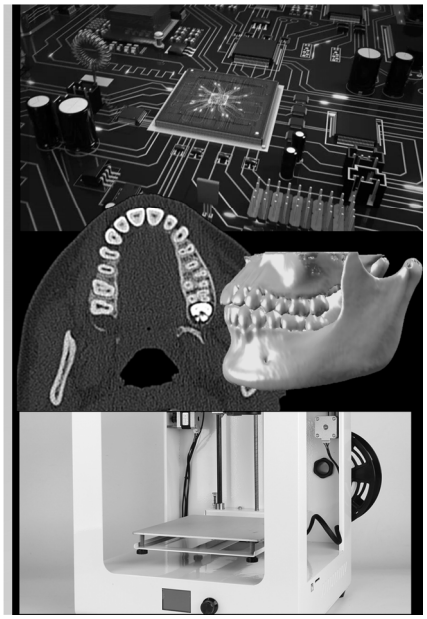
Computer sciences

Security of computers

Chia-Feng Lu 盧家鋒

Department Of Biomedical Image And Radiological Sciences, NYCU
Ext. 67308
alvin4016@nycu.edu.tw



Computer Sciences - Syllabus

Weeks	Topics
Class 10	Security of computers
Class 11	Introduction of artificial intelligence
Class 12	Introduction and practice of ChatGPT
Class 13	Applications of ChatGPT
Class 14	Using ChatGPT as a critical thinker
Class 15 (12/9)	Group preparation for final report
Class 16 (12/16)	**Final Report & Discussion**

Computer Security

- Information Security & Computer Virus
- Personal Information Security

Please download handouts from (Week 12)
http://cflu.lab.nycu.edu.tw/CFLu_course_CompSci.html

Information Security & Computer Virus

Types of virus and real cases

Information Security

Physical Security
- Security and control of the building and its surroundings.
- Proper maintenance of the network lines or power lines.

Data Security
- Data integrity and privacy; preventing damage from intruders.

Program Security
- Performance, quality control, debugging and legality of software.

System Security
- Normal operation of computers/networks; user education and training.

Common Information Security Issues

- Monitoring and misuse of personal information
  - Websites use cookies as small text files to track user behavior.
  - Number of visits, pages visited, and products purchased.
- Phishing 網路釣魚
  - Fake emails and websites as "bait" to leak private information, plant viruses, corrupt systems, or steal sensitive information.
- Wiretapping 網路竊聽
  - Improperly capturing packets from the Internet
- Hacking attacks 駭客攻擊
  - Paralysis of service attacks, mail bombs, server vulnerabilities, and Trojan horses.

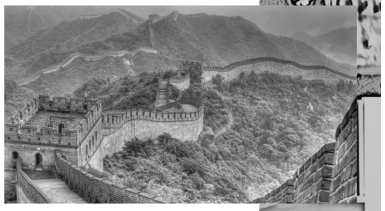
Facebook

```
Cookie:
datr=tdnZTOt21HOTpRkRzS-6tjKP;
openid_p=101045999;
act=1311234574586%2F0;
L=2;
locale=en_US;
lu=ggIZeheqTLbjoZ5Wgg;
lsd=IkRq1;
reg_fb_gate=http%3A%2F
%2Fwww.facebook.com%2Findex.php%3Flh%3Dbf0ed2e54fb
wZ3n_VN7xw1BvUw;
reg_fb_ref=http%3A%2F
%2Fwww.facebook.com%2Findex.php%3Flh%3Dbf0ed2e54fb
_VN7xw1BvUw
```


Nature of Information Security

No Eggs Can Remain Unbroken When The Nest Is Upset

覆巢之下無完卵



- Overall information security is built on a series of interlocking protection mechanisms.
- An attacker only needs to find the weakest link in the chain to completely disrupt the entire protection mechanism.

Common Types of Computer Virus

- Trojan horse/botnet (木馬/殭屍網路): 45%
  - Opens a backdoor, allowing the remote manipulation to steal accounts, data, and even use webcams.
  - The infected computer becomes a botnet for the controller, sending a large number of spam packets to paralyze the attack target.
- Computer worm (蠕蟲病毒): 25%
  - A self-replicating program that executes junk code to greatly reduce the efficiency of the computer's operation and usage.
- Macro virus (巨集病毒): 15%
  - Embedded in documents or inserted as malicious code into word-processing programs.

Signs of an Infected Computer

- **Slow start up and slow performance**
- **Suspicious hard drive activity**
- **Lack of storage space/memory capacity/missing files**
- **Crashes/restart/error messages**
- **Unexpected pop-up windows**
- **High network activity**
- **Email is hijacked**

Scan your computer with anti-virus software!

2005-2017, Ransomware (勒索病毒)

趨勢科技資安趨勢部落格 2018.10.3
https://blog.trendmicro.com.tw/?p=57054

- File encryption and ransom demand
- "Your files have been encrypted by me. If you really care about these data, I suggest you don't waste your precious time looking for a solution that doesn't exist! "
- 2015 FBI: "Suggesting victims pay up" causes controversy...

Ransomware continues to challenge law enforcement agencies

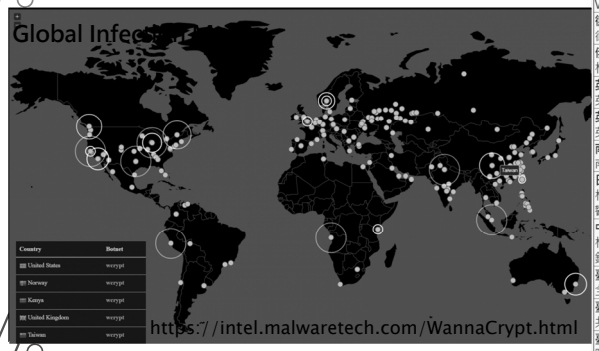
- Massachusetts police department Paid $750 in Ransom in 2013.
- The Illinois police department paid $500 in 2015.
- Dickson County (Tenn.) sheriff's office paid $572 in 2015.
- Lincoln County (Maine) sheriff's office and four rural police stations paid approximately $300 in ransom payments in 2015.
- The Alabama police department was attacked in June 2015 and refused to pay the $500 ransom, instead giving up the encrypted files.

2017, WannaCry/wcry $600 bitcoin

- The first ransomware worm with mass spreading and extortion benefits
- WNCRY extensions are used to encrypt files, targeting a total of 176 extensions, including Microsoft Office, databases, compressed files, multimedia files and extensions commonly used in programming languages.

2017, WannaCry/wcry

Originating from phishing lures users to download malware from Dropbox URL



Target OS：Microsoft Windows

法國雷諾汽車（Renault）
當諾在法國北部Sandouville的工廠，專門記錄員工生產狀況的電子版出現WannaCry勒索訊息。

德國鐵路（Deutsche Bahn）
德國鐵路車站內的電子看板遭WannaCry勒索攻擊，鐵路運行未受到影響。

俄羅斯內政部統計
根據內政部發言人表示，俄羅斯內政部約1千臺電腦受WannaCry攻擊。

英國國民保健署NHS
英國NHS旗下有16家醫院、45臺設備遭WannaCry攻擊，部分手術被迫取消。

英國日產汽車（Nissan）
英國Nissan位在Sunderland的汽車工廠，內部電腦遭WannaCry勒索攻擊。

南韓連鎖電影院CJ CGV
南韓CJ CGV電影院的廣告伺服器遭攻擊，約50間戲院受WannaCry入侵而遭殃。

日本
根據日本JPCERT統計，日本有600家公司，2,000臺電腦受WannaCry攻擊影響。

中國
根據奇虎360資安部門表示，有29,372個機構遭到攻擊，包含政府機構、大學、銀行自動提款機和醫院。

臺灣教育部統計
全臺總共10所學校（大學以下），59臺電腦受WannaCry攻擊。

臺灣電力公司
共有116臺行政電腦遭WannaCry攻擊，供電、輸電系統的電腦並未受到影響。

臺灣新北恩主公醫院
院內有3臺位於加護病房內的行動護理車的電腦，遭受WannaCry攻擊影響。

Attacks Continue to Occur

鎖定台灣企業攻擊的勒索軟體「ColdLock」，五月初發動多起攻勢，加密企業資料庫

2020/05/11 讚 134 分享

戴慈慧

https://buzzorange.com/techorange/2020/05/11/coldlock-ransor

勒索病毒全球橫行！資安專家建議企業這麼做避免受害

新頭殼newtalk｜郜敏 綜合報導
發布 2020.06.14｜10:38

讚 31

近幾個月來，包括Maze、WannaRen在內的多個勒索病毒肆虐，在美國、日本、台灣、中國等地造成災情。資安專家表示，此種病毒從早年的亂槍打鳥到近年來越來越有針對性，企業除了要建立對外的防護網外，對內也要有清楚的監控與回應機制，並為旗下每位員工建立良好的資安認知，才能將風險降到最低。

https://newtalk.tw/news/view/2020-06-14/420741

Four Symptoms of Ransomware Infection

- Unidentified external connections/links
- Strange file extensions start to appear under each directory, e.g. .crypt, .ECC, .AAA, .XXX, .ZZZ, etc.
- Ransom Note files (ransom payment instruction files) or shortcuts everywhere
- Strange shortcuts in browser toolbar

Steps to Deal With Ransomware Infection

- Disconnect the network immediately to avoid encrypting files on network drives or shared directories.
- Power off the computer immediately: The purpose of powering off the computer is to prevent the ransomware virus from continuing to encrypt the files on the computer.
- Keep the computer and report to the Information Security Center.
- Backup your data regularly.
- Don't pay!

Personal Information Security

Ten Tips for Information Security

1. Be aware of strangers

- If an unknown person moves in or out of the dormitory or research and teaching area, the management should be notified to check the situation.
- Even if you know the person, you should ask him/her the reason for entering or leaving the area that is not his/her area.
- Prevent illegal damage and theft of devices.

2. Be careful with social engineering

- Using the human relationships to steal data
  - Ex: This is the XXX center, we suspect that you are stealing other people's data and perform hacking attacks, please provide your account name and password immediately for the subsequent process.
- Pay special attention to the email
  - Sender's name.
  - Even if the email is from the same unit or someone you know, pay attention to the subject and content if it is unusual.
  - Do not open links and attachments casually.
  - Use the spam filter.

3. Log out or automatic lock

- You should log out or shut down your computer before leaving it for a long time.
  - Prevent data theft
  - Prevent theft of accounts
  - Avoid network attack
- It is recommended to set up a screen saver and lock it automatically.

4. Protect sensitive data

- Don't stick your personal account password on your laptop or screen.
- Don't put sensitive documents (account passwords, identity documents, financial and research data) on your desktop.
- No emailing of sensitive data.

5. Data sharing permissions

- Keep sensitive data separate from shared data
- Set a password and the appropriate permissions (read/write)

6. Password setting should be solid

- Passwords must be changed regularly
- Disable Guest anonymous account

密碼長度	26 英文字母	26 英文字母+10 數字	52大小寫英文字母	96 可印出字元
4	0	0	1 分鐘	13分鐘
5	0	10分鐘	1 小時	22 小時
6	50分鐘	6 小時	2.2 天	3 個月
7	22 小時	9 天	4 個月	23 年
8	24 天	10.5個月	17 年	2287 年
9	21 個月	32.6 年	881 年	21萬9000年
10	45 年	1159 年	45838 年	2100萬年

- 以中文輸入法按鍵來當成密碼
- 以英文字或數字穿插
- 以一句英文，每字字首當成密碼

7. Remote backup of important data

- Prevent important data or devices from being lost or maliciously locked.
- It is recommended to backup on different devices, but it is also necessary to confirm the security of these devices.

8. Operating system and application updates

- Hackers often use vulnerabilities to break into computers
- Operating system or application design problems
- Regular updates to the operating system or applications

9. Anti-virus software

- Install well-known anti-virus software (free versions are usually available)
- Update virus code regularly
- Keep up to date with the latest virus information
  - Newspapers and magazines
  - Anti-virus software vendors

10. Be careful when browsing the Internet

- Do not browse unknown websites, click on links or download unknown files.
- Do not install software that has not been verified as secure or authorized.
- Check for privacy policies when providing personal information.
- Make sure there is encryption when conducting online transactions.
- Cookies automatically record Internet browsing and input data, so avoid using public computers.

THE END

ALVIN4016@NYCU.EDU.TW