CE4062/CZ4062
Computer Security

Lecture 1: Introduction

Tianwei Zhang

Teaching Staff Members

Lecturers:

- Asst. Prof. Zhang Tianwei (1st half): tianwei.zhang@ntu.edu.sg
- Dr. Tay Kian Boon (2nd half, course coordinator): kianboon.tay@ntu.edu.sg

Teaching Assistants

- Wang Hanqin: hanqin001@e.ntu.edu.sg
- Zhou Jianan: jianan004@e.ntu.edu.sg

What is Computer Security

Allow intended use of computer systems

Prevent unwanted use that may cause harm

Why is there unwanted use of computer systems?

Attack Motivation – Financial Profit

Steal personal data and sell them to the black market

17 Feb 2021 09:00PM
(Updated: 18 Feb 2021 11:26AM)

Bookmark

Nearly 130,000 Singtel customers' personal information, including NRIC details, stolen in data breach

A Singtel logo is seen on its building in Singapore, Aug 11, 2016. (File photo: AFP/Roslan Rahman)

SINGAPORE: Personal information of nearly 130,000 Singtel customers was stolen after a recent data breach of a third-party file-sharing system, the local telco said on Wednesday (Feb 17).

Singtel has completed initial investigations into the breach and established which files on the Accellion file transfer appliance were accessed illegally, the company said in a news release.

cna

SINGAPORE

Singapore health system hit by 'most serious breach of personal data' in cyberattack; PM Lee's data targeted

By Kevin Kwang
@KevinKwangCNA

20 Jul 2018 05:29PM
(Updated: 18 Oct 2018 11:17AM)

Bookmark

Singapore

Singapore health system hit by 'most serious breach of personal data' in cyberattack; PM Lee's data targeted

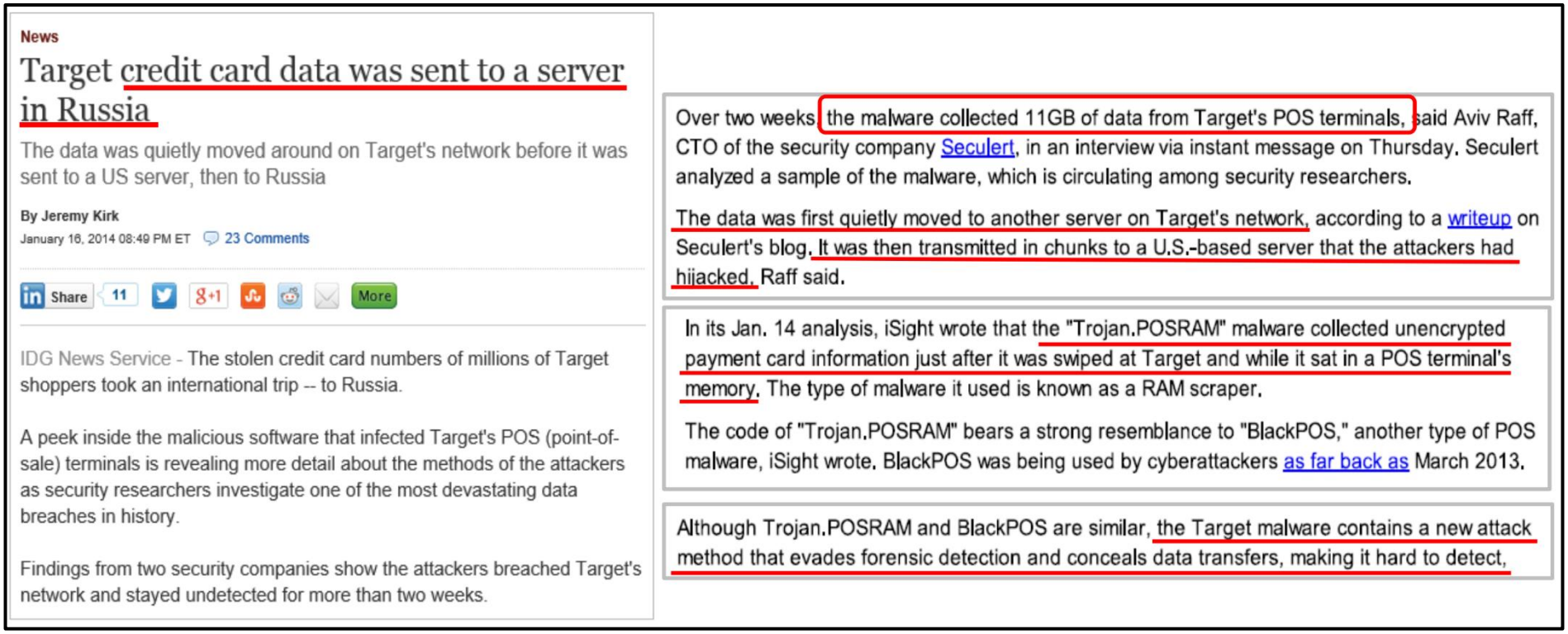
A total of 1.5 million SingHealth patients' non-medical personal data were stolen, while 160,000 of those had their dispensed medicines' records taken too, according to MCI and MOH.

Passwords and usernames of staff from MOH, MOE and other agencies stolen and put up for sale by hackers

Attack Motivation – Financial Profit

Steal credit card information or bank accounts

- Malware targeting different devices: ATM, POS machine, website…



News

Target credit card data was sent to a server in Russia

The data was quietly moved around on Target's network before it was sent to a US server, then to Russia

By Jeremy Kirk
January 16, 2014 08:49 PM ET 23 Comments

Share 11 8+1 More

IDG News Service - The stolen credit card numbers of millions of Target shoppers took an international trip -- to Russia.

A peek inside the malicious software that infected Target's POS (point-of-sale) terminals is revealing more detail about the methods of the attackers as security researchers investigate one of the most devastating data breaches in history.

Findings from two security companies show the attackers breached Target's network and stayed undetected for more than two weeks.

Over two weeks, the malware collected 11GB of data from Target's POS terminals, said Aviv Raff, CTO of the security company Seculert, in an interview via instant message on Thursday. Seculert analyzed a sample of the malware, which is circulating among security researchers.

The data was first quietly moved to another server on Target's network, according to a writeup on Seculert's blog. It was then transmitted in chunks to a U.S.-based server that the attackers had hijacked, Raff said.

In its Jan. 14 analysis, iSight wrote that the "Trojan.POSRAM" malware collected unencrypted payment card information just after it was swiped at Target and while it sat in a POS terminal's memory. The type of malware it used is known as a RAM scraper.

The code of "Trojan.POSRAM" bears a strong resemblance to "BlackPOS," another type of POS malware, iSight wrote. BlackPOS was being used by cyberattackers as far back as March 2013.

Although Trojan.POSRAM and BlackPOS are similar, the Target malware contains a new attack method that evades forensic detection and conceals data transfers, making it hard to detect,

Attack Motivation – Financial Profit

Ransomware

- Inject into the computer, encrypt the data and request for ransom

WannaCry ransomware

Attack Motivation – Politics

Government actors

Private activism

Stuxnet 'hit' Iran nuclear plans

22 November 2010

Behind the 'Flame' malware spying on Mideast computers (FAQ)

With possible ties to malware targeting Iran, the Flame spying software is seen as the latest cyber espionage attempt from a nation state.

Elinor Mills

June 4, 2012 6:28 a.m. PT

8 min read

WikiLeaks supporters disrupt Visa and MasterCard sites in 'Operation Payback'

MasterCard and Visa attacked after restricting dealings with WikiLeaks – and hackers say Twitter is next

Supporters of Julian Assange in London. WikiLeaks supporters Anonymous have launched a campaign of online attacks against perceived enemies. Photograph: Peter Macdiarmid/Getty Images

Emerging Security Issues with New Technologies and Situations

Zoom's Security and Privacy Issues

- Zoom's **randomly-generated meeting ID No. could be predicted** (and even brute-forceable), allowing bad actors to intrude, disrupt and eavesdrop on meetings. The company subsequently replaced meeting IDs with a "cryptographically strong" one and made passwords a default for users to join a meeting.
- **Security flaw in the app could let websites hijack Mac cameras**. The company subsequently patched its software and uninstalled a local web server that created the vulnerability.
- The app **sent data about a user's time zone and city, as well as details about the user's device to Facebook**, even if the user did not have a Facebook account.
- The company tightened their privacy policy after concerns surfaced about user's personal information being used to target ads.
- Zoom allegedly leaked user information because of an issue with how the app grouped contacts.
- Zoom allegedly **misled users to believe video meetings were secured with end-to-end encryption** instead of transport encryption.

Emerging Security Issues with New Technologies and Situations

Covid-19 pandemic meets new security challenges

News

Watch out for fake govt websites and links by scammers taking advantage of COVID-19 situation

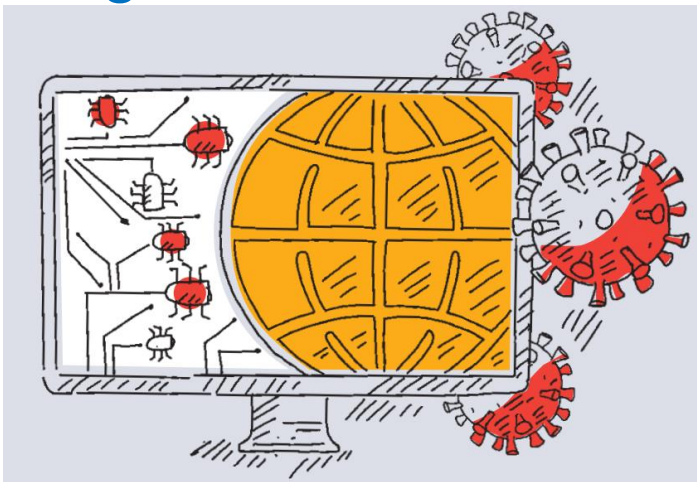
Published on 28 Apr 2020 Source: https://www.gov.sg/article/watch-out-for-fake-govt-websites-and-links-by-scammers-taking-advantage-of-covid-19-situation

SingCERT warns of fake COVID-19 contact tracing apps containing malware

Singapore 12 Jun 2020 03:59PM Source: https://www.channelnewsasia.com/news/singapore/covid-19-singcert-fake-contact-tracing-apps-download-privacy-12829624

Cybercriminals are exploiting fears of the pandemic to steal personal information

PUBLISHED WED, APR 15 2020•1:18 AM EDT Source: https://www.cnbc.com/2020/04/15/coronavirus-cybercriminals-are-targeting-people-through-phishing-scams.html



In Singapore:

384 COVID-19-related scams reported in 2020

- Uptick in number of cases involving cybercriminals attempting to capitalise on COVID-19 to steal personal information and credentials which will allow them to gain access to networks and/or make financial gains.

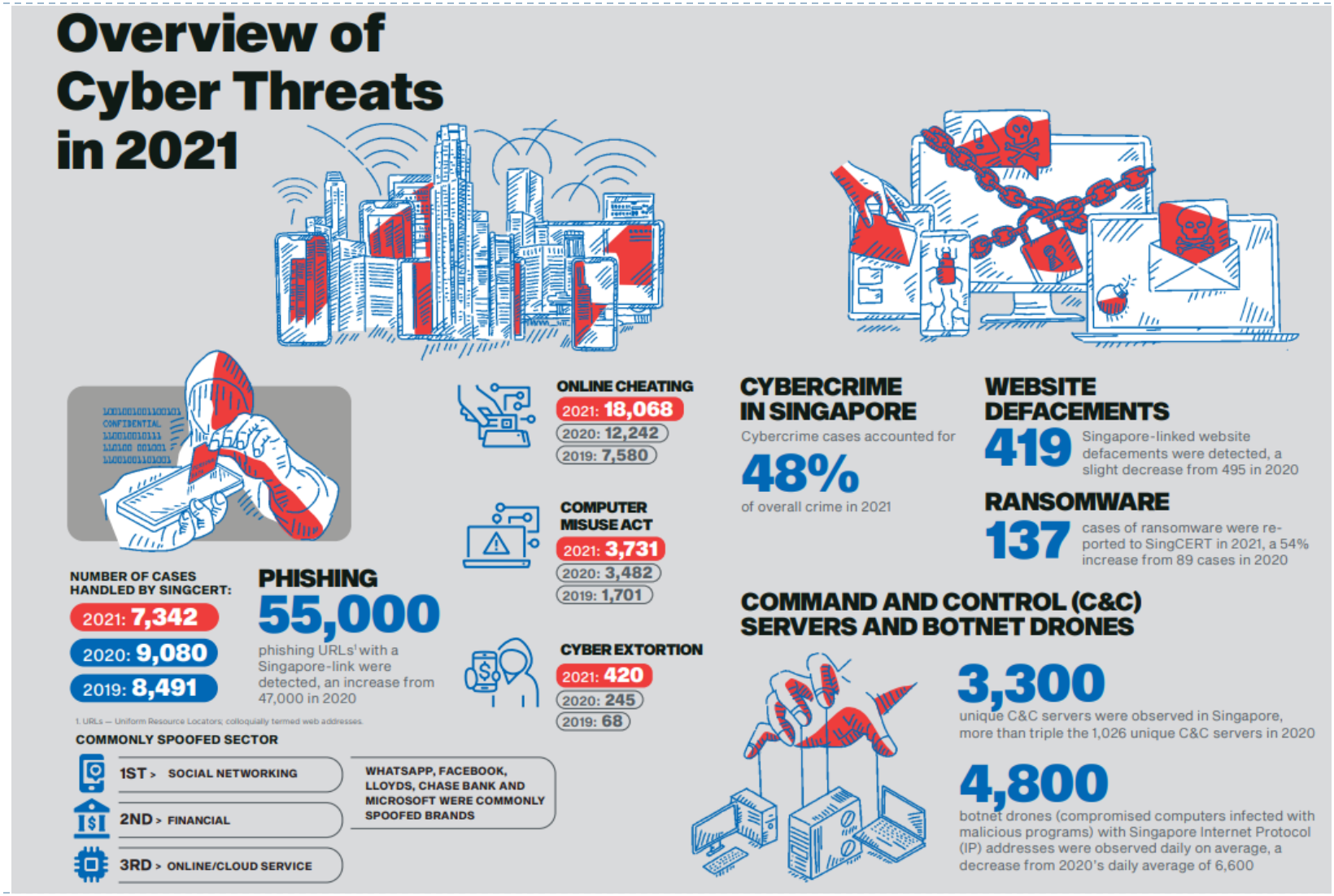
- Some malware strains deployed* include known credential-stealing malware such as AZORult, Cerberus, Lokibot and TrickBot.

- There are **fake contact tracing apps** that are embedded with malware that can be used to conduct malicious activities, such as monitoring users' activities on their devices or stealing personal data.

- These threats have proliferated across many sectors, including healthcare, manufacturing, pharmaceutical and transportation.

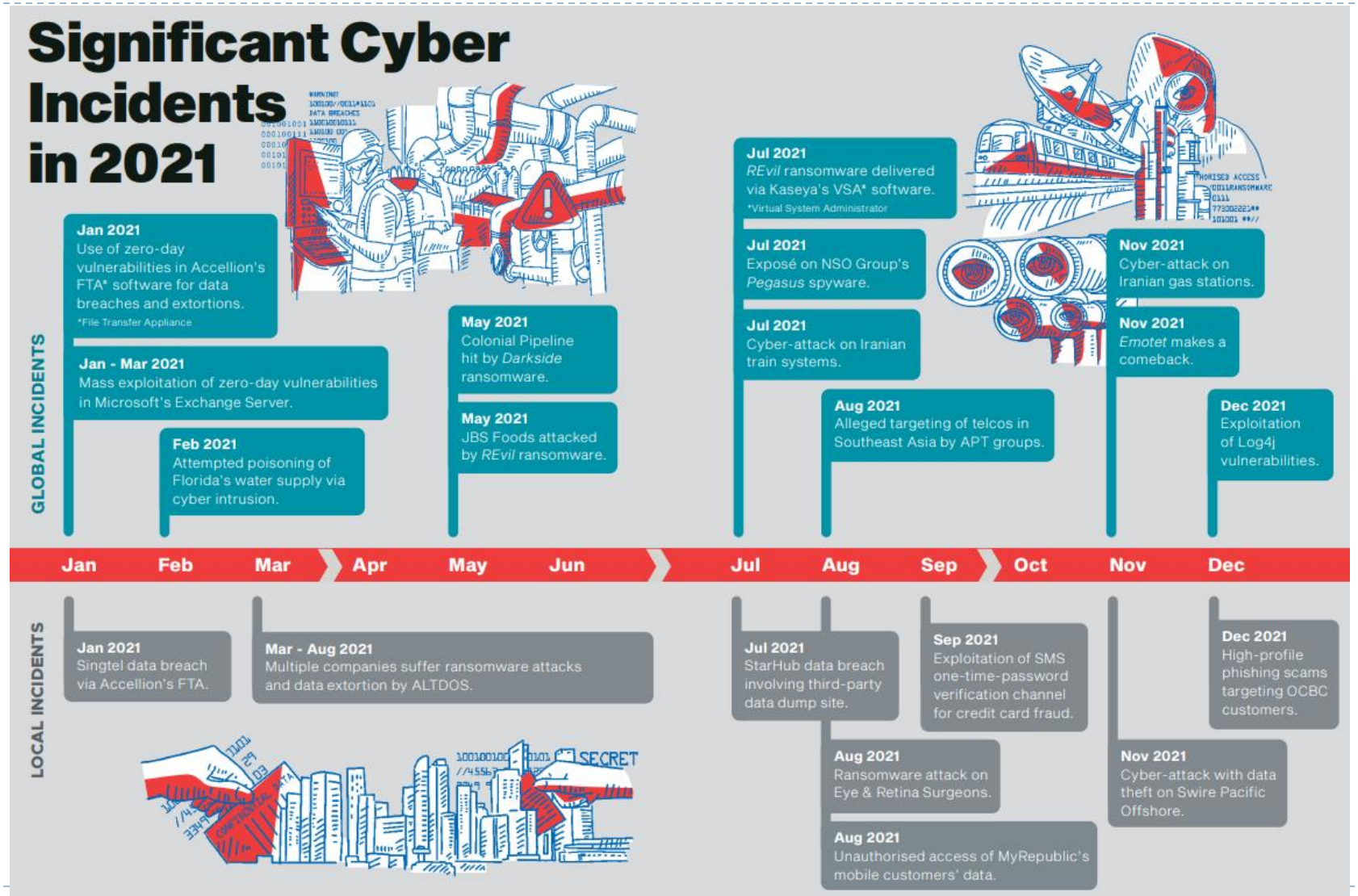
Source: Capitalising on COVID-19 Pandemic, CSA (published 1 April 2020)

Singapore Cyber Landscape 2021



https://www.csa.gov.sg/News/Publications/singapore-cyber-landscape-2021

Singapore Cyber Landscape 2021



https://www.csa.gov.sg/News/Publications/singapore-cyber-landscape-2021

Computer System Security

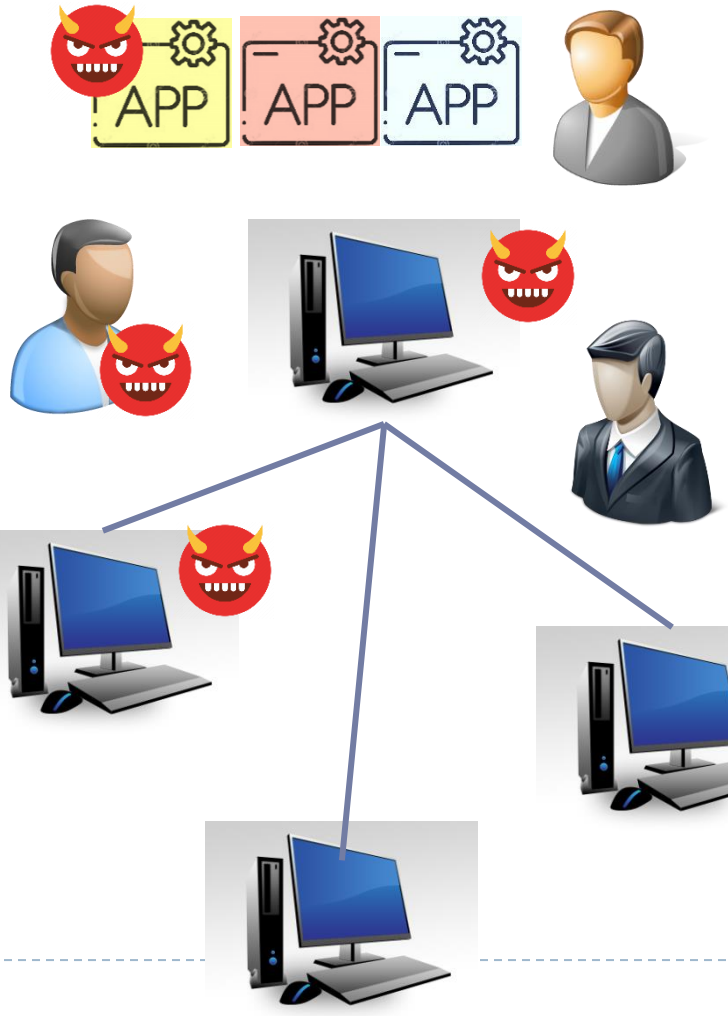
Provide a protected environment for data and their processing

Standalone computer single user monoprogram

- Physical security

Standalone computer single user multiprogram

- Physical security
- Process protection



Standalone computer multiple user

- Physical security
- Process protection
- Data protection
- User authentication

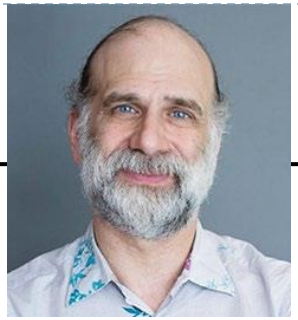
Networked computer

- Physical security
- Process protection
- Data protection
- User authentication
- Communication protection

Why is Security so Hard

"Security engineering is about building systems to remain dependable in the face of malice, error, or mischance."

-- Rose Anderson



"Security involves making sure things work, not in the presence of random faults, but in the face of an intelligent and malicious adversary trying to ensure that things fail in the worst possible way at the worst possible time … again and again. It is truly programming Satan's computer."

-- Bruce Schneier

System Security Failures

Secure information systems may be broken because:

- Cryptographic algorithms are broken
- Security features are not designed correctly
- Security features are not used correctly
- Security components are not implemented correctly
- Security components are not configured properly
- Security is not managed properly
- Threat environment may change and assumption invalid

Learning Outcome

Understand vulnerabilities associated with computer systems, and how they can be mitigated.

Understand security mechanisms in modern computer systems, its role and its importance.

Understand techniques for implementing security policies

Administrative Matters

Each week we have (full-time):

- A two-hour lecture (8:30 – 10:30am Friday, physical at LT2A)
- A one-hour tutorial (10:30 – 11:30am Monday).
  - First tutorial is in Week 3 (Public holiday – will release the video recording for e-learning)
  - Week 4 – Week 7: physical at LT1

Each week we have (part-time):

- A three-hour lecture & tutorial (starting at 7pm Monday, physical at TR+3)

Course materials will be made available through NTULearn

Assessment

2 Quizzes (35% each)

- Quiz 1: lecture slot in week 7
  - Full-time: 8:30 – 9:30am 24 February
  - Part-time: 7:00 – 8:00pm 20 February
- Quiz 2: lecture slot in week 13
  - Full-time: 8:30 – 9:30am 14 April
  - Part-time: 7:00 – 8:00pm 10 April
- Those who are validly absent must take make up quiz. Failure to do so will get 0 marks.

Assessment

Project (30% each)

- Groups of 4 students
- Each group does 2 case studies about real-world computer security incidents.
- Set in Week 14 for a 15-minute onsite presentation (10 minutes presentation + 5 minutes Q&A)
- All members must do the presentation & understand BOTH projects.
- Sign up for the groups (deadline: 11:59pm 31 January). *Make sure no duplicated names.* Note there are two tabs for full-time and part-time separately. After the deadline, we will allocate the groups for the students not in the list.
  https://docs.google.com/spreadsheets/d/16DsXxz55xMpFN36BAemUMViuRV8IdV6GrR-DQuJIK1s/edit?usp=sharing

Assessment

Project judge criterion

- Real-world computer security incidents, better to have significant impacts.
- The cases should be related to the content discussed in this course, but do not directly use the examples introduced in the lecture.
- Technical depth: describe the technical details about the mechanism of the incidents. It is recommended to perform code analysis for the vulnerabilities. Having demos will be a plus.
- Clear presentation. Able to correctly answer the questions.

Schedule (Full-time)

Week	Tutorial	Lecture	Instructor
1		Introduction	Zhang Tianwei
2		Software Security I	
3	Software Security I	Software Security II	
4	Software Security II	Software Security III	
5	Software Security III	OS Security I	
6	OS Security I	OS Security II	
7	OS Security II	Quiz 1	
8-12	Passwords & Authentication Mobile security Computer Security Case studies Introduction to Cryptography		Tay Kian Boon
13		Quiz 2	
14	Final Presentation		

Schedule (Part-time)

Week	Lecture & Tutorial	Instructor
1	Introduction	Zhang Tianwei
2	Software Security I	
3	Software Security II	
4	Software Security III	
5	OS Security I	
6	OS Security II	
7	Quiz 1	
8-12	Passwords & Authentication Mobile security Computer Security Case studies Introduction to Cryptography	Tay Kian Boon
13	Quiz 2	
14	Project presentation	

References

No required textbooks. If you want extra reading:

- D. Gollmann, Computer Security (3rd ed.), John Wiley & Sons, 2011.
- M. Bishop, Computer Security: Art and Science, Addison- Wesley, 2003.
- R. Anderson, Security Engineering, 2008.
- Erickson, Hacking: the art of exploitation, 2nd Edition, 2008.

Basics of Computer Security

- **Trust and Trusted Computing Base**
- **Threat Model**
- **Security Properties**
- **Security Strategies**
- **Design Principles of Computer Security**

Trust

The degree to which an entity is expected to behave:

- What the entity is expected to do: anti-malware can detect malicious programs; system can prevent illegal account login, etc.
- What the entity is expected not to do: the website will not expose your private data to third parties; an application will not inject virus into your system.

Security cannot be established in a computer system if no entities are trusted.

It is important to make clear what should be trusted. Otherwise, the designed security solutions may fail in practice.

Trusted Computing Base (TCB)

A set of system components (e.g., software, OS, firmware, hardware) that need to be trusted to ensure the security of the computer system

Components outside of the TCB can be malicious and misbehave.

When we design a security solution, we need to

- Assume all the components inside the TCB are secure with valid justifications.
- Prevent any damages from any components outside of the TCB.

Size of TCB

- A system with a smaller TCB is more trustworthy (we do not need to make too many assumptions, which may be violated)
- Designing a secure system with a smaller TCB is more challenging (we need to consider more malicious entities)

Threat Model

Describe the adversaries in consideration

- What is trusted and what is not trusted.
- For the untrusted entities, what resources, capabilities and knowledge they have; what actions they can perform.
- What security properties the system aim to achieve.

An example: phishing email – a malicious email with malware as the attachment

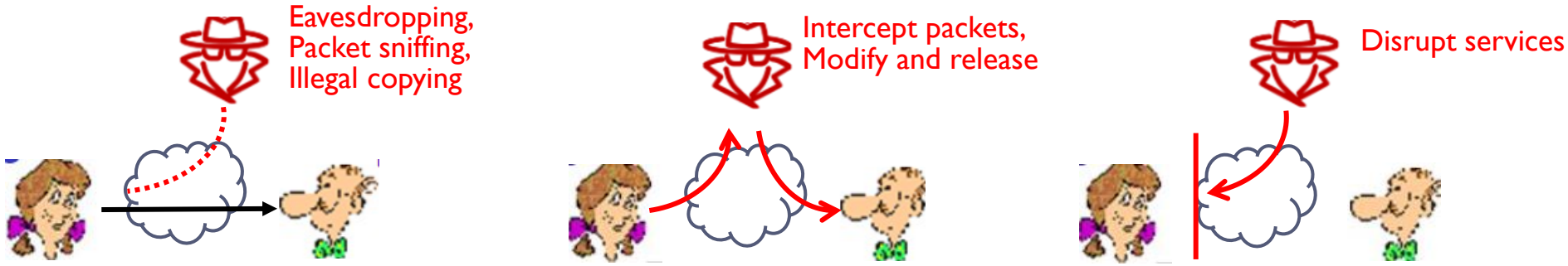
- What is trusted: hardware and OS
- What is not trusted: the email attachment.
- Adversarial capabilities: running malicious code in your computer.
- Security properties: protect the computer system such that the malware cannot steal the sensitive data, or tamper with other processes.

Security Properties

The security goals that we aim to achieve for the system.

Common security properties (CIA model)

- Confidentiality (C): prevent unauthorized disclosure of information. Sensitive information should not be leaked to unauthorized parties
- Integrity (I): prevent unauthorized modification of information. Critical system state and code cannot be altered by malicious parties
- Availability (A): prevent unauthorized withholding of information or resources. The resources should be always available for authorized users



Security Properties

Other properties

- Accountability: actions of an entity can be traced and identified
- Non-repudiation: unforgeable evidence that specific actions occur
- Authenticity: ensure the communicated entity is the correct entity.

Security Strategies

Prevention

- Take measures that prevent your system from being damaged

Detection

- Take measures so that you can detect when, how, and by whom your system has been damaged.

Reaction

- Take measures so that you can recover your system or to recover from a damage to your system.

Design Principles of Computer Security

Principle of least privilege

- An entity should be given the minimal permissions to complete its task.
- Give the privilege when needed, and revoke the privilege after use
- If granting unnecessary permissions, a malicious entity could abuse those permissions to perform the attack.

Principle of separation of privilege

- Separation of duty: for multiple entities working together, it is better to distribute privileges to different entities.
- A single malicious party cannot get all the privileges to perform the attack.

Defense in depth

- Multiple types of defenses should be layered together
- Increase the difficulty of attacking the entire system.