



# Introduction to Cybersecurity

NT101 – NETWORK SECURITY

Giảng viên: ThS. Nghi Hoàng Khoa | [khoanh@uit.edu.vn](mailto:khoanh@uit.edu.vn)





# Giới thiệu bản thân

- Nghiên cứu viên tại Phòng thí nghiệm An toàn Thông tin – E8.1 UIT InsecLab
- Chuyên môn nghiên cứu :
  - Windows/Android (Malware, Forensics, Pentesting)
  - ML- GAN cho Cybersecurity
  - CTF Player
  - (<https://inseclab.uit.edu.vn/cong-bo-khoa-hoc/>)
- Khoá 8 2013 - UIT@VNU-HCM
- Chủ nhiệm Team CTF - Câu lạc bộ An toàn Thông tin – UIT Wanna.W1n (<https://ctftime.org/team/138431>)
- Trợ giảng tại Trung tâm An ninh Mạng CNSC
- Tham gia hoạt động giảng dạy thực hành các môn: An toàn Mạng máy tính, Bảo mật Web và Ứng dụng, Cơ chế hoạt động của mã độc...



# Giới thiệu môn học



- “Network Security is amazing ... but also is a tough course”
- Các điều kiện cần có: IT005 – Nhập môn mạng máy tính. Năm vững:
  - Các khái niệm cơ bản về cách hoạt động của máy tính IP (CPU, virtual memory...)
  - Kinh nghiệm lập trình (IT001 - IT004)
  - Các khái niệm cơ bản về cách hoạt động của mạng máy tính (IT005)
- Môn học này là nền tảng cho các môn học bảo mật nâng cao tiếp theo
  - Nguyên tắc/khiến thức cơ bản, tập trung phần lớn vào mạng máy tính.





# Giới thiệu môn học

- Trang course : <https://courses.uit.edu.vn/>
- Những gì sẽ được đăng ở đây?
  - Thông báo
  - Thông tin khóa học, quy định lớp học
  - Slide, sách, bài báo
  - Bài tập, bài lab



# Mục tiêu môn học



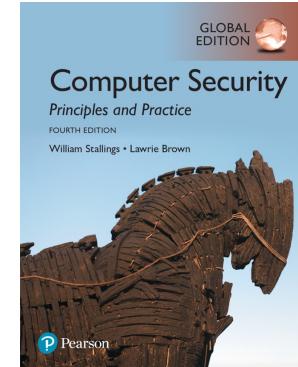
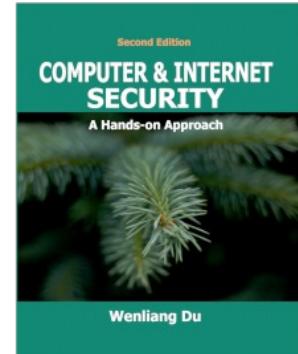
- Tìm hiểu được các kỹ thuật khai thác/tấn công
  - Cách bảo vệ và ngăn chặn các cuộc tấn công mạng phổ biến
- Tìm hiểu và sử dụng các công cụ bảo mật phổ biến và viết các công cụ
- Tìm hiểu các kiến trúc mạng an toàn
- Xây dựng “Tư duy bảo mật”
  - *Nhiều bài tập và kiểm tra để đánh giá kết quả của sinh viên*



# Tài liệu môn học



- Textbook:
  - [SEED book] Wenliang Du (2019). **Computer & internet security: A hands-on approach**, 2nd edition, ISBN-13: 978-1733003933
  - [CS book] William Stallings and Lawrie Brown (2018). **Computer Security: Principles and Practice**, 4<sup>th</sup> Edition, ISBN 978-0-13-479410-5
- Nguồn khác (có thể sẽ được chỉ định):
  - Tin tức, tài liệu kỹ thuật
  - Nghiên cứu bài báo



This course's lectures are designed for UIT students based on these books above and some lecture notes and materials from CSE 488/644 course in Syracuse University, US; CS155 course in Stanford University, US, and CS481/681 course University of North Carolina at Greensboro, US. **For educational purposes only.**





- Lecture 01 - **Introduction to Cybersecurity**
- Lecture 02 - **Cybersecurity basis: Principles and concepts**
- Lecture 03 - **OS Security, Malware threats**
- Lecture 04 - **Network and Internet Security: The big picture and TCP/IP revision**
- Lecture 05 - **Packet Sniffing and Spoofing**
- Lecture 06 - **Data Link Layer security**
- Lecture 07 - **Network Layer security**
- Lecture 08 - **Transport Layer security**
- Lecture 09 - **Application Layer security: DNS attacks**
- Lecture 10 - **Network Defenses: Firewalls, IDPS, Honeypot overview**
- Lecture 11 - **Privacy, Anonymity, and Censorship**
- Week 12-13-14-15 - **Seminar: Recent topics in Network Security**





- Đọc thêm! Đọc trước các nội dung trong textbook trước khi đến lớp
  - Bài giảng sẽ đi nhanh; Mong đợi các câu hỏi và thảo luận, khuyến khích ghi chú!
  - Đừng để không theo kịp bài học
  - Trao đổi, học tích cực trong lớp – điểm thưởng
- Luyện tập nhiều! Một số trang web và khoá học đề xuất:
  - **SEED Labs** (Network section) - <https://seedsecuritylabs.org/>
  - **CTF: Hack The Box** - <https://www.hackthebox.eu/> / - Try Hack Me - <https://tryhackme.com> - Root-me - <https://www.root-me.org>
  - **CEH v12** - <https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/>
  - **OSCP** - <https://www.offensive-security.com/pwk-oscp/>
  - **Online course:** <https://www.udemy.com/course/du-internet-security/>



# Bài tập, kiểm tra và đánh giá



- Câu hỏi, trao đổi – cộng điểm (không phải lúc nào cũng có)
- Làm bài tập về nhà (1-3 tuần)
- Không thi giữa kỳ
- Đồ án:
  - Team từ 2 đến 4 thành viên
  - Đề tài và đăng ký: TBA trong buổi tiếp theo
- Thi cuối kỳ: TBA

Thành phần	Phần trăm
Bài tập, hoạt động trên lớp	10%
Đồ án	20%
Thực hành	20%
Thi cuối kỳ	50%





- Vui lòng đến lớp đúng giờ. Nếu việc đi học trở thành vần đề (ít hơn 2/3 số buổi) sẽ chuyển thành điểm
- Hãy là người trưởng thành, tôn trọng mọi người và chịu trách nhiệm trước mọi hành động của mình
- Không làm việc riêng trong lớp



# Một vài điều quan trọng



- Tôi muốn bạn “thành công”
  - “thành công” có nghĩa là “học hỏi”, không nhất thiết phải “đạt điểm cao” (tùy bạn)
- Đạo đức và chuyên nghiệp:
  - Trung thực trong học tập – đừng đầu hàng trước sự cám dỗ
  - Nội dung bạn gửi phải là 100% công sức bạn bỏ ra - trích dẫn rõ ràng bất kỳ nguồn dữ liệu mà bạn tham khảo, có ảnh hưởng đến nội dung của bạn
  - Hoàn thành công việc - đừng cẩu thả và lười biếng
  - Không “thử nghiệm” với các hệ thống trái phép
- Khám phá
  - Thực hành trên hệ thống máy ảo hoặc được phép
  - Tài liệu môn học (slides, readings, assignments, labs...) lưu hành nội bộ

# Liên hệ với giảng viên



- Khuyến khích gửi mail: [khoanh@uit.edu.vn](mailto:khoanh@uit.edu.vn)
  - Vui lòng thêm tiêu đề email với “**NT101.classcode**”
- Văn phòng: **E8.1** (Phòng thí nghiệm An toàn Thông tin – UIT InSecLab)
- Giờ làm việc: 8h -17h từ Thứ Hai đến Thứ Bảy
  - Vui lòng gửi email trước cho tôi nếu bạn định đến vào giờ hành chính
- *Nếu bạn muốn làm việc với tôi (nghiên cứu, đồ án, luận văn...), hãy tìm hiểu ở website [inseclab.uit.edu.vn](http://inseclab.uit.edu.vn) hoặc để xuất ý tưởng của bạn*



# Câu hỏi (nếu có)





# Outline

- Giới thiệu môn học
- **Giới thiệu về Cybersecurity**
  - Thực trạng hiện tại
  - Các mối đe doạ (Threats)
  - Các lỗ hổng (Vulnerabilities)



# Cybersecurity – Giới thiệu



# An toàn thông tin là gì?

- Định nghĩa An toàn thông tin (NIST):

*“The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.”*

- Xem xét 3 mục tiêu lớn của ATTT:

- Tính bảo mật: Tránh tiết lộ thông tin trái phép
- Tính toàn vẹn: Tránh sửa đổi trái phép thông tin
- Tính sẵn có: Đảm bảo thông tin và hệ thống kịp thời bởi những người được cho phép



# Information Security vs. Cyber Security vs. Network Security



- Cybersecurity là gì (aka. Computer Security) ?
  - là tập hợp con của information security
  - là hoạt động bảo vệ mạng, máy tính và dữ liệu của tổ chức khỏi các cuộc truy cập trái phép, tấn công hoặc thiệt hại do các hoạt động khác.
- Network Security là gì?
  - là tập hợp con của cybersecurity
  - nhằm mục đích bảo vệ bất kỳ dữ liệu nào đang được gửi qua các thiết bị trong mạng để đảm bảo rằng thông tin không bị thay đổi hoặc bị chặn.

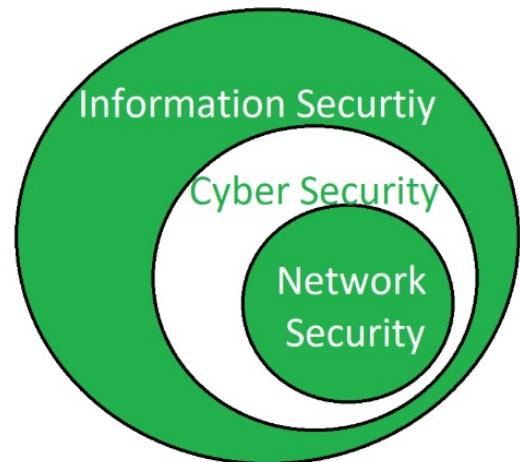


Photo: <https://www.geeksforgeeks.org/>



# Thực trạng An ninh mạng hiện tại

- Nghiên cứu toàn cầu mới của ISACA cho thấy mặc dù dịch COVID-19 diễn ra thì ngành nghề lĩnh vực an ninh mạng vẫn ổn định.
  - Nhưng tình trạng thiếu nhân sự vẫn diễn ra do ngày càng có nhiều cuộc tấn công mạng.

## Hiring Managers Struggle to Find Qualified Candidates



**72%**  
of those who reported that less than 25 percent of their applicants are well qualified have unfilled positions longer than three months.

ISACA: <http://www.isaca.org/state-of-cybersecurity-2021>



# Thực trạng An ninh mạng hiện tại (tt)

- Kỹ năng kỹ thuật vẫn cần nhu cầu đáng kể
  - Ứng viên toàn diện với các kỹ năng mềm - thách thức



ISACA: <http://www.isaca.org/state-of-cybersecurity-2021>

# Thực trạng An ninh mạng hiện tại (tt)

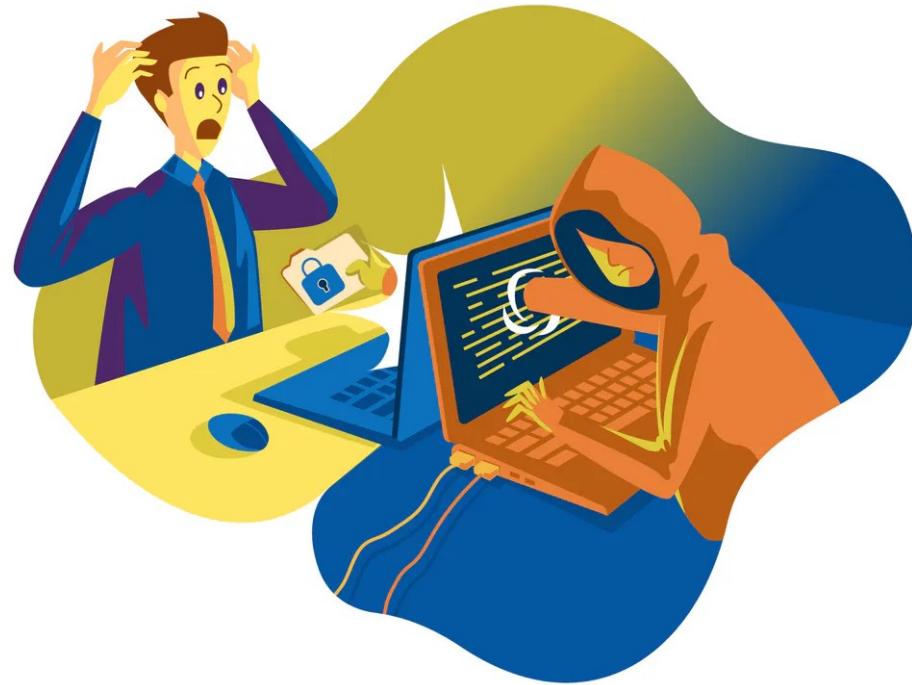


- Rất nhiều phần mềm lỗi (bug)
- Tội phạm mạng không ngừng gia tăng và tổn thất lớn
- Social engineering cực kỳ hiệu quả
- Tiền có thể kiếm được từ việc tìm kiếm và khai thác các lỗ hổng



# Security Threats

## Hacker và tội phạm mạng – điều gì thúc đẩy họ?



Xem thêm: [https://www.ted.com/playlists/who\\_are\\_the\\_hackers](https://www.ted.com/playlists/who_are_the_hackers)



# Tiền, quyền lực và cái tôi – thúc đẩy tội phạm mạng



Cambridge  
Dictionary

**hacker**  
(noun)

a person who is skilled in the use of computer systems, often one who illegally obtains access to private computer systems

- Hacker - tội phạm mạng là những người liên quan đến việc phá vỡ/vượt qua bảo mật máy tính
- Có bao nhiêu loại hacker ?
  - Black Hat hackers (crackers)
  - White Hat hackers (ethical hackers)
  - Gray Hat hackers
- *“Hacking has evolved from teenage mischief into a billion-dollar growth business.”*



[Under the hoodie: why money, power, and ego drive hackers to cybercrime](#)





# Who are the hackers?

- Bạn có biết ai là hacker trẻ nhất thế giới được biết đến không?



Kristoffer von Hassel (2009)

<https://thingscyber.com/10-youngest-hackers-who-caused-chaos/>

The Register  
Biting the hand that feeds IT

DATA CENTRE SOFTWARE SECURITY DEVOPS BUSINESS PERSONAL TECH SCIENCE EMERGENT TECH BOOTNOTES LECTURES

Business • Policy

**Bedroom NASA hacker set to bite pillow in choky**

Pinecrest boy pining for freedom

By Linda Harrison 22 Sep 2000 at 14:52

A Florida teenager was banged up for six months yesterday after admitting he hacked into NASA systems.

Jonathan James, known as "c0mrade" on the Net, pleaded guilty to intercepting 3,300 emails, stealing passwords, and nicking data from 13 NASA computers - including some involved with the International Space Station.

The not-so-sweet 16-year-old will do time in a Florida detention centre - he was just 15 when the crimes occurred. "Breaking into someone else's property, whether it's a robbery or a computer intrusion, is a serious crime," said Attorney General Janet Reno, AP reported.

According to the Miami Herald, the lad sat in his bedroom in Pinecrest, Southern Florida, and used his Gateway Pentium 266 computer to access some of the world's most top-secret information.

He was busted by federal agents from Fort Lauderdale touting weapons and bulletproof vests. But not before he had downloaded \$1.7 million in NASA proprietary software that supports its environmental systems. Apparently it

SHARE ▾

CPO MAGAZINE

HOME NEWS INSIGHTS RESOURCES

CLOUD CYBER SECURITY NEWS 5 MIN READ

**Twitter Hack Apparently Masterminded by Group of Kids as Young as 17**

Company Confirms Social Engineering Provided Access to Extensive Customer Service Tools

SCOTT IKEDA • AUGUST 11, 2020

HACKERS

**The Kid Who Hacked NASA Servers at Age 13 Now Has His Own Television Show**

NEXT ARTICLE

Add to Queue

Walter O'Brien

Walter O'Brien, Founder & CEO, Scorpion Computer Services

Image credit: YouTube





# Who are the hackers? (tt)

- Thành viên chính phủ
- Người trong cuộc



Ashley Pugh | Cyber Security  
Jun '18

## How Stuxnet almost started World War III

There have been multiple occasions since World War II ended in 1945 that the world thought it would be engulfed in another global conflict: the [1979 NORAD computer glitch](#), the Cold War, the [Cuban Missile Crisis](#) (my history GCSE means I can tell you a lot about those), and the [Black Brant scare](#) to name a few.

The Stuxnet computer worm is another such incident, and probably won't be the last now that Donald Trump likes to play games of "my weapons are bigger than yours", which I have no doubt they are.

Stuxnet was a malicious software that targeted control systems in the Natanz nuclear facility in Iran. It enters a computer connected to the system through an infected removable hard-drive, expected to be a USB stick, then the worm uploaded itself onto the plant's computer system. It is still not known if Stuxnet was uploaded accidentally or deliberately. If done deliberately, it would have been the work of a double agent.

MICROSOFT \ TECH \

## Microsoft has warned 10,000 people that nation-state hackers are targeting them

1,600 personal Microsoft accounts affected

By Tom Warren | @tomwarren | Jul 18, 2019, 4:38am EDT



W I F C B

Hackers Take Down the Most Wired Country in Europe

JEREMY BAKER BUSINESS 06.21.07 12:00 PM

## HACKERS TAKE DOWN THE MOST WIRED COUNTRY IN EUROPE

The minister of defense checked the Web page again — still nothing. He stared at the error message: For some reason, the site for Estonia's leading newspaper, the Postimees, wasn't responding. Jaak Aaviksoo attempted to pull up the sites of a couple of other papers. They were all down. The former director of the University of Tartu Institute of Experimental Physics and Technology had been the Estonian defense minister for only four weeks. He hadn't even changed the art on the walls.

An aide rushed in with a report. It wasn't just the newspapers. The leading bank was under siege. Government communications were going down. An enemy had invaded and was assaulting dozens of targets.

Outside, everything was quiet. The border guards had reported no incursions, and Estonian airspace had not been violated. The aide explained what was going on: They were under attack by a rogue computer network.

Forbes

EDITORS' PICK | 30,773 views | Mar 27, 2020, 05:25am EDT

## Google Confirms 40,000 Nation-State Cyber Attack Warnings Issued

Davey Winder Senior Contributor ©  
Cybersecurity  
I report and analyze breaking cybersecurity and privacy stories

NBC NEWS

ELECTIONS

## Russians penetrated U.S. voter systems, top U.S. official says

By Cynthia McCormick, William M. Arkin and Kevin Moranah / Feb. 07, 2018 / 4:39 PM ET / Updated Feb. 08, 2018 / 7:39 AM ET

The U.S. official in charge of protecting American elections from hacking says the Russians successfully penetrated the voter registration rolls of several U.S. states prior to the 2016 presidential election.

In an exclusive interview with NBC News, [Jeanette Manfra](#), the head of cybersecurity at the Department of Homeland Security, said she couldn't talk about classified information publicly, but in 2016, "We saw a targeting of 21 states and an exceptionally small number of them were actually successfully penetrated."

Jeff Johnson, who was DHS secretary during [the Russian intrusions](#), said, "2016 was a wake-up call and now it's incumbent upon states and the Feds to do something about it before our democracy is attacked again."

"We were able to determine that the scanning and probing of voter registration databases was coming from the Russian government."

There is no evidence that any of the registration rolls were altered in any fashion, according to U.S. officials.

# Động cơ phổ biến



- Tài chính, tống tiền, thông tin thị trường chợ đen

## Two years after WannaCry, a million computers remain at risk

The threat posed by the leaked NSA tools remains a concern

Zack Whittaker @zackwhittaker 4:37 am +07 • May 13, 2019



## Incident Of The Week: Garmin Pay Million To Ransomware Hackers W Rendered Systems Useless

It is believed that Garmin paid the \$10 million

Tags: Ransomware Attack Hackers



[Records Exposed: N/A | Industry: Technologic Attack: Ransomware]

On July 23, Garmin users went to Twitter to concern over inaccessible website features. Four days later, Garmin official statement confirming that a cyber attack had taken place. It users that no PII (personal identifying information) was compromised

### The Facts:

Garmin is most commonly known for its fitness tracking capabilities in wearables, but the corporation also operates in the aviation space. Critical planes whose aviation infrastructure relies on Garmin technology were the hack.

Hackers deployed the ransomware tool WastedLocker, which encrypts company's digital infrastructure. In the case of Garmin, website functions, customer support, and user applications were all affected. Unlike typical ransomware software,

PHÁP LUẬT

## 'Trùm hacker' là sinh viên lớp kỹ sư tài năng

15:41 17/01/2014

Số tiền kiếm được từ việc bán thông tin thẻ tín dụng chôm chia, cựu sinh viên lớp kỹ sư tài năng của Trường ĐH Bách khoa TP.HCM đưa hết cho bố để mua đất.

Cục Cảnh sát hình sự phối hợp với Cục Cảnh sát phòng, chống tội phạm sử dụng công nghệ cao vừa triệt phá "thế giới ngầm" (gọi tắt là UG) của bọn tội phạm sử dụng công nghệ cao, bắt 9 người.

Mở rộng vụ án, Cơ quan CSĐT Bộ Công an bắt giữ thêm một số người khác, trong đó đáng chú ý có 1 "trùm hacker", chuyên hack vào các tài khoản của người nước ngoài để trộm cáp thông tin thẻ tín dụng (cc).

Tìm ra "trùm hacker" là một sinh viên của lớp Kỹ sư tài năng

Đó là Nguyễn Văn Hòa (23 tuổi, trú tại khu phố 6, phường 3, TP Đông Hà, tỉnh Quảng Trị) hiện đang là sinh viên lớp kỹ sư tài năng (Đại học Bách khoa TP.HCM).

Hóa học rất giỏi, đặc biệt là về công nghệ thông tin. Hòa có thể ngồi nhiều giờ, nhiều ngày để nghiên cứu và viết lập trình. Nguyên nhân đẩy Hòa vào con đường phạm tội chính là việc tham gia vào diễn đàn "thế giới ngầm" (gọi tắt là UG) - trở thành công cụ để kiếm tiền bất hợp pháp những người khác.



# Các cuộc tấn công mạng khét tiếng hàng đầu trong lịch sử



- Who needs a gun when you have a keyboard?
  - 1988: Morris Worm – the first Internet worm
  - 1994: Mitnick attack
  - 2000: MafiaBoy attack
  - 2008: Kaminsky attack
  - ...
  - 2014: Heartbleed attack
  - 2016: Mirai Botnet: The fall of the Internet
  - 2017: WannaCry: A real epidemic
  - ...



10 hacker mũ đen hàng đầu thế giới

**How about Vietnamese hackers?**

<https://www.kaspersky.com/blog/five-most-notorious-cyberattacks/24506/>  
[https://en.wikipedia.org/wiki/List\\_of\\_security\\_hacking\\_incidents](https://en.wikipedia.org/wiki/List_of_security_hacking_incidents)

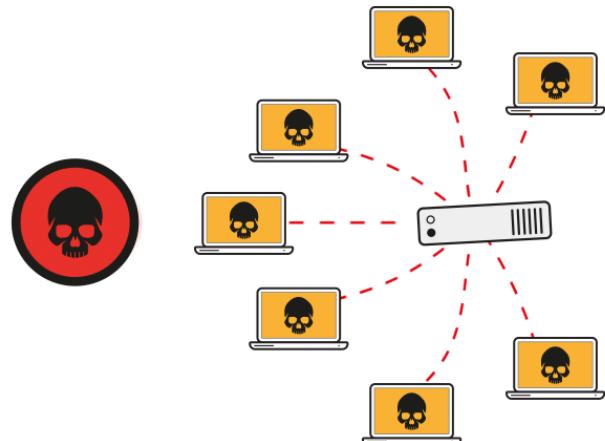


# Tại sao hacker xâm nhập hệ thống?



## 1. Đánh cắp địa chỉ IP và băng thông

- Mục tiêu của kẻ tấn công: trông giống như một người dùng Internet bình thường
- Sử dụng địa chỉ IP của máy hoặc điện thoại bị nhiễm để:
  - Spam
  - Denial of Service
  - Click fraud



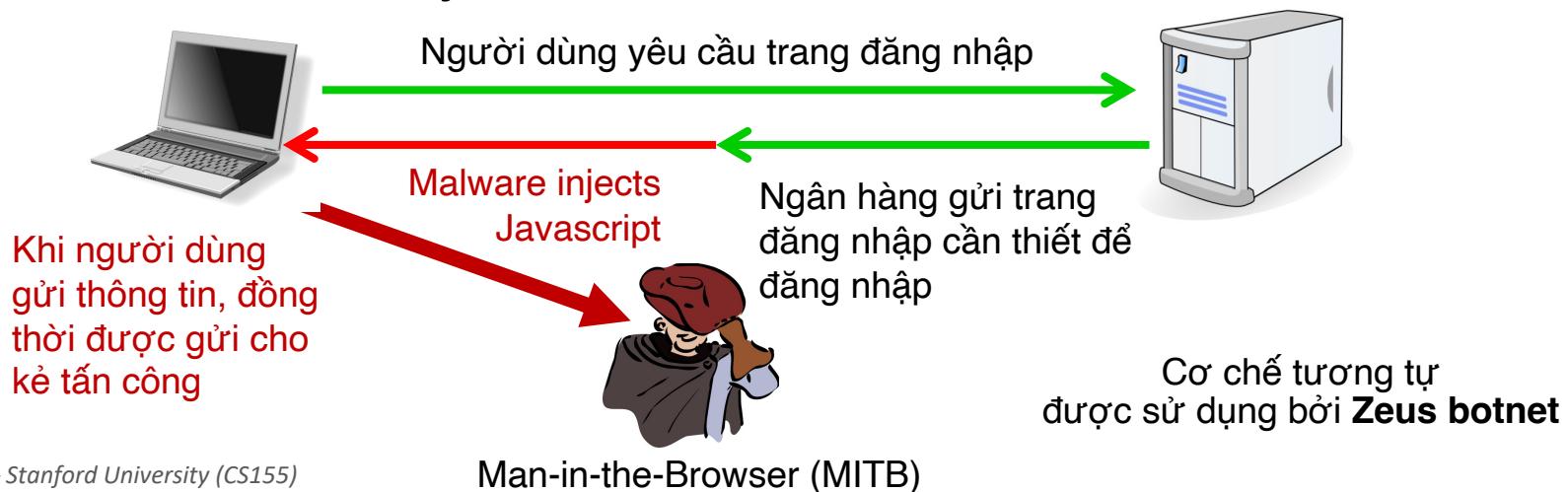
Dan Boneh – Stanford University (CS155)



# Tại sao hacker xâm nhập hệ thống? (tt)

## 1. Đánh cắp thông tin đăng nhập của người dùng

- Mục tiêu của kẻ tấn công: mật khẩu ngân hàng, mật khẩu công ty, mật khẩu chơi game...
- Ví dụ: **Silent Banker trojan**



# Phần mềm độc hại trong lĩnh vực tài chính



- 1 Trojan-Spy.Win32.Zbot
- 2 Trojan.Win32.Nymaim
- 3 Trojan.Win32.Neurevt
- 4 SpyEye
- 5 Trojan-Banker.Win32.Gozi
- 6 Emotet
- 7 Caphaw
- 8 Trickster
- 9 Cridex/Dridex
- 10 Backdoor.Win32.Shiz

- ghi lại mật khẩu ngân hàng qua keylogger
- phát tán qua email spam và các trang web bị tấn công
- duy trì quyền truy cập vào PC để cài đặt trong tương lai



# Các cuộc tấn công trên điện thoại

**Ví dụ:** FinSpy spyware.

- Hoạt động trên **iOS and Android** (và Windows)
  - Sau khi cài đặt: thu thập danh bạ, lịch sử cuộc gọi, vị trí địa lý, văn bản, tin nhắn trong các ứng dụng trò chuyện được mã hóa...
- Cài đặt như thế nào?
  - Android pre-2017: links in SMS / links in E-mail
  - iOS and Android post 2017: physical access



<https://www.kaspersky.com/blog/finspy-commercial-spyware/27606/>



# Tại sao kiểm soát máy?

## 3. Ransomware

### TOP 10 most widespread encryptor families

Name	Verdict	%*	
1	WannaCry	Trojan-Ransom.Win32.Wanna	23.56
2	(generic verdict)	Trojan-Ransom.Win32.Phny	16.81
3	GandCrab	Trojan-Ransom.Win32.GandCrypt	12.17
4	(generic verdict)	Trojan-Ransom.Win32.Gen	6.26
5	(generic verdict)	Trojan-Ransom.Win32.Crypmod	5.08
6	(generic verdict)	Trojan-Ransom.Win32.Encoder	4.65
7	Shade	Trojan-Ransom.Win32.Shade	2.66
8	PolyRansom/ VirLock	Virus.Win32.PolyRansom Trojan-Ransom.Win32.Win32.PolyRansom	2.43
9	(generic verdict)	Trojan-Ransom.Win32.Crypren	2.28
10	Stop	Trojan-Ransom.Win32.Stop	1.94



- Worm spreads via a vuln. in SMB (port 445)
- Apr. 14, 2017: Eternalblue vuln. released by ShadowBrokers
- May 12, 2017: Worm detected
  - (3 weeks to weaponize)

## Vấn đề toàn cầu

Kaspersky Security Bulletin 2019

# Tấn công Server-side



- Đánh cắp dữ liệu: số thẻ tín dụng, sở hữu trí tuệ, thông tin khách hàng.
- Ví dụ: Equifax (Tháng 7 2017),  $\approx 143M$  dữ liệu “khách hàng” bị ảnh hưởng
  - Đã khai thác lỗ hổng đã biết trong Apache Struts (RCE)
  - Nhiều cuộc tấn công tương tự kể từ năm 2000
- Động cơ chính trị
  - DNC, Tunisia Facebook (Tháng 2. 2011), GitHub (Tháng 3. 2015)
- Lây nhiễm cho người dùng đang truy cập

## Vietnam bank exposed to security breach with 2M accounts leaked

Anh Kiet

*The Hanoitimes* - According to the hacking source, it has full records of all the bank users.

Personal data of two million bank accounts of a Hanoi-based bank have been exposed online, according to Vietnamese media.

Litur\*\*\* user posted on the Raidforums saying it is possessing confidential data of two million Vietnamese user accounts of Maritime Bank (MSB) including full name, identity card number, telephone number, home address, date of birth, gender, email and occupation of the customers.

**Vietnam cautions against Zoom after alleged data breach affecting over 500,000 accounts**

Wednesday, April 15, 2020, 16:12 GMT+7



Small toy figures are seen in front of displayed Zoom logo in this illustration taken March 19, 2020. Vietnam's cybersecurity regulator has urged locals to stay away from the fast-growing app Zoom due to data security concerns. Photo: Reuters

**Vietnam's cybersecurity regulator has advised state agencies, lenders, and firms against using the popular video conferencing platform Zoom for their online meetings after it was alleged that the personal particulars of more than 500,000 Zoom accounts have been leaked.**

### Highlights

Vietnam PM approves nationwide roll-out of chip-based ID cards

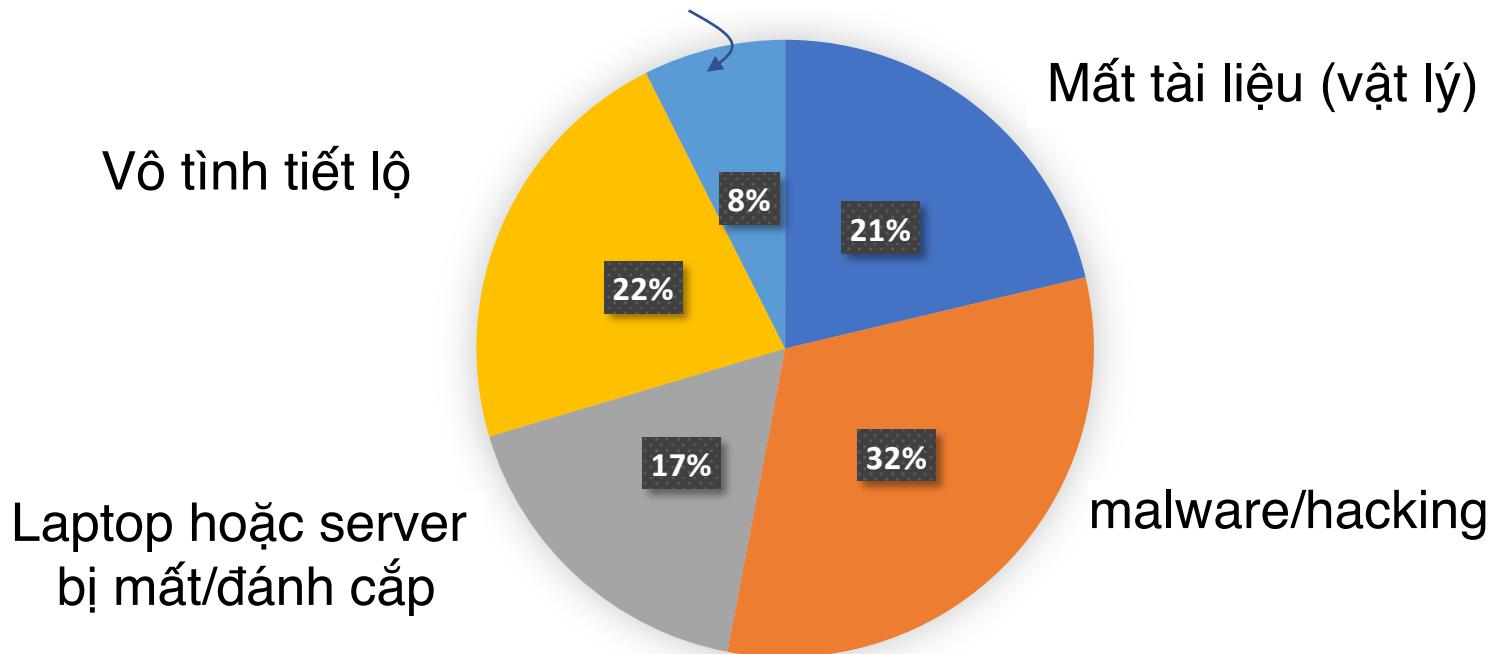
The Authority of Information Security under the Ministry of Information and Communications issued an advisory on Monday about concerns over the security vulnerability of Zoom, which has boomed in popularity.

# Vulnerabilities – Làm sao hacker có thể vào được?



# Cách các công ty mất dữ liệu khách hàng

Tấn công từ bên trong



PrivacyRights.org, 2020



# Vulnerabilities (tt)



- Có thể đến từ các lỗi trong phần mềm (thiết kế hoặc triển khai)

**Ví dụ: Buffer overflow**  
Được sử dụng đầu tiên và phổ biến  
trong Internet worm (*the Morris worm vào năm 1988*) - và vẫn là  
một trong những vấn đề lớn nhất hiện nay!

[https://cwe.mitre.org/top25/archive/2020/2020\\_cwe\\_top25.html](https://cwe.mitre.org/top25/archive/2020/2020_cwe_top25.html)

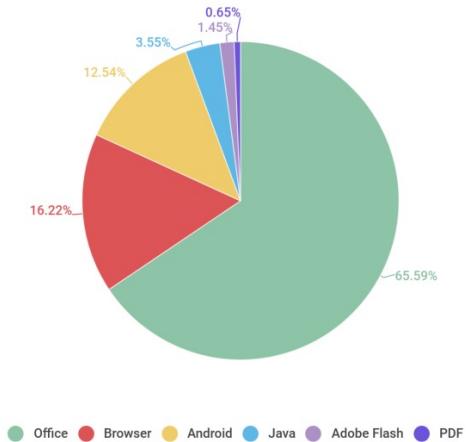
The screenshot shows the homepage of the Common Weakness Enumeration (CWE) website, specifically the "CWE Top 25" section for 2020. The page features a header with the CWE logo and the text "Common Weakness Enumeration A Community-Developed List of Software & Hardware Weakness Types". To the right, there's a "CWE TOP 25 Most Dangerous Software Weaknesses" badge. The main content area is titled "2020 CWE Top 25 Most Dangerous Software Weaknesses" and includes links for "Top 25", "Analysis", "Methodology", "Scoring Metrics", "On the Cusp", "Limitations", and "Remapping". Below this, a section titled "Introduction" provides a brief overview of the CWE Top 25, stating it is a demonstrative list of common and impactful issues experienced over two calendar years. It highlights that these weaknesses are dangerous because they are easy to find, exploit, and can allow adversaries to take over systems, steal data, or prevent applications from working. The page also explains how the list is created, mentioning the use of CVE data from NIST's National Vulnerability Database and CVSS scores. At the bottom, a section titled "The CWE Top 25" lists the top 25 weaknesses with their names and scores. A blue arrow points from the text "một trong những vấn đề lớn nhất hiện nay!" towards this table.

Rank	ID	Name	Score
[1]	CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	46.82
[2]	CWE-787	Out-of-bounds Write	46.17
[3]	CWE-20	Improper Input Validation	33.47
[4]	CWE-125	Out-of-bounds Read	26.50
[5]	CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer	23.73
[6]	CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20.69
[7]	CWE-200	Exposure of Sensitive Information to an Unauthorized Actor	19.16
[8]	CWE-416	Use After Free	18.87



# Vulnerabilities (tt)

- Các ứng dụng dễ bị tổn thương đang được khai thác
  - Tấn công độc hại được chia nhỏ theo loại ứng dụng mục tiêu (Kaspersky Security Bulletin 2019)



<https://www.cvedetails.com/top-50-products.php?year=2019>

## Top 50 Products By Total Number Of "Distinct" Vulnerabilities in 2019

Go to year: [1999](#) [2000](#) [2001](#) [2002](#) [2003](#) [2004](#) [2005](#) [2006](#) [2007](#) [2008](#) [2009](#) [2010](#) [2011](#) [2012](#) [2013](#) [2019](#) [2020](#) [All Time Leaders](#)

	Product Name	Vendor Name	Product Type	Number of Vulnerabilities
1	<a href="#">Android</a>	<a href="#">Google</a>	OS	414
2	<a href="#">Debian Linux</a>	<a href="#">Debian</a>	OS	360
3	<a href="#">Windows Server 2016</a>	<a href="#">Microsoft</a>	OS	357
4	<a href="#">Windows 10</a>	<a href="#">Microsoft</a>	OS	357
5	<a href="#">Windows Server 2019</a>	<a href="#">Microsoft</a>	OS	351
6	<a href="#">Acrobat Reader Dc</a>	<a href="#">Adobe</a>	Application	342
7	<a href="#">Acrobat Dc</a>	<a href="#">Adobe</a>	Application	342
8	<a href="#">Cpanel</a>	<a href="#">Cpanel</a>	Application	321
9	<a href="#">Windows 7</a>	<a href="#">Microsoft</a>	OS	250
10	<a href="#">Windows Server 2008</a>	<a href="#">Microsoft</a>	OS	248
11	<a href="#">Windows Server 2012</a>	<a href="#">Microsoft</a>	OS	246
12	<a href="#">Windows 8.1</a>	<a href="#">Microsoft</a>	OS	242
13	<a href="#">Windows Rt 8.1</a>	<a href="#">Microsoft</a>	OS	235
14	<a href="#">Ubuntu Linux</a>	<a href="#">Canonical</a>	OS	190
15	<a href="#">Fedora</a>	<a href="#">Fedoraproject</a>	OS	184
16	<a href="#">Chrome</a>	<a href="#">Google</a>	Application	177
17	<a href="#">Linux Kernel</a>	<a href="#">Linux</a>	OS	170
18	<a href="#">Iphone Os</a>	<a href="#">Apple</a>	OS	156



# Vulnerabilities (tt)



- Có thể đến từ việc cấu hình không tốt (Misconfiguration)

## Open Invitation to Hackers: Misconfigured Cloud Servers

Many companies use cloud servers to store their data. Despite their great advantage, misconfigured servers may expose sensitive data, mistake which is an open invitation to hackers to dump and use a company's data for their malicious activities.

### How is it possible?

4th party service providers, such as cloud storage providers, improve their cyber resilience as much as possible. They publish best practices on how to use their cloud services and provide options to keep the data public or private, a feature configured by companies who accommodate cloud servers. Any misconfiguration may expose data to the public and first ones notice these exposed data would be hackers and hacktivists. It is no wonder that Security Misconfiguration is #6 in OWASP Top 10.

The following three events occurred in the month of August may give hints about what may happen.



**OWASP TOP 10**

**A6: SECURITY MISCONFIGURATION**

 OWASP  
Open Web Application Security Project



## Vấn đề lớn

## NETWORKWORLD

### Hidden threat on corporate nets: misconfigured gear

New configuration debugger automatically fixes scripts for routers, firewalls and more



By Carolyn Duffy Marsan

Network World | JUN 8, 2009 1:00 AM PT

An invisible security weakness is lurking in most corporate networks in the form of millions of lines of code that represent the configuration scripts for all the devices on the network.

With corporate networks averaging 15 devices for every 100 users, ensuring accurate configurations has become a major challenge for network managers. Until now, manual processes or home-grown tools were the only options for configuration debugging.

Enter Telcordia, which is selling a new product called [IP Assure](#) that automatically debugs the configurations on IP devices including routers, switches, firewalls and load balancers. IP Assure checks configurations for 750 parameters to ensure accuracy, implementation of best practices and compliance with an organization's security policies.

Rajesh Talpade, chief scientist with Telcordia, says misconfigured network gear is a universal problem. When Telcordia analyzed 1,500 multi-vendor routers, switches and firewalls on eight corporate networks, it found errors in all the devices.

"We'll ask a company to give us 50 configuration files that we'll analyze at no cost," Talpade says. "We always find something wrong."

[Misconfigured network gear](#) represents a major security threat. Gartner estimates that 65% of cyberattacks exploit misconfigured systems.

Network [performance and reliability](#) also are affected by misconfigured gear, with Yankee Group estimating that 62% of IP network downtime is due to configuration errors.



# Vulnerabilities (tt)

- Đến từ yếu tố con người (đào tạo kém)

## Weak employee training leaves entire industries vulnerable to phishing

The Education and Transport industries are at the highest risk of cyber attacks due to phishing, because of weak employee training



Employee training needs to be improved when it comes to cyber security.

Weak employee training is the main reason industries are left vulnerable to phishing cyber attacks — this is the conclusion of Proofpoint's fourth annual **2019 Beyond the Phish report**, based on data from 130 million questions answered by end users across 16 industries.

"Cybercriminals are experts at gathering personal information to launch highly targeted and convincing attacks against individuals," said [Amy Baker](#), vice president of Security Awareness Training Strategy and Development for Proofpoint. "Implementing ongoing and effective security awareness training is a necessary foundational pillar when building a strong culture of security. Educating employees about cyber security best practices is the best way to empower users to understand how to protect their and their employer's data, making end users a



### Employees: The Biggest Threat to Security

Originally published by CloudMosa, Inc. on June 12th 2018 ★ 1,908 reads



With the rising frequency and intensity of data breaches, businesses are rightfully concerned about the potential compromise of their corporate data. Often ignored by the majority of enterprises, but widely understood among security experts, is the fact that the biggest security vulnerabilities usually lie within their own walls. These companies spend millions of dollars to protect themselves against a fast array of external cybersecurity threats, but neglect the internal risk and exposure created by their own employees.

In fact, the [majority](#) of today's breaches can be traced directly back to internal negligence. Many hacks are successfully executed with information stolen from unwitting employees, which can be an expensive mistake. According to IBM, the average cost of a data breach is currently evaluated at [\\$3.6 million](#) globally. That gives organizations an incredible incentive to ensure that their employees are secure, but many don't offer the appropriate training and thus can't properly safeguard their workers.



## THE DROPPED DRIVE HACK

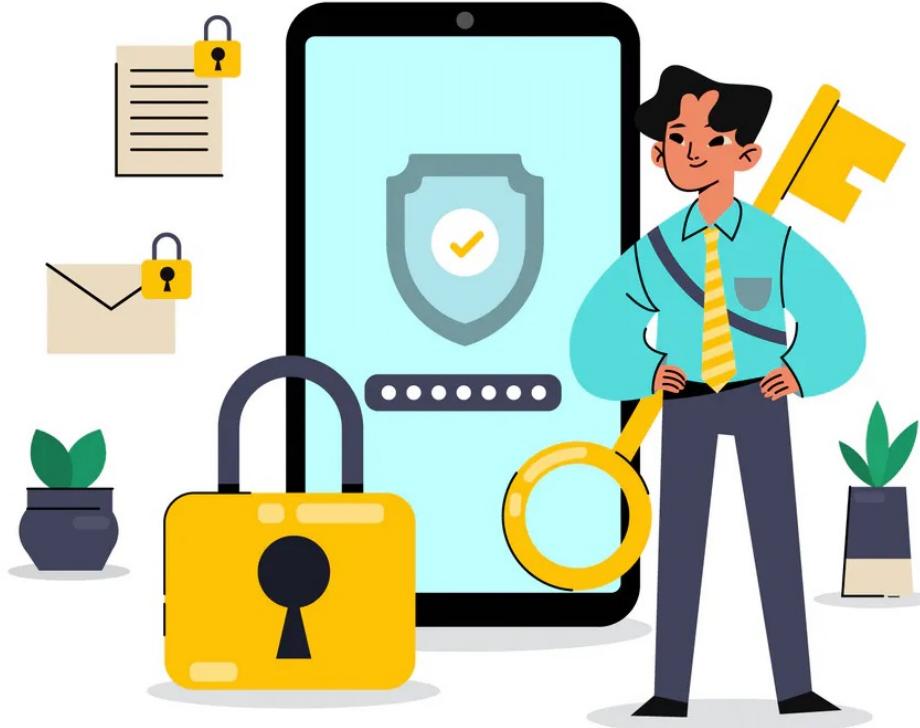
The dropped drive hack

\*LOOK, TO CALL this “idiotic” shows a poor understanding of user behavior. If you find a loose thumb drive, in your own parking lot, with your own organization’s logo on it, you pick it up and insert it *because you are trying to help*. For good reason. Suppose that the CEO dropped it and it has vital business information in there? Are you supposed to drop it in the incinerator as if it were a deadly toxin? It’s a lost thumb drive, and the odds of it being a hack are ten thousand to one.

\*It's like finding a car in your parking lot with the lights on and the motor running, and thinking that it must be a terrorist car-bomb. Maybe, yeah. Are you idiotic to turn off the key and shut the door? No.

\*They say that Stuxnet got deployed like this. Awesome hack, Stuxnet.

# Thị trường lỗ hổng



# Làm sao bán được 0day?



- Lựa chọn 1: chương trình bug bounty
  - Google Vulnerability Reward Program: up to \$31,337
  - Microsoft Bounty Program: up to \$100K
  - Apple Bug Bounty program: up to \$200K
  - Pwn2Own competition: \$15K
  - Hackerone
- Lựa chọn 2:
  - Zerodium: up to \$2M for iOS, \$2.5M for Android (2019)
  - ...

hackerone

SOLUTIONS ▾ PRODUCTS ▾ WHY HACKERONE ▾ COMPANY ▾ RESOURCES ▾

HOME > PRESS RELEASES > AUGUST 29, 2019

[< Back to Archive](#)

## SIX HACKERS BREAK BUG BOUNTY RECORD, EARNING OVER \$1 MILLION EACH ON HACKERONE

August 29, 2019

Bounty awards increased 65% on average as a quarter of all vulnerabilities reported are being classified as high to critical severity

SAN FRANCISCO-- August 29, 2019 -- HackerOne, the number one hacker-powered pentesting and bug bounty platform, today announced that six individual hackers have earned over one million dollars each from hacking. A bounty — or bug bounty — is a monetary award given to a hacker who finds and reports a valid security weakness to an organization so it can be safely resolved. Thanks to these six hackers five thousand unique security flaws have been fixed, protecting millions of people.

In March 2019, HackerOne announced that Santiago Lopez, known as [@try\\_to\\_hack](#), a 19-year-old hacker from Argentina, was the world's first hacker to earn \$1 million with bug bounty programs. Now, Mark Litchfield ([@mlitchfield](#)) from the U.K., Nathaniel Wakelam ([@nnwakelam](#)) from Australia, Frans Rosen ([@fransrosen](#)) from Sweden, Ron Chan ([@ngalog](#)) from Hong Kong, and Tommy DeVoss ([@dawggyg](#)) from the U.S. joined the \$1M hacker ranks by hacking for improved internet security.

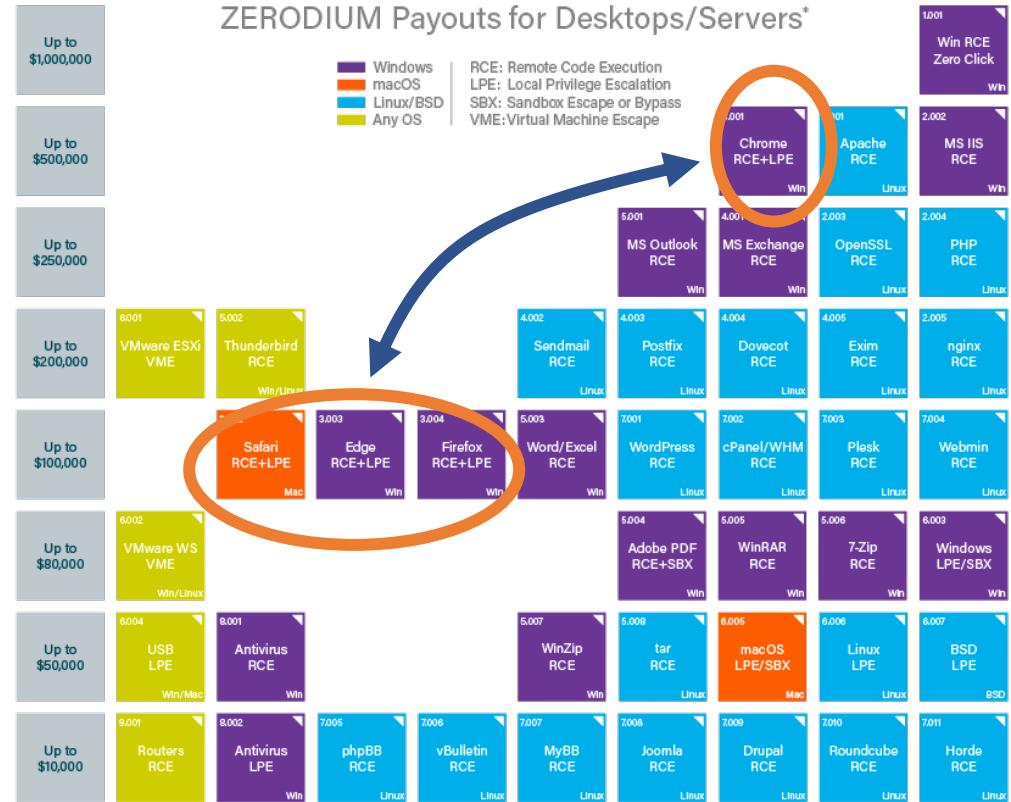
"I am incredibly proud to see that my work is recognized and valued," said 19 year old [@try\\_to\\_hack](#), the world's first hacker to earn \$1M. "Not because of the money, but because this achievement represents the information of companies and people being more secure than they were before, and that is incredible."



# Zerodium Payouts (Khoản chi trả)



- RCE: remote code execution
- LPE: local privilege escalation
- SBX: sandbox escape



Source: Zerodium

\* All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.

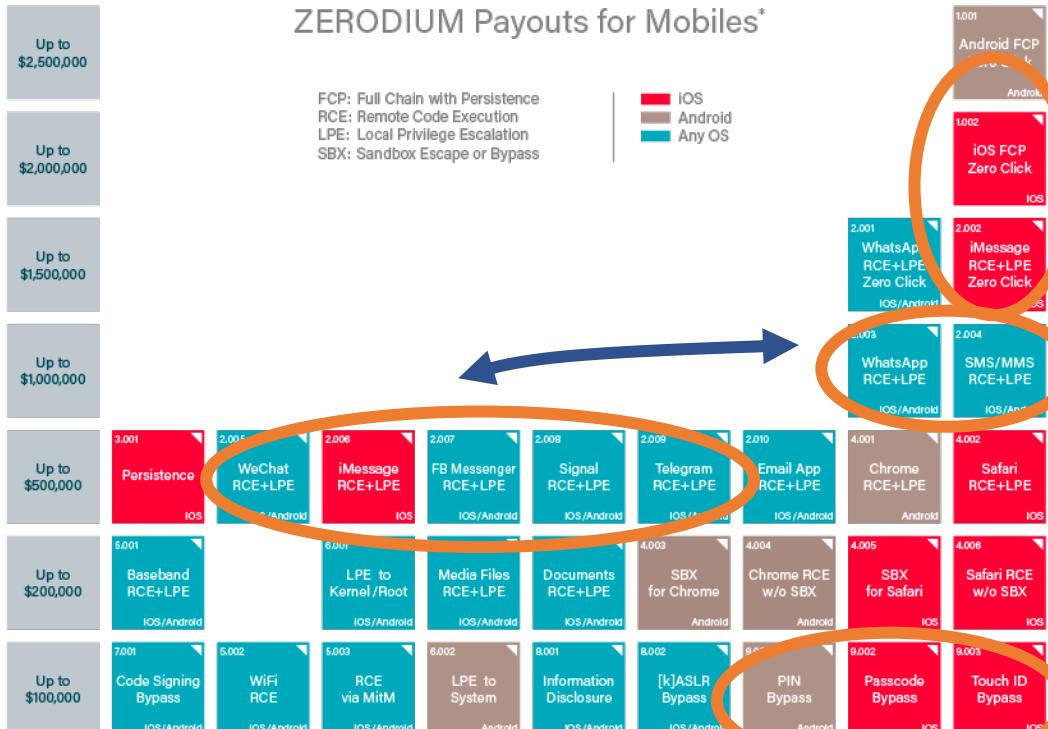
2019/01 © zerodium.com



# Zerodium Payouts (Khoản chi trả)



- RCE: remote code execution
- LPE: local privilege escalation
- SBX: sandbox escape



\* All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.

2019/09 © zerodium.com

Source: Zerodium



# Case study: Zerodium



## How the acquired security research is used by ZERODIUM?



ZERODIUM extensively tests, analyzes, validates, and documents all acquired vulnerability research and reports it, along with protective measures and security recommendations, solely to its clients subscribing to the ZERODIUM Zero-Day Research Feed.

## Who are ZERODIUM's customers?



ZERODIUM customers are government organizations (mostly from Europe and North America) in need of advanced zero-day exploits and cybersecurity capabilities.



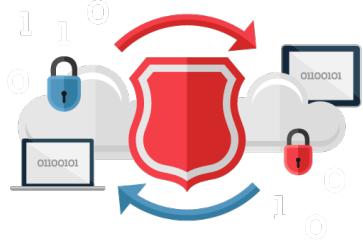
# Môn học tập trung vào...



Threats



Attacks



Defense

## Scope

Applications	(DNS and BGP)
Transport Layer	(TCP and UDP)
Network Layer	(IP and ICMP)
Data Link Layer	(Ethernet and ARP)
Physical Layer	

- Môn học này bao gồm các nguyên tắc trong an toàn mạng máy tính
- Phần lớn môn học này tập trung vào:
  - Xác định các **mối đe dọa** mạng (ai tấn công và tại sao),
  - **Tấn công** mạng và các lỗ hổng (cách chúng xâm nhập),
  - và **Phòng thủ** (cách ngăn chặn hoặc giảm thiểu chúng)  
*>>> Các chủ đề về quyền riêng tư và an toàn mạng gần đây*



# Buổi kế tiếp...



Sẵn sàng cho lớp học sau:

- Chủ đề dự kiến: Cybersecurity basis - Principles and concepts
- Tài liệu:
  - CS Book – Chapter 1
  - Paper (giao sau)
- Tìm thành viên trong nhóm của bạn (tối đa 4 sinh viên / nhóm).



# Luật An Toàn Thông Tin Mạng





# Thông tin chung

- Số: 86/2015/QH13
- Gồm 8 chương, 54 điều
  - Điều 7: “Các hành vi bị nghiêm cấm”
- Áp dụng: 01/7/2016



## Điều 7: Các hành vi bị nghiêm cấm



1. Ngăn chặn việc truyền tải thông tin trên mạng, can thiệp, truy nhập, gây nguy hại, xóa, thay đổi, sao chép và làm sai lệch thông tin trên mạng trái pháp luật.
2. Gây ảnh hưởng, cản trở trái pháp luật tới hoạt động bình thường của hệ thống thông tin hoặc tới khả năng truy nhập hệ thống thông tin của người sử dụng.
3. Tấn công, vô hiệu hóa trái pháp luật làm mất tác dụng của biện pháp bảo vệ an toàn thông tin mạng của hệ thống thông tin; tấn công, chiếm quyền điều khiển, phá hoại hệ thống thông tin.



## Điều 7: Các hành vi bị nghiêm cấm (tt)



4. Phát tán thư rác, phần mềm độc hại, thiết lập hệ thống thông tin giả mạo, lừa đảo.
5. Thu thập, sử dụng, phát tán, kinh doanh trái pháp luật thông tin cá nhân của người khác; lợi dụng sơ hở, điểm yếu của hệ thống thông tin để thu thập, khai thác thông tin cá nhân.
6. Xâm nhập trái phép bí mật mật mã và thông tin đã mã hóa hợp pháp của cơ quan, tổ chức, cá nhân; tiết lộ thông tin về sản phẩm mật mã dân sự, thông tin về khách hàng sử dụng hợp pháp sản phẩm mật mã dân sự; sử dụng, kinh doanh các sản phẩm mật mã dân sự không rõ nguồn gốc.



## Điều 8: Xử lý vi phạm



- Người nào có hành vi vi phạm quy định của Luật này thì tùy theo tính chất, mức độ vi phạm mà bị xử lý kỷ luật, xử phạt vi phạm hành chính hoặc bị truy cứu trách nhiệm hình sự; nếu gây thiệt hại thì phải bồi thường theo quy định của pháp luật.



# Tổng kết



- Nhận thức về vấn đề tuân thủ pháp luật liên quan đến an toàn thông tin mạng
- Cổng thông tin điện tử:

<https://vanban.chinhphu.vn/default.aspx?pageid=27160&docid=183196>



# Đến lượt các bạn



**Danh sách các sự cố bảo mật do hack** bao gồm các sự kiện quan trọng hoặc đáng chú ý trong lịch sử hack và bẻ khóa bảo mật, từ năm 1903 đến nay.

[https://en.wikipedia.org/wiki/List\\_of\\_security\\_hacking\\_incidents](https://en.wikipedia.org/wiki/List_of_security_hacking_incidents)

Công việc của bạn là chọn ra một sự cố do hack mà bạn ấn tượng nhất, tìm hiểu và tóm tắt trong một báo cáo dài một trang.

*(Expected: when, who, where, why, how and references)*



# Hôm nay, kết thúc!

- Nghi Hoàng Khoa
- khoanh@uit.edu.vn
- inseclab.uit.edu.vn
- NT101 – An toàn Mạng máy tính

