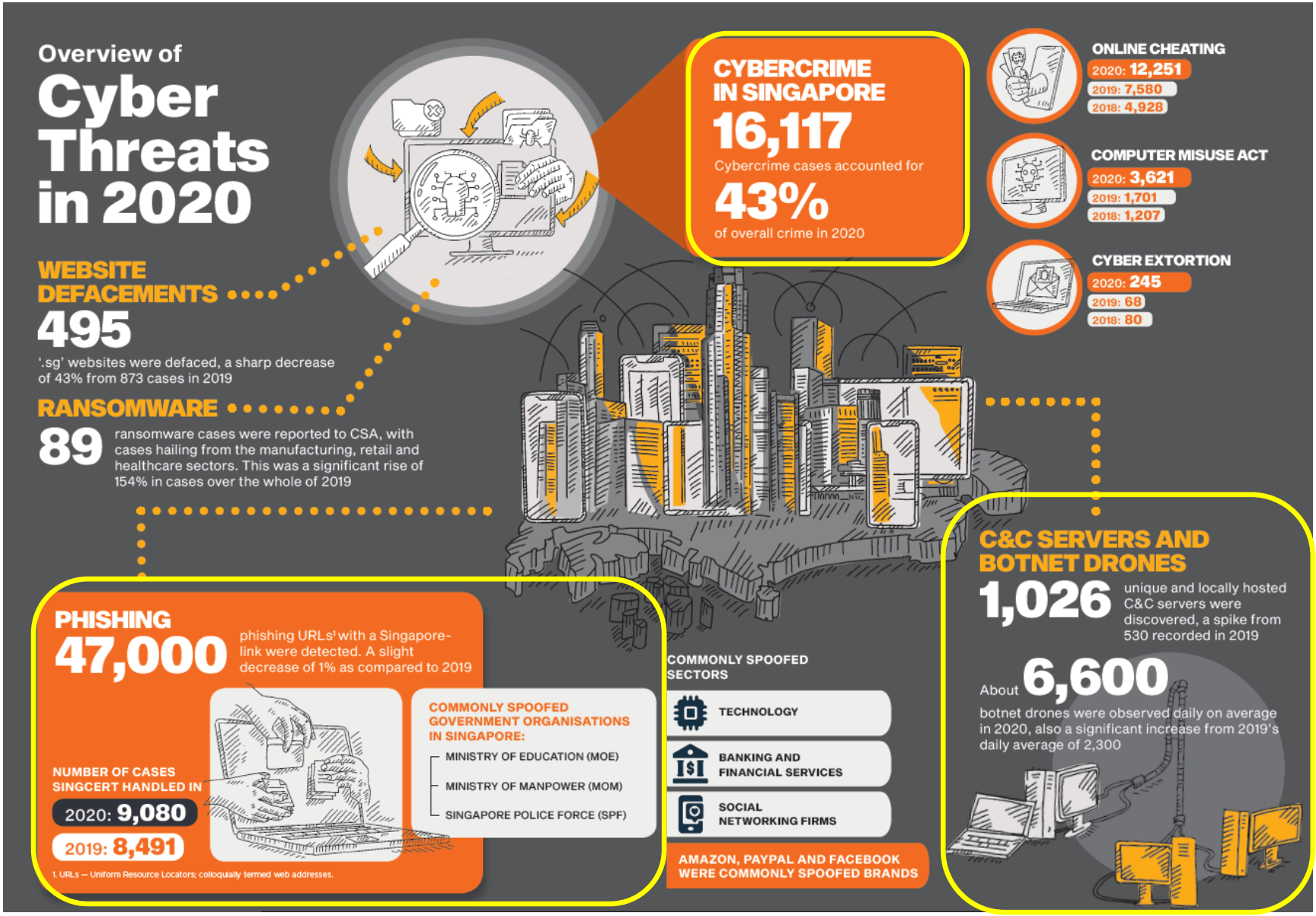
Hacking: It's Fun, ***Do not*** Cross the Yellow/Red Line

Singapore Cyber Landscape

Singapore Cyber Landscape 2020

- Annual snapshot of **cyber landscape** in Singapore
- "***Singapore Cyber Landscape 2020***",
  by Cyber Security Agency of Singapore, July 2021:
  - Spotlight on cyber threats
  - WWW.TARGET.SG
  - A retrospective look
  - Looking back to look forward
- See:
  https://www.csa.gov.sg/news/publications/singapore-cyber-landscape-2020

Cyber Threats in 2020

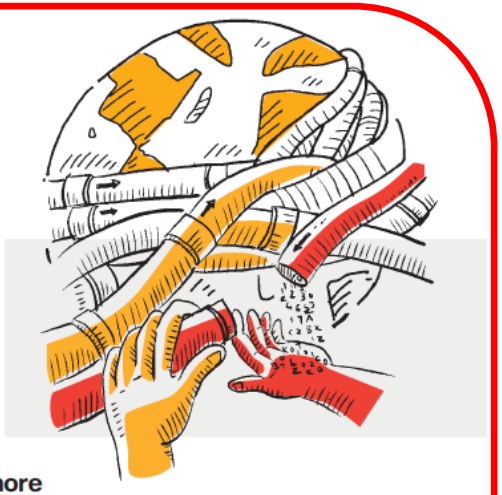


Cyber Threats in 2020

Local Case Studies

This section features selected case studies of companies and individuals that were compromised by various cyber threats, and lessons that can potentially avoid a recurrence.

SolarWinds Supply-chain Breach



A Global Storm Blows Ashore

What Happened?

The interdependencies of the global technology supply chain meant that local systems were not spared the fallout from the SolarWinds breach. On 23 December 2020, a local organisation was observed to have been affected by the SolarWinds breach. One of the affected organisation's IT systems – which had SolarWinds *Orion* installed – had downloaded the infected update and thus became exposed to the malware. However, the hackers were subsequently found to have "deactivated"[20] the malware, possibly indicating that they were not interested in the organisation.

Follow-up Action

CSA investigated the incident and advised the company on the proper remediation measures, including scanning for related Indicators of Compromise (IOCs) and running anti-virus scans on all systems. No further suspicious activities, malicious processes or signs of intrusion were found.

20. Deactivated mode is when the malware has been disabled and will no longer perform any network activity.

Ransomware Incidents in Small and Medium Enterprises

Putting All Your Eggs in One Basket

What Happened?

In August 2020, staff from an F&B business discovered that their company servers and devices were infected with *NetWalker*, a prevalent ransomware strain. The ransom note instructed the victim to visit a webpage on the Dark Web to view the ransom demands. As the company had also stored its backups on the affected servers, none of its data could be recovered.

Follow-up Action

A report was made to the Singapore Police Force (SPF), and the company was also given a list of cybersecurity companies to assist in remediation efforts. However, as both primary and backup systems were affected by the ransomware, the company was unable to recover its data and had to rebuild its IT system from scratch.

Backing Up Instead of Backing Down

What Happened?

In September 2020, a creative firm suffered a ransomware infection resulting in the complete shutdown of three database servers, as well as the encryption of files within these servers. None of its data was observed to have been stolen. The ransomware involved, called *JungleSec*, was first discovered in late 2018 and is rarely observed in Singapore. It is known to infect servers through Intelligent Platform Management Interface (IPMI)[21] cards.

Follow-up Action

All three database servers were taken down and reformatted immediately after the incident. The databases were rebuilt from a backup from the previous day. The database servers as well as their IPMI interfaces, including the unaffected ones, were isolated and access was further tightened. A cybersecurity firm was engaged to assist with containment measures, review the company's data protection policies and processes, and conduct vulnerability assessment and penetration testing.

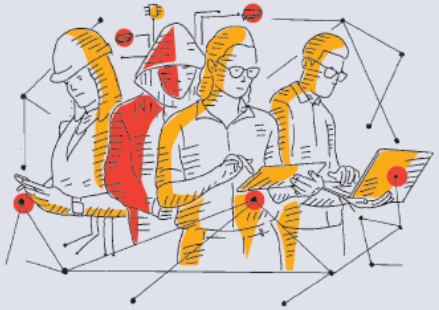
TAKEAWAYS

Prevention is key to avoid falling victim to ransomware. Organisations need to put in place strong preventive measures to secure their systems. These include measures such as formulating a backup and recovery plan, performing data backups regularly, storing data offline and not connected to the organisation's network as certain ransomware variants can propagate across the network.

21. IPMI is a set of computer interface specifications which are built into server motherboards or installed as an add-on card and allows remote administration of a computer.

Cybersecurity Trends to Watch

If he had left the breach to the IT department instead, this cyber-attack could have had serious consequences to public health. On the other hand, if it is true as alleged that SolarWinds was breached with the help of a default password "solarwinds123" which had been left unchanged for two years, then that lack of vigilance is unacceptable. Vigilance includes timely patching of vulnerabilities once they are disclosed, such as those in Microsoft Exchange Server. The importance of patching known vulnerabilities is one of the lessons we should have learned from the SingHealth data breach of 2018.



Vigilance is also needed in ensuring cybersecurity for Singapore's many impressive and visionary digital transformation projects, such as autonomous vehicles, autonomous delivery robots, e-payments for hawkers, personal learning devices for students, blockchain projects, and artificial intelligence projects. These can only be secured through effective communication and cooperation among project owners, regulators, cybersecurity experts, and end users.

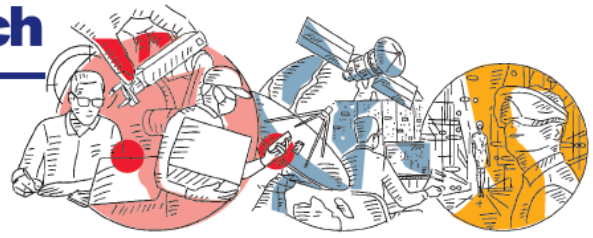
Fortifying Digital Defences for Our Future

Further, the call to digitally transform Singapore essentially means that data will be central to how our lives are lived. We will increasingly use data to fuel the decisions we make on a daily basis. Governments and businesses rely on it for managing society and making business and economic decisions. Data is the bounty that cybercriminals, state-sponsored actors, and hacktivists seek. Despite the enormous role it plays, it is an ongoing struggle to secure it. As a city is only as structurally secure as the foundations upon which it is built, so too is a networked infocommunication framework functioning off data sources and repositories. The proposition for coherent cybersecurity protection may be in deeming the data industry sector as a foundational critical information infrastructure, allowing it to be more stringently regulated. With this, we could work towards comprehensive data security and enforce transparency in and accountability for data use and management – all players and stakeholders in the public and private sectors will be required to coordinate and collaborate in bolstering cybersecurity measures for data protection.

Finally, the messaging around the notion of "digital transformation" and becoming a Smart Nation must change across the landscape. It must communicate holistically the strengths, weaknesses, opportunities, and threats involved in this enterprise, and it must be an ongoing process. It must reflect the sobering imperatives of engaged cybersecurity practice, in lockstep with the promises of a brilliant future with the benefits of digitalisation. In practice, this translates to requiring active cybersecurity practice in the context of empowering digital transformation. This messaging must be owned by, passed on, and acted upon within our cybersecurity landscape – because in reality, the landscape is all of us. Hopefully, future editions of the SCL will be able to reflect such transformation.

LOOKING BACK TO LOOK FORWARD

Cybersecurity Trends to Watch



NEAR TERM
Risk of Remote Workforce, Increased Risk of Supply-chain Attacks and the Ransomware Threat

MEDIUM TERM
Cybersecurity of Space Infrastructure

LONG TERM
Hyper-Connectivity and the Metaverse

NEAR TERM: Risk of Remote Workforce

What Is It?

Social distancing measures during the COVID-19 pandemic have led to the rapid adoption of remote working. Overnight, many organisations had to implement new processes and systems to facilitate business continuity. Threat actors were quick to capitalise on this expanded – and often more vulnerable – attack surface brought about by these new work-from-home ecosystems.

Why Does It Matter?

Remote working is here to stay, even after the pandemic. It has become an increasingly attractive alternative to working from the office[41]. Companies have found that remote working reduces overheads, without reducing employee efficiency.

Poorly configured network and software systems to facilitate remote work can expose organisations to greater risk of cyber-attacks. Defending the infrastructure needed to sustain a large remote workforce against malicious threat actors will present a daunting challenge for organisations moving forward.

NEAR TERM: Increased Risk of Supply-chain Attacks

What Is It?

Organisations often rely on vendors, such as technology firms and managed service providers, for products and services to support their business operations. Cyber threat actors have exploited such interdependencies to carry out supply-chain attacks. Supply-chain attacks involve targeting an organisation by exploiting weak links and trusted relationships in the supply network.

Why Does It Matter?

A successful breach in the supply chain, as seen in the SolarWinds incident, provides cyber threat actors a single pivoting point to multiple victims. The compromise of a trusted supplier – or a popular and widely-used product – can result in massive and widespread

41. The Straits Times article published on 24 March 2021 said that 9 in 10 employees in Singapore wanted to continue working from home for reasons such as flexibility and cost savings.

Singapore's Safer Cyberspace Masterplan 2020

- "***Singapore's Safer Cyberspace Masterplan***",
  Cyber Security Agency of Singapore, 2020,
  https://www.csa.gov.sg/news/press-releases/safer-cyberspace-masterplan-launch

- From its **executive summary**:
  "As Singapore embarks on its digital transformation toward a **Smart Nation and Digital Economy**, Singaporeans and our enterprises will also face **increasing cyber threats** as more of our citizens and businesses go online. **Cybersecurity** will be a **critical enabler** of our push toward digitalisation. Without **robust cybersecurity** in place, our systems and networks remain open and vulnerable for malicious threat actors to exploit our digital assets and data."

- It comprises the following ***three thrusts***:
  - Securing our core digital **infrastructure**
  - Safeguarding our cyberspace **activities**
  - Empowering our **cyber-savvy population**

Safer Cyberspace Masterplan 2020: Why?

Prevention — Better than cure?

With technology touching all parts of our lives today, cybercriminals have many opportunities to make a quick buck. What if we could make it more difficult for threat actors to commit malicious cyber activities in the first place, and can swiftly detect and respond to an incident after it happens? This is the approach of the Masterplan, which focuses on upstream measures to prevent and detect malicious cyber activities.

An analogy from the physical world parallel to cyberspace would be preventive healthcare. Doctors advocate a healthy lifestyle and regular health screening in order to nip diseases in the bud before they become severe. The cyber equivalent of preventive health needs to be implemented, to better protect Singapore and Singaporeans in the digital domain. While there will inevitably be events that we cannot foresee in the cyber and the health domains, taking early preventive measures will avoid a vast majority of unpleasant and costly events from happening later on. In addition, just as how we are encouraged to go for regular health check-ups to detect the onset of health conditions early, we want to adopt the cyber equivalent of detecting and responding to malicious cyber activities swiftly when they arise.

The analogy further extends to the roles of the Government, community, enterprises and the public. To encourage good preventive health habits, the Government puts in place community exercise corners and works with the food industry to reduce the amount of sugar in our food products, to make it easier for individuals to adopt a healthy lifestyle. Yet individuals continue to bear the responsibility to exercise and consume food and beverages with healthier food labels.

This is parallel to cybersecurity — the Government will put in place upstream measures to make it more difficult for actors to conduct malicious cyber activities on us, but the community, enterprises and individuals must continue to take personal responsibility for their safety and security in the digital domain.

Singapore is highly dependent on the digital domain for business and our daily lives

98%

Households with Internet access[1]

6H 48M Daily time spent online[2]

94% Business Broadband Adoption[3]

SGD 37 BILLION
(USD 27 BILLION)
Singapore's estimated Internet Economy in 2025[4]

While the initiatives in the Masterplan will make our cyberspace more secure over time, it is unrealistic to expect that all malicious cyber activities can be prevented. With the contours of cyberspace constantly changing, new threats will emerge, and unknown vulnerabilities will be found. The Government will play its part to support a safe and secure cyberspace, but the community, enterprises and individuals need to remain vigilant in cyberspace and continue adopting practices to keep themselves safe and secure online. Ensuring the cybersecurity of our digital assets and data is our collective responsibility.

Individuals and businesses remain exposed to malicious cyber activities

28% of Singaporeans surveyed said they were victim to at least one cyber incident in 2019[5]

Almost 2 in 5 of all cyber incidents in Singapore target SMEs[6]

SGD 18.9 MILLION
(USD 13.8 MILLION)
is the estimated loss to a large enterprise from a cyber-attack. The average cost to a medium-sized enterprise is $26,000.[7]

58%

of enterprises that use the Internet for work have no cybersecurity measures[8]

[1] Infocomm Media Development Authority. "Annual Survey on Infocomm Usage in Households and by Individuals for 2019", 2019, https://www.imda.gov.sg/-/media/imda/files/research-and-statistics/survey-report/2019-hh-public-report_09032020.pdf
[2] We are Social. "Digital 2020 Singapore", 12 February 2020, https://wearesocial.com/sg/digital-2020/singapore
[3] Infocomm Media Development Authority. "Annual Survey on Infocomm Usage by Enterprises for 2019", 2019, https://www.imda.gov.sg/-/media/imda/files/industry-development/fact-and-figures/infocomm-usage-business/infocomm-usage-survey-public-report-2019.pdf
[4] Google & Temasek / Bain. "e-Conomy SEA 2019", 3 Oct 2019. https://blog.google/documents/47/SEA_Internet_Economy_Report_2019.pdf
[5] Cyber Security Agency of Singapore. "CSA Public Awareness Survey 2019", 21 August 2020, https://www.csa.gov.sg/news/press-releases/csa-public-awareness- survey-2019
[6] Cyber Security Agency of Singapore. "Singapore Cyber Landscape 2017", 19 June 2018, https://www.csa.gov.sg/news/publications/singapore-cyber-landscape-2018
[7] Frost Sullivan. "Understanding the Cybersecurity Threat Landscape in Asia Pacific: Securing the Modern Enterprise in a Digital World", 17 May 2018, https://news.microsoft.com/apac/2018/09/18/cybersecurity-threats-to-cost-organizations-in-asia-pacific-us1-75-trillion-in-economic-losses/
[8] Infocomm Media Development Authority. "Annual Survey on Infocomm Usage by Enterprises for 2019", 2019, https://www.imda.gov.sg/-/media/imda/files/industry-development/fact-and-figures/infocomm-usage-business/infocomm-usage-survey-public-report-2019.pdf

Safer Cyberspace Masterplan 2020: Threat Actors

WHO ARE WE DEFENDING AND WHAT ARE WE DEFENDING AGAINST?

Since the inception of the Cybersecurity Act in 2018, we have made significant progress in ensuring that our CIIs that support essential services are robustly defended. We are focusing our attention now on developing a more detailed and concrete plan to ensure that other users of our cyberspace are sufficiently defended. These users include ordinary users, enterprises (especially small and medium ones), and organisations. For many of them, the Internet is an inextricable part of their lives and work, but more can and should be done to help ensure that their experience on the Internet is a safer and more secure one. If they are unable to protect or defend themselves against cyber-attacks, many of them may suffer distress or even financial loss. While CSA has conducted extensive outreach and engagement efforts in the past, our survey results suggest that this group remains vulnerable to cyber threats.

In addition, as the level of digital activity increases, the types of malicious cyber threat actors and the methods that they employ have also become more diverse and sophisticated. These actors deploy a variety of tactics to seize control of devices, gain access to personal data, or in severe cases, cause disruption of services. These range from sending phishing e-mails, directing individuals to malicious websites, to deceiving users to download malware-laden software.

Cyber Threat Actors Targeting Singapore and their Motivations

Advanced Persistent Threats (APTs)

APTs operate stealthily and with sophistication, often hiding in networks for prolonged periods to plan their targeted attacks. APTs — which may refer to the type of attack, or the threat actor or group — are also often state-sponsored. Their motivations include disruption of services and operations, espionage to gather privileged information, and financial gain.

Hacktivists

Hacktivism involves hacking (i.e. breaking into a computer system) and defacing webpages to promote a political or ideological message. Online activism through hacking has become an increasingly attractive alternative to conducting physical street protests, as the Internet affords hacktivists anonymity and wider reach.

Cybercriminals

This group of threat actors typically adopt social engineering techniques to lure their victims, predominantly for financial gain. Cases include online cheating, cyber extortion and unauthorised access to computer material and data. The anonymity provided by the Internet and borderless nature of cyberspace allow cybercriminals to operate freely, and law enforcement agencies need to work closely with the public to collectively tackle the scourge of cybercrime.

Safer Cyberspace Masterplan 2020: Conclusion

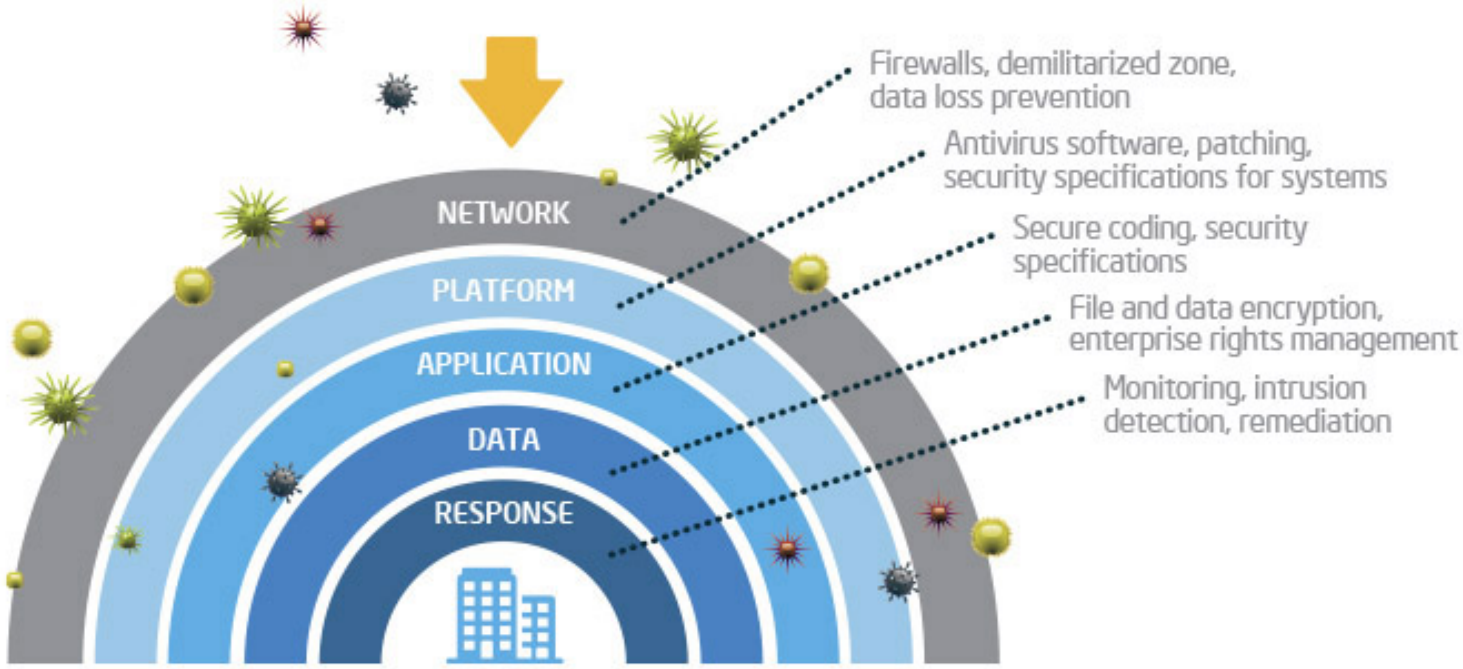
Conclusion

Toward a Safer and More Secure Cyberspace for Singapore and Singaporeans

The Safer Cyberspace Masterplan augments existing efforts to safeguard our Digital Economy and Smart Nation, and protect Singapore's cyberspace against cyber threats.

We want to work toward an inclusive, secure and thriving cyber ecosystem that undergirds digital opportunities and supports national digitalisation efforts. This is a cyberspace that Singaporeans from all walks of life must create and safeguard together to chart our collective digital future.

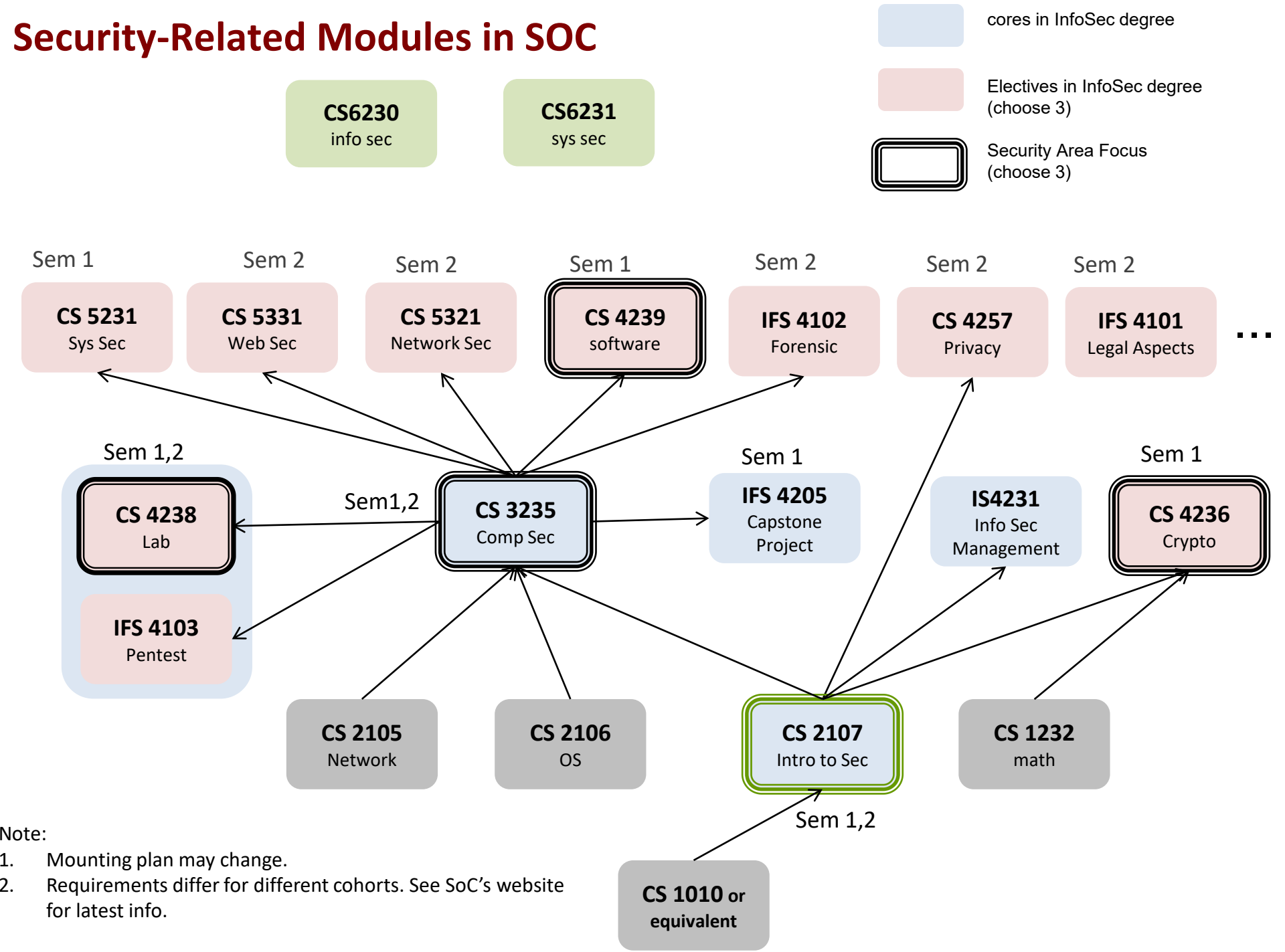
Summary: Layered Defense Approach



From: https://itpeernetwork.intel.com/layered-protection-for-a-mobile-business/

Your Next Steps

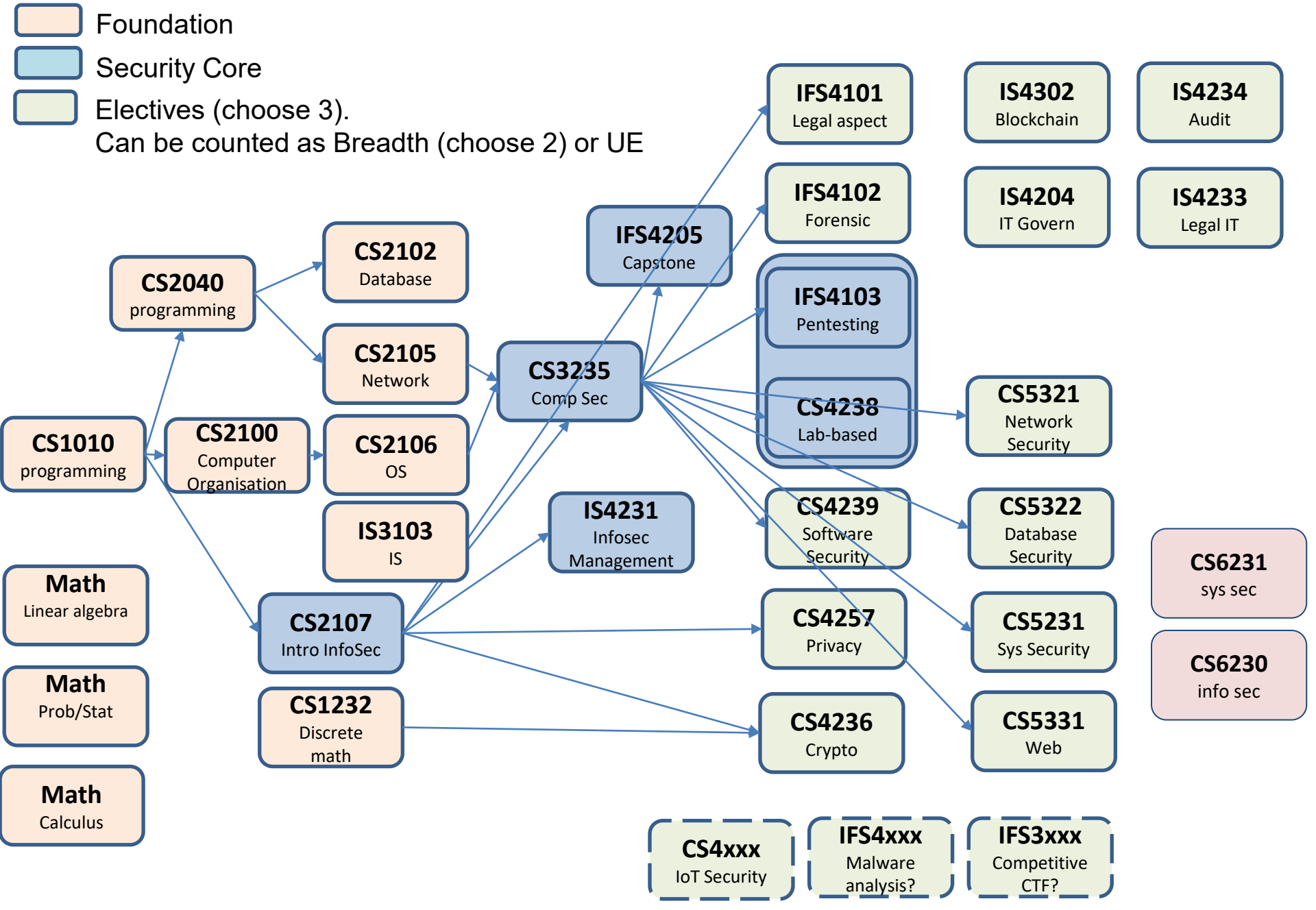
Security-Related Modules in SOC

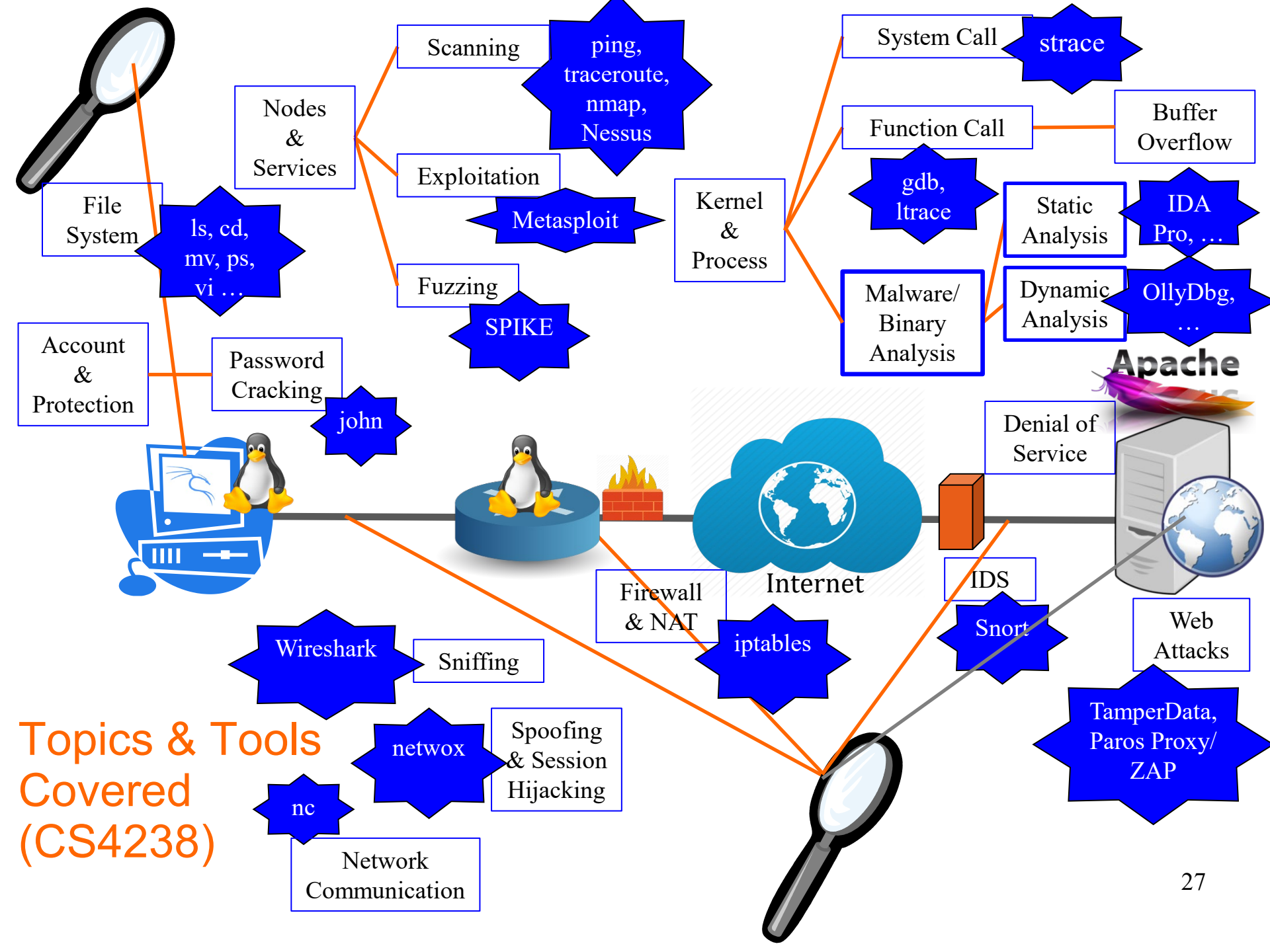


Note:

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

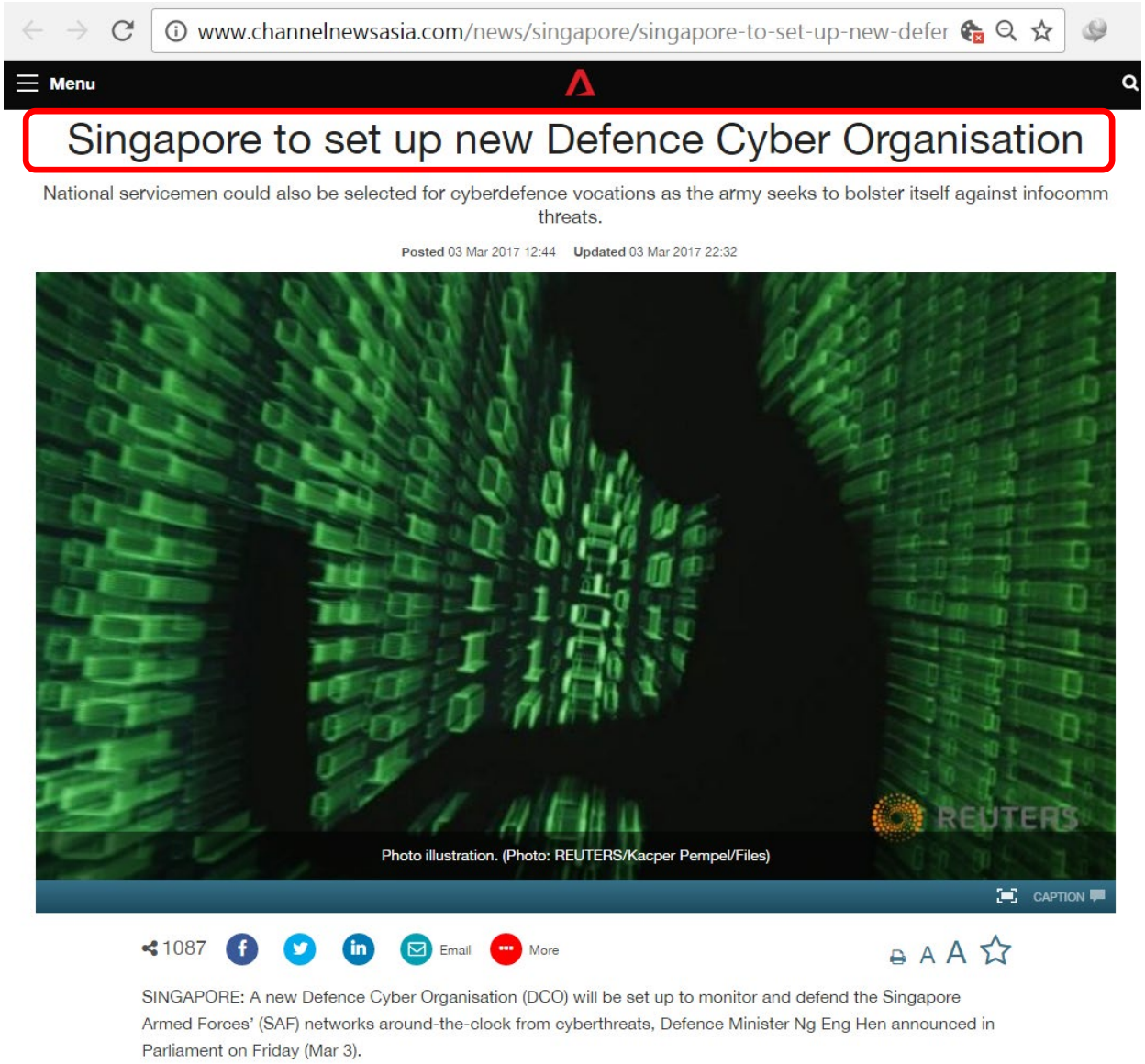
Security-Related Modules and BCOMP InfoSec Requirements





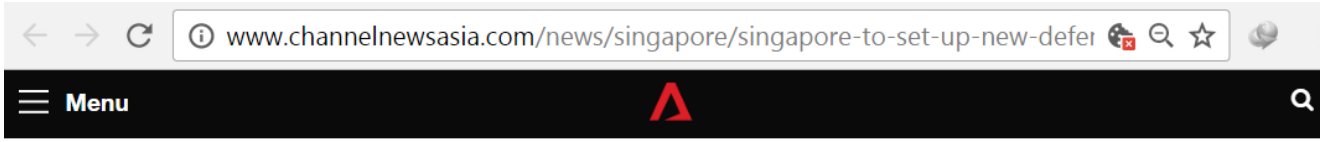
Topics & Tools Covered (CS4238)

Recent News Items (2017)



Channel News Asia, Mar 3, 2017

Recent News Items (2017)



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

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

Our *"Guest Lecturer"*

Mr. Wong Choon Bong,
Cyber Security Agency of Singapore:

"***Cybersecurity: A Growing Sector with Good Jobs***"
(https://www.youtube.com/watch?v=ClPHcBjrz3c)

- *Question: "Why should students explore cybersecurity?"*
- 8 Reasons:
  1. Cybersecurity has gone mainstream
  2. Cybersecurity is a fast-growing sector with good jobs
  3. Cybersecurity is an interesting and diverse field
  4. Together, we can stop the bad guys
  5. Cybersecurity is a national priority
  6. We are developing a vibrant cybersecurity ecosystem
  7. Many education and sponsorship opportunities
  8. Career and skills development pathways

The Rest of the Semester:
Final Exam

Final Exam

- Open book, **2** hours, NUS approved calculators, total: **45** marks
- The same **online e-exam** and **invigilation arrangements**
- **Wednesday, 1 Dec 09:00-11:00 *morning*** (*please double-check the time again!*)
- **Format**:
  - Q1: Security Terminology (10 marks)
  - Q2: MCQs (10 marks)
  - Q3: Structured-based questions (25 marks)
- **Covered materials**: ***all* lectures and tutorials**, which also include:
  - Cryptography
  - Authentication & authentication protocol
  - Network security
  - Firewall rules
  - Access control
  - Web security
  - Secure programming

NATIONAL UNIVERSITY OF SINGAPORE

CS2107 — INTRODUCTION TO INFORMATION SECURITY

(Semester 1: AY2021/22)

Time Allowed: 2 Hours

INSTRUCTIONS TO STUDENTS

1. This assessment paper contains **THREE** questions and comprises **SIXTEEN** printed pages.
2. Answer **ALL** questions.
3. Write your answer within the given box in each question on this question paper.
4. This is an **OPEN BOOK** assessment.
5. 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	25		
Total	45		

Thanks!
(And Please Congratulate Yourself Too!)