CS2107

Lecture 0

Admin + Overview

CS2107

Lecturer: Chang Ee-Chien

Tutors (tutorials): Vijeth Tumkur Aradhya, Sriram Sami, … TBA

Tutors (assignments): TBA

References:

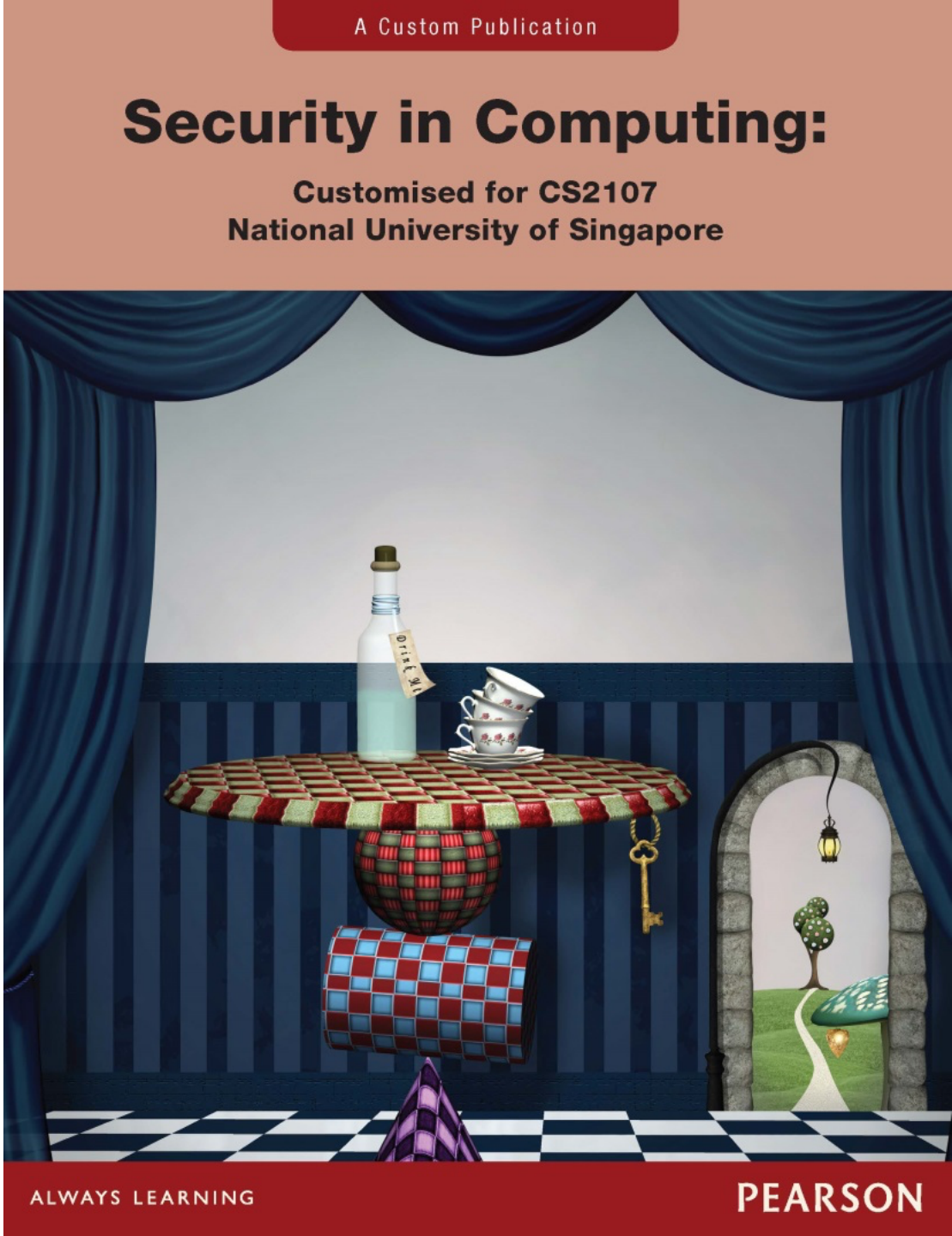
- Security in Computing (5th ed). Prentice Hall.
  Customized version (Chapter 1 to 6) available in Co-ops.
  (Many examples.)
  In our slides, the reference [PFx.y] refer to chapter x section y of this book.
- Computer Security (3rd ed), Dieter Gollman, Wiley. (Very concise. Abstract concepts clearly explained. Good to have if you plan to take higher level security courses.)
- Security Engineering (2nd ed), Ross Anderson. (Free online! Very comprehensive.)

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

Luminus:

- Lecture notes
- Forum

Available in **NUS Co-op @ Forum**



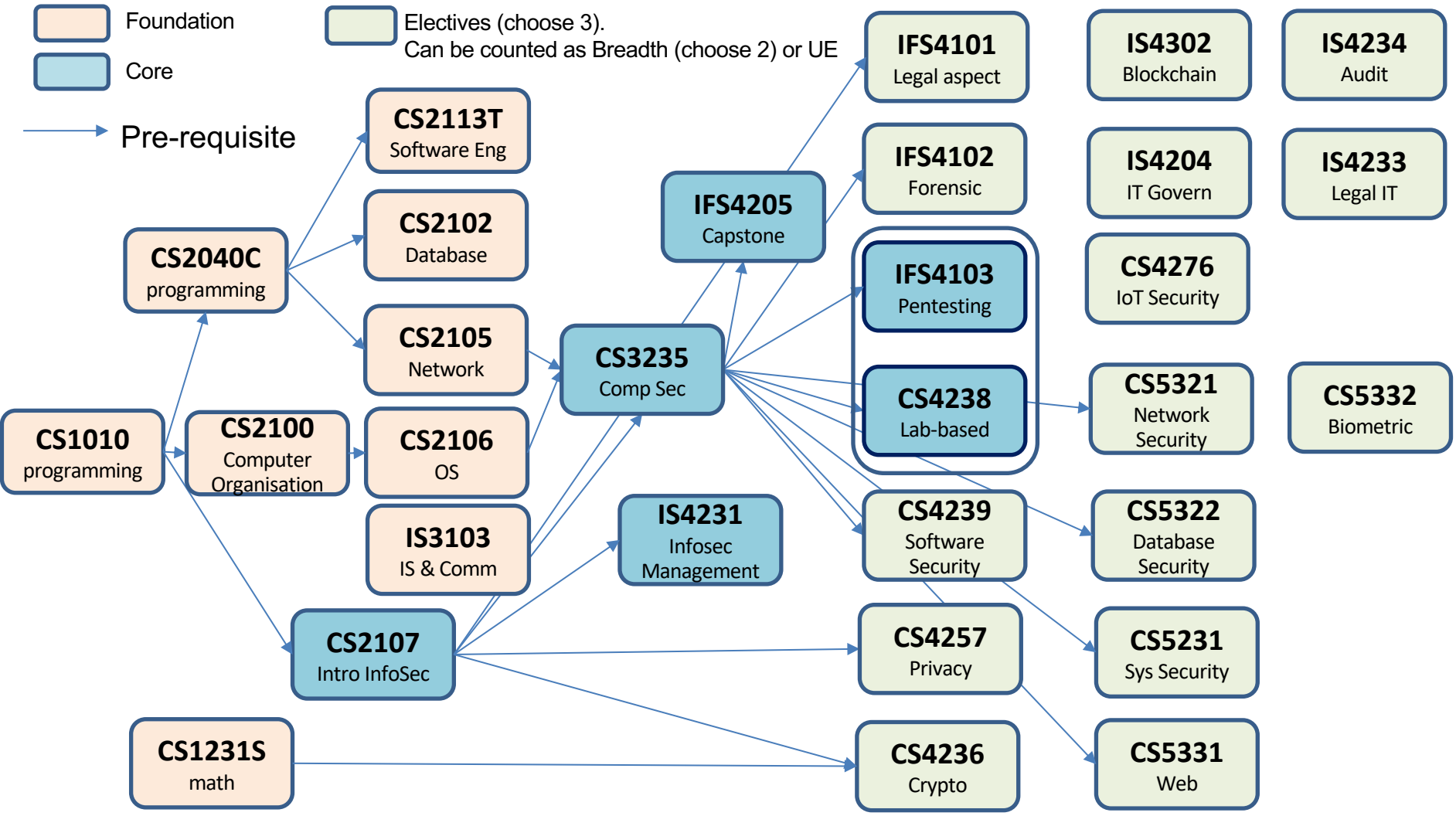
Teaching Mode

- 12 Lectures
- 9 Tutorials

(tentative)

- 2 CTF assignments (40%)
- Online quiz(s) during lecture (15%)
- Tutorial attendance/participation (10%)
- 1 Group Presentation on open-ended topic (5%)
- Final Quiz (Last Lecture) assignment (30%)

Security-related modules and BCOMP InfoSec requirements



Plagiarism

- Based on “honor system”. When found, will be seriously dealt with. At least 2, 3 grade downward or escalating to university.

Quiz: Allow to access web. No interaction at all.

Assignment: While discussion is encouraged, sharing of “flag” and program (that you are supposed to write) is considered plagiarism. Using existing tools in public domain is accepted. We would make clear the scope when releasing the assignment.

Evidences: Witnesses. Access-log.

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

Who

- All IT professionals.
- Preparation for in-depth studies in security.

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.

Tentative Schedule

Wk	Lecture				tutorial	
1	1		Introduction. C-I-A. Classical Cipher	cryptanlaysis on classical ciphers	-	
2	2		Encryption	Dictionary attacks Phlishing	-	
3	3		Password, 2 factor, phishing	DDoS email/SMS spoofing	C-I-A, key-strength, encryption	
4	4		Data Integrity. Hash, Mac, Signature	Email spoofing proxy re-encryption	Password. Padding Oracle	Release Assignment 1
5	5		Authentication Protocol (PKI, Certificate)		Buffer	
6	6		Network Security	DNS attack. ARP attack	Hash, mac	Deadline
7	(Recess)					
7	7		Network Security + Group presentation topics		Signature + PKI	
8	8		Access control		Proxy re-encryption	Mid-term(?)
9	9		Secure Programming		Network Security Access control	Release Assignment 2
10	10		Secure Programming		Secure Program	
11	11		Web-security	XSS	group presentations	Deadline
12	12		Reserved		group presentations	
13	13		- Quiz, assignment(?) **Reserve this date.**			
	Exam					

0.2 What is Computer/Info Security

- System may fail, which could be due to operator mistakes (*e.g. a system file is accidentally deleted, which later leads to system "crashed"*), hardware failures, poor implementation (*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 concerned with 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.*)

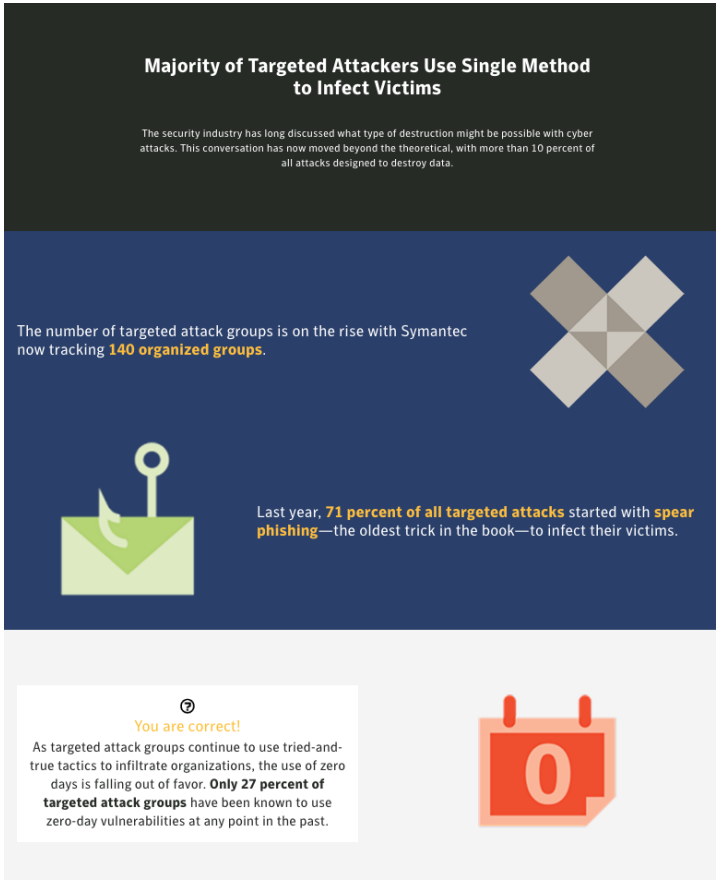
see [PF3.1page157] Undocumented Access Point (a form of *backdoor*)

Why important?

Attacks Trend

- Semantec 2018 Internet Security Threat Report

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



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

Read the executive summary

2018

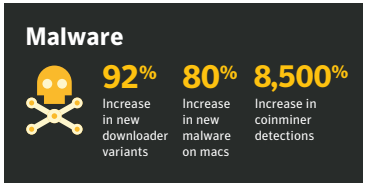
(2018) https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-executive-summary-en.pdf
(2019) https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-executive-summary-en.pdf
(2009) http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xv_04-2010.en-us.pdf

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.

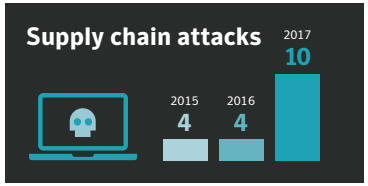
Coin mining attacks explode

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.



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.



Spike in software supply chain attacks

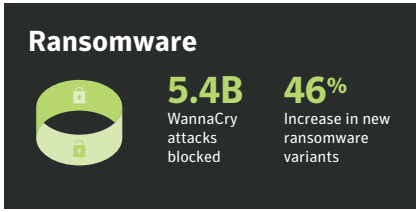
Despite the EternalBlue exploit wreaking havoc in 2017, the reality is that vulnerabilities are becoming increasingly difficult for attackers to identify and exploit. In response to this, Symantec is now seeing an increase in attackers injecting malware implants into the supply chain to infiltrate unsuspecting 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.

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.



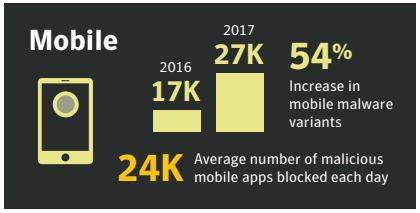
Drop in zero days can't halt the rise in targeted attacks

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.



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

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.

RANSOMWARE

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.

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 Definitions: C-I-A triad

- **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.

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. some view that “Non-repudiation” as fundamentally different from “Integrity”. Read the context carefully.

- Confidentiality
  - Anonymity, Privacy
  - Covert Channel
  - Plausible deniability.
- Integrity
  - Non-Repudiation (digital signature)
  - Integrity (data integrity, process integrity)
  - Authenticity.
- Other(?)
  - Accountability
  - Traitor-Tracing
  - etc

Adversary Model: Which system is more secure?

- While the previously mentioned security definition describe the requirement, very often they alone is not rigorous enough to pin-point the security achieved (still ambiguous.. e.g "encryption achieves confidentiality".). One rigorous way to describe/evaluate the security of 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 giving:
  - the attacker's goals
  - the attacker's resources (including information and services it has access to).

  This description is also known as attack model, adversary model, security model.

- Under an adversary model, we can compare two systems. If some attacks are successful on S_1, whereas S_2 can prevent all possible attacks (under the adversary model), then S_2 is more secure than S_1 w.r.t. the attack model.

Understand the security requirements

- To protect a system, it is important to first understand the security requirements. Before adopting a “cool” security mechanism, evaluate whether it can indeed achieve the intended requirements. (e.g. many jump to adopt blockchain without knowing what it can achieve).

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

Why so difficult to be secure

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), and existing protocol (e.g. DNS) that was designed much earlier. (good recent example: zoom)

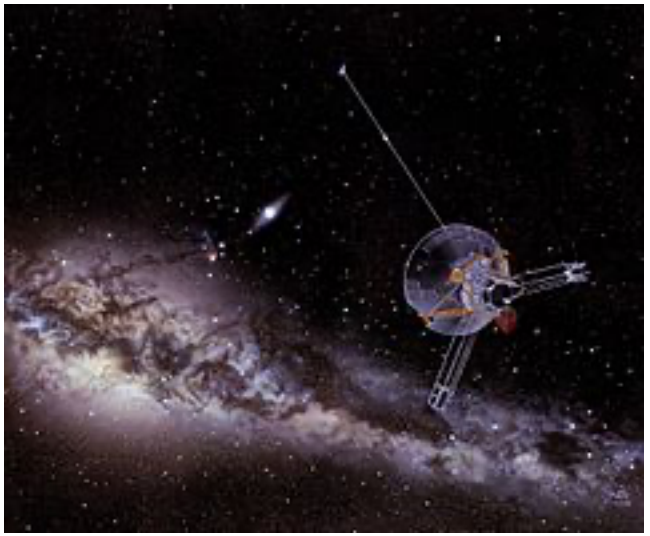
- **(Difficult to formulate requirements)** Difficult to scope the appropriate security requirements. Designers not aware of many possible attack scenarios (e.g. side-channel attack).

- **(Difficult to Design)** System most vulnerable at its weakest point, and there are many constraints.

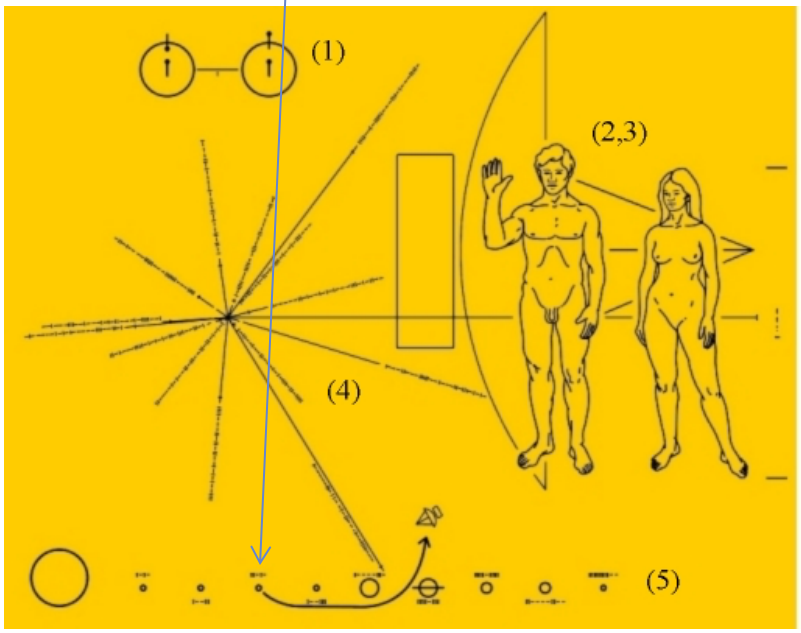
- **(Implementation Flaw)** Even if the design is secure, the system may not be properly implemented, especially for large, complex systems. Also, it is difficult to verify that implementation is correct.

- **(Difficult to manage)** Human in-the-loop. Complexity leads to configuration errors, mismanagement of patches, credential, etc.

Pioneer 10 program… didn't they think from an adversarial alien's point of view?



"we are here, please visit us…"



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

Many network protocols openly broadcast its present and welcome connections…

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

CVE and zero-day vulnerabilities

- 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. (not to confuse 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 attack exploiting these vulnerabilities is deployed, 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/*

Saw this in website. While it is good to keep software up-to-date, but does it really protect against zero-day?

https://us.norton.com/internetsecurity-emerging-threats-how-do-zero-day-vulnerabilities-work-30sectech.html

Things to remember about zero-day vulnerabilities

1. Keep your software up-to-date to help protect yourself against a zero-day vulnerability.
2. Check for a solution when a zero-day vulnerability is announced. Most software vendors work quickly to patch a security vulnerability.
3. Don't underestimate the threat. Cybercriminals will seek to exploit security holes and gain access to your devices and your personal information. They can use your information for a range of cybercrimes including identity theft, bank fraud, and ransomware.
4. Always use a reliable security software to help keep your devices safe and secure.

Implementation errors among CVE

- E.g. Heartbleed* is listed as **CVE-2014-0160.**
- A significant portion of reported vulnerabilities are "implementation errors". 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

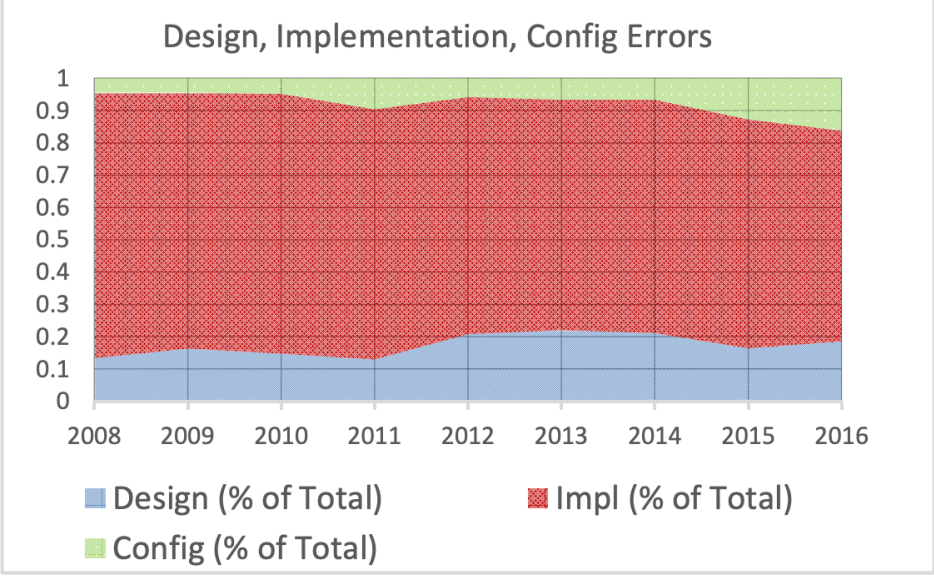


Fig. 2. Vulnerability Class Trends, 2008-2016

*: to be covered in secure programming.

Trade-off in Security

There is a trade-off of the Security with ease-of-use, performance and cost.

- (***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.

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 ***control*** of a ***vulnerability***

Remarks

Remarks on security terminologies

There are many inconsistent usages of security terminologies. For e.g. the term "privacy" in the following statement

"HTTPS provides privacy, integrity and authenticity for .."

refer to confidentiality (i.e. if Alice uses the free airport wifi, and submit a report to IVLE via HTTPS, even the airport operator is unable to know the content of the report), whereas the "privacy" in

"social networking sites vary in the level of privacy offered"

"Advocates have raised the issue of privacy in mobile advertisement."

refers to revelation of personal information like age, salary, locations, that the individuals do not intend to share (e.g. Alice installed a calculator apps on mobile phone. The apps obtains the GPS location and contact list, and share it with another company.)

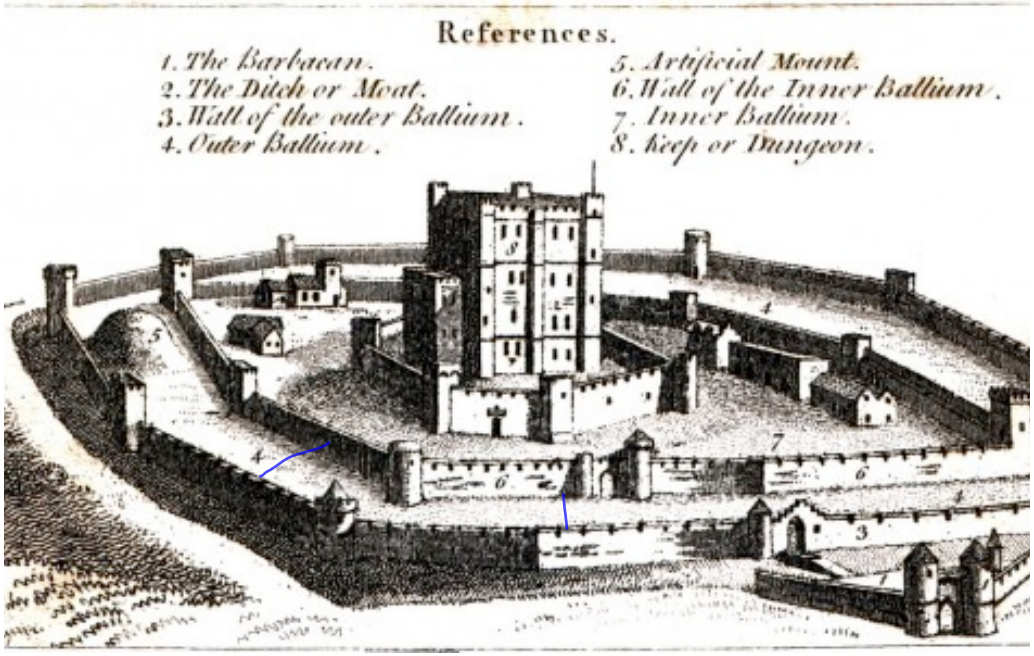
There is no single definition of security. Different fields, experts, documents may use different definitions. When reading a document, take special note of the context.

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

Attackers:
Capture the whole city; Steal info; Disrupt services; Ransom etc.