Introduction to Computer Security

Syllabus

Chi-Yu Li (2020 Spring)
Computer Science Department
National Chiao Tung University

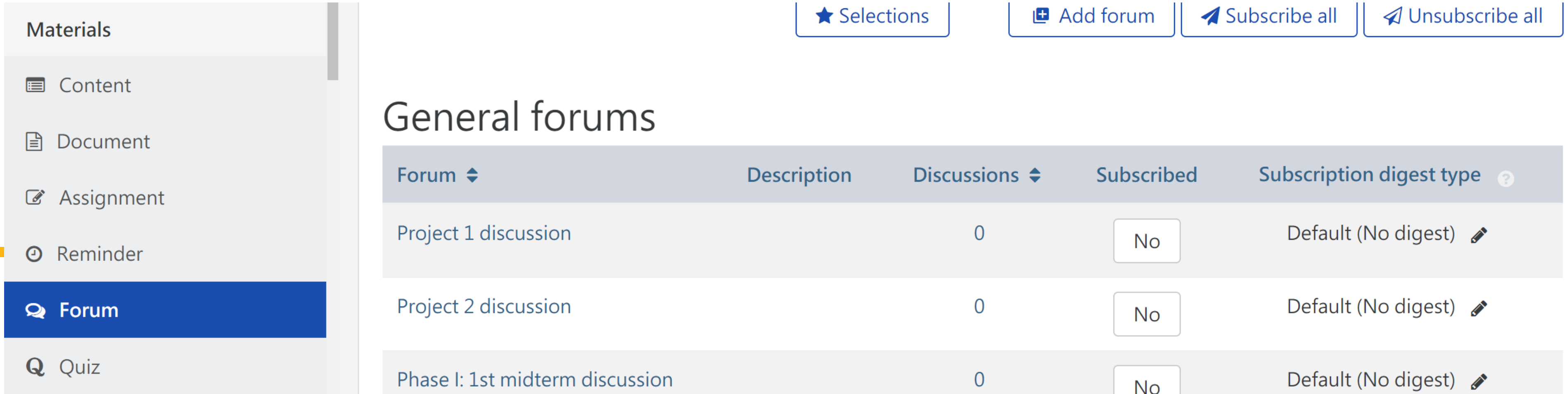
Course Information

- Course Name: Introduction to Computer Security
  - Lectures: 2B 5EF
  - Location: EC114

- Instructor: Chi-Yu Li (李奇育)
  - Email: chiyuli@cs.nctu.edu.tw
  - Office: EC529
  - Office hours: Thu. 2:30-4:30pm

Course Assistant Information

- TAs
  - Wei-Xun Cheng, Chui-Hao Chiu, Po-Yi Chou, Yi-Chen Hsieh
  - Email: ics2020@nems.cs.nctu.edu.tw
- Online office Hours: QC3 Sync Classroom
  - Tue. 1:30-4:30pm
  - F2F by appointment
- Discussion Forum on New E3



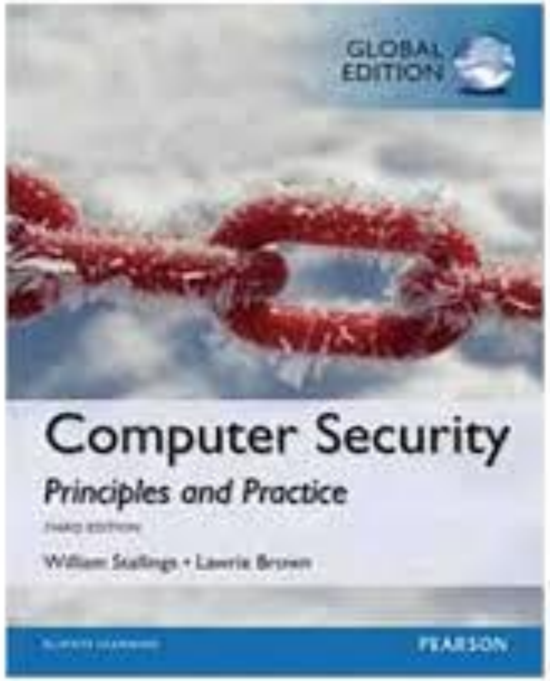
General forums

Forum	Description	Discussions	Subscribed	Subscription digest type
Project 1 discussion		0	No	Default (No digest)
Project 2 discussion		0	No	Default (No digest)
Phase I: 1st midterm discussion		0	No	Default (No digest)

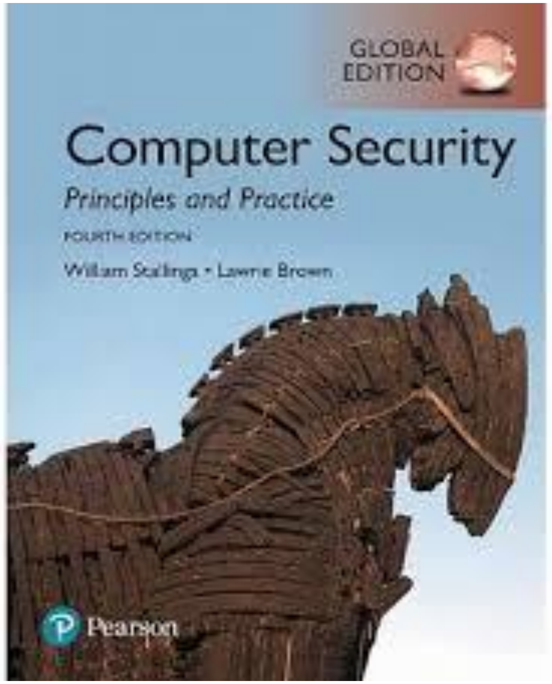
Textbook

- Computer Security: Principles and Practice
  - William Stallings and Lawrie Brown, Pearson

3rd Global Edition, 2014



4th Global Edition, 2018



What this Course is About …

- Part I: an introduction to a variety of topics in computer security
  - Computer security technology and principles
    - Cryptographic tools, user authentication, access control
    - Database security, malicious software, DoS, intrusion, firewalls
  - Software and system security
    - Buffer overflow, software security, OS security, cloud and IoT security
  - Network security
    - Internet security protocols and applications
    - Wireless and cellular network security

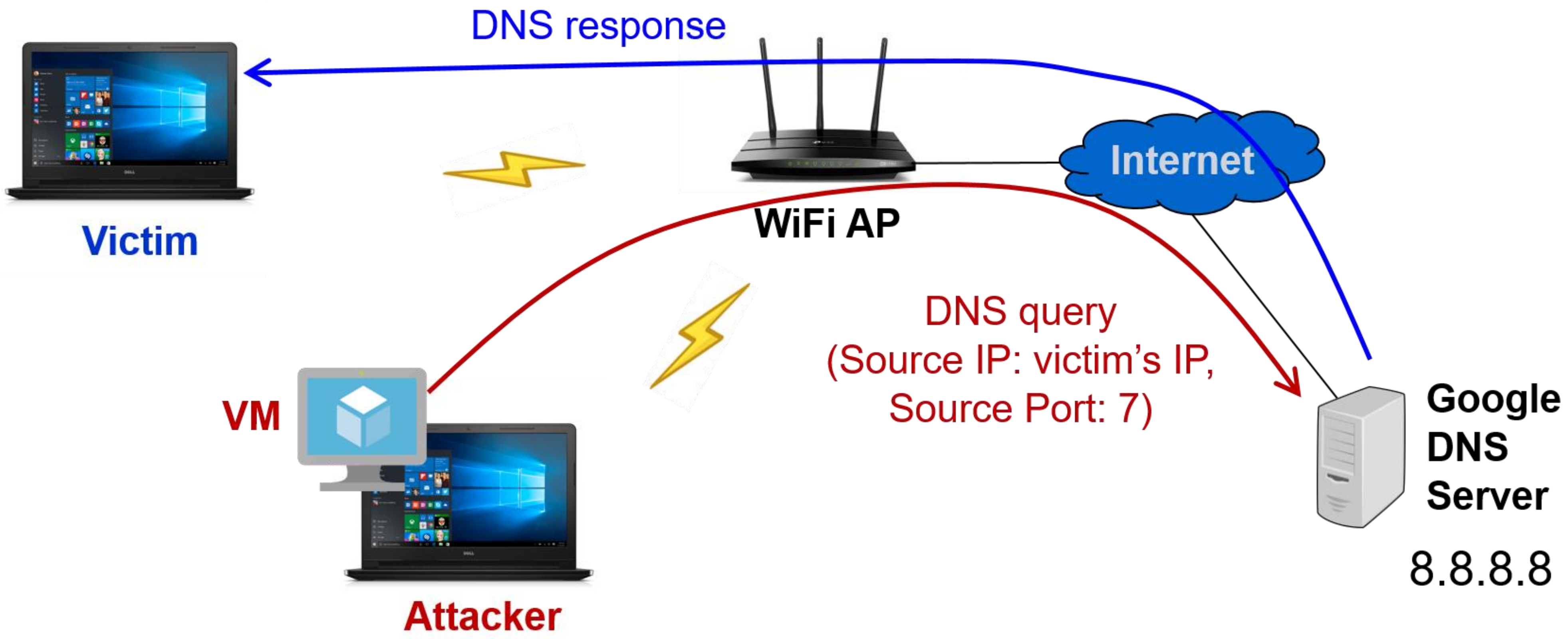
What this Course is About … (Cont.)

- Part II: a training of hand-on skills in computer security
  - A capstone course
    - Apply what you have learned into computer security
  - Recommended prerequisites
    - Computer networks, operating systems, network programming, and cryptography
  - Four projects
    - Project 1: Network security
    - Project 2: Wireless network security
    - Project 3: System (Linux) security
    - Project 4: Buffer overflow and software security

Projects

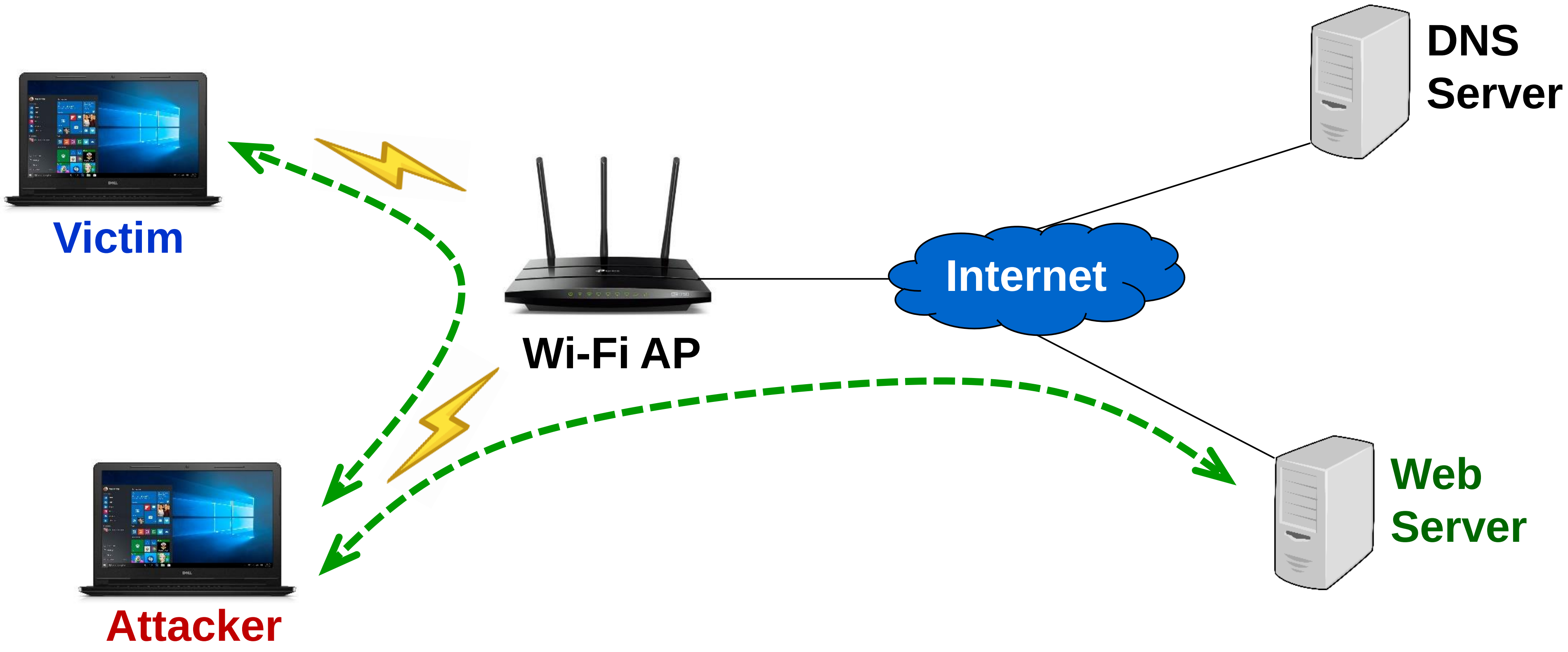
- Project 1: DNS Reflection and Amplification Attacks
- Project 2: Phishing Attacks in Wi-Fi Networks
- Project 3: Worms Replication through SSH and Its Detection
- Project 4: Capture The Flag (CTF)
  - Problems related to buffer overflow and software security

Project 1: DNS Reflection and Amplification Attacks



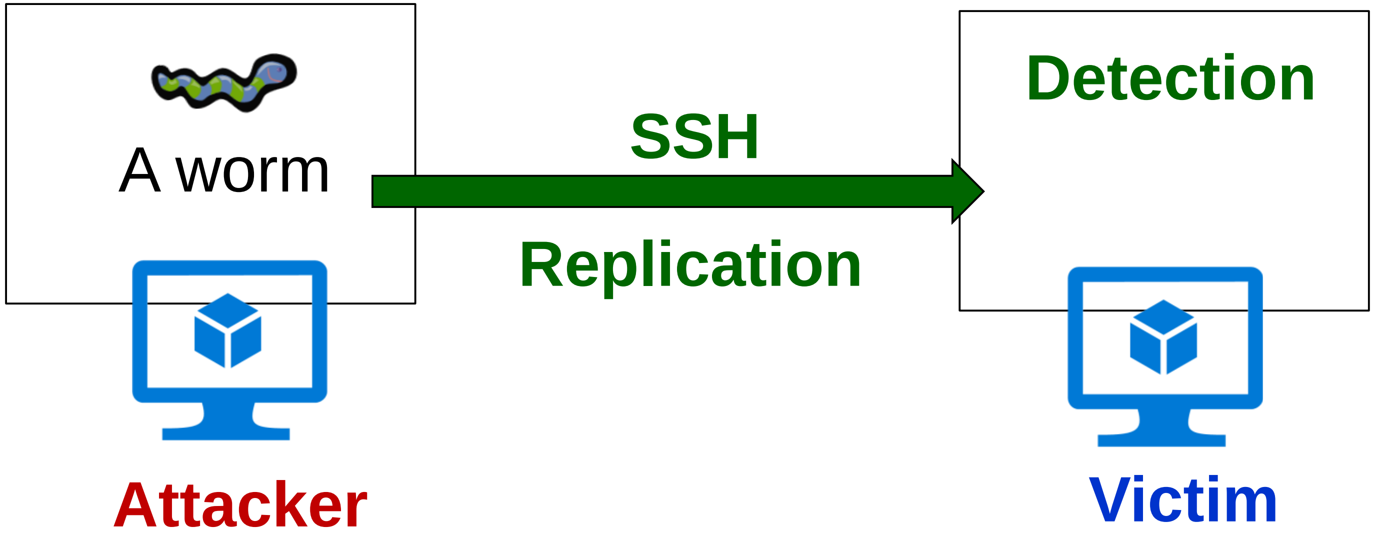
- Learned techniques
  - □ (1) Raw socket programming; (2) IP packet spoofing; (3) packet tracing; (4) DNS query fabricating

Project 2: Phishing Attacks in Wi-Fi Networks



- Learned techniques
  - □ (1) Wi-Fi packet tracing; (2) ARP spoofing; (3) DNS spoofing; (4) MITM attack

Project 3: Worms Replication through SSH and Its Detection



- Learned techniques
  - □ (1) System login with public key authentication; (2) analysis of abnormal processes on Linux; (3) routine task scheduling on Linux

Project 4: Capture The Flag (CTF)

- A type of crypto-sport
  - Goal: learning to secure a machine
  - How?
    - Giving a set of challenges
    - A “Flag” is obtained when a challenge is countered

From Wikipedia

- A toy example

```
$ python -c 'v = input(); print("flag:foobar") if v == "1" else print("failed")'
```

- Learned techniques
  - (1) Identifying misuse of C/Linux functions; (2) Identifying buggy codes; (3) Reverse engineering

Tentative Schedule

Phase I

- □ Overview
- □ Denial-of-Service (DoS) attacks
- □ Cryptographic tools
- □ User authentication
- □ Wireless network security
- □ 1st Midterm Exam (4/24)

Project 1

- Release: 3/13
- Deadline: 4/9

Project 2

- Release: 4/10
- Deadline: 5/7

Phase II

- □ Access control
- □ Internet authentication applications
- □ Malicious software
- □ Buffer overflow
- □ Software security
- □ 2nd Midterm Exam (5/22)

Project 3

- Release: 5/1
- Deadline: 5/28

Project 4

- Release: 5/15
- Deadline: 6/23

Phase II

Phase III

- □ Database and data center security
- □ Intrusion detection
- □ Firewalls and intrusion prevention system
- □ OS security
- □ Cloud and IoT security
- □ Internet security protocols and standards
- □ Cellular network security
- □ Final Exam (6/19)

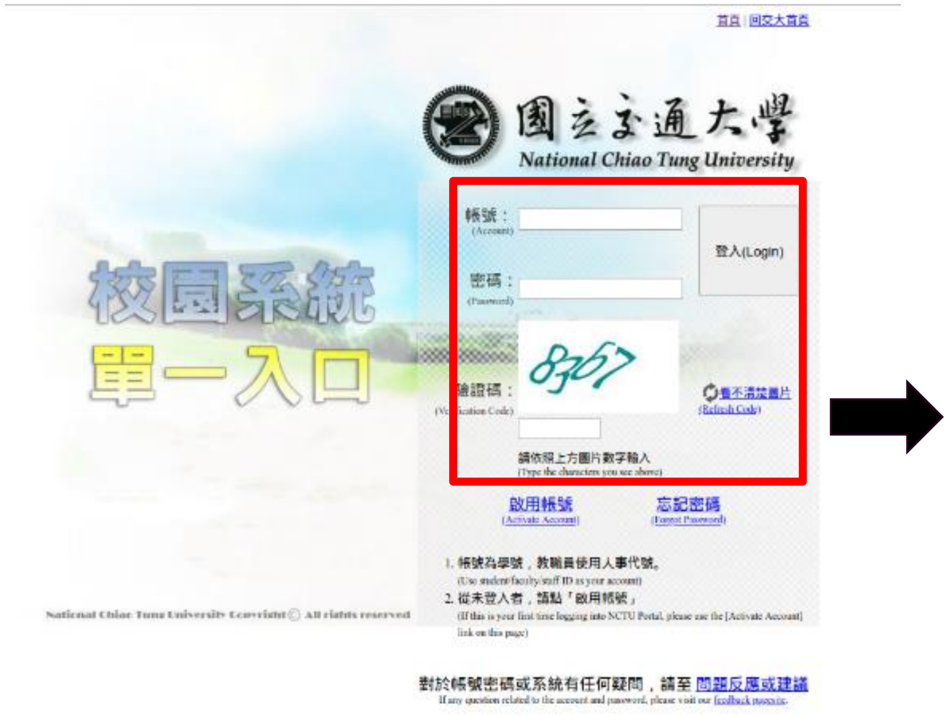
How will We Proceed?

- Slides (posted on New E3) + Blackboard-writing
- You are allowed to raise questions in Chinese
- You are encouraged to
  - attend our online office hours
  - ask/discuss your questions on the online forum
  - be absent if you feel sick or sleepy
- Course policies
  - No makeup exam! No cheating!
  - Projects: collaboration/plagiary/copy is prohibited between different teams
    - Projects 1-3: up to two team members
    - Project 4: no team-up

Roll Call for COVID-19

- Online roll call
  - QR code: directing to a per-class google form
  - Google form: inputting student ID and claimed seat
  - NCTU Google Suite: linking the form to a NCTU email
- Prerequisites
  - Sign up for G suite with your NCTU email
  - Register your email (NCTU G-Suite) for the roll call in a given form
- For each class
  - Sign in with your roll-call email, and scan the QR code to sign up and claim a seat
    - Allowed to submit only once per email
    - Will resolve any seat conflict later

How to Sign Up for G Suite?



首頁 | 回交大首頁
國立交通大學
National Chiao Tung University
校園系統
單一入口

帳號：(Account)

密碼：(Password)

驗證碼：(Verification Code)

請依照上方圖片數字輸入 (Type the characters you see above)

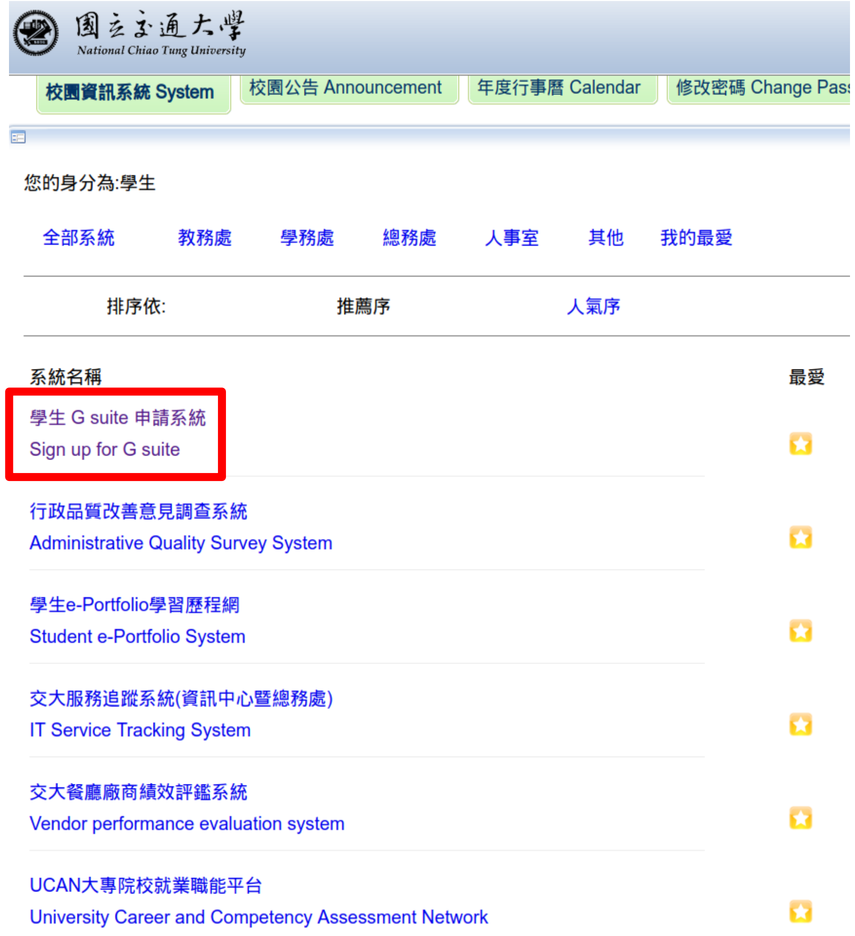
登入(Login)
看不清楚圖片 (Refresh Code)
啟用帳號 (Activate Account)
忘記密碼 (Forgot Password)

1. 帳號為學號，教職員使用人事代號。(Use student/faculty/staff ID as your account)
2. 從未登入者，請點「啟用帳號」(If this is your first time logging into NCTU Portal, please use the [Activate Account] link on this page)

對於帳號密碼或系統有任何疑問，請至 問題反應或建議

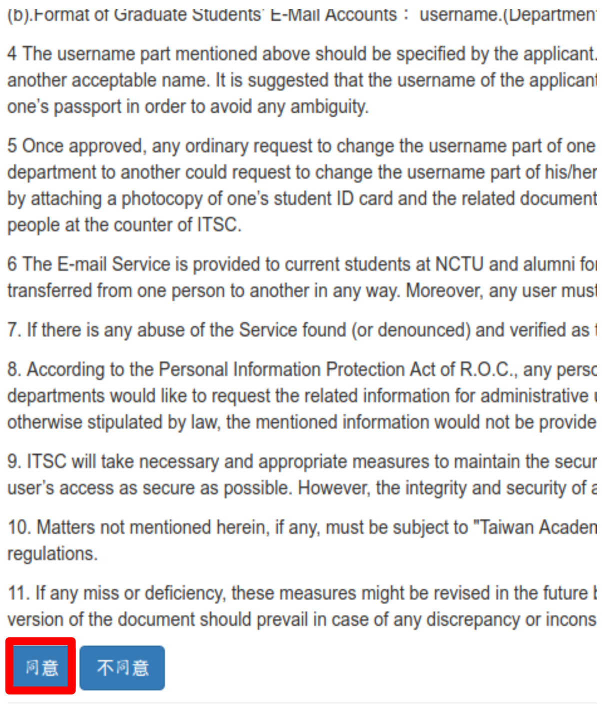
If any question related to the account and password, please visit our feedback page.

National Chiao Tung University Copyright © All rights reserved



您的身分為:學生

系統名稱	最愛
學生 G suite 申請系統 Sign up for G suite	☆
行政品質改善意見調查系統 Administrative Quality Survey System	☆
學生e-Portfolio學習歷程網 Student e-Portfolio System	☆
交大服務追蹤系統(資訊中心暨總務處) IT Service Tracking System	☆
交大餐廳廠商績效評鑑系統 Vendor performance evaluation system	☆
UCAN大專院校就業職能平台 University Career and Competency Assessment Network	☆



(b).Format of Graduate Students' E-Mail Accounts： username.(Departmen

4 The username part mentioned above should be specified by the applicant. another acceptable name. It is suggested that the username of the applican one's passport in order to avoid any ambiguity.

5 Once approved, any ordinary request to change the username part of one department to another could request to change the username part of his/her by attaching a photocopy of one's student ID card and the related document people at the counter of ITSC.

6 The E-mail Service is provided to current students at NCTU and alumni fo transferred from one person to another in any way. Moreover, any user mus

7. If there is any abuse of the Service found (or denounced) and verified as

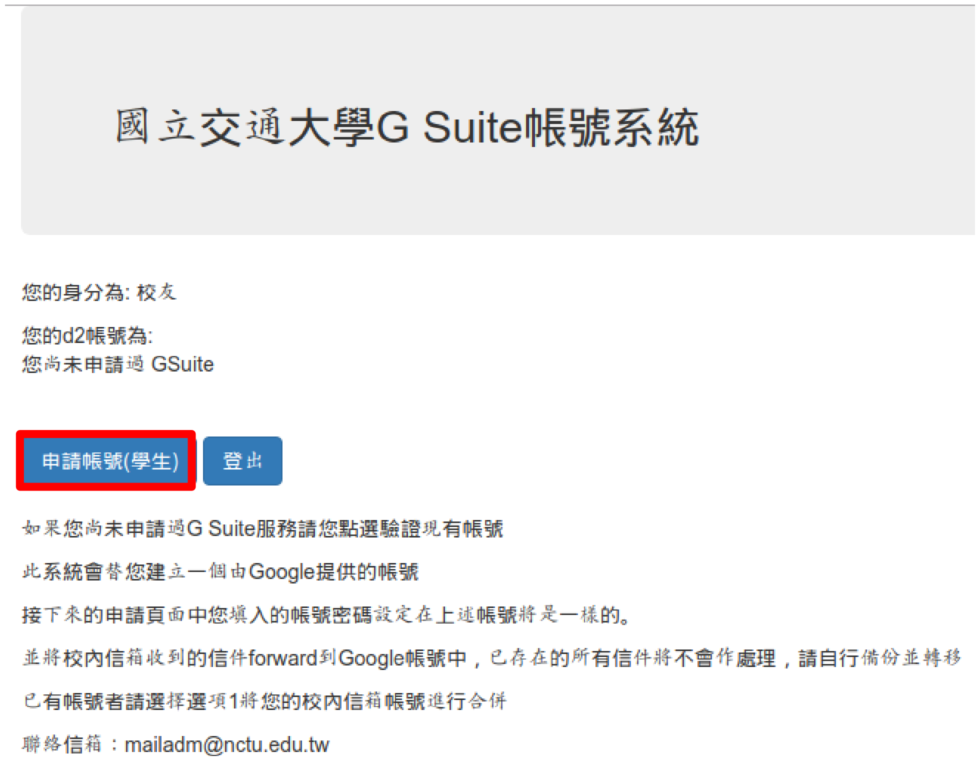
8. According to the Personal Information Protection Act of R.O.C., any persc departments would like to request the related information for administrative otherwise stipulated by law, the mentioned information would not be provide

9. ITSC will take necessary and appropriate measures to maintain the secur user's access as secure as possible. However, the integrity and security of a

10. Matters not mentioned herein, if any, must be subject to "Taiwan Acaden regulations.

11. If any miss or deficiency, these measures might be revised in the future version of the document should prevail in case of any discrepancy or incons

How to Sign Up for G Suite? (cont.)



國立交通大學G Suite帳號系統

您的身分為: 校友

您的d2帳號為:
您尚未申請過 GSuite

如果您尚未申請過G Suite服務請您點選驗證現有帳號

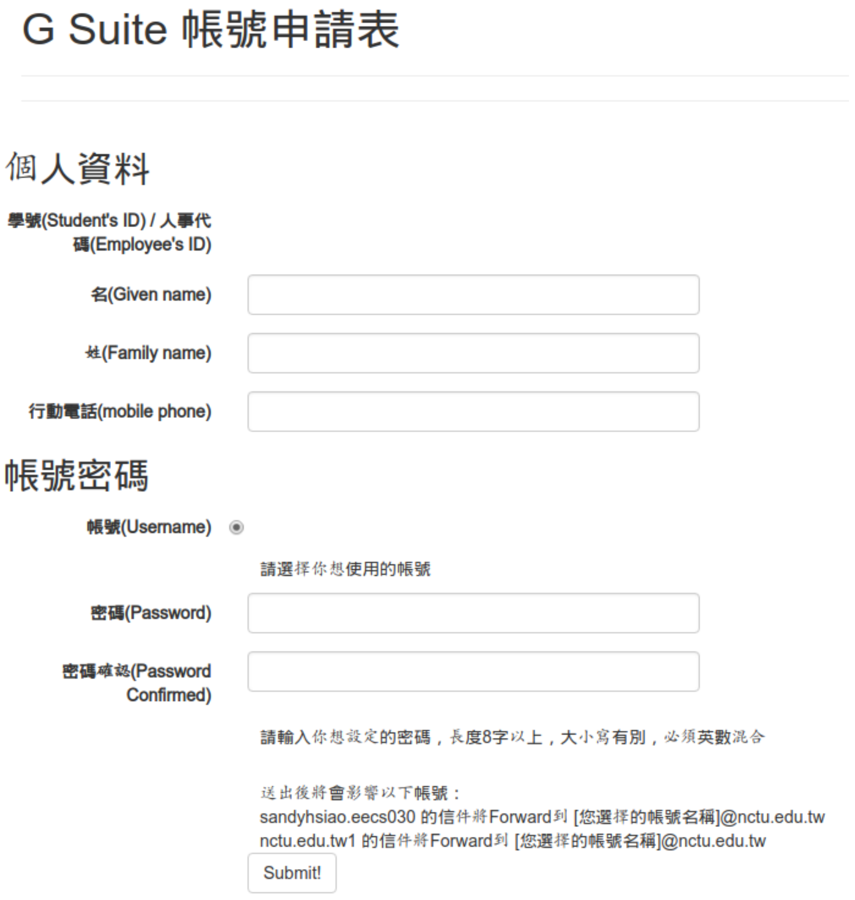
此系統會替您建立一個由Google提供的帳號

接下來的申請頁面中您填入的帳號密碼設定在上述帳號將是一樣的。

並將校內信箱收到的信件forward到Google帳號中，已存在的所有信件將不會作處理，請自行備份並轉移

已有帳號者請選擇選項1將您的校內信箱帳號進行合併

聯絡信箱：mailadm@nctu.edu.tw



G Suite 帳號申請表

個人資料

學號(Student's ID) / 人事代碼(Employee's ID)

名(Given name)

姓(Family name)

行動電話(mobile phone)

帳號密碼

帳號(Username) ●

請選擇你想使用的帳號

密碼(Password)

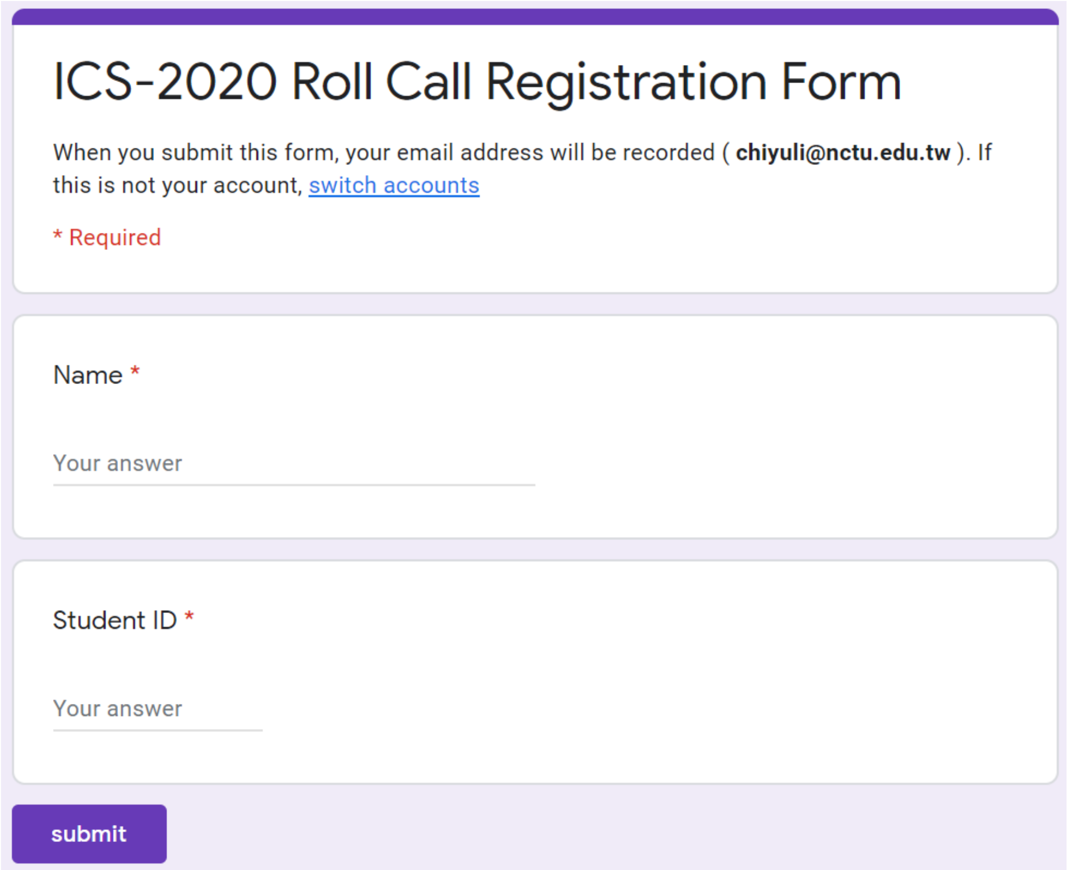
密碼確認(Password Confirmed)

請輸入你想設定的密碼，長度8字以上，大小寫有別，必須英數混合

送出後將會影響以下帳號：
sandyhsiao.eecs030 的信件將Forward到 [您選擇的帳號名稱]@nctu.edu.tw
nctu.edu.tw1 的信件將Forward到 [您選擇的帳號名稱]@nctu.edu.tw

Register Your Email (NCTU G-Suite) for Roll Call

- Link: https://forms.gle/veUjTBT2bX3Z4euX9



ICS-2020 Roll Call Registration Form

When you submit this form, your email address will be recorded (**chiyuli@nctu.edu.tw**). If this is not your account, switch accounts

* Required

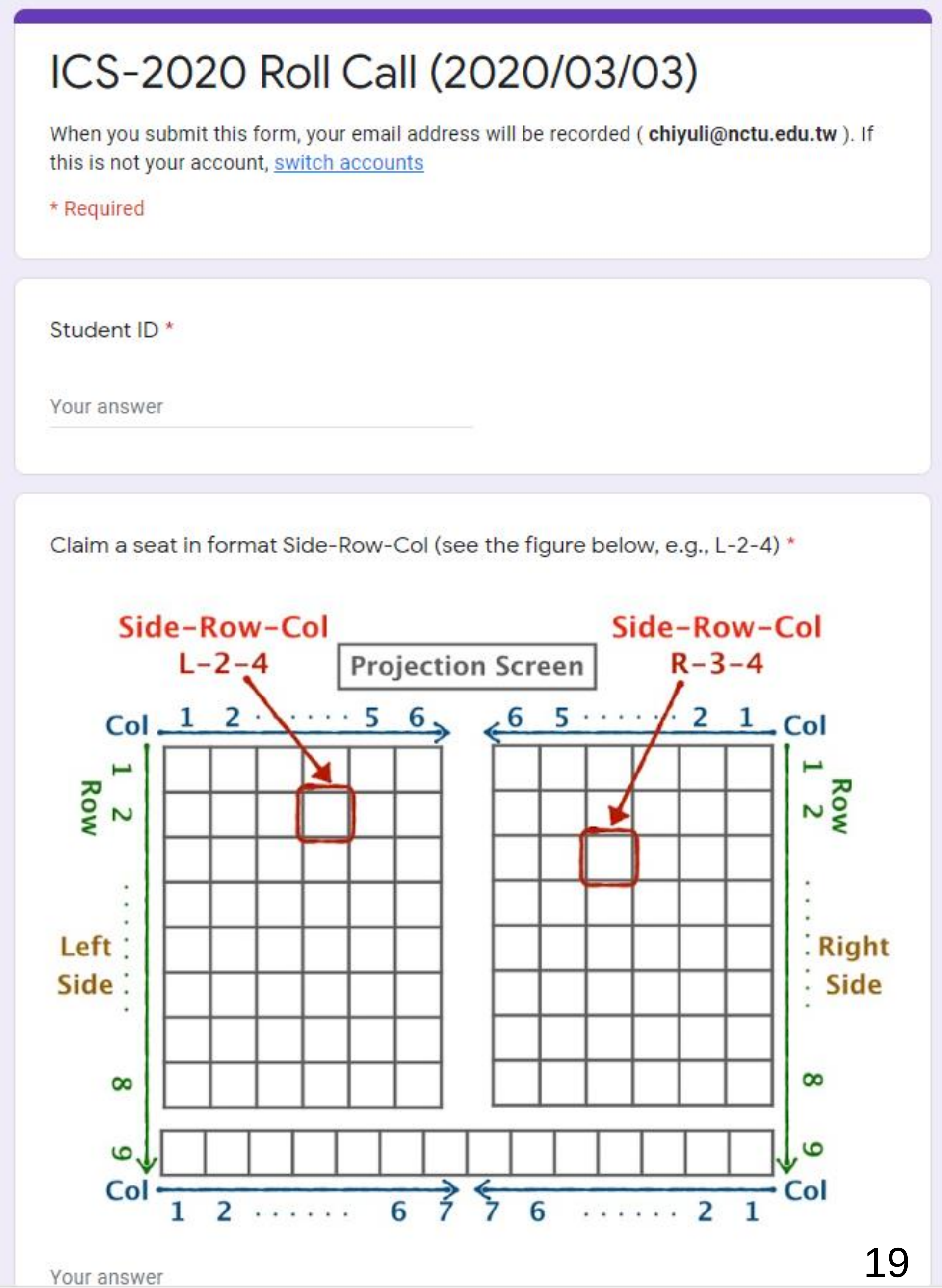
Name *

Your answer

Student ID *

Your answer

Sign Up for a Roll Call



ICS-2020 Roll Call (2020/03/03)

When you submit this form, your email address will be recorded (**chiyuli@nctu.edu.tw**). If this is not your account, switch accounts

* Required

Student ID *

Your answer

Claim a seat in format Side-Row-Col (see the figure below, e.g., L-2-4) *

Your answer

Grading Policies

- Four projects: 48% (12% each)
- Two midterm exams: 32% (16% each)
- Final exam: 20%
- Attendance
  - 10 points from each exam: show up at least two times in a month
  - 1st midterm: March; 2nd midterm: April; final: May

Why is Cyber Security so Important?

- Most computing devices are network-connected
  - □ All have risks: attacks from the network/Internet

Servers

Cyber (Network) Attack ➔ > 400 billion US dollars in Global Losses

from US CSIS (Center for Strategic and International Studies) 2014 Report

Why are Cyber Attacks so Popular?

- High returns at low risk and low cost
  - Low cost: Attacks require only network-connected devices; large-scale attacks
  - Low risk: difficult to be traced back; IP can be hidden or Botnet
  - Returns >> Cost
- Two major attack types
  - Social engineering
    - Tricking a user into granting access
  - Vulnerability Exploitation
    - Taking advantage of a design/implementation/operational flaw to gain access

Four Popular Cyber Attacks

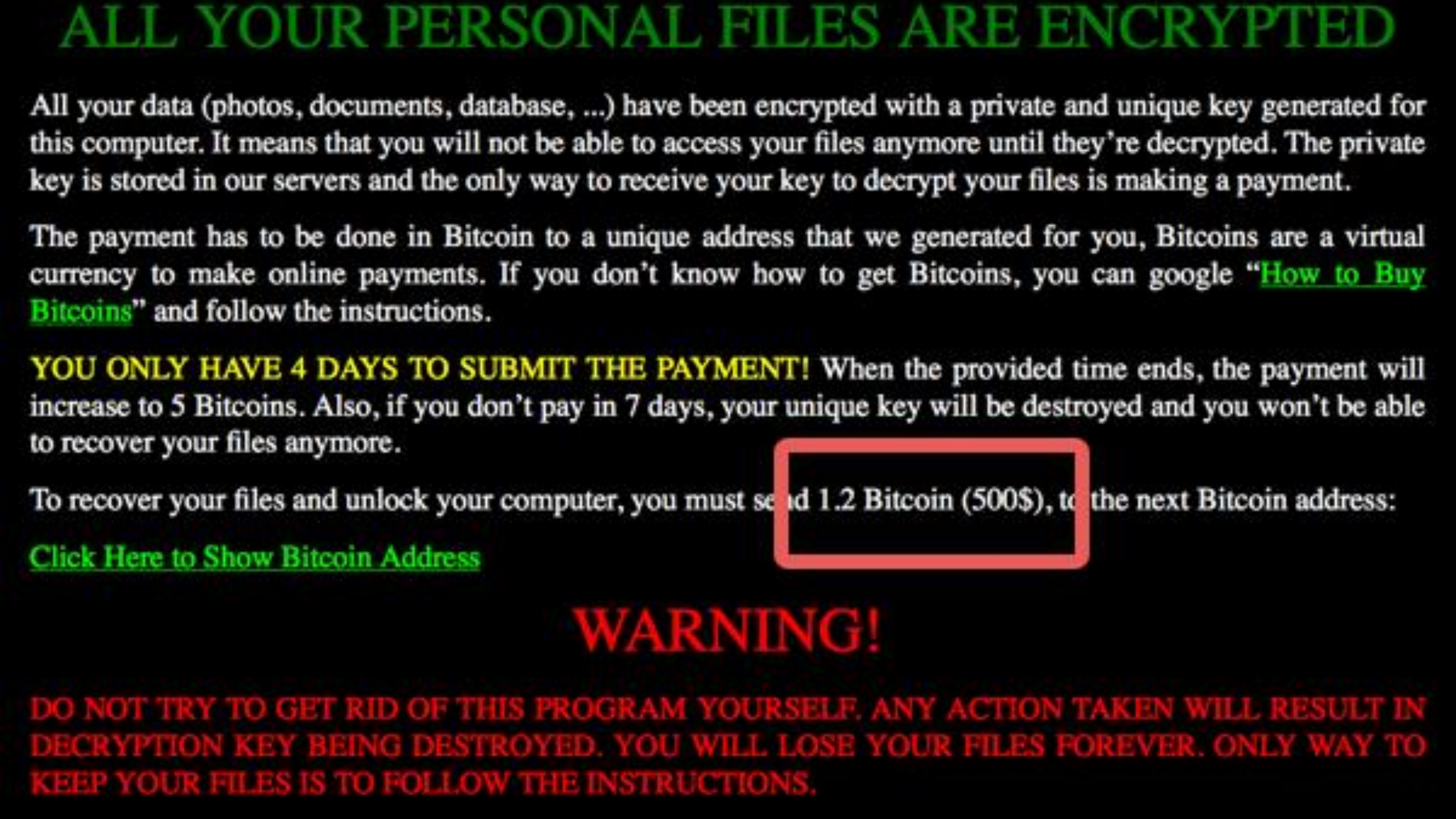
- Ransomware
- Data Breach
- Business Email Compromise
- IoT Security Threats

According to IC3 (Internet Crime Complaint Center) and IBM X-Force Report 2016

Example I: Ransomware

- Malware encrypts the victim's data and requests payment to decrypt it
  - □ Infection by social engineering
  - □ E.g., victim clicks a malicious link or opens a malicious file from an email

- By IC3
  - □ Ransomware has attacked hospitals, schools, and many individuals/companies
  - □ Ransom Money in US: 2016 Q1 (200 million) >> 2015 whole year (24 million)



ALL YOUR PERSONAL FILES ARE ENCRYPTED

All your data (photos, documents, database, ...) have been encrypted with a private and unique key generated for this computer. It means that you will not be able to access your files anymore until they're decrypted. The private key is stored in our servers and the only way to receive your key to decrypt your files is making a payment.

The payment has to be done in Bitcoin to a unique address that we generated for you, Bitcoins are a virtual currency to make online payments. If you don't know how to get Bitcoins, you can google "How to Buy Bitcoins" and follow the instructions.

YOU ONLY HAVE 4 DAYS TO SUBMIT THE PAYMENT! When the provided time ends, the payment will increase to 5 Bitcoins. Also, if you don't pay in 7 days, your unique key will be destroyed and you won't be able to recover your files anymore.

To recover your files and unlock your computer, you must send 1.2 Bitcoin (500$), to the next Bitcoin address:

Click Here to Show Bitcoin Address

WARNING!

DO NOT TRY TO GET RID OF THIS PROGRAM YOURSELF. ANY ACTION TAKEN WILL RESULT IN DECRYPTION KEY BEING DESTROYED. YOU WILL LOSE YOUR FILES FOREVER. ONLY WAY TO KEEP YOUR FILES IS TO FOLLOW THE INSTRUCTIONS.

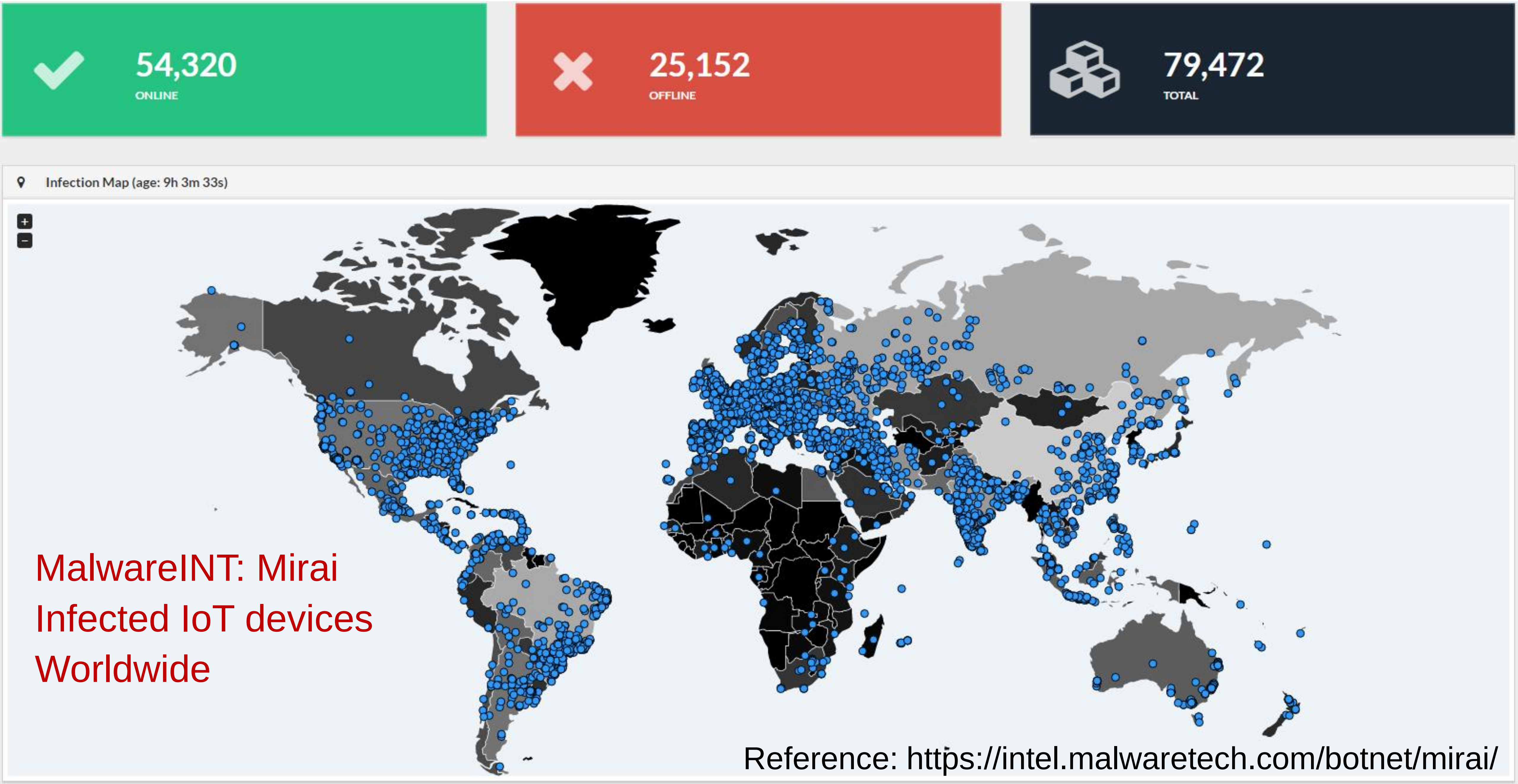
Example II: Data Breach

- [IBM X-Force Report 2016] there is leakage of 2.1 billions personal data entries in 2016
  - Even from famous companies: Yahoo, LinkedIn, etc.
- [Verizon Statistics 2015] more 75% are business interests
  - Cause by three attack manners: Hacking, Malware, Phishing
  - Companies averagely need 201 days to find root causes
  - More than 75% companies do not have any SOP for data breach attacks

Example III: Popular Password Attack

- Malware Mirai turns computer systems running Linux into “bots”
  - Bots can be remotely controlled
  - Targets: IoT devices (e.g., remote cameras and home routers)

- How does the infection work? Popular password attack
  - Hundreds of thousands of IoT devices using default settings
  - A database of more than 60 common factory default usernames/passwords
    - E.g. admin/admin



54,320
ONLINE

25,152
OFFLINE

79,472
TOTAL

Infection Map (age: 9h 3m 33s)

MalwareINT: Mirai
Infected IoT devices
Worldwide

Reference: https://intel.malwaretech.com/botnet/mirai/

Malware Mirai: Damage

- DDOS (Distributed Denial of Service) attacks
  - □ By a large number of IoT devices
- 21 Oct. 2016: Attack a DNS (Domain Name System) system
  - □ Many web services suffer from DoS (Denial of Service)

GitHub twitter NETFLIX airbnb …

Question?