CS2107
Introduction to Information Security

Lecture 0

Admin + Overview

0.1 What is CS2107?

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

[Who Need to Take]

- All IT professionals
- Preparation for in-depth studies in cybersecurity

Modular Credits (MCs)

4

Prerequisite(s)

CS1010 or its equivalence

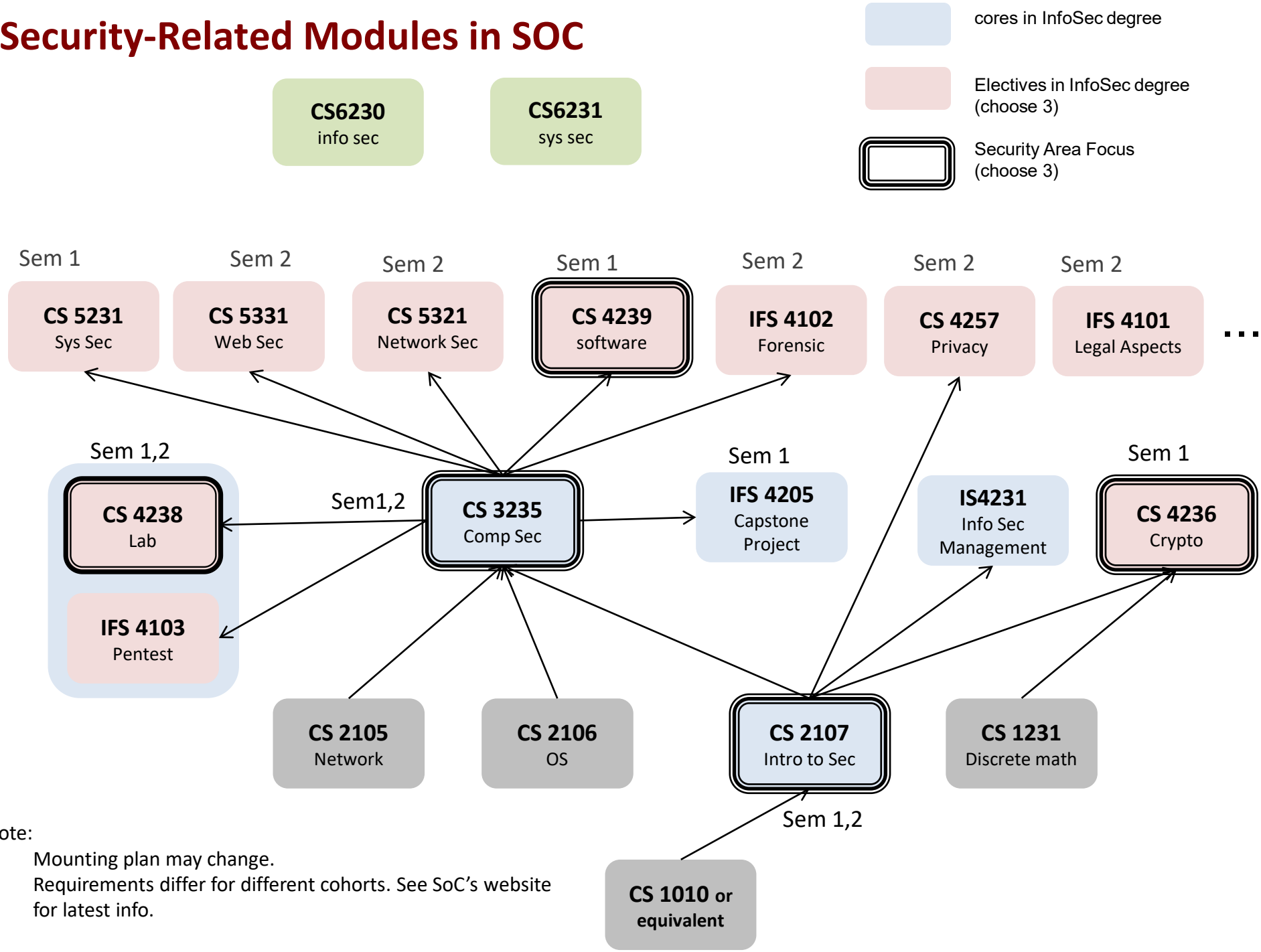
Preclusion(s)

Nil

Weekly Workload

- Lecture: 2 hrs
- Tutorial: 1 hrs
- Project: 3 hrs
- Preparation: 4 hrs

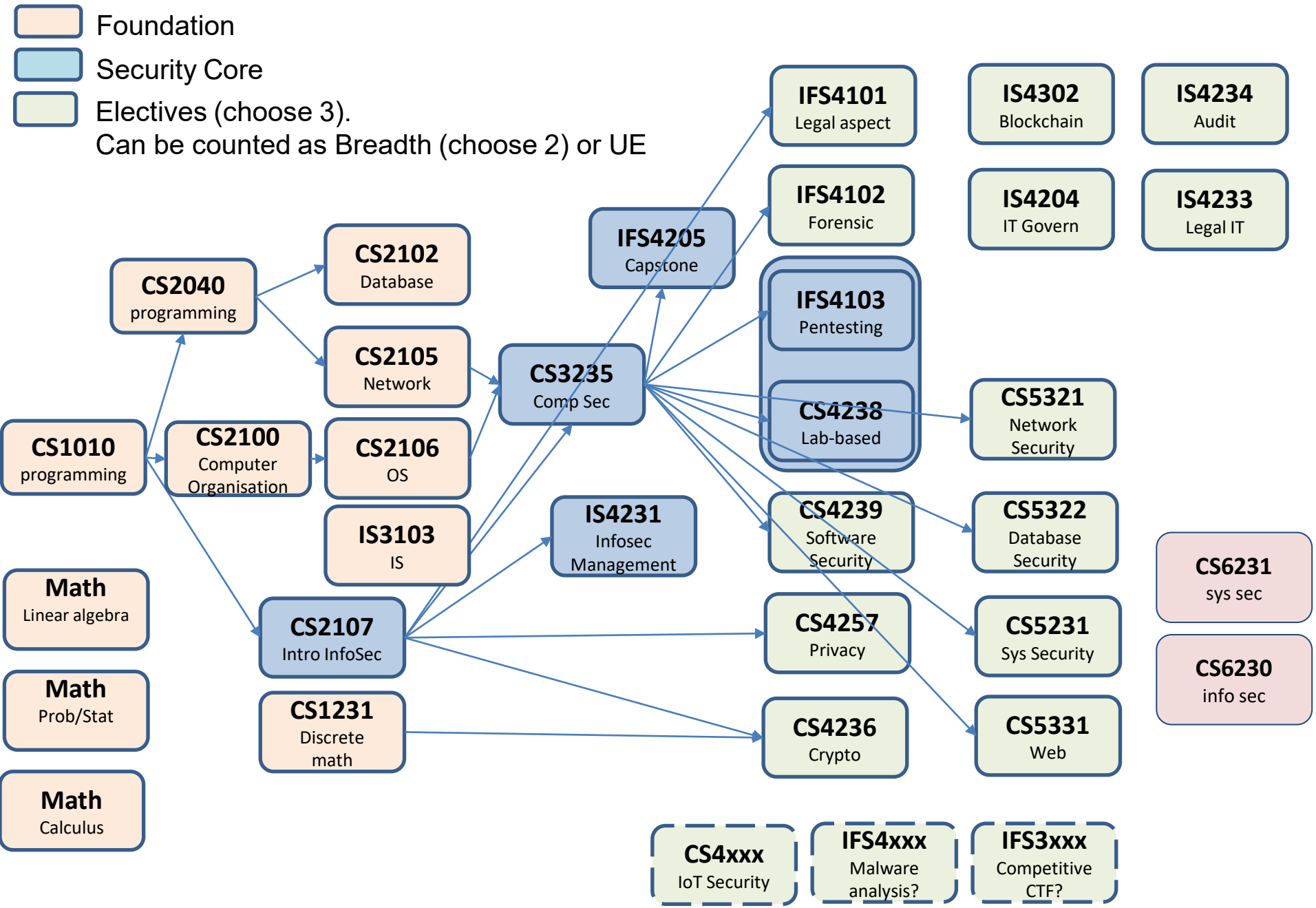
Security-Related Modules in SOC



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



Some of the Terms Encountered in This Module

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, RSA, Certificate, Public Key Infrastructure, Digital Signature.

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

SSL, TLS, HTTPS, Secure channel on the Internet.

DDOS, Syn flood, Wireshark, Spoofing, Sniffing, Cache poisoning, Tor.

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

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

0.2 Module Admin

Teaching Mode

- 13 Lectures
- 9 Tutorials (from Week 3): the last 2 tutorials for group presentation
- Continuous Assessment (55%):
  - 2 Assignments (25%)
  - 1 Mid-term quiz (15%): after the recess week
  - 1 LumiNUS online assessment (5%): 1 week before reading week
  - 1 Group presentation on open-ended topic (5%)
  - Tutorial attendance (5%): 5 out of 9 tutorials, ≥25 mins/session, based on Zoom's meeting-attendance reports
- Final Exam (45%): open-book, no Internet

Teaching Staff

Lecturer: Sufatrio (Rio)

TAs (tutorials): Terence Ng, Brian Yen, Caesar Zhang, Zeng Jun

TAs (assignments): Lee Yu Choy, Yang Cheng Long, Daniel Lim

Slides:

- Based on A/P Chang Ee-Chien's
- Extended with additional explanations and illustrations
- Being revamped to include more cryptography and secure channel: *more about this on the next slide*

CS2107 LumiNUS: *check it regularly*!

- Uploaded lecture notes, tutorial notes, assignment briefs
- Forum: for announcement and discussion, including on group presentation matters (group formation, topic allocation, etc.)

What's New in CS2107 This Year

- More crypto!
  - More in-depth coverage: gives a *deeper understanding* of crypto
  - More rigorous definition & analysis: for *firmer foundations*
  - Develop a *stronger basis* for important "secure communication channel": secure communications & transactions over insecure public network
- Parts of software security are shifted to CS3235:
  - OS security (access control), deeper aspects of network & web security
  - Can be covered better after CS2105 and CS2106
- Main goals of the module enhancement:
  - To better understand how crypto is used in practice (real world)
  - To minimize overlap with CS3235
- Crypto analysis coverage and approach:
  - Basic threat modeling, cryptographic goals, cryptosystem security
  - Not so formal, intuitive explanation is also given

Main References

- "**Security in Computing**" (5th ed), Charles P. Pfleeger et al., Prentice Hall

  Customized version (Chapter 1 to 6) from Pearson is available in NUS Co-ops

  Notation: Throughout the slides, the reference **[PF*x*.*y*]** refer to Chapter *x* Section *y*

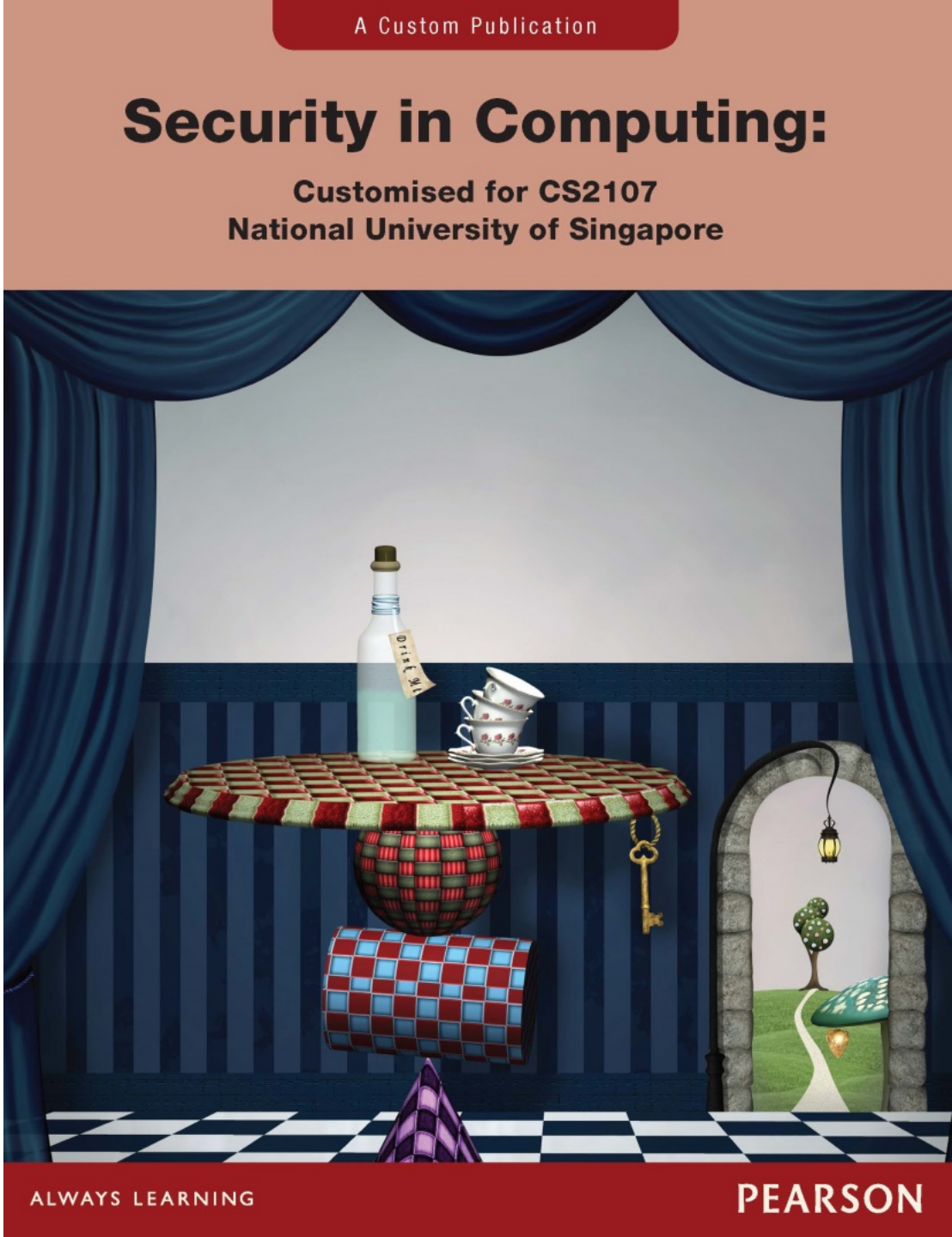
- "**Serious Cryptography: A Practical Introduction to Modern Encryption**", Jean-Philippe Aumasson, No Starch Press, 2017

- "**Security Engineering**" (2nd ed), Ross Anderson, Wiley

  Free online version at:

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

Available (?) at **NUS Co-op @ Forum**



Tentative Schedule

Week	Topic & Covered Attacks		Tutorial	HW
1	Introduction, Cryptography/Encryption	Cryptanalysis on classical ciphers	-	
2	Cryptography/Encryption	Cryptanalysis on classical ciphers	-	
3	Cryptography/Encryption (modern ciphers)	Cryptanalysis on modern ciphers	1. Intro, Encryption	
4	Authentication/Password, Multi-factor authentication, Phishing	Dictionary attacks, Phishing	2. Password, 2FA	A1
5	Authenticity: Data origin, Hash, MAC, Signature	Birthday attacks, Email/SMS spoofing	3. Authenticity: birthday attacks, hash	
6	PKI, Certificate, Authentication protocol	Proxy re-encryption, Protocol attacks	4. PKI, PKI attacks	
7	*Mid-term quiz*		Past mid-term discussion	
8	Secure channel, Key-exchange, SSL/TLS, HTTPS	TLS/HTTPS usage attacks	Mid-term quiz discussion	A2
9	Network Security, DNS, DDOS, Firewall	DNS attack, ARP attacks, DDoS attacks	5. Renegotiation attack	
10	Secure programming: Background, Data representation, Call stack	Heartbleed bug	6. Network security	
11	Secure programming: Buffer overflow attacks, Integer overflow attacks, Malware	Buffer overflow attacks, Integer overflow attacks	7. Secure programming	
12	Web security	XSS, CSRF, SQLI	Project presentations	OA
13	Guest lecture (TBD), Review		Project presentations	

Notes on Lectures and Tutorials

- Attendance will *not* be taken during lectures:
  - But please attend them still if possible
  - Otherwise, check the uploaded recordings
  - Pay attention and participate in class and tutorials
- *Do* attend your tutorials with your assigned tutorial group: claim your 5% participation marks
- Do *not* disturb/distract others and … yourself!
  - No chatting
  - No Pokemon or games
  - No watching videos

Reminders on Assignments

- Avoid plagiarism:
  - Group study is fine, but do not copy answers
  - Your TAs may ask you to *satisfactorily explain* your answers (before granting marks of correct answers)
- LumiNUS forum usage:
  - For discussions on assignments:
    - You can ask questions and share ideas
    - *But* don't reveal your answers!
  - Please be courteous, even when disagreeing with others

0.3 Why CS2107 and Information Security

Rampant Security Attacks: Internet is a Dangerous Place

ST SINGAPORE POLITICS ASIA **WORLD** VIDEOS LIFESTYLE FOOD MORE

WORLD › United States **Europe** Middle East Americas Africa

Chaos as hospitals, telcos and schools hit

1 of 2 A window announcing the encryption of data including a requirement to pay appears on an electronic timetable display at the railway station in Chemnitz, eastern Germany, last Friday. PHOTOS: AGENCE FRANCE-PRESSE

The Straits Times, May 14, 2017

PUBLISHED MAY 14, 2017, 5:00 AM SGT

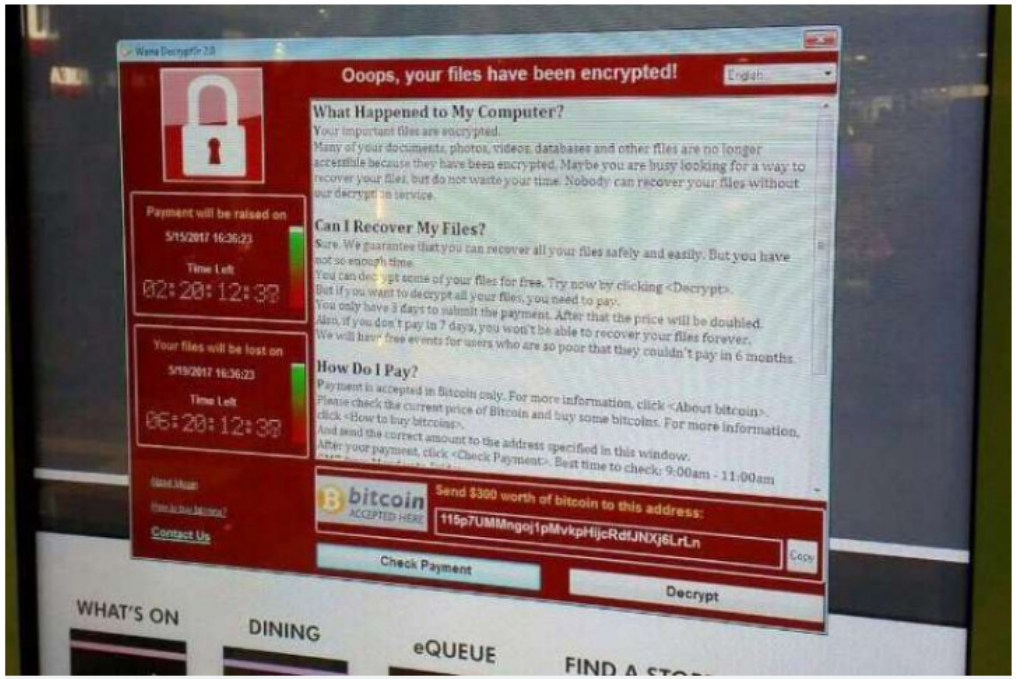
Including in Singapore!

www.straitstimes.com/singapore/global-ransomware-attack-hits-digital-directory-at-tiong-ba

ST SINGAPORE POLITICS ASIA WORLD VIDEOS LIFESTYLE FOOD MORE

SINGAPORE > Courts & Crime Education Housing Transport Health Manpower Environm

Singapore malls, users hit in cyber attack



A digital display at Tiong Bahru Plaza shows a ransomware message. PHOTO: REDDIT

PUBLISHED MAY 14, 2017, 7:20 PM SGT

The Straits Times, May 14, 2017

Including in Singapore!

We set you thinking
TODAY
WEDNESDAY 14 AUGUST 2019

SingHealth cyber attack a result of human lapses, IT system weaknesses: COI report

By CYNTHIA CHOO

Reuters file photo

The SingHealth cyber attack happened because of lapses by employees and vulnerabilities with the system.

Published 10 JANUARY, 2019 UPDATED 10 JANUARY, 2019

Ref: https://www.todayonline.com/singapore/singhealth-cyber-attack-result-human-lapses-it-system-weaknesses-coi-report

WEF Global Risks Report 2018

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Top 10 risks in terms of

Impact

1. Weapons of mass destruction
2. Extreme weather events
3. Natural disasters
4. Failure of climate-change mitigation and adaptation
5. Water crises
6. Cyberattacks
7. Food crises
8. Biodiversity loss and ecosystem collapse
9. Large-scale involuntary migration
10. Spread of infectious diseases

Categories

- Economic
- Environmental
- Geopolitical
- Societal
- Technological

From: "The Global Risks Report 2018, 13th Edition", World Economic Forum, 2018.

WEF Global Risks Report 2018

Top 10 risks in terms of

Likelihood

1. Extreme weather events
2. Natural disasters
3. Cyberattacks
4. Data fraud or theft
5. Failure of climate-change mitigation and adaptation
6. Large-scale involuntary migration
7. Man-made environmental disasters
8. Terrorist attacks
9. Illicit trade
10. Asset bubbles in a major economy

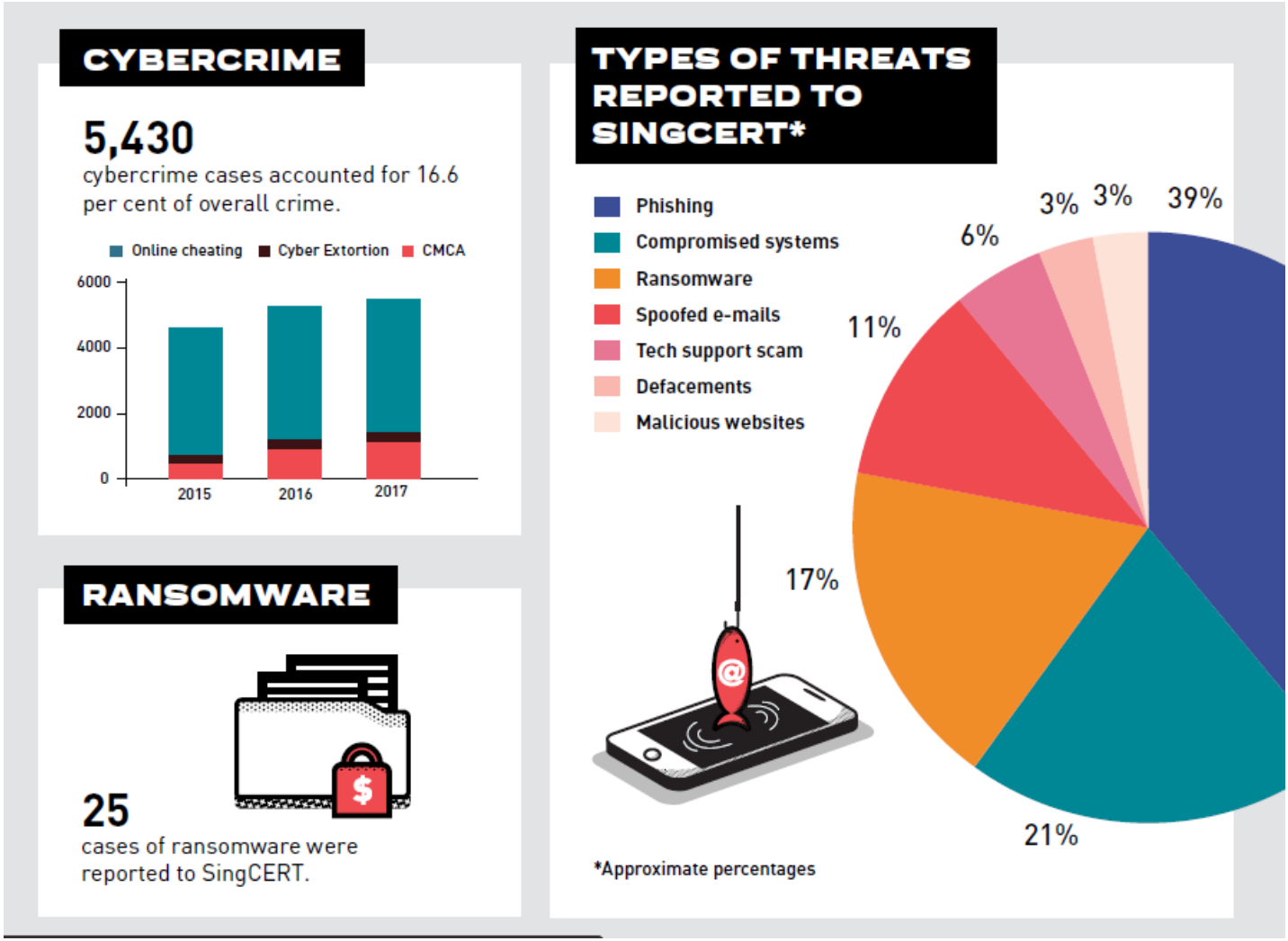
From: "The Global Risks Report 2018, 13th Edition", World Economic Forum, 2018.

WEF Global Risks Report 2018: From Executive Summary

Cybersecurity risks are also growing, both in their prevalence and in their disruptive potential. Attacks against businesses have almost doubled in five years, and incidents that would once have been considered extraordinary are becoming more and more commonplace. The financial impact of cybersecurity breaches is rising, and some of the largest costs in 2017 related to ransomware attacks, which accounted for 64% of all malicious emails. Notable examples included the WannaCry attack—which affected 300,000 computers across 150 countries—and NotPetya, which caused quarterly losses of US$300 million for a number of affected businesses. Another growing trend is the use of cyberattacks to target critical infrastructure and strategic industrial sectors, raising fears that, in a worst-case scenario, attackers could trigger a breakdown in the systems that keep societies functioning.

From: "The Global Risks Report 2018, 13th Edition", World Economic Forum, 2018.

Singapore Cyber Landscape 2017



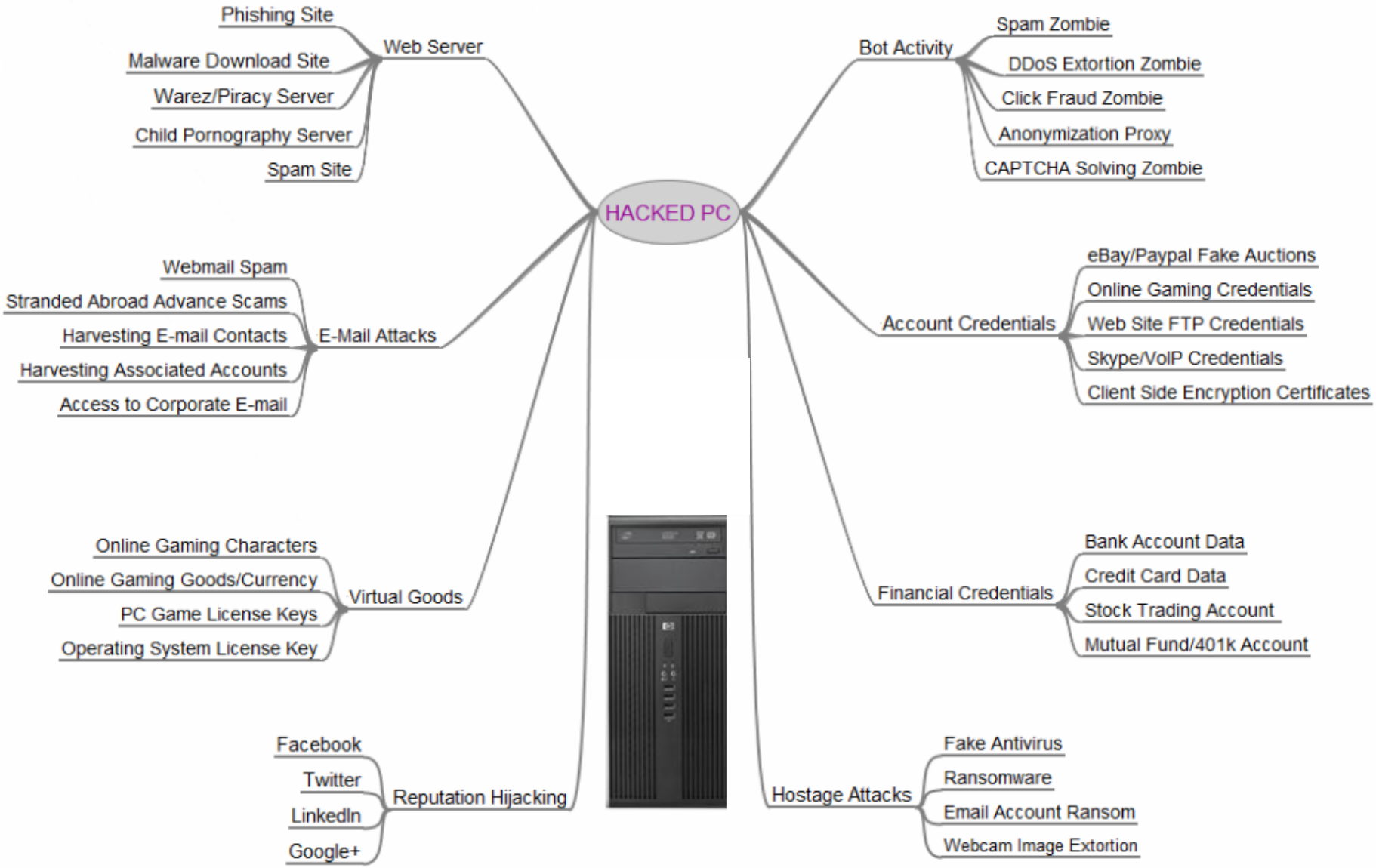
From: Singapore Cyber Landscape 2017,
Cyber Security Agency of Singapore, 2018

Singapore Cyber Landscape 2017

2017 saw more vulnerabilities disclosed and disruptive attacks happening than in previous years. More cyber-attacks are likely. Cybersecurity is a team sport – we all have a part to play, and we all need to play our part well. We can start by practising good cyber hygiene. While we do what we can as individuals, the Singapore Government will also continue to work with stakeholders here and internationally towards a safe and trustworthy cyberspace.

From: Singapore Cyber Landscape 2017,
Cyber Security Agency of Singapore, 2018

The Value a Hacked PC: (Yes) The Stakes are Very High



https://krebsonsecurity.com/2012/10/the-scrap-value-of-a-hacked-pc-revisited/

Yet, Some Possible Excuses

- Still some famous *last words* out there:
  - “Nobody would bother to hack us”
  - “Our expensive network firewall will keep us safe”
  - “Our users have completed their acceptance tests”
  - “We are now adding good security measures into our system”
  - “*What's the worst that could happen*?”
  - …

0.4 What is Computer/Information/ Cyber Security?

Some Background

- System may fail, which could due to:
  - Operator mistakes: e.g. a system file is accidentally deleted, which later leads to a system crash
  - Hardware failures
  - Poor implementation: e.g. Year 2000 (Y2K) problem
- Some failure are inflicted by *deliberate human actions* that are designed to cause failure
- Cyber security is concerned with such intentional failures

Some Background

- Examples:
  1. An attacker carries out a particular combination of steps on the ATM to withdraw money without being recorded www.wired.com/2014/11/nashville/.
     (Such combination of steps is extremely unlikely to occur by mistake.)
  2. An attacker who uses objects resembling valid coins to buy drinks from vending machines.

See [PF3.1 page157]
Undocumented Access Point (a form of *back door*)

In this module,
"read": Part of the teaching materials. Read it.
"see": Information that is good to know.
"optional": Optional information.

Some Background

You may have seen similar "clueless" advertisement *:

> *"Studies have shown that there is a growing threat of mobile malwares and growing concern of privacy. Our secure contacts management system ensures that the contacts list in your mobile phone is securely protected, even under hostile environment. Our secure cloud service employs state-of-the-art Advanced Encryption Standard (AES), together with defense-grade secure mobile platform, to provide a practical and secure BYOD (Bring Your Own Device) solution to secure your valuable client list."*

The term "secure" appears many times, but what does it mean?

We need more refine and precise definitions of "security".

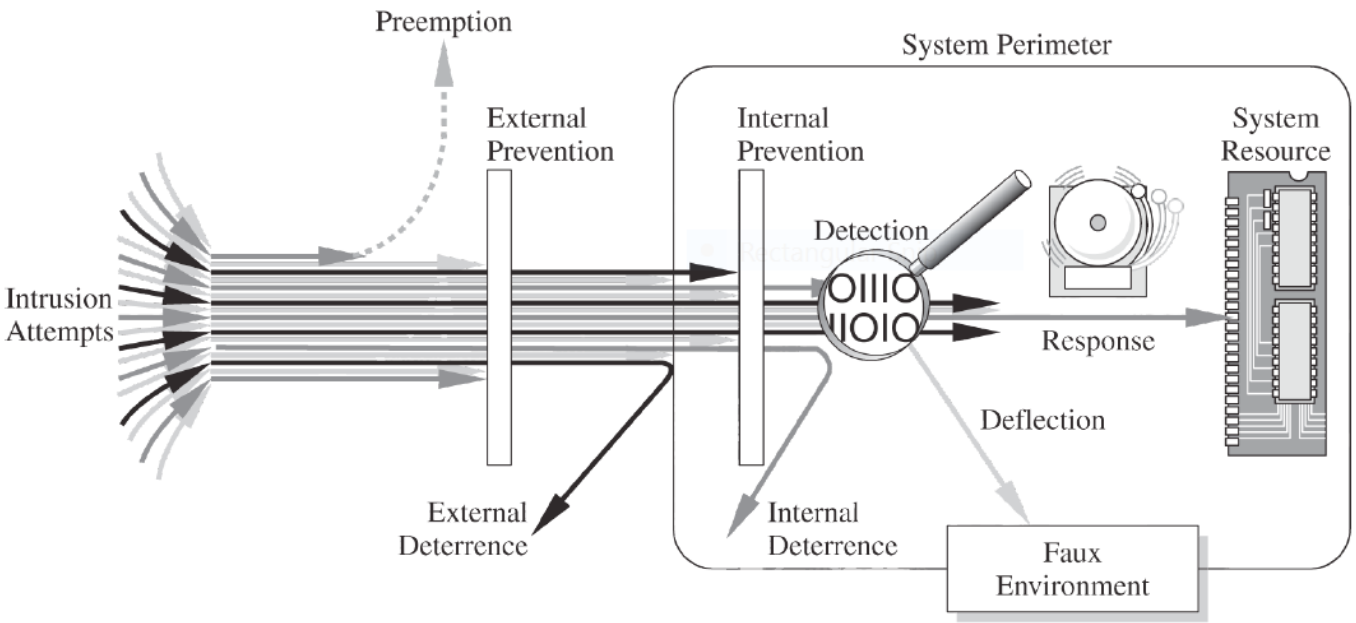
* I make this up. This advertisement is not real.

Assets, Threat, Vulnerability and Control

- Security is about the protection of **assets** (objects of value):
  - Hardware
  - Software
  - Data and information
  - Reputation: which is intangible
- (See [PF1], which gives detailed elaboration on *Threat-Vulnerability-Control*)
- ***Threat***: A set of circumstances that has the potential to cause loss or harm
  - E.g. an attacker who controls the workstation in the lecture room could maliciously gather sensitive information such as passwords
- ***Vulnerability***: a weakness in the system
  - E.g. anyone can reboot the system from USB or disk to gain control

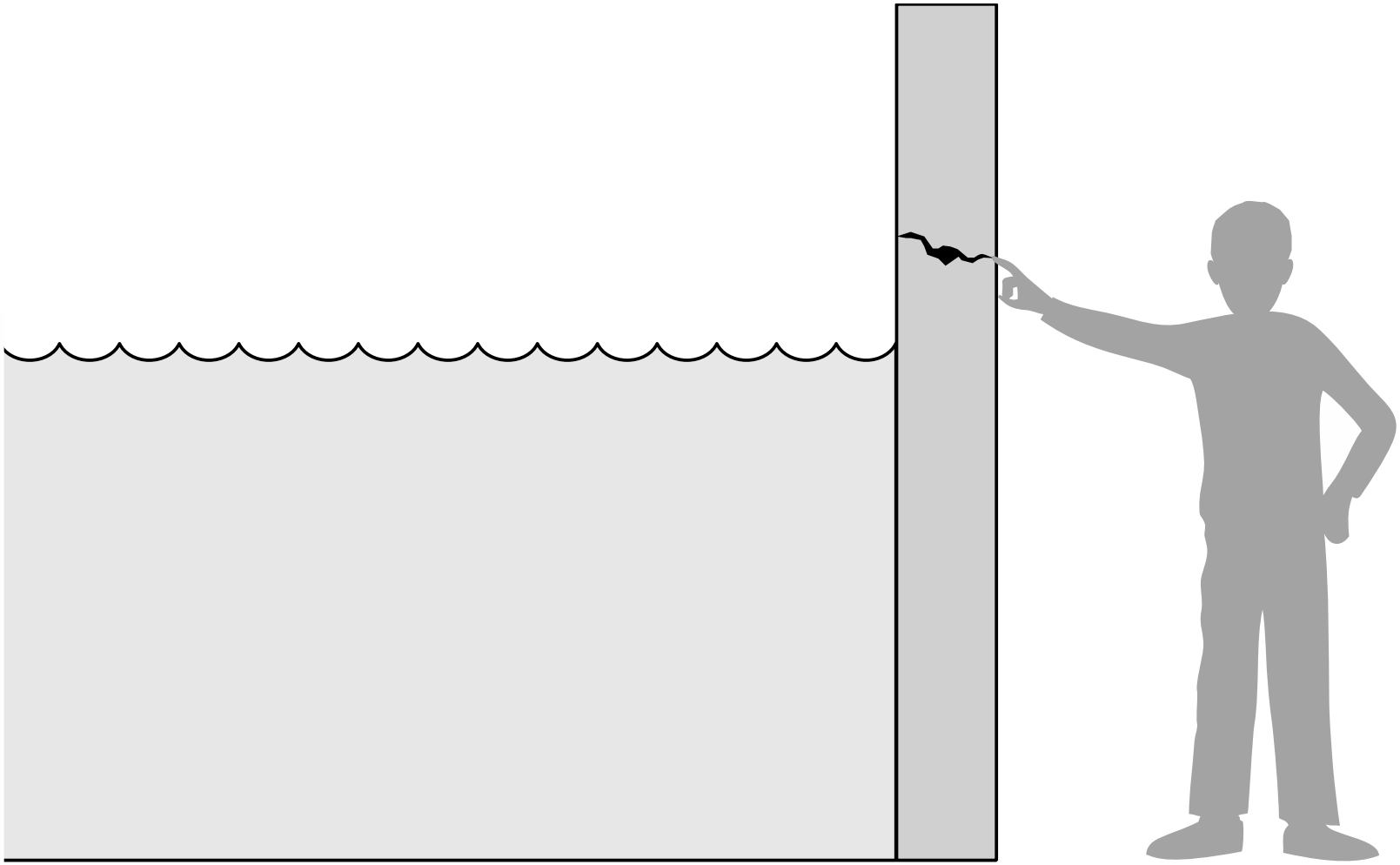
Assets, Threat, Vulnerability and Control

- ***Control***: A control, countermeasure, security mechanism is a mean to counter threats
  - E.g. restrict physical access to the workstation, disable USB booting, etc.
  - See [PF1.5] on prevent, deter, deflect, detect, mitigate, recover



A ***threat*** is blocked by ***control*** of a ***vulnerability***

Threat, Vulnerability and Control: Analogy



Another Look at Security Terminologies

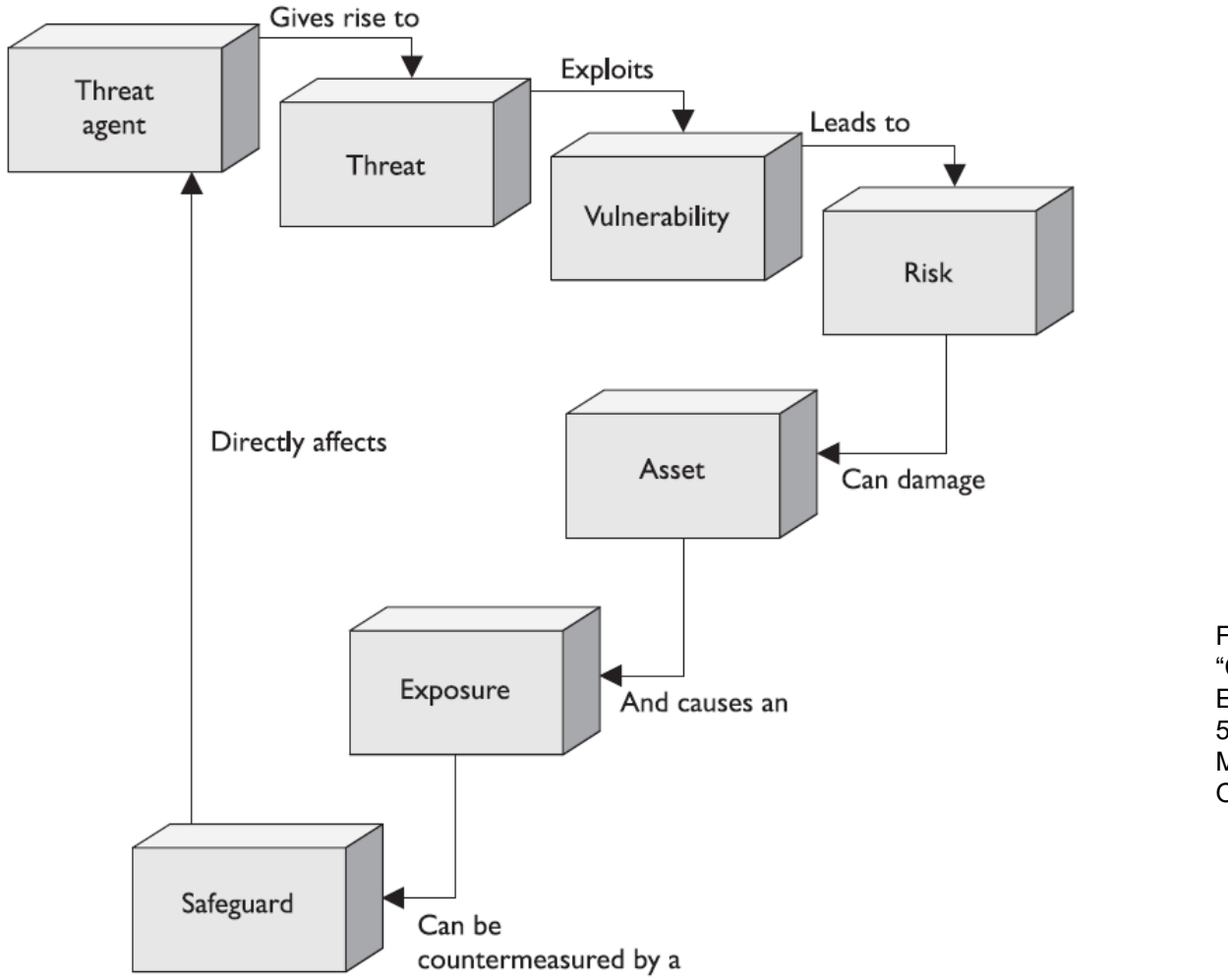


Figure 3-3 The relationships among the different security components

From: Shon Harris, "CISSP All-in-One Exam Guide", 5th Edition, 2010, McGraw-Hill Osborne Media

Note: The term "*safeguard*" is used for "*control*" in the diagram

Different Types of Controls

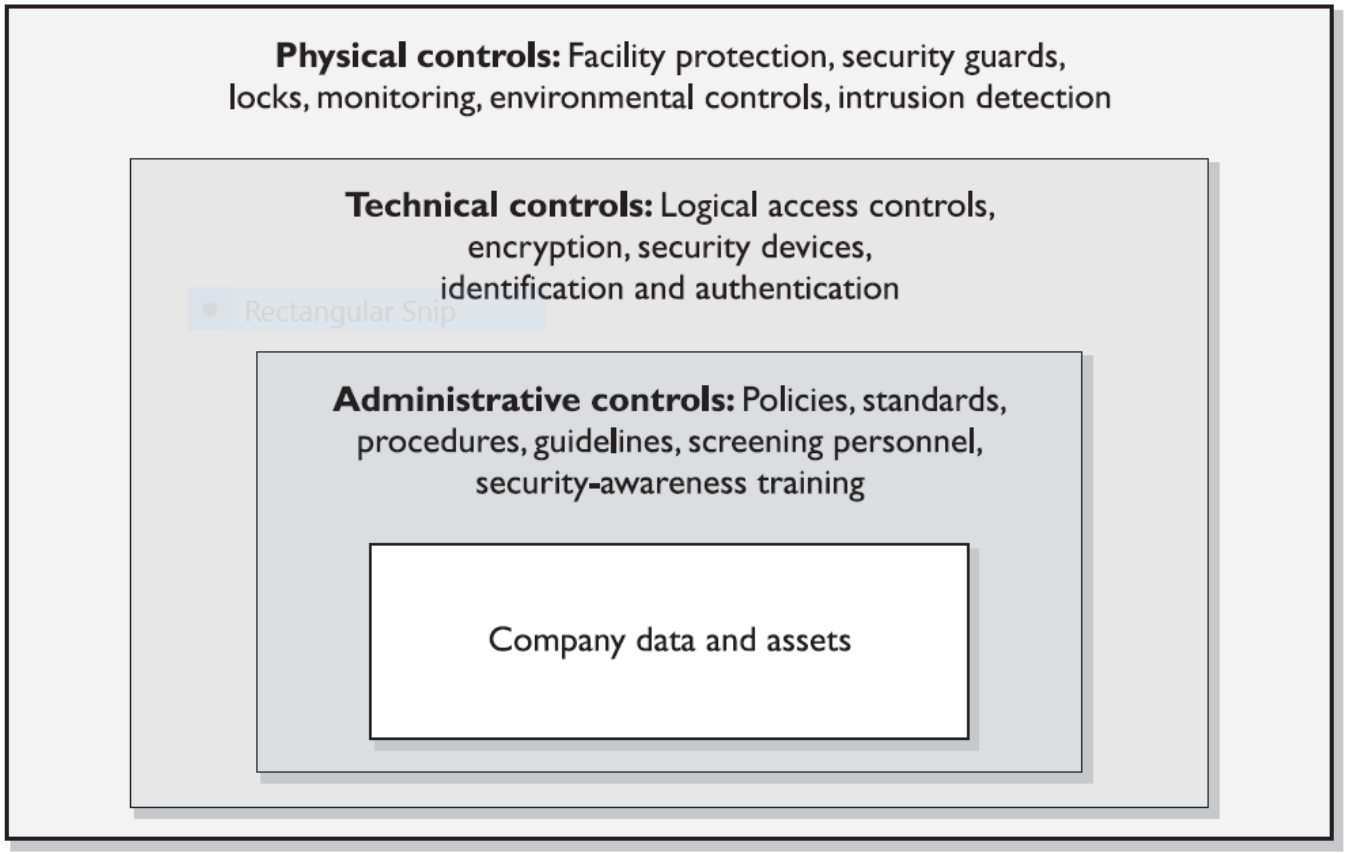


Figure 3-1 Administrative, technical, and physical controls should work in a synergistic manner to protect a company's assets.

From: Shon Harris, "CISSP All-in-One Exam Guide", 5th Edition, 2010, McGraw-Hill Osborne Media

Security Definitions: C-I-A Triad

- **Confidentiality:**
  - + The ability to ensure that an asset is *viewed* only by authorized parties
  - - Prevention of *unauthorized disclosure* of information
- **Integrity:**
  - + The ability to ensure that an asset is *modified* only by authorized parties
  - - Prevention of *unauthorized modification* of information or processes
- **Availability:**
  - + The ability to ensure that an asset can be *used* by any authorized parties
  - - Prevention of *unauthorized withholding* of information or resources

1. Confidentiality

- Edward Snowden leaked classified NSA information.
  From NSA's point of view, this is a breach of ***confidentiality***.
- A student "hacked" into the university system and *downloaded* the examination reports. He now know the marks obtained by each student.

  Confidentiality of the exam result is thus compromised.

2. Integrity

- A student "hacked" into the university system and *modified* his own grade.

  Integrity of the exam result is compromised.

3. Availability

- Chewing gum sticking to a car's door lock.
- A *botnet* floods a Web server with HTTP requests.
  A legitimate HTTP request now takes longer time to be processed. Thus, the QoS significantly degraded.
  In the extreme scenarios, the Web service is denied.

  This is a ***distributed denial of service attack*** (DDoS) on the Web server, which compromise ***availability***.

Notes:

There are also other requirements like:

- ***Authenticity***: logins, password checks, message sender/origin.
- ***Accountability***, including ***non-repudiation*** of a prior commitment.

Some literatures treat these as different requirements.
Some group them under C-I-A, e.g., very often,
"authenticity" is treated as "integrity".
(Hence, read the context carefully).

Quiz 0-1

- Which security requirements are compromised below?
  "An application is being modified by an attacker.
  The compromised application carries out key-logging:
  it captures the password entered by the user and sends
  it to the attackers."
- Answer? Please use Zoom Poll 1

Remarks on Security Terminology

- There are many inconsistent usages of security terms
- For e.g. the term "privacy" in the following statement "*HTTPS provides privacy, integrity & authenticity for …*" could mean *confidentiality*
- *Why?*
- A sample relevant scenario:
  If Alice uses a free airport WiFi, and submit a report to LumiNUS via HTTPS, even the airport operator is unable to know the content of the report

Remarks on Security Terminology

- Whereas the "privacy" in:
  - *"Social networking sites vary in the level of privacy offered."*
  - *"Advocates have raised the issue of privacy in mobile advertisement."*

  could means revelation of *personal information* like age, salary, that the individuals do not intend to share
- Sample scenario: Alice uses a calculator app on her mobile phone. The app obtains the GPS location and contact list, and shares it with another company.
- There is **no single definition** of security:
  Different fields, experts, documents may use different definitions. Hence, do take special note of the context.

Difficulty in Achieving Security

- **Security is not considered** during the early design stage
- It is often **difficult to formulate security requirements**
- There can be **various design constrains**
- It is **difficult to verify** that a design achieves the intended security requirements
- Even if the design is secure, the system **may not be properly implemented**, especially for large, complex systems
- A deployed system is most vulnerable at its **weakest point**
- Even a secure system can still be **difficult to manage**, particularly with *human in the loop*: configuration errors, mismanagement of patches/credentials/etc.

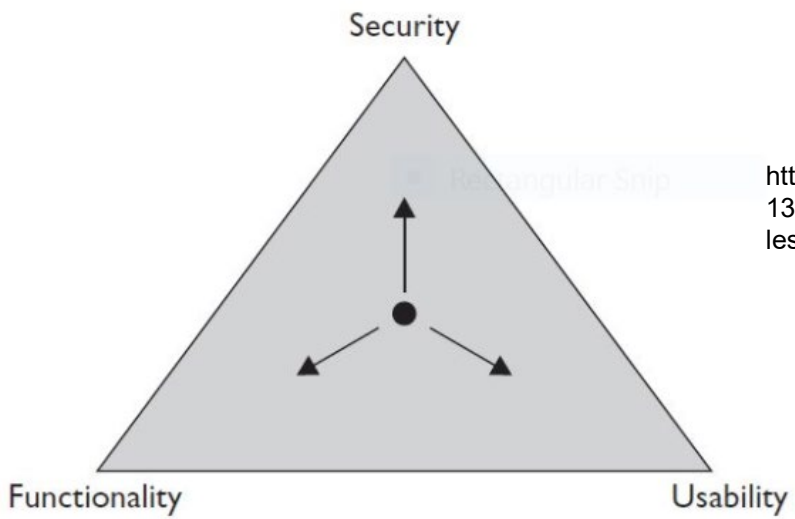
In this module, we will look into examples to illustrate how systems fails, and various protection mechanisms in overcoming the above difficulties

Trade-off in Security

There is a trade-off between security and:

- **Ease-of-use**: Security mechanisms interfere with working patterns users originally familiar with
- **Performance:** Security mechanisms consumes more computing resources
- **Cost:** Security mechanisms are expensive to develop

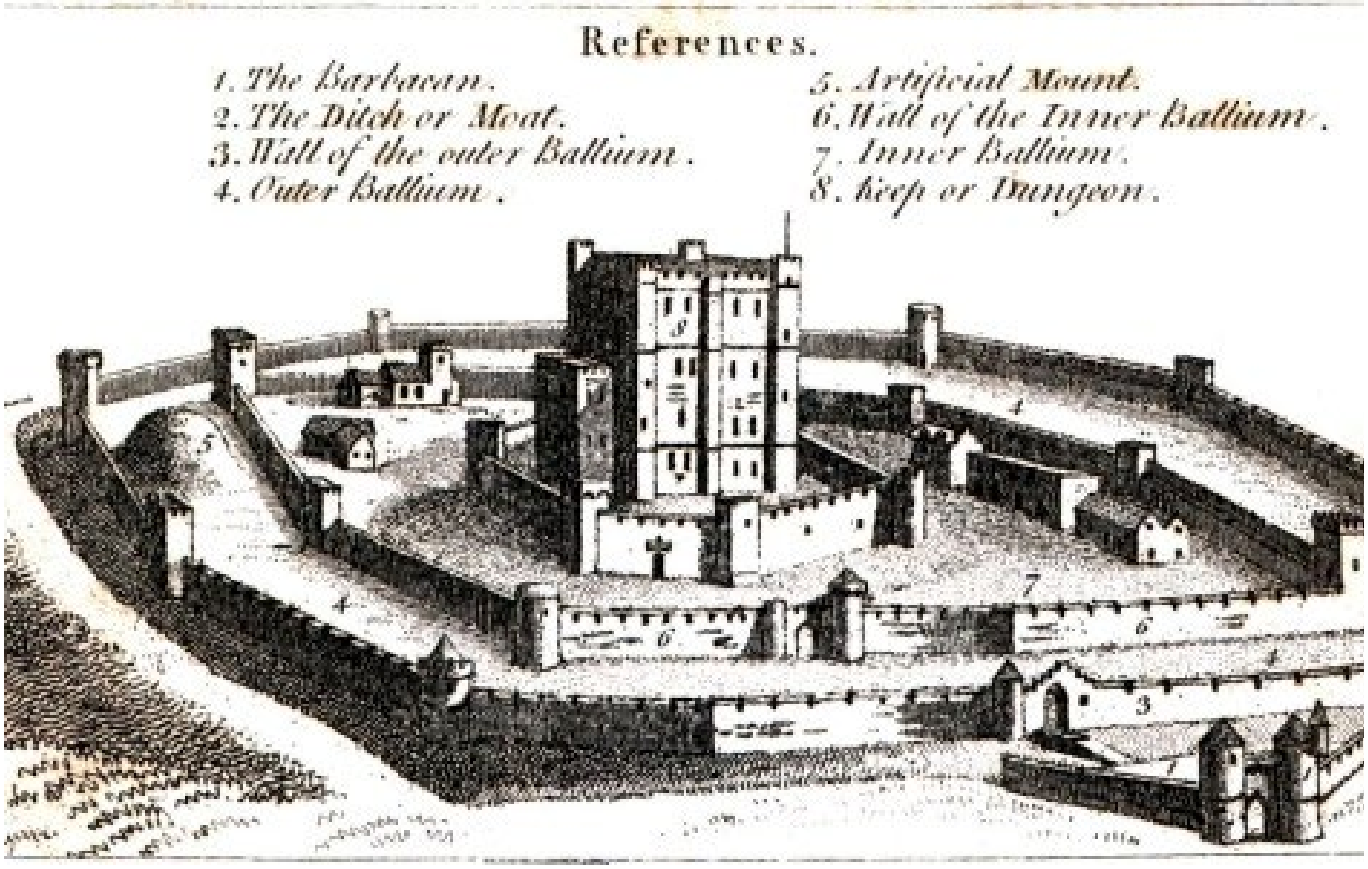
Security, Functionality and Ease-of-Use Triangle: the more secure something is, the less usable and functional it becomes



https://www.linkedin.com/pulse/20140619200426-136462609-the-more-secure-something-is-the-less-usable-and-functional-it-becomes

“Security: Computing in an *Adversarial* Environment”

We are facing “smart” adversaries who actively look for vulnerabilities



See https://smartbear.com/blog/test-and-monitor/what-medieval-castles-can-teach-you-about-web-secu/

“Security: Computing in an *Adversarial* Environment”

Town-protecting castles:

- **Services:**
  - Markets, admin office, etc.
- **Users:**
  - Citizens, travelers, etc.
- **Attackers’ goals:**
  - Capture the whole city, steal info, disrupt services, etc.
- **Protection mechanisms**:
  - All-round defense: “security depends on the weakness point”
  - Layered defense
  - Access control: e.g. castle/door guards
  - Other measures: dummy target, death trap, obscurity, …