CS2107

Topic 0

Admin + Overview

CS2107

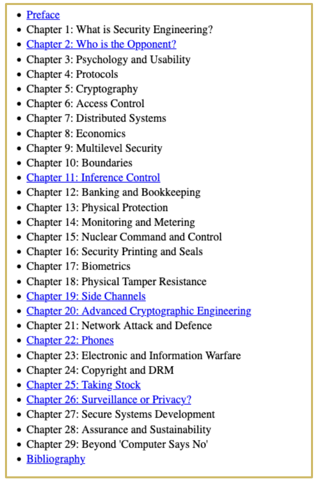
Lecturers:	Chang Ee-Chien, Nitya Lakshmannan
Tutors (tutorials):	Ang Jing Xuan Selwyn, Arshdeep Singh Kawatra, Dominic Khoo Yong Xiang, Lim Choong Kai Joshua, Hrishiraj Mandal, Shen Jiamin, Song Yuexi, Timothy Quek Jing Yuan, Zhu Yongze.
Tutors (assignments):	NUS Greyhats. Cao Yitian, Yeo Beng Jun Vincent, Wu Yuewei, Lee Kai Xuan, (Shen Jiamin, Arshdeep)

Textbook not required. Some good references:

- Security in Computing (5th ed). Prentice Hall. (many examples and detailed explanation. Could be too “lengthy” to some students).
  Customized version (Chapter 1 to 6) available in Co-ops (co-op no longer replenishing. Might have some left over).
- Computer Security (3rd ed), Dieter Gollman, Wiley. (Very concise. Abstract concepts clearly explained. Good to have if you plan to take higher level security courses.)
- Security Engineering (3rd ed), Ross Anderson. Very comprehensive. (2nd edition free online!)

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

Security Engineering (3rd ed)



- Preface
- Chapter 1: What is Security Engineering?
- Chapter 2: Who is the Opponent?
- Chapter 3: Psychology and Usability
- Chapter 4: Protocols
- Chapter 5: Cryptography
- Chapter 6: Access Control
- Chapter 7: Distributed Systems
- Chapter 8: Economics
- Chapter 9: Multilevel Security
- Chapter 10: Boundaries
- Chapter 11: Inference Control
- Chapter 12: Banking and Bookkeeping
- Chapter 13: Physical Protection
- Chapter 14: Monitoring and Metering
- Chapter 15: Nuclear Command and Control
- Chapter 16: Security Printing and Seals
- Chapter 17: Biometrics
- Chapter 18: Physical Tamper Resistance
- Chapter 19: Side Channels
- Chapter 20: Advanced Cryptographic Engineering
- Chapter 21: Network Attack and Defence
- Chapter 22: Phones
- Chapter 23: Electronic and Information Warfare
- Chapter 24: Copyright and DRM
- Chapter 25: Taking Stock
- Chapter 26: Surveillance or Privacy?
- Chapter 27: Secure Systems Development
- Chapter 28: Assurance and Sustainability
- Chapter 29: Beyond 'Computer Says No'
- Bibliography

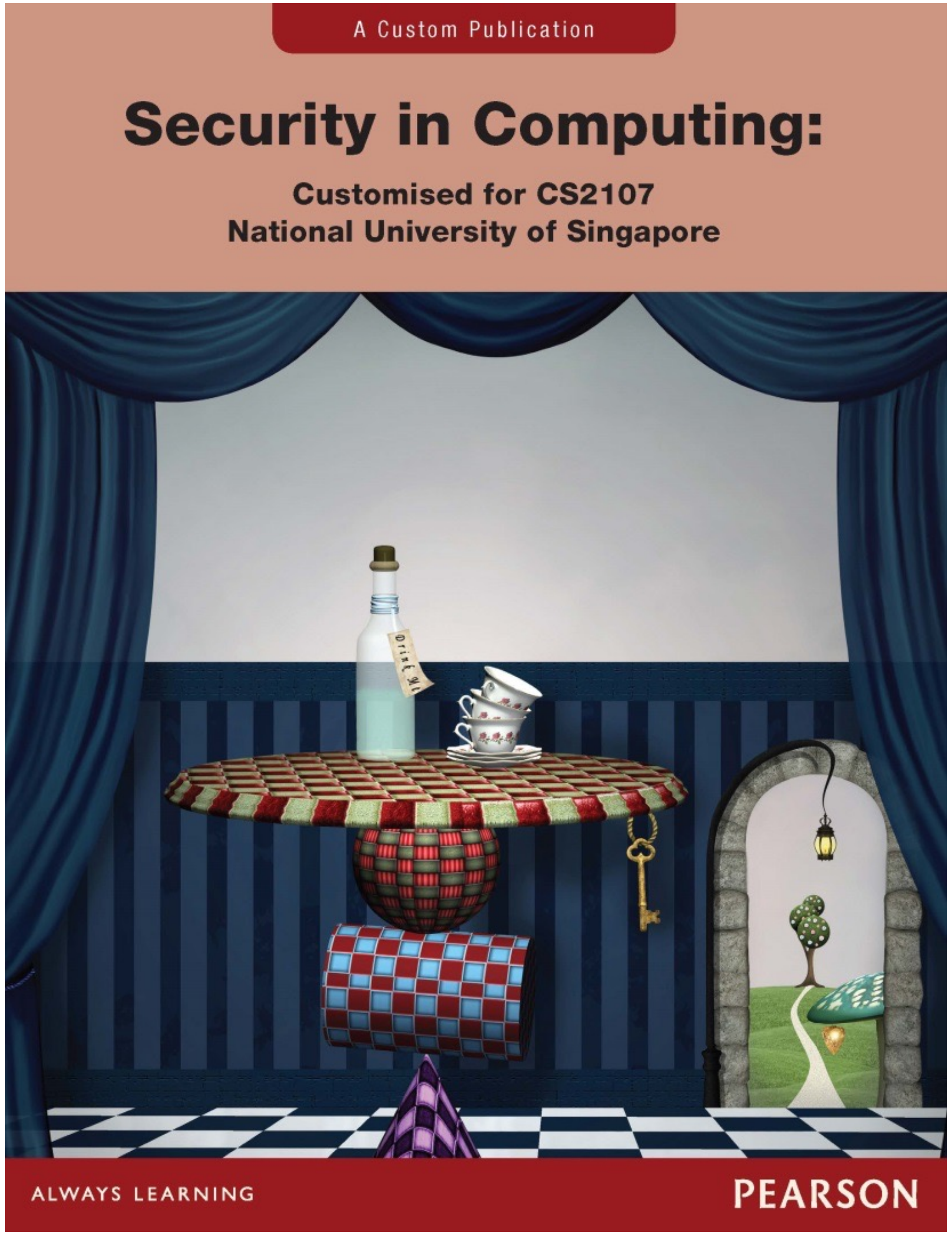
Canvas

- Lecture notes
  - Links with “***read***”: Part of the lecture. Required.
  - Links with “***see***”: References. Optional. Good to browse.
  - Links with no label: Citations. Indicating source of info. (In academic material, sources needed to be cited).
- Forum

Lecture

- Students can either attend f2f or online, although f2f is encouraged.
- Students are expected to attend lecture in “realtime”.
- Lectures will be recorded. The recordings are for revision. In the events that lead to lost of recording (e.g. system crashed while recording, human errors), there would not be another new recording.

Co-op not longer replenishing. Might have some left over. Non-essential.



A Custom Publication

Security in Computing:

Customised for CS2107
National University of Singapore

ALWAYS LEARNING

PEARSON

Pearson

NUS COOP Est. 1969

9789814718448

Teaching Mode

- 12 Lectures

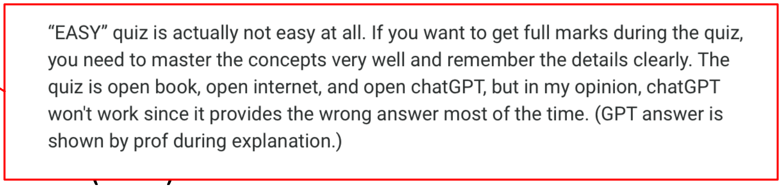
- 9 Tutorials

- Grading (Subjected to changes. Changes would be updated in this slide)

a)	Take-home CTF assignments	(10+10)	(20%)
b)	MCQ quiz during lecture (Best 4 out of 5).	(2.5+2.5+2.5+2.5)	(10%)
c)	Mid-Term (During Lecture time. Venue TBD. Closed book +1 cheat-sheet)		(17%)
d)	Tutorial attendance		(8%)
e)	Exam (f2f, Closed book + two A4 cheat-sheets)		

I plan to make it easy in this semester

Student's comment in NUSMOD



"EASY" quiz is actually not easy at all. If you want to get full marks during the quiz, you need to master the concepts very well and remember the details clearly. The quiz is open book, open internet, and open chatGPT, but in my opinion, chatGPT won't work since it provides the wrong answer most of the time. (GPT answer is shown by prof during explanation.)

https://nusmods.com/courses/CS2107/introduction-to-information-security

- Efforts: 18% (b,d); Hand-on: 20% (a); Understanding: 62% (c,e).
- Exam & Midterm:
  - Easy (almost all got it correct) ~20%
  - Medium (majority got it correct)~40%
  - Difficult (minority got it correct) ~40%

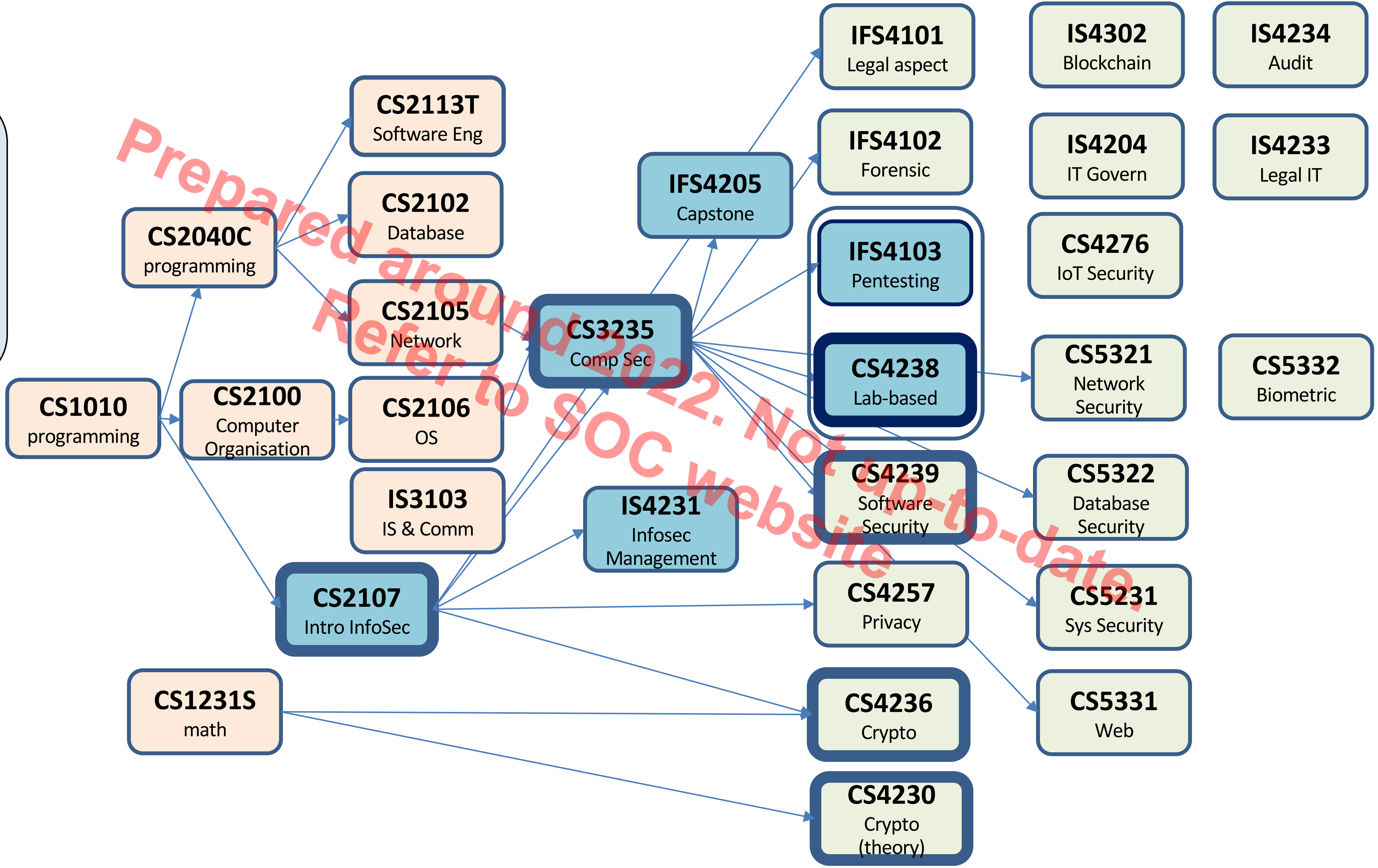
Security-related modules (2022 & outdated. Nonetheless, still gives a good overview)

Pre-requisite

BCOMP Infosec

- Foundation
- Core
- Electives

BCOMP CS's security focus area:
at least 3



CS1010 programming

CS1231S math

CS2040C programming

CS2100 Computer Organisation

CS2107 Intro InfoSec

CS2113T Software Eng

CS2102 Database

CS2105 Network

CS2106 OS

IS3103 IS & Comm

CS3235 Comp Sec

IS4231 Infosec Management

IFS4205 Capstone

IFS4101 Legal aspect

IFS4102 Forensic

IFS4103 Pentesting

CS4238 Lab-based

CS4239 Software Security

CS4257 Privacy

CS4236 Crypto

CS4230 Crypto (theory)

IS4302 Blockchain

IS4204 IT Govern

CS4276 IoT Security

CS5321 Network Security

CS5322 Database Security

CS5231 Sys Security

CS5331 Web

IS4234 Audit

IS4233 Legal IT

CS5332 Biometric

Plagiarism

Based on “honor system”. When found, will be seriously dealt with. At least 2, 3 grade downward. Would notify university.

In lecture Quiz: Allow to access web. LLM allowed. No interactions with human.

Assignment: While discussion is encouraged, sharing of “flag” and program (essentially materials submitted) is considered plagiarism. Using tools in public domain is allowed, except tools that are specifically developed for CS2107 assignments.

Evidences: Witnesses, Access-log.   (there were a case where students colluded online for in-lecture quiz and wrongly unmuted the lecture zoom session).

0.1 What is CS2107

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, SQL, XSS, ...)
• Understand basic security requirements.	(e.g. C-I-A, security threat model)
• Understand basic defense mechanisms.	(e.g. crypto, PKI, access control)
• Awareness of common pitfalls in implementation.	(e.g. Secure programming, wrong usage of crypto).
• Develop “adversarial” thinking	(i.e. think from the attacker’s perspective)

Who

- All IT professionals.
- Preparation for in-depth studies in security. (Required for BCOMP Infosec and BCOMP CS Security focus area).

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.

Schedule (Lecture LT8, 2pm Thursday)

Wk	Lecture (Thursday 10am LT11)				tutorial	In-lecture Quiz	
1	14 Aug		Introduction. C-I-A. Classical Cipher (Topic/"Module" 0,1)		-		
2	21 Aug		Encryption (Topic 1)	pitfall	-		
3	28 Aug		Password, 2 factor, phishing (Topic 2)	Phishing	T1: C-I-A, key-strength, encryption.	Q1	
4	4 Sep		Data Integrity. Hash, Mac, Signature (Topic 3)	Padding oracle	T2: Padding oracle		
5	11 Sep		Data Integrity. (Topic 3)	Online vs offline	T3: Password (online vs offline), hash.	Q2	
6	18 Sep		Authentication Protocol (PKI, Certificate) (Topic 4)		T4: Birthday Attack. Conf vs authen		Release Assignment 1
7	(Recess)						
8	2 Oct		Authentication (Topic 4)		T5: Authentication	Q3	
9	9 Oct		(Mid-term)		T6: Proxy re-encryption		Assignment 1 deadline
10	16 Oct		Network Security (Topic 5)	DNS, ARP attack	T7: Forward secrecy		Release Assignment 2
11	23 Oct		Access control (Topic 6)		T8: Re-neg	Q4	
12	30 Oct		Secure Programming (Topic 7)		T9: Secure Programming		Deepavali + well-being day
13	6 Nov		Web Security (Topic 8)		T10: Case studies	Q5	
14	13 Nov		Attack Kill-chain Demo. Briefing.		T11: review+buffer		Assignment 2 Deadline
	Exam (*Check the date on official site*)						

0.2 What is Computer/Info Security

- System may fail, which could be due to operator mistakes (*e.g. files accidentally deleted, admin forget to renew certificate*), hardware failures (*e.g. hard-disk clash (very common), power failure*), poor implementation & configuration (*for e.g. year 2000 problem*), etc.

- Many systems are robust against typical noise. However, some failure are inflicted by deliberate human actions that are designed to cause failure (*attackers exploit the weakest point*). Security is about such intentional failures. (*e.g. (1) an attacker who carries out a particular combination of steps on the ATM to withdraw money without being recorded* http://www.wired.com/2014/11/nashville/ *. Such combination of steps is extremely unlikely to occur by mistake. (2) an attacker uses objects resemble coins to buy drinks from vending machines.*)

"It is a security issue only when there is a bad guy."

- comment from a CS2107 student on what he had learned.

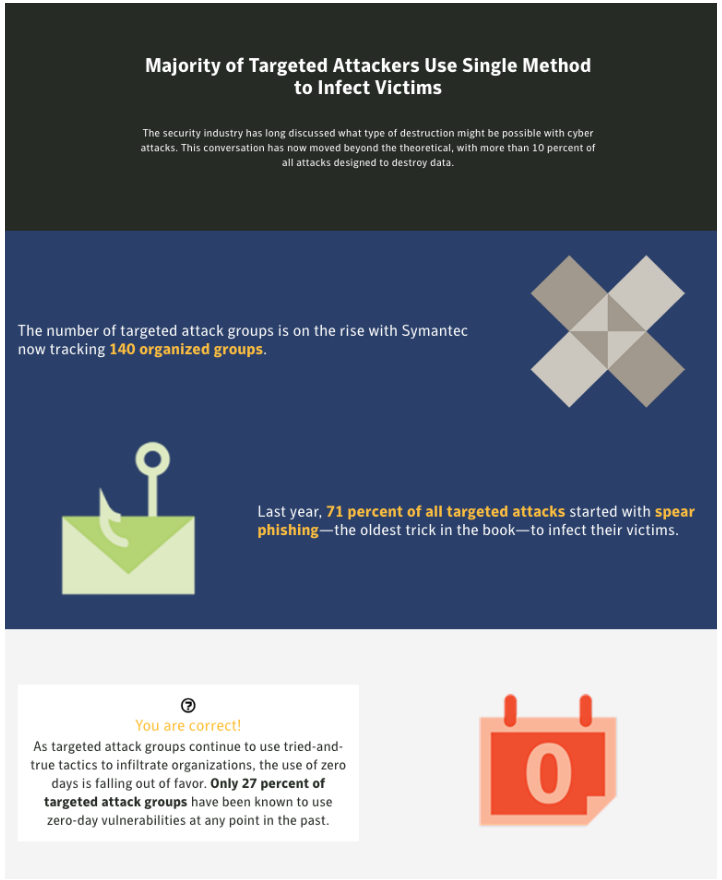
Why important?

Attacks Trend

- Symantec (Broadcom) 2018 Internet Security Threat Report

https://www.broadcom.com/support/security-center/publications/archive?

Very good overview, unfortunately it was only up to 2019.



Majority of Targeted Attackers Use Single Method to Infect Victims

The security industry has long discussed what type of destruction might be possible with cyber attacks. This conversation has now moved beyond the theoretical, with more than 10 percent of all attacks designed to destroy data.

The number of targeted attack groups is on the rise with Symantec now tracking **140 organized groups**.

Last year, **71 percent of all targeted attacks** started with **spear phishing**—the oldest trick in the book—to infect their victims.

You are correct!

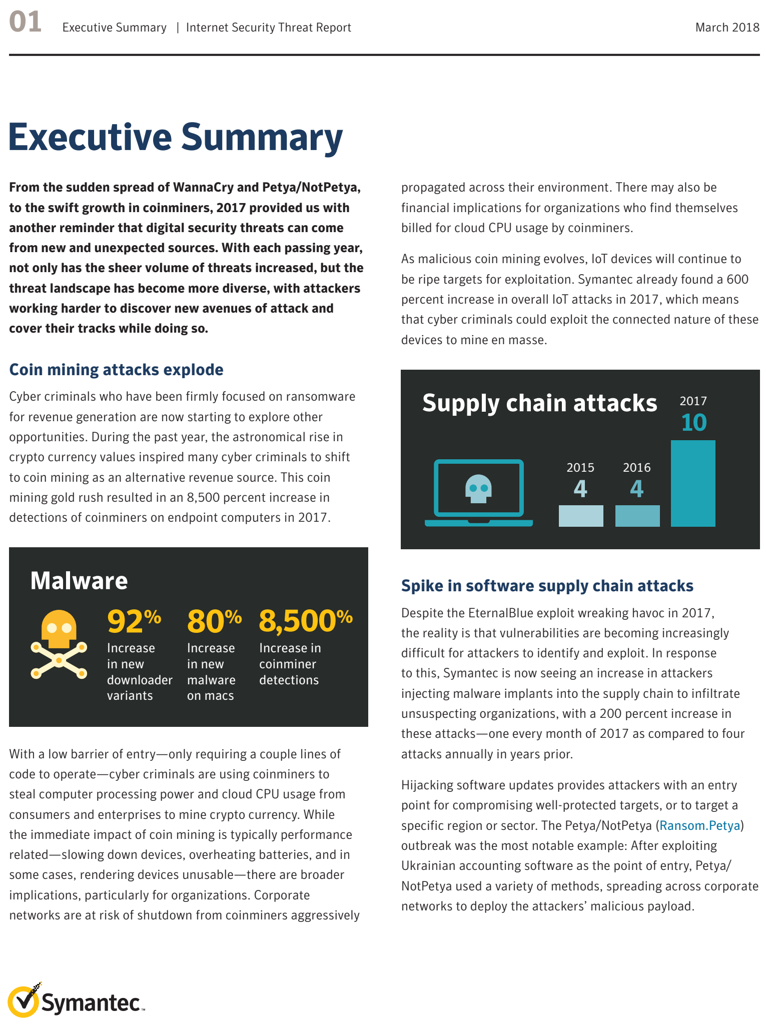
As targeted attack groups continue to use tried-and-true tactics to infiltrate organizations, the use of zero days is falling out of favor. **Only 27 percent of targeted attack groups** have been known to use zero-day vulnerabilities at any point in the past.

From https://www.symantec.com/security-center/threat-report

Eg of threat report

2018

(2018) https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-executive-summary-en.pdf
(2019) https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-executive-summary-en.pdf
(2009) http://www.securityprivacyandthelaw.com/uploads/file/symantec%202009.pdf



01 Executive Summary | Internet Security Threat Report March 2018

Executive Summary

From the sudden spread of WannaCry and Petya/NotPetya, to the swift growth in coinminers, 2017 provided us with another reminder that digital security threats can come from new and unexpected sources. With each passing year, not only has the sheer volume of threats increased, but the threat landscape has become more diverse, with attackers working harder to discover new avenues of attack and cover their tracks while doing so.

Coin mining attacks explode

Cyber criminals who have been firmly focused on ransomware for revenue generation are now starting to explore other opportunities. During the past year, the astronomical rise in crypto currency values inspired many cyber criminals to shift to coin mining as an alternative revenue source. This coin mining gold rush resulted in an 8,500 percent increase in detections of coinminers on endpoint computers in 2017.

Malware

92% Increase in new downloader variants

80% Increase in new malware on macs

8,500% Increase in coinminer detections

With a low barrier of entry—only requiring a couple lines of code to operate—cyber criminals are using coinminers to steal computer processing power and cloud CPU usage from consumers and enterprises to mine crypto currency. While the immediate impact of coin mining is typically performance related—slowing down devices, overheating batteries, and in some cases, rendering devices unusable—there are broader implications, particularly for organizations. Corporate networks are at risk of shutdown from coinminers aggressively propagated across their environment. There may also be financial implications for organizations who find themselves billed for cloud CPU usage by coinminers.

As malicious coin mining evolves, IoT devices will continue to be ripe targets for exploitation. Symantec already found a 600 percent increase in overall IoT attacks in 2017, which means that cyber criminals could exploit the connected nature of these devices to mine en masse.

Supply chain attacks

2015 4

2016 4

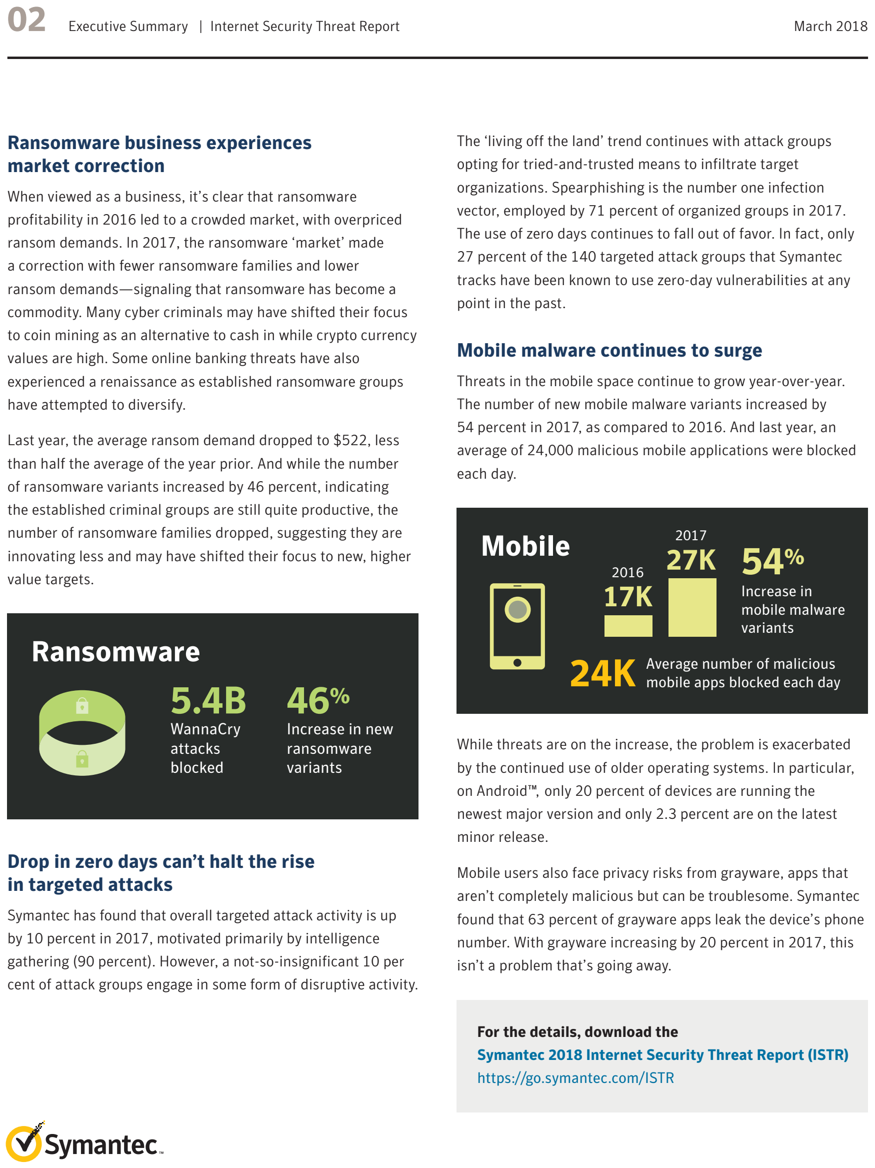
2017 10

Spike in software supply chain attacks

Despite the EternalBlue exploit wreaking havoc in 2017, the reality is that vulnerabilities are becoming increasingly difficult for attackers to identify and exploit. In response to this, Symantec is now seeing an increase in attackers injecting malware implants into the supply chain to infiltrate unsuspecting organizations, with a 200 percent increase in these attacks—one every month of 2017 as compared to four attacks annually in years prior.

Hijacking software updates provides attackers with an entry point for compromising well-protected targets, or to target a specific region or sector. The Petya/NotPetya (Ransom.Petya) outbreak was the most notable example: After exploiting Ukrainian accounting software as the point of entry, Petya/NotPetya used a variety of methods, spreading across corporate networks to deploy the attackers' malicious payload.

Symantec.



02 Executive Summary | Internet Security Threat Report March 2018

Ransomware business experiences market correction

When viewed as a business, it's clear that ransomware profitability in 2016 led to a crowded market, with overpriced ransom demands. In 2017, the ransomware 'market' made a correction with fewer ransomware families and lower ransom demands—signaling that ransomware has become a commodity. Many cyber criminals may have shifted their focus to coin mining as an alternative to cash in while crypto currency values are high. Some online banking threats have also experienced a renaissance as established ransomware groups have attempted to diversify.

Last year, the average ransom demand dropped to $522, less than half the average of the year prior. And while the number of ransomware variants increased by 46 percent, indicating the established criminal groups are still quite productive, the number of ransomware families dropped, suggesting they are innovating less and may have shifted their focus to new, higher value targets.

Ransomware

5.4B WannaCry attacks blocked

46% Increase in new ransomware variants

Drop in zero days can't halt the rise in targeted attacks

Symantec has found that overall targeted attack activity is up by 10 percent in 2017, motivated primarily by intelligence gathering (90 percent). However, a not-so-insignificant 10 per cent of attack groups engage in some form of disruptive activity.

The 'living off the land' trend continues with attack groups opting for tried-and-trusted means to infiltrate target organizations. Spearphishing is the number one infection vector, employed by 71 percent of organized groups in 2017. The use of zero days continues to fall out of favor. In fact, only 27 percent of the 140 targeted attack groups that Symantec tracks have been known to use zero-day vulnerabilities at any point in the past.

Mobile malware continues to surge

Threats in the mobile space continue to grow year-over-year. The number of new mobile malware variants increased by 54 percent in 2017, as compared to 2016. And last year, an average of 24,000 malicious mobile applications were blocked each day.

Mobile

2016 17K

2017 27K

54% Increase in mobile malware variants

24K Average number of malicious mobile apps blocked each day

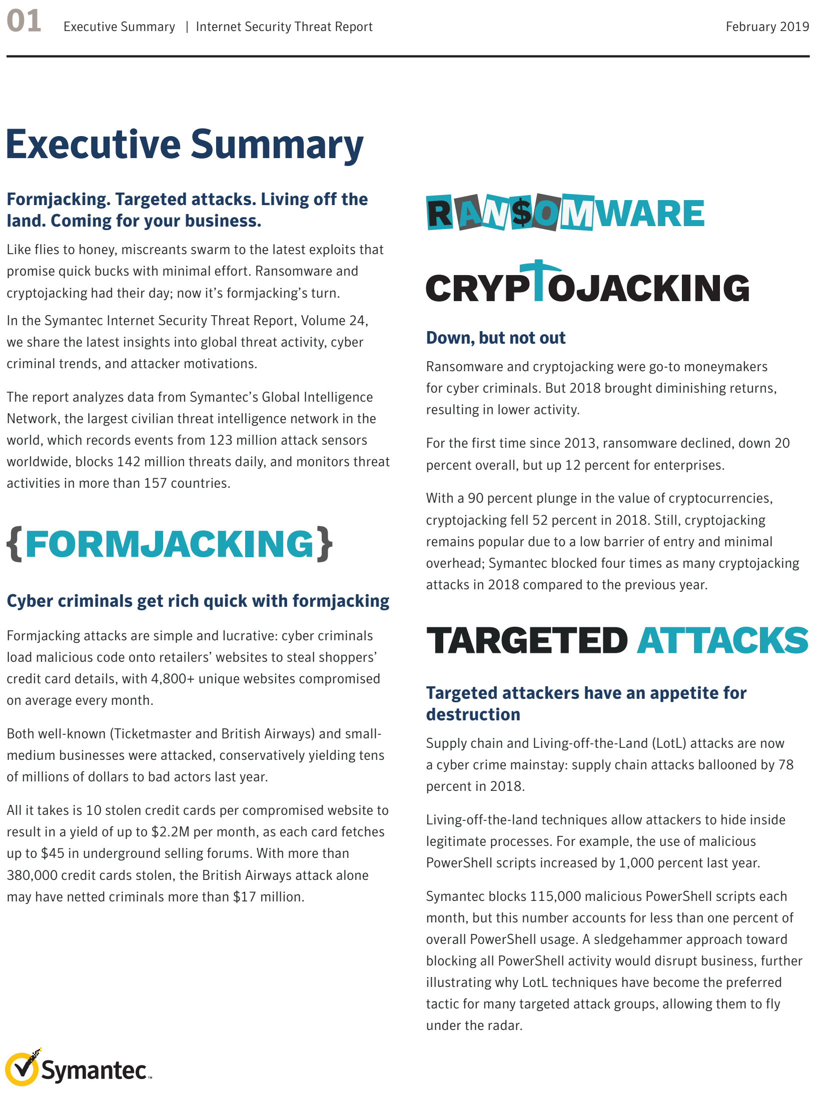
While threats are on the increase, the problem is exacerbated by the continued use of older operating systems. In particular, on Android™, only 20 percent of devices are running the newest major version and only 2.3 percent are on the latest minor release.

Mobile users also face privacy risks from grayware, apps that aren't completely malicious but can be troublesome. Symantec found that 63 percent of grayware apps leak the device's phone number. With grayware increasing by 20 percent in 2017, this isn't a problem that's going away.

For the details, download the
Symantec 2018 Internet Security Threat Report (ISTR)
https://go.symantec.com/ISTR

Symantec.

2019



01 Executive Summary | Internet Security Threat Report February 2019

Executive Summary

Formjacking. Targeted attacks. Living off the land. Coming for your business.

Like flies to honey, miscreants swarm to the latest exploits that promise quick bucks with minimal effort. Ransomware and cryptojacking had their day; now it's formjacking's turn.

In the Symantec Internet Security Threat Report, Volume 24, we share the latest insights into global threat activity, cyber criminal trends, and attacker motivations.

The report analyzes data from Symantec's Global Intelligence Network, the largest civilian threat intelligence network in the world, which records events from 123 million attack sensors worldwide, blocks 142 million threats daily, and monitors threat activities in more than 157 countries.

{FORMJACKING}

Cyber criminals get rich quick with formjacking

Formjacking attacks are simple and lucrative: cyber criminals load malicious code onto retailers' websites to steal shoppers' credit card details, with 4,800+ unique websites compromised on average every month.

Both well-known (Ticketmaster and British Airways) and small-medium businesses were attacked, conservatively yielding tens of millions of dollars to bad actors last year.

All it takes is 10 stolen credit cards per compromised website to result in a yield of up to $2.2M per month, as each card fetches up to $45 in underground selling forums. With more than 380,000 credit cards stolen, the British Airways attack alone may have netted criminals more than $17 million.

RAN$OMWARE

CRYPTOJACKING

Down, but not out

Ransomware and cryptojacking were go-to moneymakers for cyber criminals. But 2018 brought diminishing returns, resulting in lower activity.

For the first time since 2013, ransomware declined, down 20 percent overall, but up 12 percent for enterprises.

With a 90 percent plunge in the value of cryptocurrencies, cryptojacking fell 52 percent in 2018. Still, cryptojacking remains popular due to a low barrier of entry and minimal overhead; Symantec blocked four times as many cryptojacking attacks in 2018 compared to the previous year.

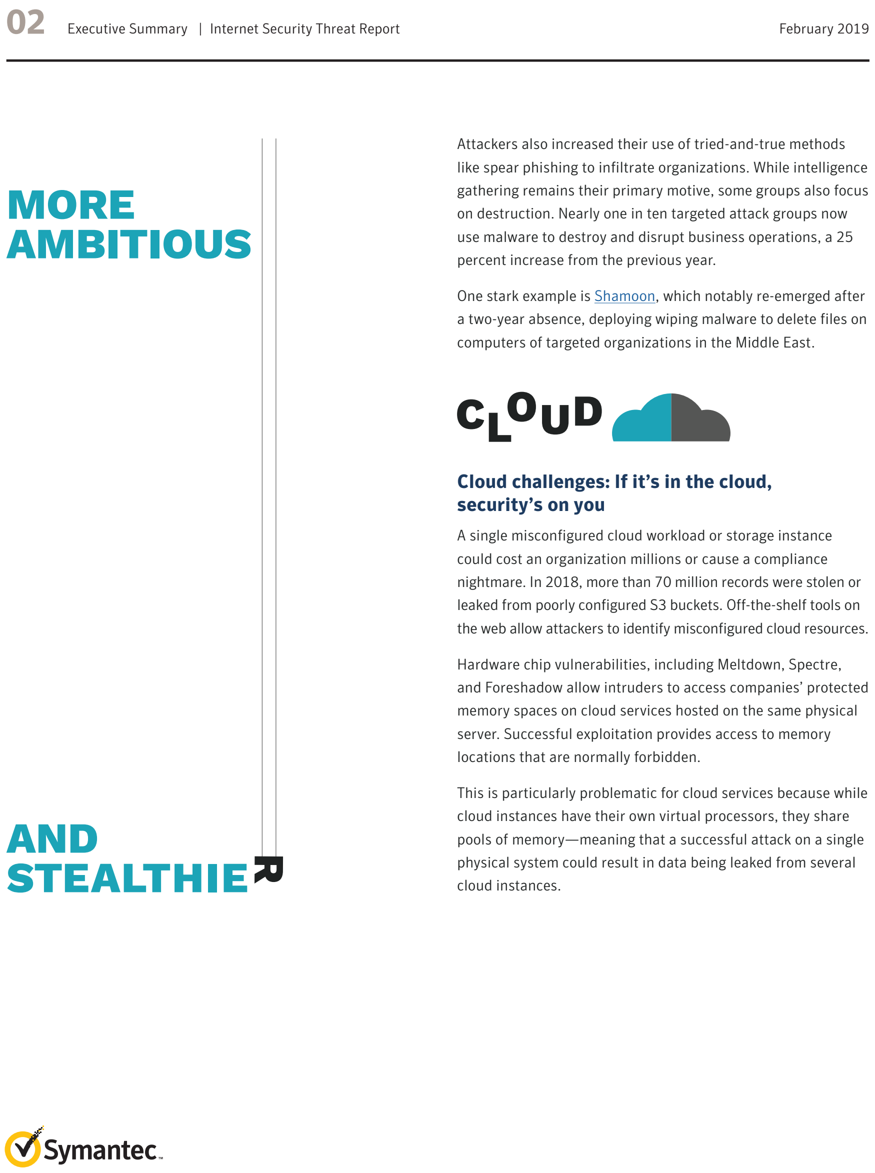
TARGETED ATTACKS

Targeted attackers have an appetite for destruction

Supply chain and Living-off-the-Land (LotL) attacks are now a cyber crime mainstay: supply chain attacks ballooned by 78 percent in 2018.

Living-off-the-land techniques allow attackers to hide inside legitimate processes. For example, the use of malicious PowerShell scripts increased by 1,000 percent last year.

Symantec blocks 115,000 malicious PowerShell scripts each month, but this number accounts for less than one percent of overall PowerShell usage. A sledgehammer approach toward blocking all PowerShell activity would disrupt business, further illustrating why LotL techniques have become the preferred tactic for many targeted attack groups, allowing them to fly under the radar.



02 Executive Summary | Internet Security Threat Report February 2019

MORE AMBITIOUS

AND STEALTHIER

Attackers also increased their use of tried-and-true methods like spear phishing to infiltrate organizations. While intelligence gathering remains their primary motive, some groups also focus on destruction. Nearly one in ten targeted attack groups now use malware to destroy and disrupt business operations, a 25 percent increase from the previous year.

One stark example is Shamoon, which notably re-emerged after a two-year absence, deploying wiping malware to delete files on computers of targeted organizations in the Middle East.

CLOUD

Cloud challenges: If it's in the cloud, security's on you

A single misconfigured cloud workload or storage instance could cost an organization millions or cause a compliance nightmare. In 2018, more than 70 million records were stolen or leaked from poorly configured S3 buckets. Off-the-shelf tools on the web allow attackers to identify misconfigured cloud resources.

Hardware chip vulnerabilities, including Meltdown, Spectre, and Foreshadow allow intruders to access companies' protected memory spaces on cloud services hosted on the same physical server. Successful exploitation provides access to memory locations that are normally forbidden.

This is particularly problematic for cloud services because while cloud instances have their own virtual processors, they share pools of memory—meaning that a successful attack on a single physical system could result in data being leaked from several cloud instances.

IoT

Your favorite IoT device is an attacker's best friend

Although routers and connected cameras make up 90 percent of infected devices, almost every IoT device is vulnerable, from smart light bulbs to voice assistants.

Targeted attack groups increasingly focus on IoT as a soft entry point, where they can destroy or wipe a device, steal credentials and data, and intercept SCADA communications.

And industrial IT shaped up as a potential cyber warfare battleground, with threat groups such as Thrip and Triton vested in compromising operational and industrial control systems.

ELECTION INTERFERENCE 2018

Did your social media feed sway an election?

With all eyes on the 2018 US Midterms, thankfully, no major disruptions landed. But social media continued as a hyperactive battlefield.

Malicious domains mimicking legitimate political websites were discovered and shut down, while Russia-linked accounts used third parties to purchase social media ads for them.

Social media companies took a more active role in combatting election interference. Facebook set up a war room to tackle election interference; Twitter removed over 10,000 bots posting messages encouraging people not to vote.

Get the details. Download the Symantec 2019 Internet Security Threat Report (ISTR)
https://go.symantec.com/ISTR

Security requirements*

*: some called these “goals”, “components” or “properties”.

How to describe “Security”

- The term “secure”, “privacy”, “trusted” appears in many different contexts and are often abused.
  - Secure operation system, Secure cloud, Secure Customers List Management, …
  - Privacy-preserving computation, privacy-enhancing technologies,…
  - Trusted computing, trust management, trustzone, …
  - Military grade encryption, …

- What does it mean? How to describe the security of a system?

- We need more precise definitions and terminologies.

Security Requirements: C-I-A triad

Broadly, “security” could be classified into these 3 requirements:

- **Confidentiality**

  Prevention of unauthorized disclosure of information.

- **Integrity**

  Prevention of unauthorized modification of information or processes.

- **Availability**

  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 compromised.

2. Integrity

- A student "hacked" into the university system and modified the grade. ***Integrity*** of the exam result is compromised.

- An application is being modified by an attacker. The integrity of the application is being compromised. The compromised application carries out key-logging: it captures the password entered by the user and sends it to the attackers. As a result, the confidentiality of the user password is compromised.

NSA: National Security Agency (USA)

3. Availability

- Chewing gum sticking to the car door lock.
- A botnet floods a web-server with large number of http requests. A legitimate http request now takes longer time to be processed. Thus, the quality of the service significantly degraded. In the extreme case, the web-server crashed and not able to provide web service. This is a ***distributed denial of service attack*** (DDoS) on the web-server, which compromise ***availability***.

Other Requirements

There are many other requirements. Some literatures group them under C-I-A, whereas some argue that they are fundamentally different requirements. For e.g. many view “Non-repudiation” as a special case of Integrity, while some view it fundamentally different. Read the context carefully. In this class, we treat “non-repudiation” as ”I”.

- Confidentiality
  - Anonymity, Privacy
  - Covert Channel

- Integrity
  - Non-Repudiation (digital signature)
  - Authenticity.
  - LLM Jailbreak prevention.
  - Deepfake detection.

- Other(?)
  - Accountability (e.g. monitoring and management of system log. Under I ?)
  - Traitor-Tracing (e.g. watermarking. Under C?)
  - Plausible deniability (Under C or I?)
  - etc

Threat Model

aka (Attack/Threat/Security) (model/setting/scenario). all 9 combinations.

- C-I-A is a broad definition. We might still need a more precise way to describe the security requirement.

- E.g.,
  - Consider the fingerprint system that unlocks mobile phone. What type of attack it can prevent. An attacker who pressing his/her fingerprint on the sensor? An attacker who has the owner’s fingerprint and can fabricate a physical copy? An attacker who can dissembles the phone and read the storage? Or an attacker who wants to steal information of the owner fingerprints?

  - Consider a secure CRM (customer relation management) solution aims to protect contacts (information of the customers). The contacts are stored in the cloud which could be pulled by mobile phones. What does “secure” means, and who are the attackers? Is the attacker a by-passer who try to extract contacts from lost phone? Or a “man-in-the-middle” between the phones and the cloud? Or an employee who wants to download all the contacts and illegally sell the info?

Threat Model: Which system is more secure?

- One rigorous way to describe the security achieved by a system is by describing the class of attacks that it can prevent. The system is considered secure w.r.t. those class of attacks.

- We can describe a class of attacks by:
  - the attacker's goals
  - the attacker's capabilities (e.g. information and services it has access to)

  This description is known as attack model, threat model, adversary model or security model.

- With an attack model, we can compare two systems. If some attacks are successful on system S_1, whereas S_2 can prevent all attacks described by the model, then S_2 is more secure than S_1 w.r.t. the attack model.

Why threat model?

- To protect a system, it is important to first understand the threat model. (e.g. many jump to adopt blockchain without evaluating the security requirement).

- Do not adopt mismatch protection mechanism. Some examples would be studied later.

Why so difficult to be secure

Trade-off in Security

There is a trade-off of ***security*** with ***ease-of-use***, ***performance*** and ***cost***.

- (***ease-of-use***) Security mechanisms interfere with working patterns users originally familiar with. (aka ***usability***).
- (***performance***) Security mechanisms consumes more resources and lowers performance.
- (***cost***) Security mechanisms are expensive to develop and manage.

- Difficulty in achieving Security

- **(Security not considered)** Many systems do not consider security during the early design stage. In the early stage, typically the main concerns are on usability, cost and performance. This applied to new systems (e.g. online game, zoom), and existing protocol (e.g. DNS) that was designed much earlier.

- **(Difficult to formulate requirements)** Difficult to scope the appropriate security requirements. Designers not aware of many possible attack scenarios (e.g. many side-channel were discovered recently. Earlier implementation of crypto didn't consider the threat).

- **(Difficult to Design)** System most vulnerable at its weakest point, and there are many constraints. (E.g we understand email spoofing very well. But there is no practical foolproof design.)

- **(Implementation Bugs)** Even if the design is secure, the system may not be properly implemented, especially for large, complex systems. Also, it is difficult to verify whether an implementation is correct.

- **(Difficult to operate/manage)** Human in-the-loop. Complexity leads to configuration errors, mismanagement of patches, credential, etc. (e.g. developers' accounts remain in production system)

Known vulnerabilities: CVE and zero-day

- CVE (Common Vulnerabilities and Exposures) is a repository containing discovered vulnerabilities. The repository is public, and thus the whole community is aware of the vulnerabilities. It is a list of entries—each containing an identification number, a description, and at least one public reference. Recently well-known: Log4j.

(not to confuse CVE with CWE, a related but different repository on vulnerabilities. A CWE is a form/concept, while a CVE is an actual instances. A few CVE could belong to a same CWE.)

- Some vulnerabilities are discovered but not yet published. These are called “zero-day” vulnerabilities. If an attacker deploy attacks on zero-day vulnerabilities, the victims have “zero-day” to react.
- Zero-day vulnerabilities are not easy to get.

“Zerodium, a company that buys and sells zero day research, lists $1.5 million as the top price it will pay for a single submission. The company paid out $600,000 per month for undisclosed vulnerabilities, according to a 2015 interview with the CEO.”

Cyberscoop, *https://www.cyberscoop.com/zero-day-vulns-are-rarer-and-more-expensive-than-ever/*

Implementation errors among CVE

E.g.

- Heartbleed* : **CVE-2014-0160**
- Log4j : **CVE-2021-44832**

A significant portion of reported vulnerabilities are considered as "implementation bugs". See report from NIST (National Institute of Standards and Technology):

D. R. Kuhn, M.S. Raumak, R. Kacker, *An Analysis of Vulnerability Trends, 2008-2016*, https://ws680.nist.gov/publication/get_pdf.cfm?pub_id=923379

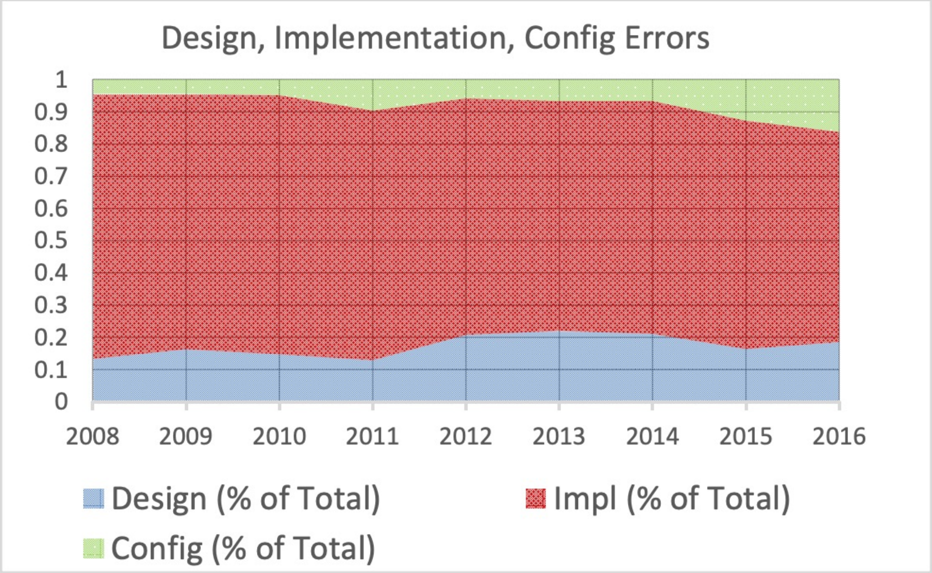


Fig. 2. Vulnerability Class Trends, 2008-2016

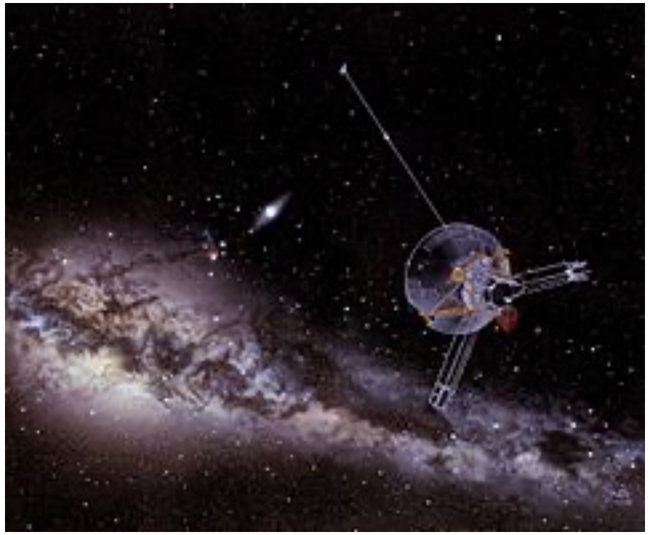
*: to be covered in secure programming.

Lack of “Adversarial thinking” during design

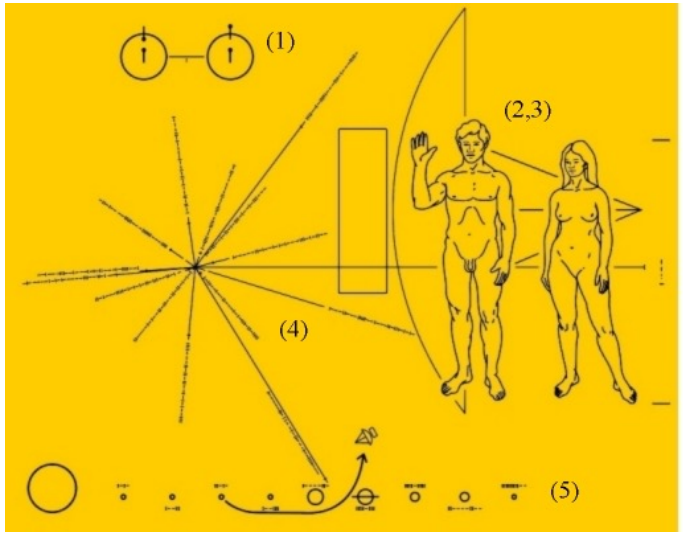
One of the learning outcome of this course is to develop “adversarial thinking”, i.e. always assume that there are attackers who try to compromise the system and think like them.

Sound straightforward but often overlooked (particularly early computer systems).

Consider Pioneer 10 program which is carrying the following plaque into deep space, with information on Earth’s location and human. Didn’t the rocket scientists think from the alien’s point of view?



https://en.wikipedia.org/wiki/Pioneer_10



List of Images:

1) The Hydrogen Atom

2) The Happy Couple

3) The Pioneer Spacecraft

4) Distances and Directions to 14 Pulsars

5) The Solar System

http://paulgazis.com/Humor/RealPioneerPlaque/RealPioneerPlaque.htm

Many network protocols, when first designed, openly broadcast its address and welcome connections. “hello, my name/address is 1112411. Anyone want to connect?”

(If a mobile device continuously broadcasts this information, a curious eavesdropper could track its location by deploying sensors in various places.)

Remarks

Some other notions: Threat-Vulnerability-Control

Threat: A set of circumstances that has the potential to cause loss or harm.

(e.g. an attacker with control of the workstation in the lecture theatre could maliciously gather sensitive info such as passwords)

Vulnerability: a weakness in the system.

(e.g. anyone can reboot the workstation from USB or Disk to gain control).

Control: A control, countermeasure, security mechanism is a mean to counter threats. (see [PF1.5]
Prevent, Deter, Deflect, Mitigate, Detect, Recover)

(e.g. restrict physical access to the workstation, disable USB booting).

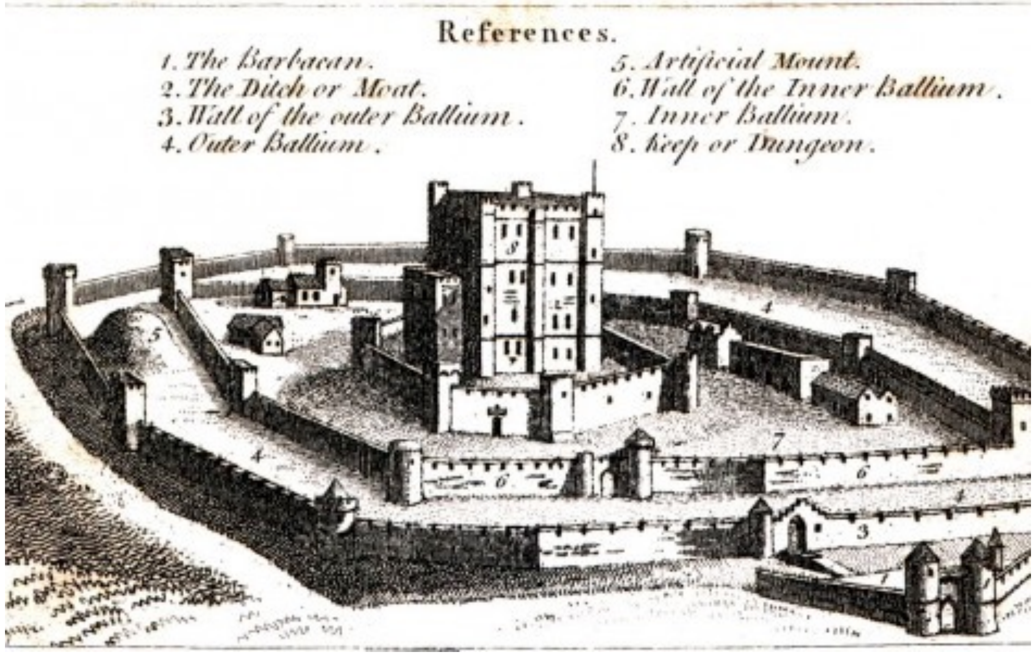
A ***threat*** is blocked by ***contro**l* of a ***vulnerability***

Analogy with Medieval Castle.

- We are facing smart adversaries who are actively looking for vulnerabilities.
- Protection mechanisms
  - All round defense: “Security depends on the weakness point.”
  - Layered defense.
  - Access control
  - etc (Death trap, obscurity,…)

More than that:

- Different types of attackers with different goals and capabilities.
- A wide range of security requirements.



see http://blog.smartbear.com/design/what-medieval-castles-can-teach-you-about-web-security/

Services:
markets; admin office; etc

Users:
citizens; travelers, etc

Attacker’s goals:
Capture the whole city;
Steal info;
Disrupt services;
Ransom etc.

Summary & Takeaways

- Need precise formulation of “Security” for analysis.
- C-I-A requirement.
- Aware of
  - Security Trade-off (usability, cost)
  - Difficulty to achieve
    - Attackers go for the weakest point,
    - Implementation flaw,
    - legacy system, don’t-care,
    - Designers not aware of the attack scenarios (info attacker can access, attacker’s goal)
    - human error.
  - Need to be managed
  - Adversarial thinking in analysis (think like the attacker when analyzing a system)