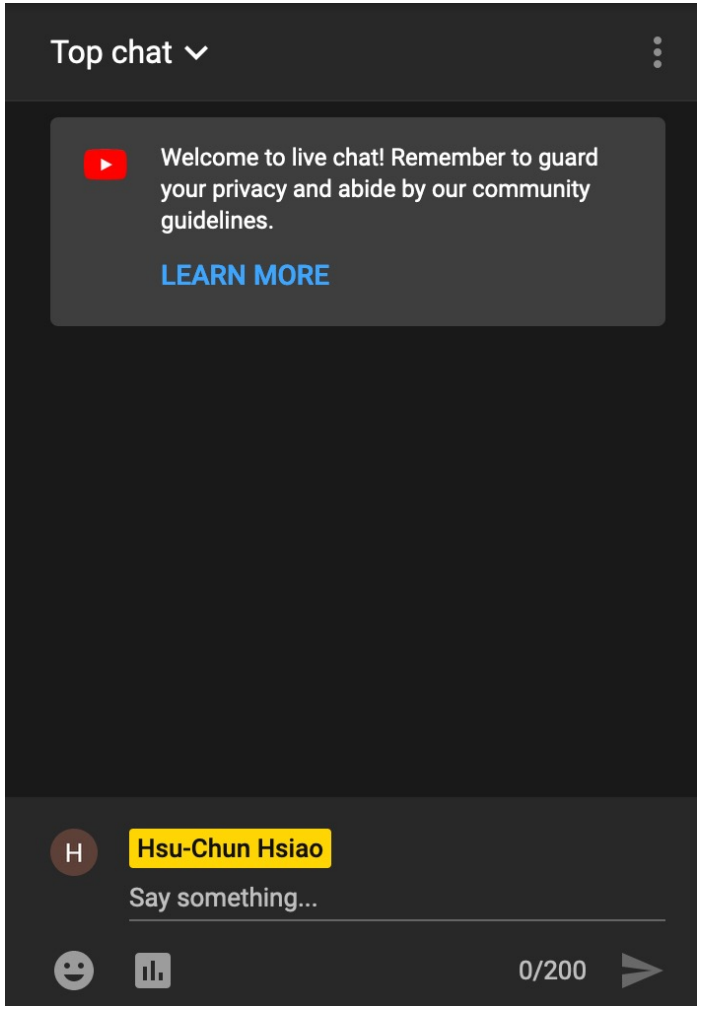
Cyber Security - I

Hsu-Chun Hsiao
Computer Science and Information engineering
National Taiwan University
hchsiao@csie.ntu.edu.tw

Ask questions on Slido

Real-time interaction / answering via chatroom



蕭旭君 | Hsu-Chun Hsiao

學經歷

國立臺灣大學 資訊工程學系 副教授（現職）
臺大醫院 資訊室資安組 組長（現職）
美國卡內基美隆大學 電機與電腦工程 博士
國立臺灣大學 電機工程學系 學士/碩士

國立臺灣大學 National Taiwan University

Carnegie Mellon University

研究興趣

資訊安全
- 網路安全
- 應用密碼學
- 自動化軟體弱點挖掘

獲獎記錄

吳大猷先生紀念獎
科技部年輕學者獎助
Delta Research Excellence Award
ACM CyberW Early Career Award Honorable Mention


NSLAB


NSLAB


BALSN


HITCON×BALSN
資安交流經典賽
2020 TAIWAN CTF


Japanese Shabu-Shabu
SHABUSATO

+

+

研究領域

高可用性網路

自動化漏洞挖掘

物聯網安全

網路隱私

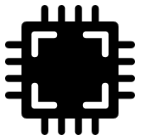
應用場域
關鍵基礎設施

醫療

政府機關

通訊

金融



科學園區

交通

Two-week Agenda

- Security 101 – 什麼是資訊安全？
- 進階主題
  - 高可用性網路 – 網路被癱瘓了連不上？
  - 物聯網安全 – 按個鍵就控制紅綠燈、汽車、電網？
  - 資安與社會 – 資安離我很遙遠？
  - 網路隱私 – 為什麼廣告都知道我喜歡什麼？
  - 自動化漏洞挖掘 – 打 001011 就能入侵電腦、盜走上億元？
  - 資安與倫理 – 研究的再現性與道德駭客
- 如何選擇資安這條路

Homework (Deadline: 10/15 midnight)

- Write a report on a recent security incident or countermeasure
- Content requirements
  - your report should include the following sections
    - (30%) Summary (timeline, cause, etc.)
    - (30%) Impact or implications on security
    - (30%) Your reflection
    - (10%) References
  - “Recent” means within the last 5 years
- Format requirements
  - No more than one page
  - You can write in either English or Chinese

Homework (Deadline: 10/15 midnight)

- Example topics
  - Zoombombing
  - SolarWinds supply chain attack
  - ProxyLogon
  - Poly Network attack
  - TLS 1.3
  - DNS-over-HTTPS
  - FLoC (Federated Learning of Cohorts)
- Reference sites
  - https://www.ithome.com.tw/security
  - https://thehackernews.com/
  - https://www.schneier.com/
  - https://en.wikipedia.org/wiki/Category:Hacking_in_the_2020s

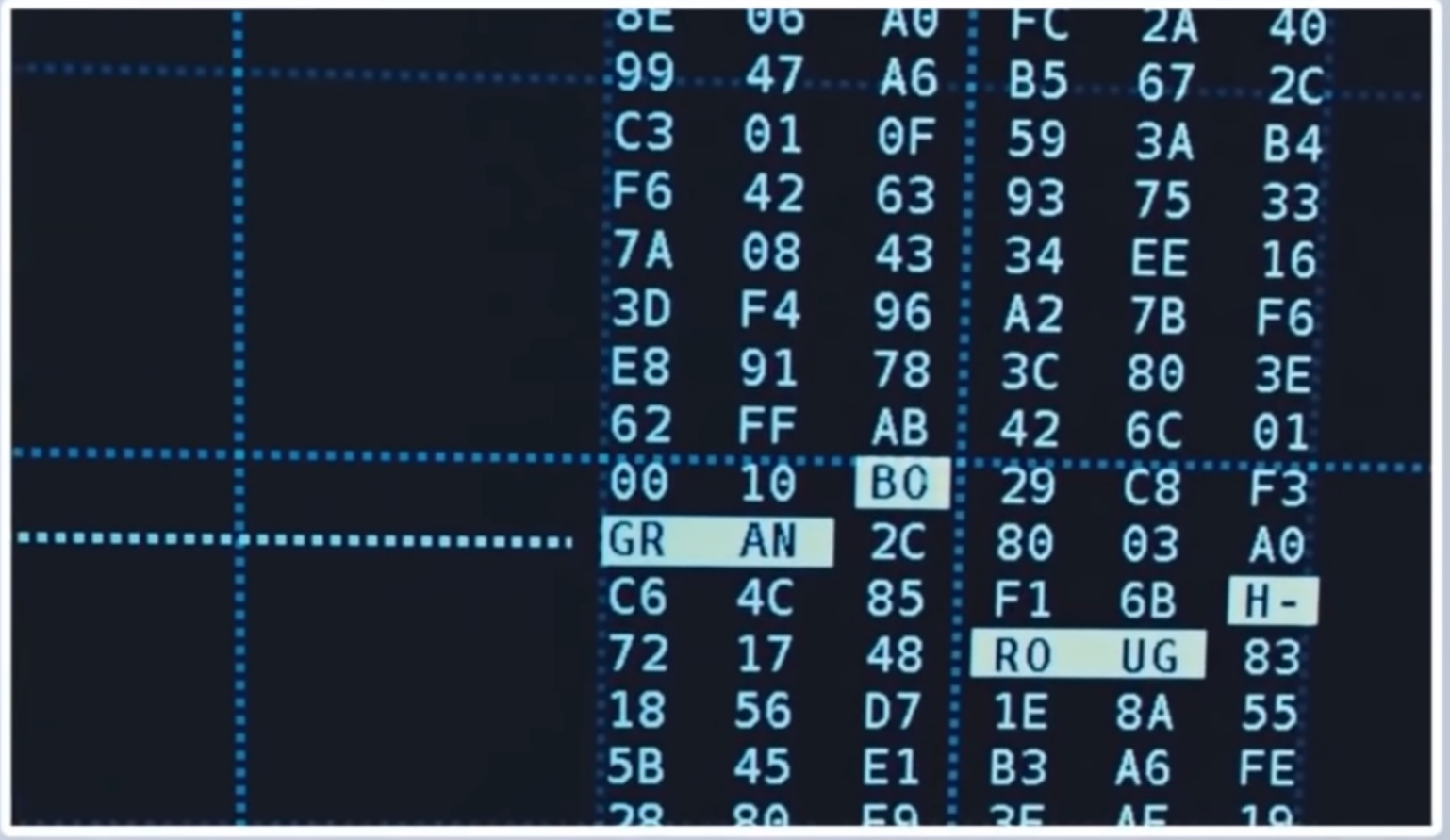
Security 101 – 什麼是資訊安全？

Security in movies

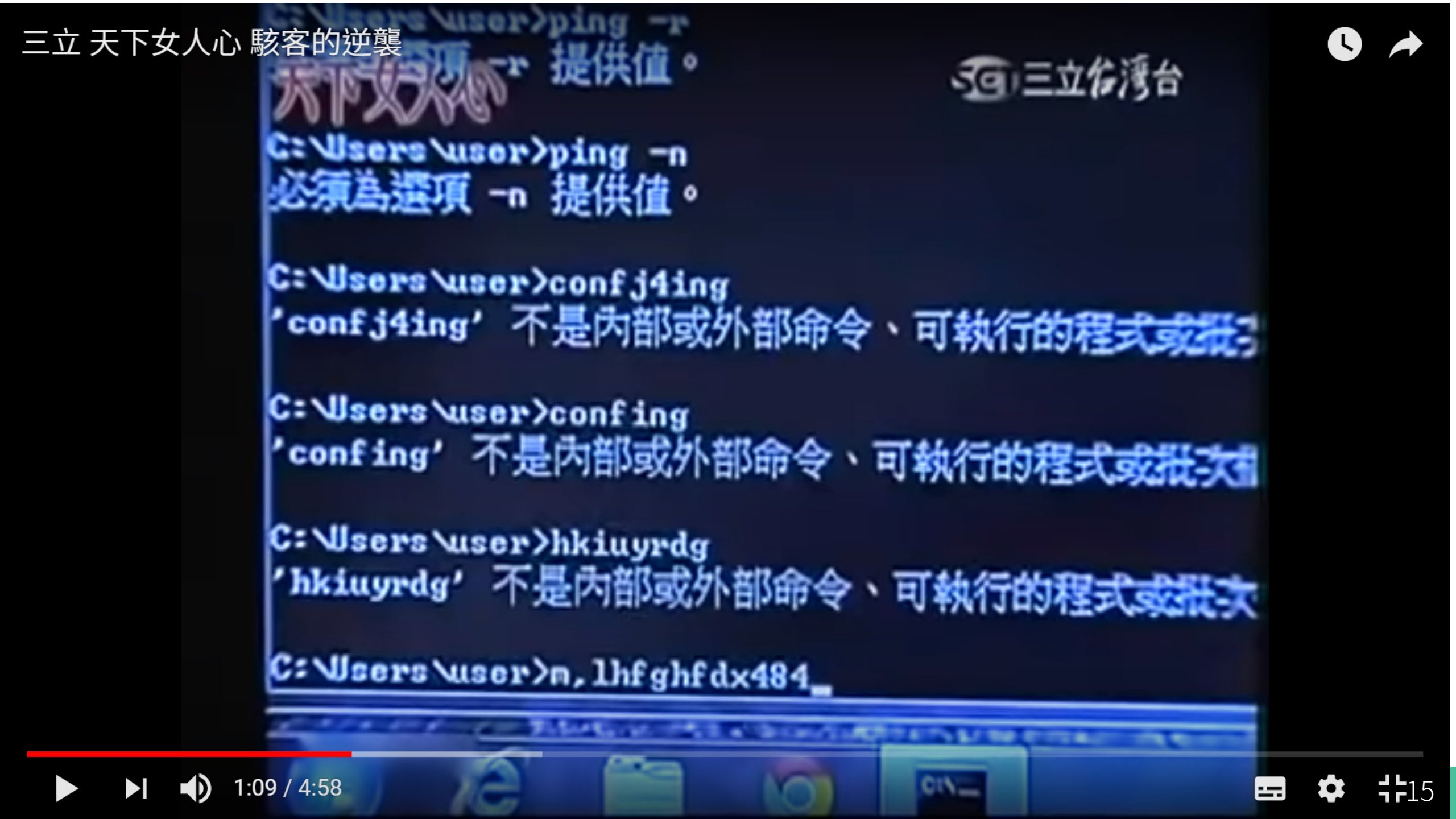
- Hacker Breaks Down 26 Hacking Scenes From Movies & TV (2018)
  - https://www.youtube.com/watch?v=SZQz9tkEHIg
  - 中文字幕版：https://www.youtube.com/watch?v=1jdsosLM_Jg
- Hacker Breaks Down Hacking Scenes From Movies & TV (2021)
  - https://www.youtube.com/watch?v=lsCrY2vWSr8
  - 中文字幕版：https://www.youtube.com/watch?v=GTPwCB5zxek

00:14《劍魚》中的駭客畫面
00:52《偷天換日》中駭入交通號誌
01:38《宅男特務》中駭入聯邦準備系統
02:29《007：空降危機》中軍情六處遭駭
03:26《網路駭客》與其他駭客一較高下
04:34《戰爭遊戲》中1980年代的駭客技術
05:21《創：光速戰記》中的存取伺服器
06:04《駭客軍團》中駭入醫院系統
06:55《重返犯罪現場》中阻止駭客行為
07:15《Live殺人網站》中的阻擋駭客入侵
08:19《CSI：網路犯罪》中的誘餌式廣告
09:03《網路上身》中的病毒反組譯
09:55《靈書妙探》中的突破防火牆
10:51《駭客任務：重裝上陣》中駭入電力公司
11:52《鋼鐵人2》中用手機駭入
12:32《摩登褓姆》中的電腦效能竊用
13:20《終極警探4.0》中的病毒執行
13:50《神鬼駭客：史諾登》中的監控行為
14:23《社群網戰》中的駭客馬拉松
15:11《變形金剛》外星人入侵
15:55《魔鬼戰將2》中破壞加密系統
16:22《黑帽駭客》中美國國安局的駭入行動
17:21《復仇者聯盟2：奧創紀元》奧創駭入賈維斯
18:11《犯罪心理》中的駭客對決
19:26《神鬼尖兵》中的電話飛客
20:07《演算法》中透過電子郵件駭入

00:15駭入政府系統《X檔案》
01:49 封鎖系統《侏羅紀公園》
03:25 解碼加密檔案《偷天密碼》
04:51 使用其他硬體駭入《防火牆》
06:07 駭入智慧冰箱《矽谷群瞎傳》
07:09 駭入ATM密碼《魔鬼終結者2》
07:53 摧毀硬碟《地心毀滅》
09:28 法拉第籠《全民公敵》
10:09 聲音分析《鷹眼》
11:21 阻斷服務攻擊《無敵破壞王2》
12:15 侵入電視頻道《V怪客》
13:20 入侵股市《我是誰》
14:31 利用自駕車輛《玩命關頭8》
15:47 盜取身份《不可能的任務4》
16:48 MagSpoof裝置《駭客軍團》
17:55 《美國隊長2：酷寒戰士》
19:27 釣魚攻擊《瞞天過海：八面玲瓏》
20:24 發現蠕蟲《黑客》
20:58 能力測驗《神鬼駭客：史諾登》

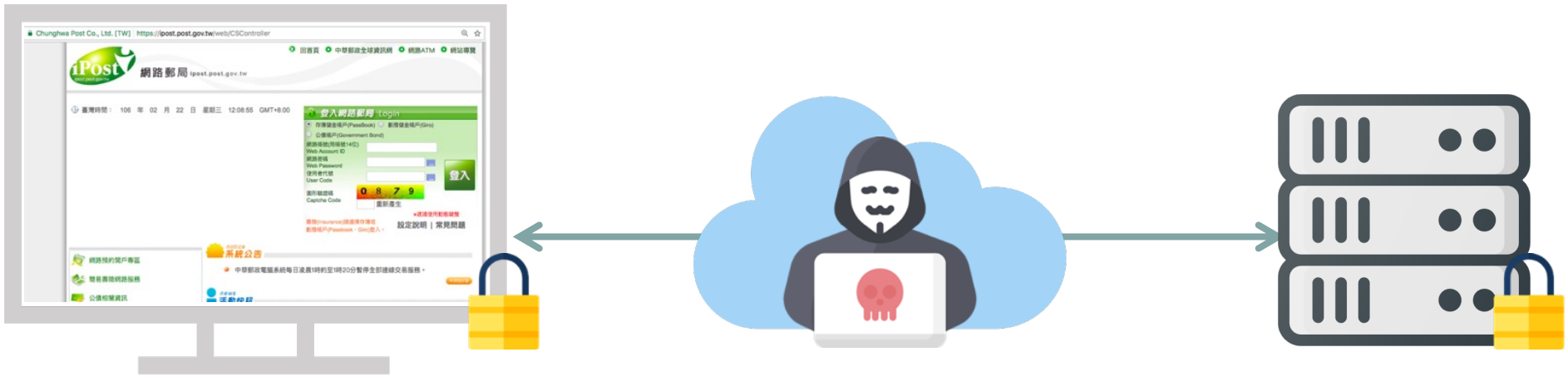


畫面中出現了十六進制代碼 可能是病毒


三立台灣台
C:\Users\user>ping -r
-r 提供值。
C:\Users\user>ping -n
必須為選項 -n 提供值。
C:\Users\user>confj4ing
'confj4ing' 不是內部或外部命令、可執行的程式或批
C:\Users\user>confing
'confing' 不是內部或外部命令、可執行的程式或批次
C:\Users\user>hkiuyrdg
'hkiuyrdg' 不是內部或外部命令、可執行的程式或批次
C:\Users\user>n,lhfghfdx484_

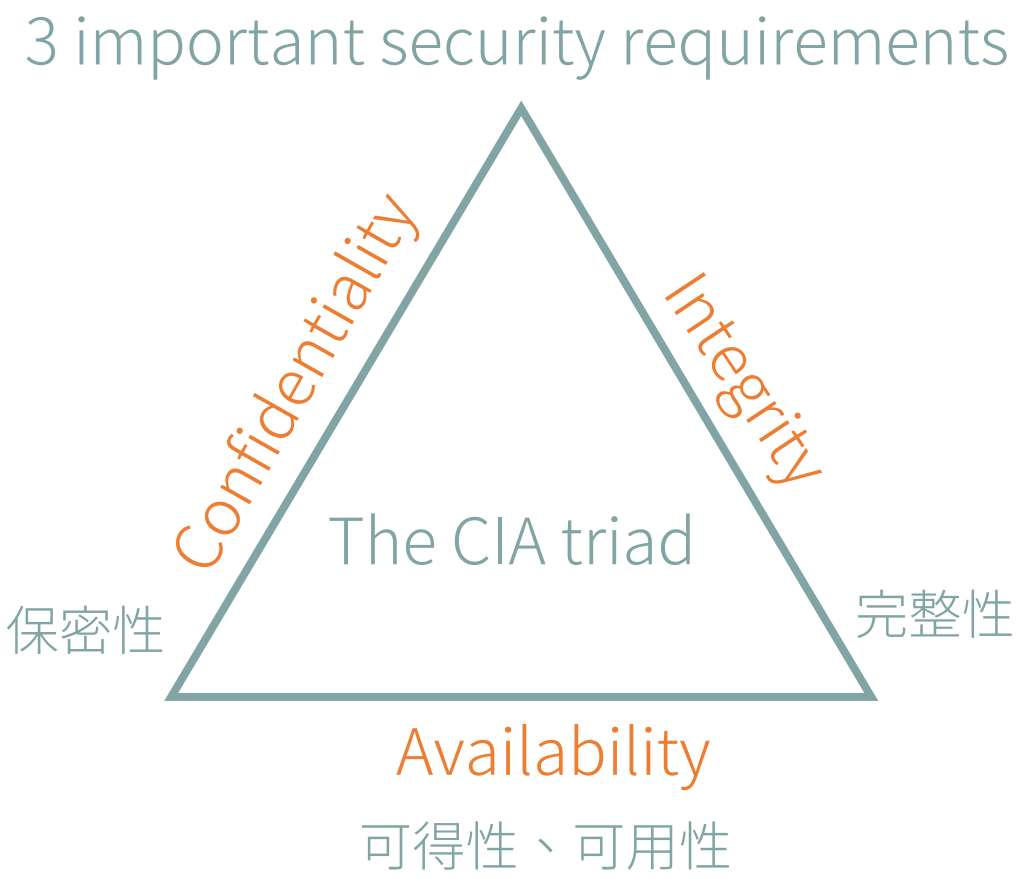
What is security?

- Protect assets (e.g., data & communication) from unauthorized actions
- Security requirements = properties that the protection should achieve
- Attackers = entities attempt to do unauthorized actions



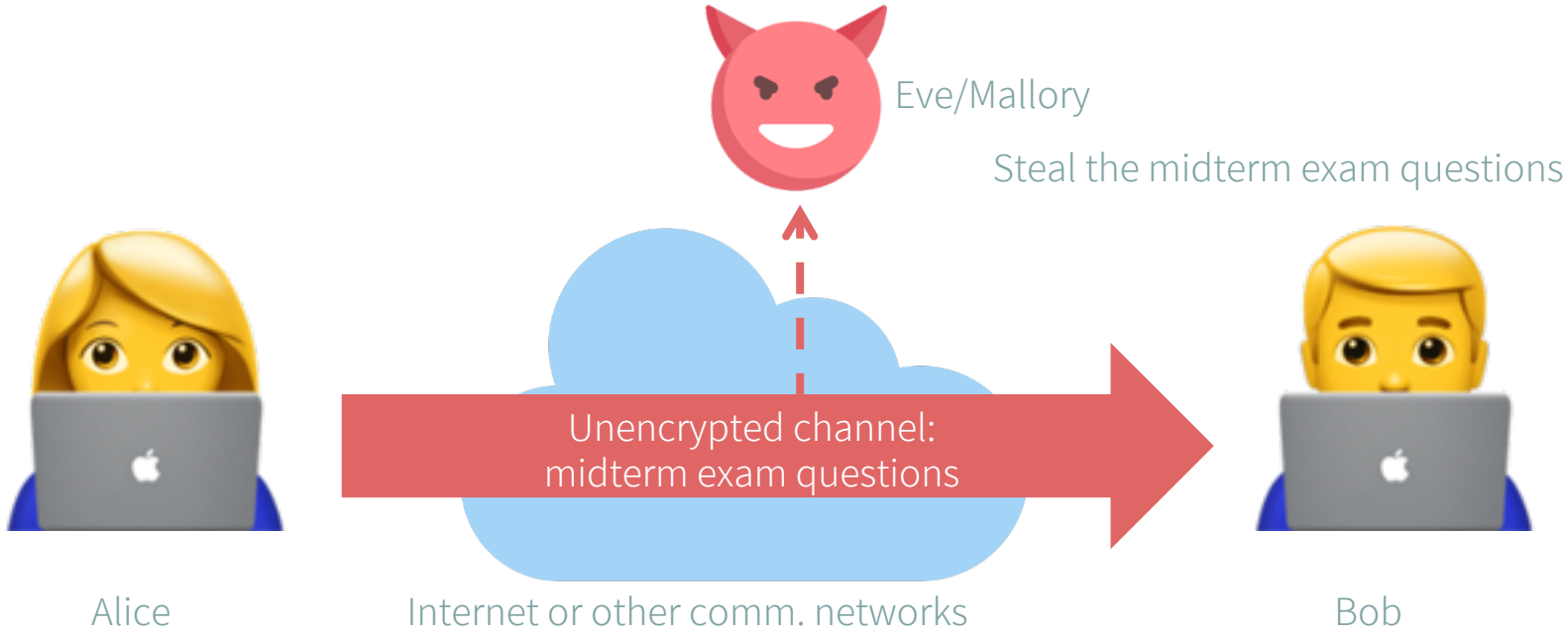
What is security?

- Security requirements are properties that the protection should achieve



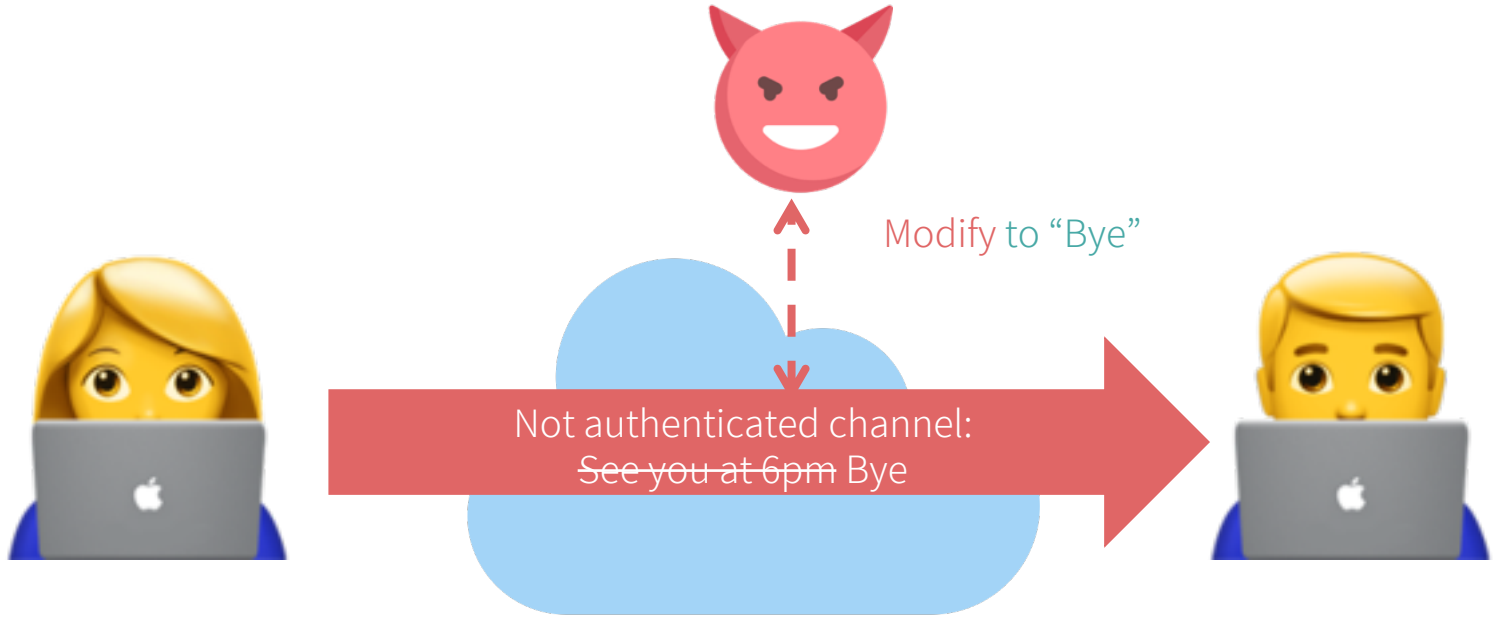
Confidentiality (保密性)

- Confidentiality is protection from unauthorized disclosure
- Eavesdropping on messages violates confidentiality



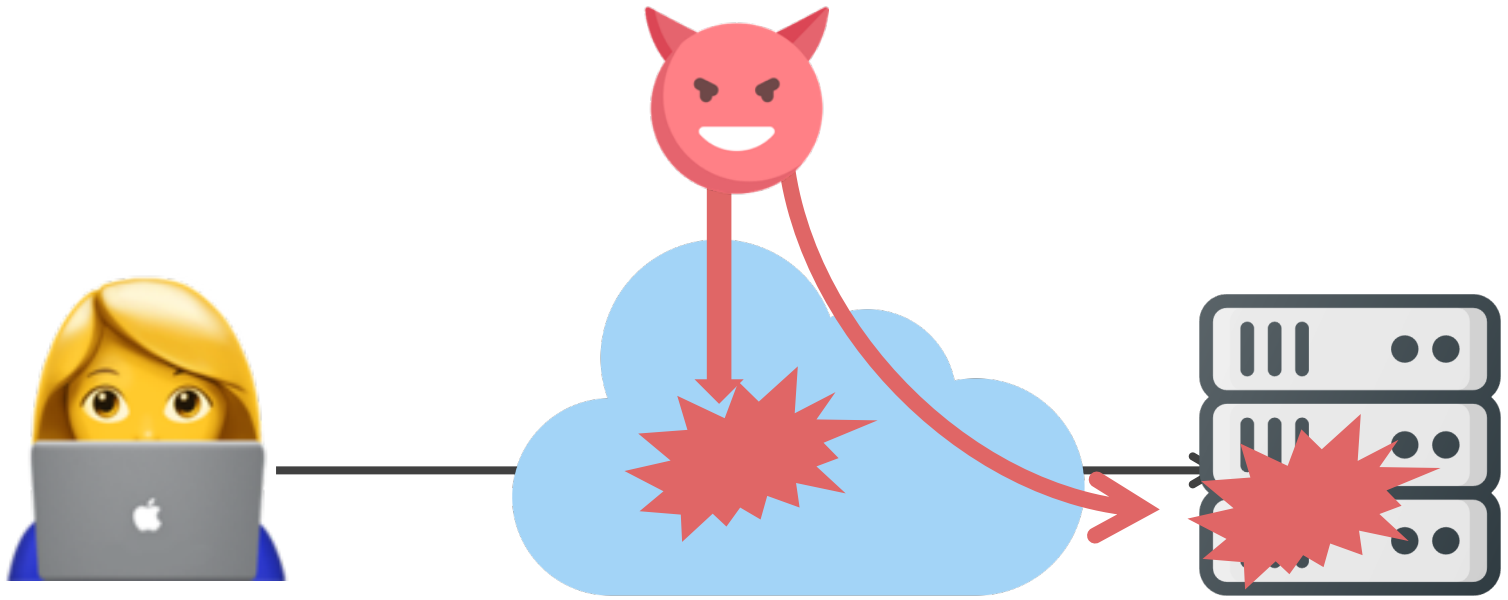
Integrity (完整性)

- Integrity is protection from unauthorized changes
- Modification of messages violates integrity



Availability (可用性)

- Availability ensures intended users can access service
- Denial of Service violates availability



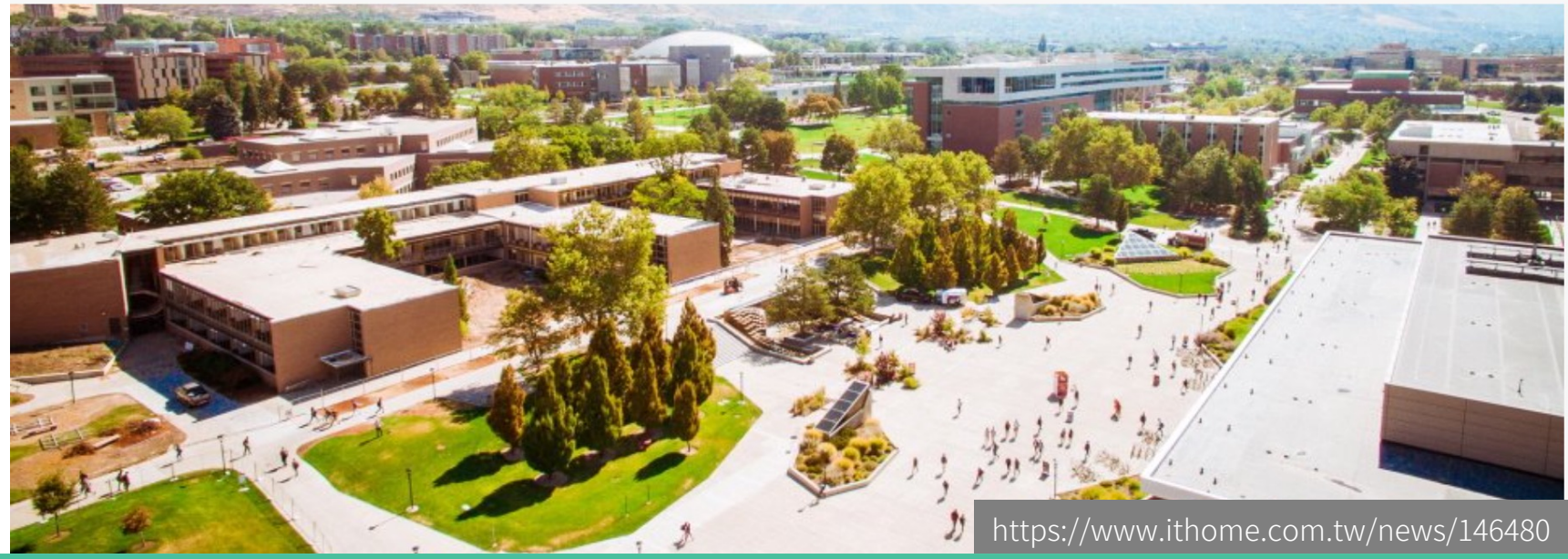
Exercise: Which security requirement is violated?

去年美國當地學校受到77次的勒索軟體攻擊，光是停機成本就損失66億美元

過去勒索軟體駭客並不特別青睞教育單位，相關攻擊案件在2018年只有10件，但2019年就激增到96件，2020年也有77件，同時駭客也愈趨鎖定大型學校為目標

文/ 陳曉莉 | 2021-09-01 發表

讚 6.7 萬 按讚加入iThome粉絲團 讚 98 分享



https://www.ithome.com.tw/news/146480

Exercise: Which security requirement is violated?

泰國政府一個含有逾1億筆旅客個資的資料庫於網上曝光

隸屬於泰國某政府機關的ElasticSearch資料庫未做好安全防範，導致近十年來曾造訪該國人士的姓名、護照號碼等個資被公開於網路上

文/ 林妍溱 | 2021-09-22 發表

讚 6.7 萬 按讚加入iThome粉絲團 讚 79 分享

https://www.ithome.com.tw/news/146815

Exercise: Which security requirement is violated?

美淨水廠系統遭駭客入侵，差點把強鹼濃度提升100倍

不明人士疑似利用淨水廠員工使用的第三方遠端電腦控制軟體TeamViewer，來駭入水廠內部系統

文/ 林妍溱 | 2021-02-09 發表

按讚加入iThome粉絲團

情境示意圖，Photo by Nathan Dumlao on unsplash

https://www.ithome.com.tw/news/142702

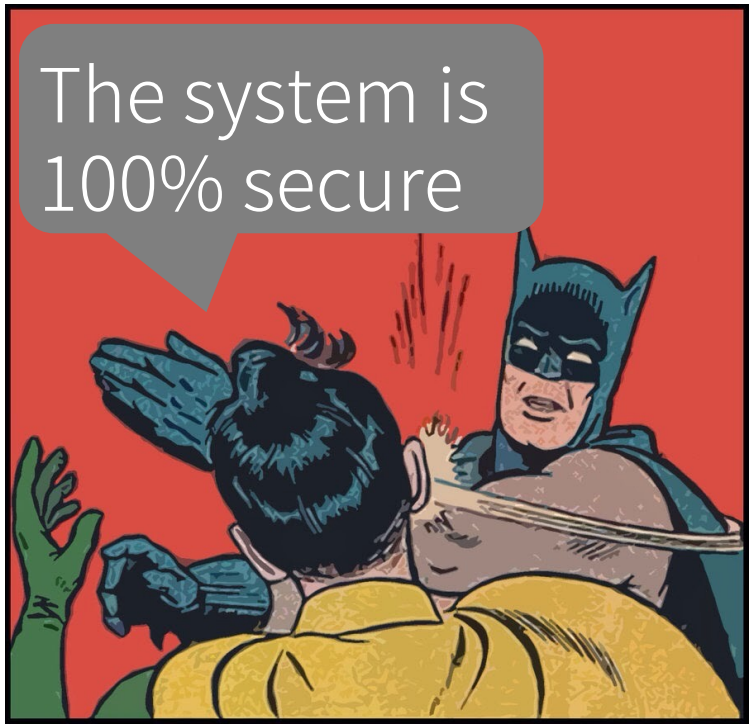
Other security requirements

- Authorization (授權)
- Access control (存取控制)
- Accountability (可歸責性)
- Auditability (可稽核性)
- Authenticity (鑑別性)
- Non-repudiation (不可否認性)
- Anonymity (匿名)
- Privacy (隱私)
- …

Threat model

Assumptions about the adversary

A well-defined threat model is a must to reason about security!



- 為什麼不能防禦所有攻擊？
  - 未知的攻擊 (zero-day attacks)
  - 難以掌控的因素
    - 如使用者的使用方式
  - 實務上的考量，如
    - 預算有限
    - 效能需求

The system
provides [Security Requirement]
against [Threat Model]
under [Assumption]

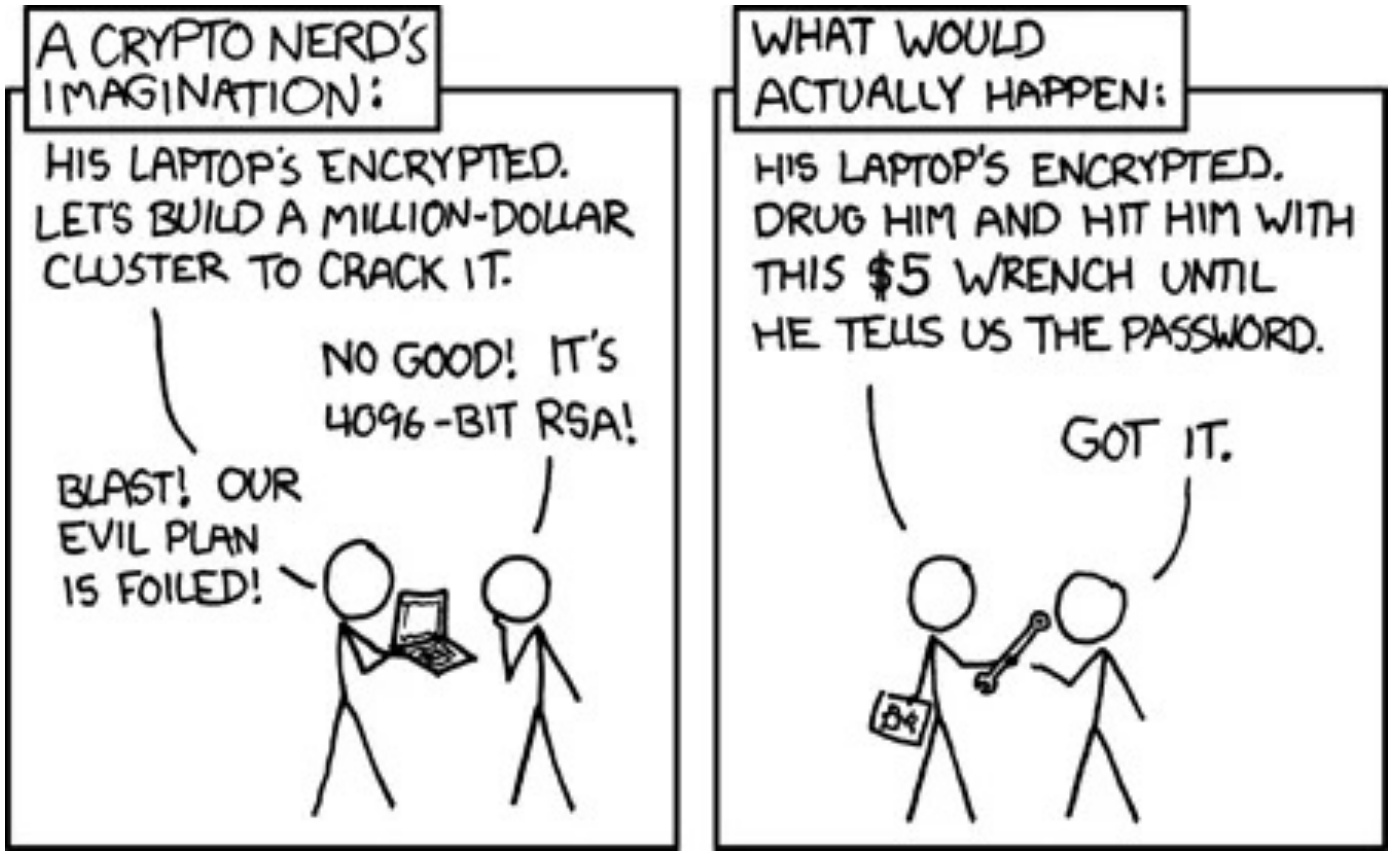
The system
provides [Security Requirement]
against [Threat Model]
under [Assumption]

例子

- System = ATM提款系統
- Security requirement= 身份認證
- Threat model = 撿到提款卡並亂試pin碼
- Assumption = 使用者沒把pin碼寫在卡片套上
  或是用生日當pin碼

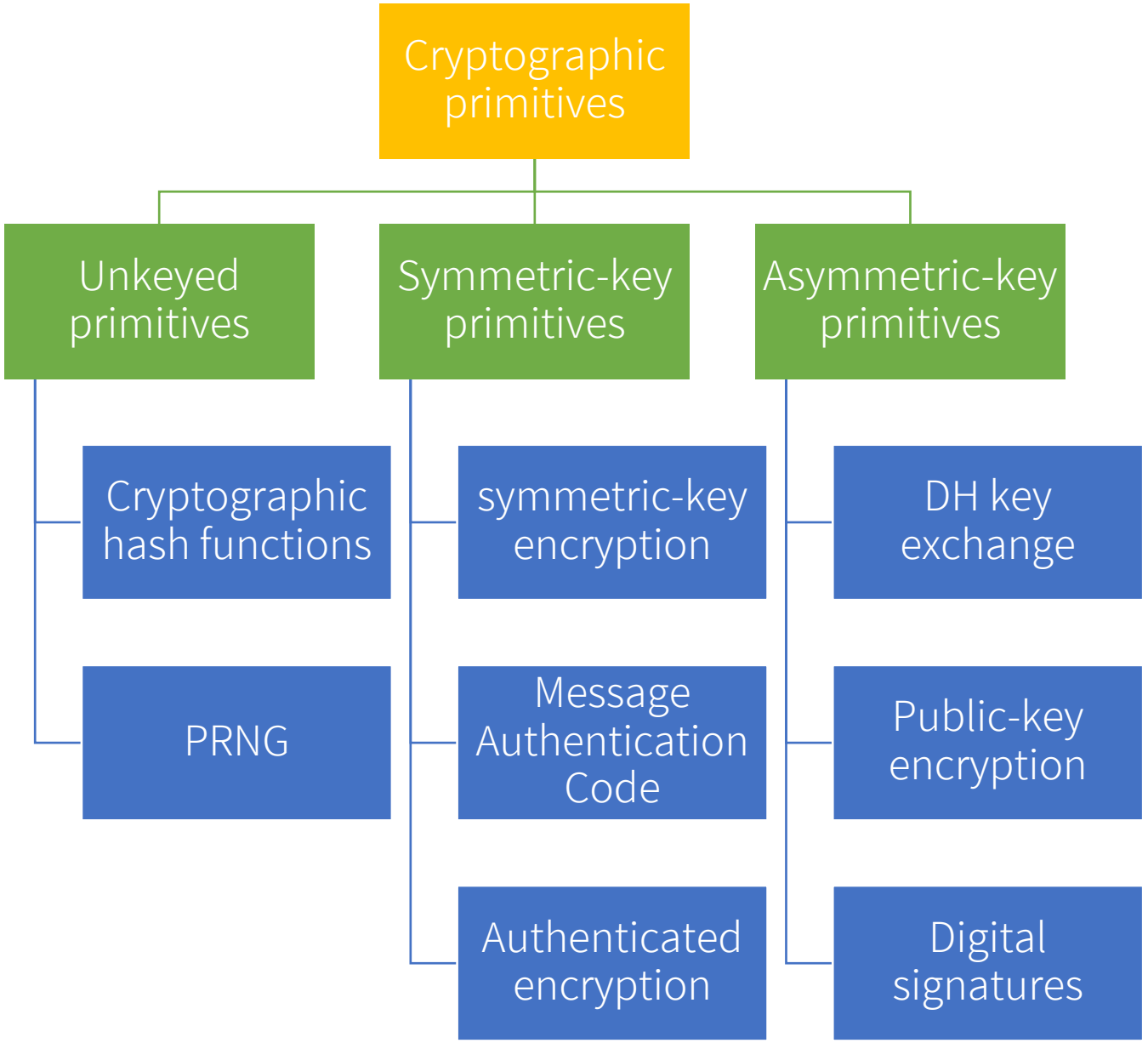
Principle #1: Defining a reasonable threat model

Principle #2: Security is only as strong as the weakest link
安全性取決於最弱的環節



密碼學 Cryptography

- Mathematical tools to protect data at rest and data in motion from adversaries
- Security of cryptosystems relies on mathematical modeling and proofs based on plausible assumptions.
- (Modern) cryptography is more than encryption.



Two-week Agenda

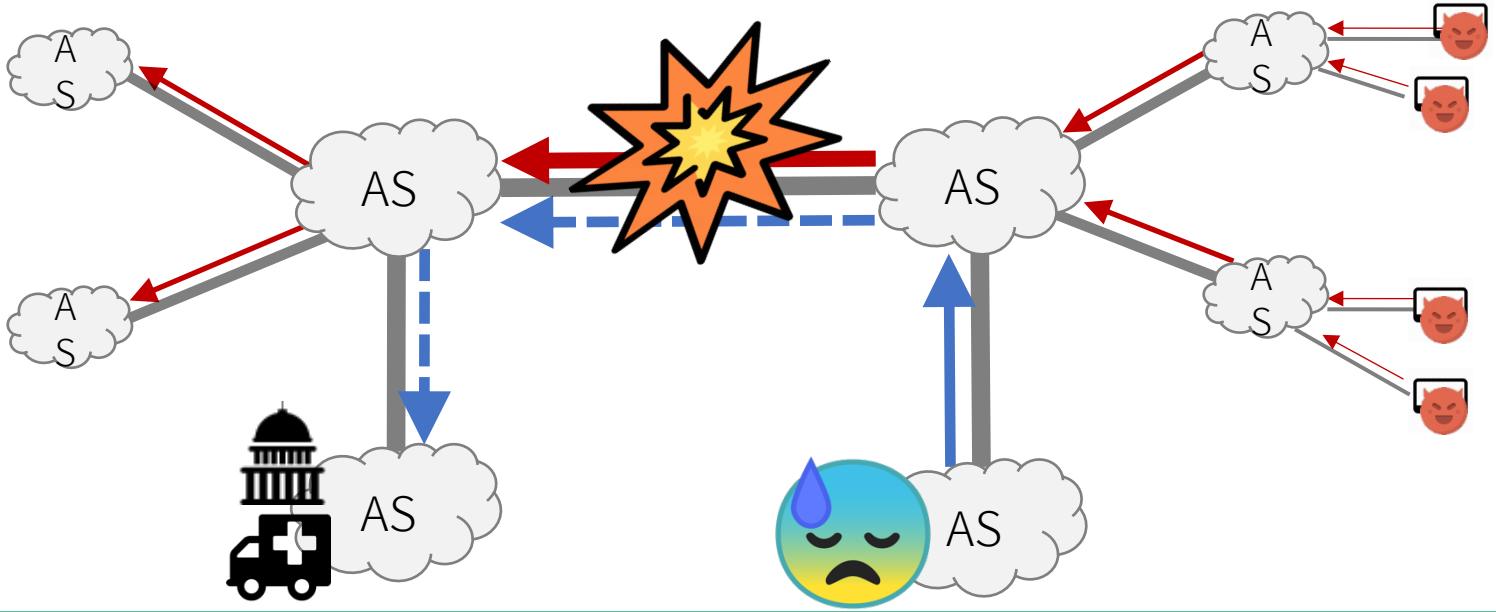
- Security 101 – 什麼是資訊安全？
- 進階主題
  - 高可用性網路 – 網路被癱瘓了連不上？
  - 物聯網安全 – 按個鍵就控制紅綠燈、汽車、電網？
  - 資安與社會 – 資安離我很遙遠？
  - 網路隱私 – 為什麼廣告都知道我喜歡什麼？
  - 自動化漏洞挖掘 – 打 001011 就能入侵電腦、盜走上億元？
  - 資安與倫理 – 研究的再現性與道德駭客
- 如何選擇資安這條路

High-availability Network

高可用性網路

High-availability Network

- 研究挑戰：現行防禦多為 best effort，未能提供任何 guarantee
- 我們的研究主題
  - Smarter DDoS attack and defense
  - Locating faulty or malicious routers
  - Identifying overuse network flows
  - Future Internet



什麼是 DDoS?

Distributed Denial of Service

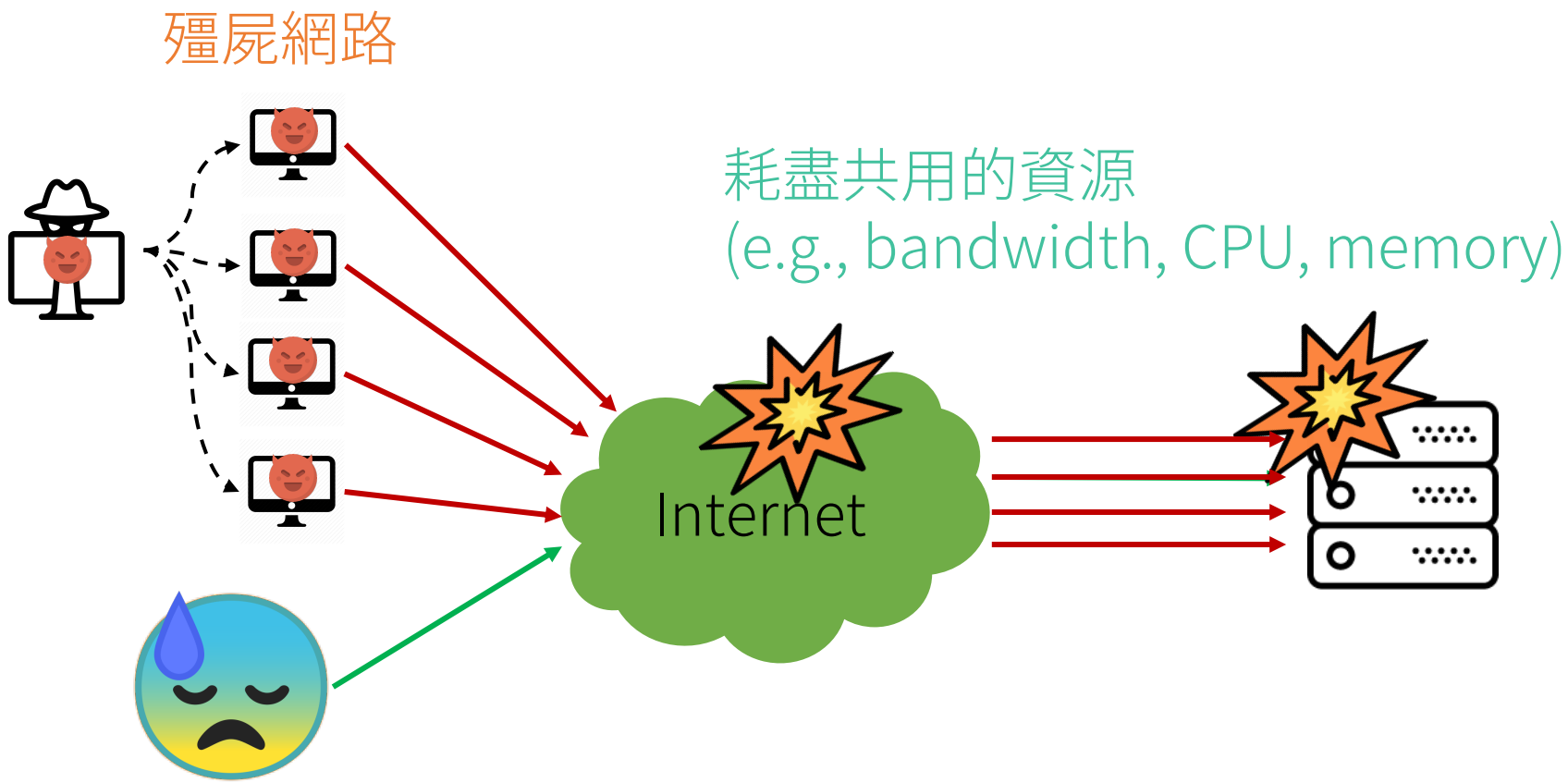
分散式 阻斷服務攻擊

有很多攻擊來源
提高攻擊強度、降低被偵測的風險

讓使用者無法使用想要的服務

分散式阻斷服務攻擊

常見形式



Why DDoS?

- 恐嚇勒索
- 商業競爭
- 聲東擊西
- 前導攻擊
- 政治示威

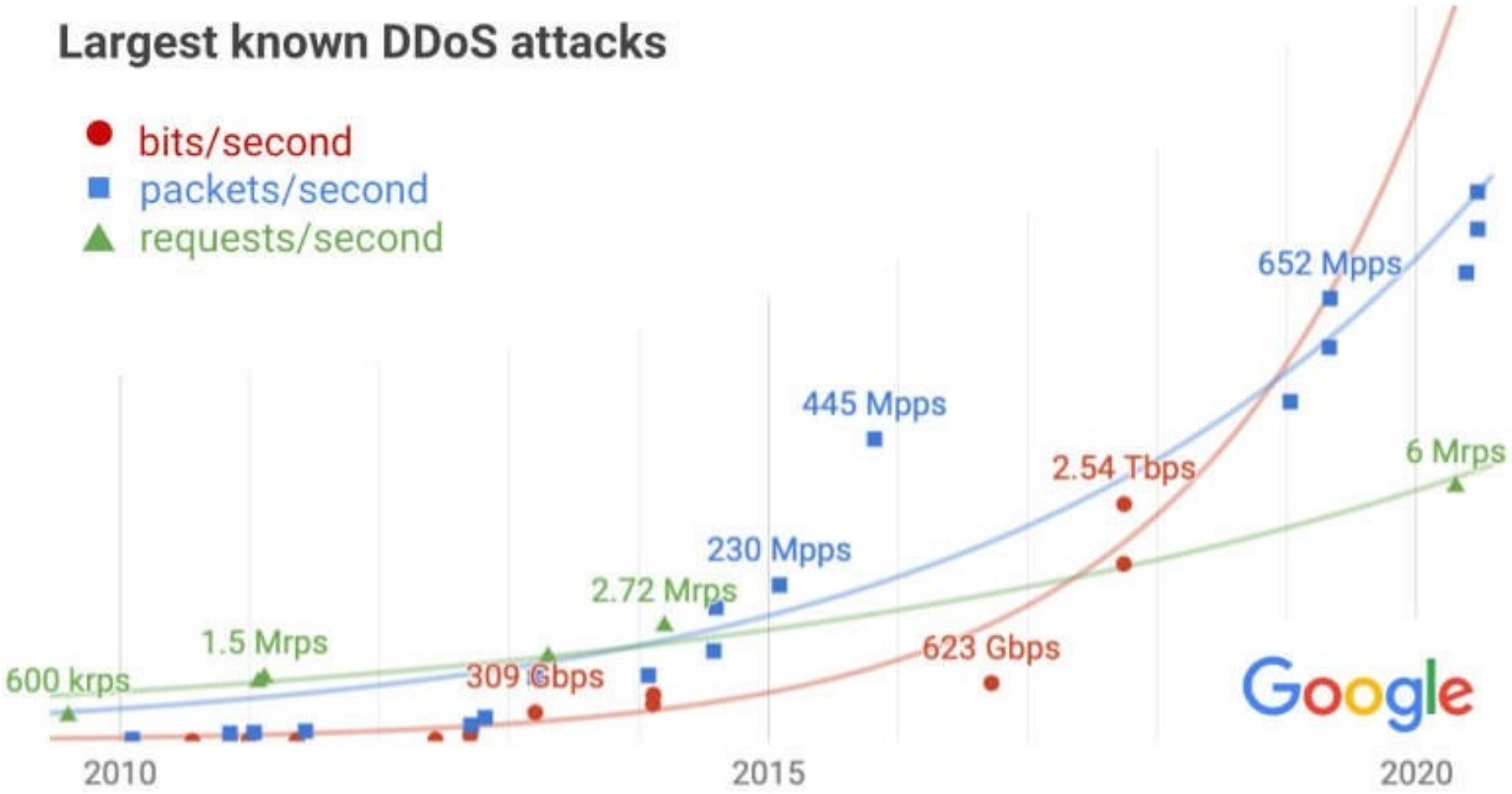
博奕網站遭史上第三大800 GB流量勒索式DDoS攻擊

一家博奕網站近日遭到勒索軟體組織發動每秒800GB流量的DDoS攻擊，是歷來第三大攻擊事件，同時也使用前所未見的攻擊途徑

文/ 林妍溱 | 2021-04-02 發表

讚 6.7 萬 按讚加入iThome粉絲團 讚 264 分享

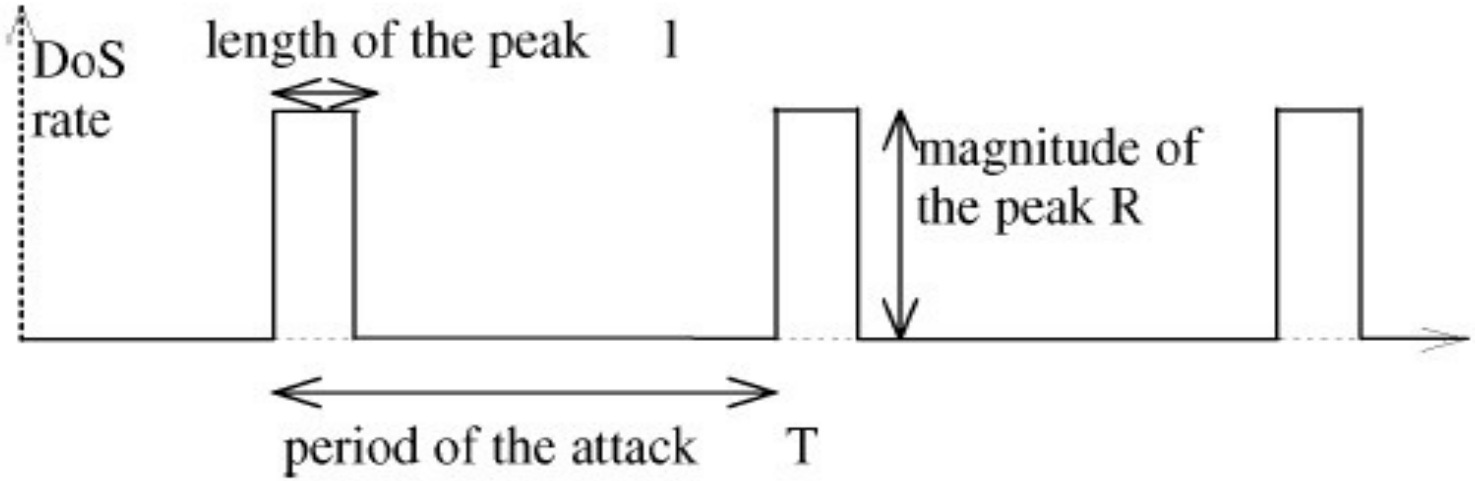
DDoS attacks grow in volume, frequency and sophistication

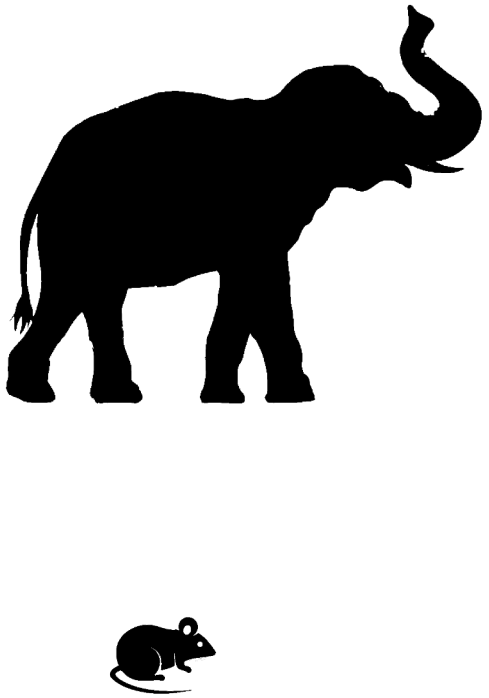


https://www.zdnet.com/article/google-says-it-mitigated-a-2-54-tbps-ddos-attack-in-2017-largest-known-to-date/

Example of our research direction: Smarter DDoS attacks

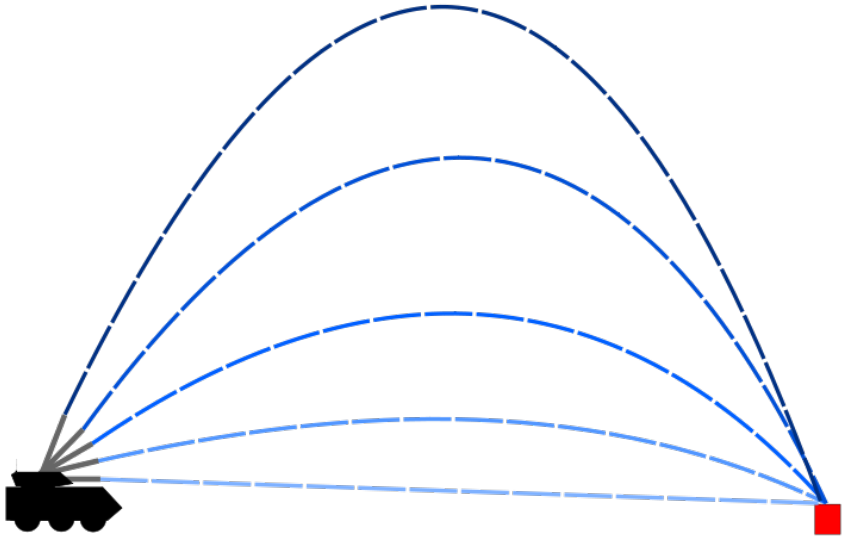
- Can we achieve the same effect by sending low-rate attack traffic?
- "Square-wave" or pulsating DDoS attacks
  - Exploit TCP congestion control feature
  - Exploit cloud's scaling mechanism

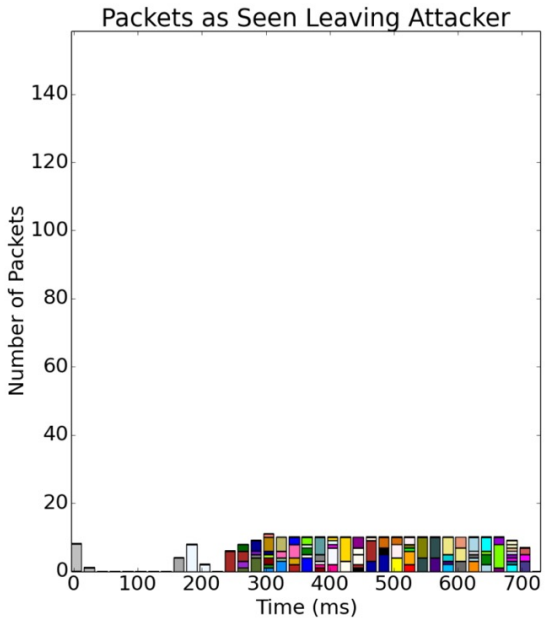


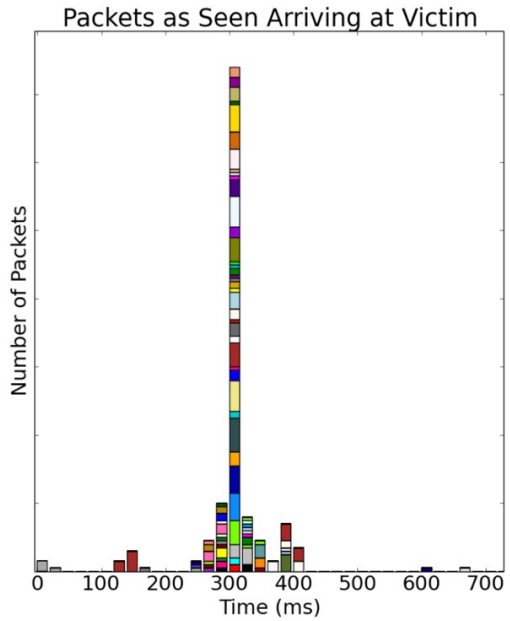


Example of our research direction: Smarter DDoS attacks

- Temporal lensing -- concentrate a flow in time
- Idea: “multiple rounds simultaneous impact”
- So that a low-bandwidth source can also perform a pulsating DDoS attack

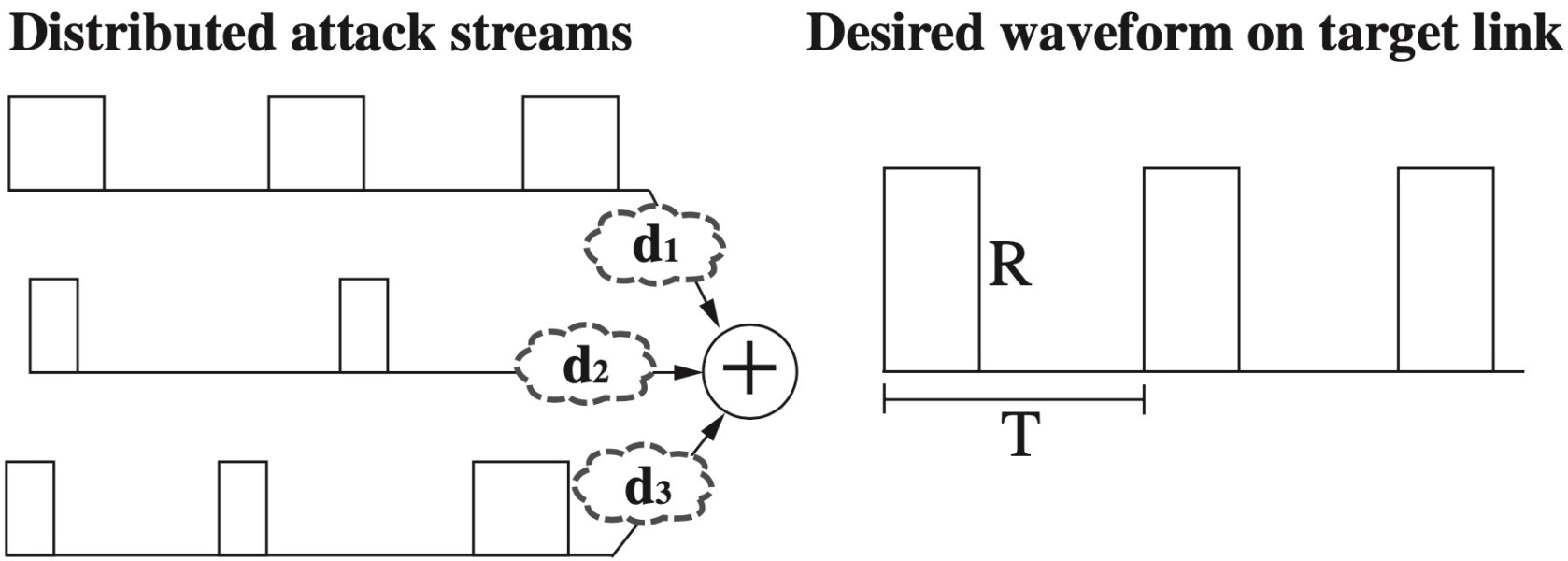






R. Rasti, M. Murthy, and V. Paxson, “Temporal Lensing and its Application in Pulsing Denial of Service Attacks,” in IEEE Symposium on Security and Privacy, 2015.

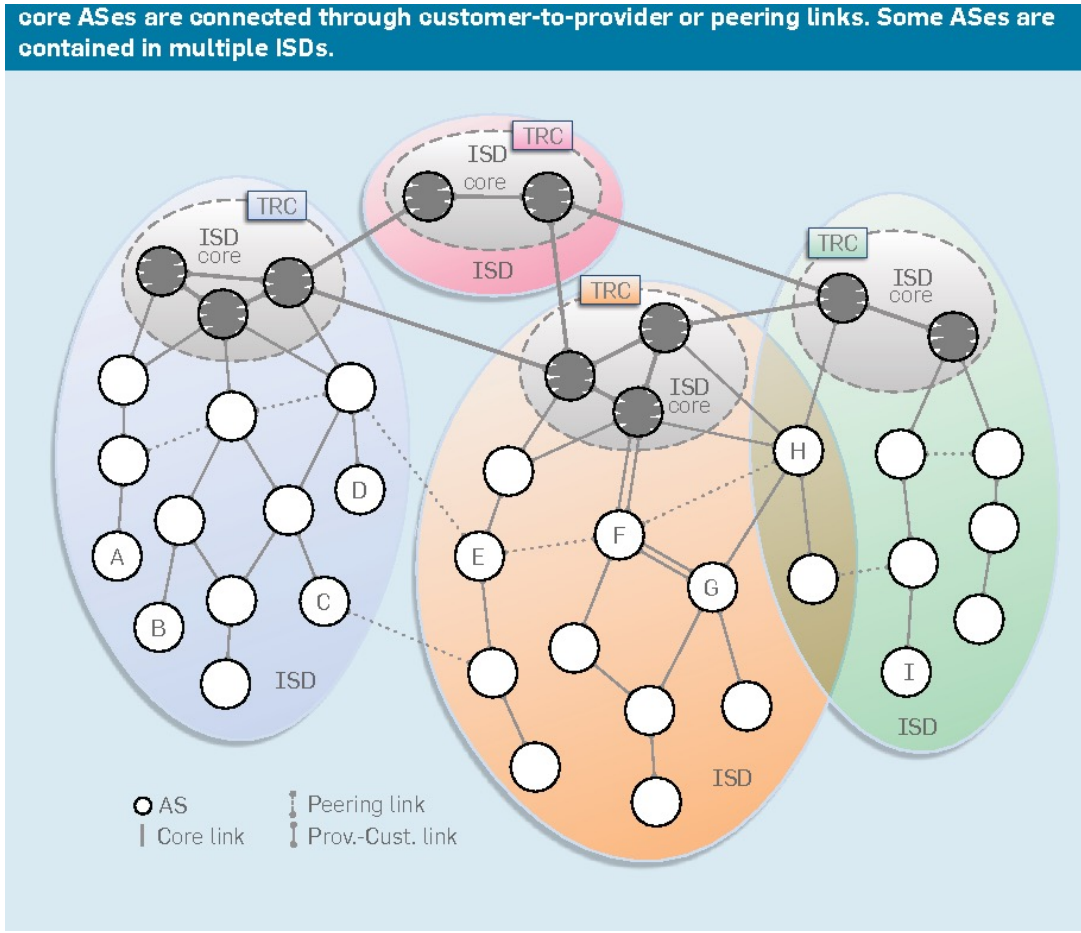
Example of our research direction: Smarter DDoS attacks



Y.-M. Ke, C.-W. Chen, H.-C. Hsiao, A. Perrig, V. Sekar. CICADAS: Congesting the Internet with Coordinated And Decentralized Pulsating Attacks. In ACM Asia Conference on Computer and Communications Security (ASIACCS), May 2016.

Example of our research direction: A better Internet

- The Internet was not designed for security
- Need additional mechanisms to ensure the authenticity of IP, TCP, BGP and DNS
- Ad hoc fixes vs. new internets?
  - "SCION is the first clean-slate Internet architecture designed to provide route control, failure isolation, and explicit trust information for end-to-end communication."



https://www.scion-architecture.net

Two-week Agenda

- Security 101 – 什麼是資訊安全？
- 進階主題
  - 高可用性網路 – 網路被癱瘓了連不上？
  - 物聯網安全 – 按個鍵就控制紅綠燈、汽車、電網？
  - 資安與社會 – 資安離我很遙遠？
  - 網路隱私 – 為什麼廣告都知道我喜歡什麼？
  - 自動化漏洞挖掘 – 打 001011 就能入侵電腦、盜走上億元？
  - 資安與倫理 – 研究的再現性與道德駭客
- 如何選擇資安這條路

IoT Security

物聯網安全

IoT Security

- 研究挑戰：Different capabilities, different requirements
- 我們的研究主題
  - Emerging threats to IoT platforms
  - Secure IoT device bootstraping and key management
  - Automated IoT firmware analysis

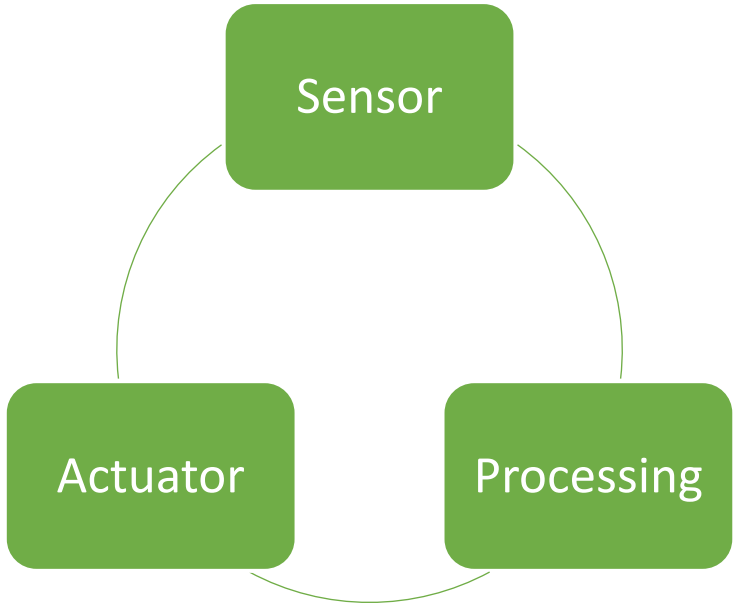
What is Internet of Things (IoT)?

Things that connect to/via the Internet

What is Internet of Things (IoT)?

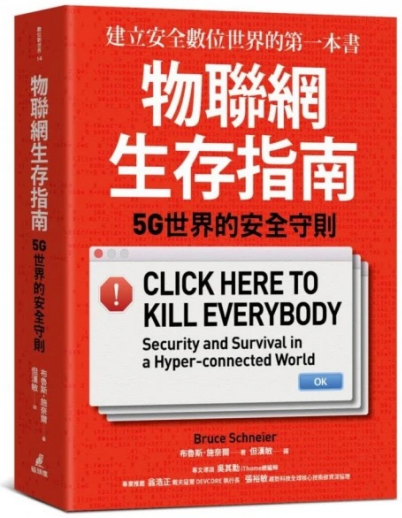
Things that connect to/via the Internet

Things that interact with physical world



Why should we care about IoT security?

"We are building an internet that senses, thinks, and acts." -- Bruce Schneier



Greater impact: Cyber attack affects physical world

Larger scale: Billions of public accessible (and hackable) devices

Greater Impact: Cyber attack affects physical world

Reference: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

Greater Impact: Cyber attack affects physical world

Reference: https://www.theguardian.com/technology/2017/aug/31/hacking-risk-recall-pacemakers-patient-death-fears-fda-firmware-update
https://edition.cnn.com/2013/10/20/us/dick-cheney-gupta-interview/index.html

Greater Impact: Cyber attack affects physical world


Self-driving car

Pacemakers

Thermostats

Reference: https://thehackernews.com/2016/08/hacking-thermostat.html

Greater Impact: Cyber attack affects physical world


Self-driving car

Pacemakers

Thermostats

Images: Evtimov et al

Camouflage graffiti and art stickers cause a neural network to misclassify stop signs as speed limit 45 signs or yield signs.

Reference: https://iotsecurity.engin.umich.edu/physical-adversarial-examples-for-object-

Greater Impact: Cyber attack affects physical world


Self-driving car

Pacemakers

Thermostats

Images: Evtimov et al

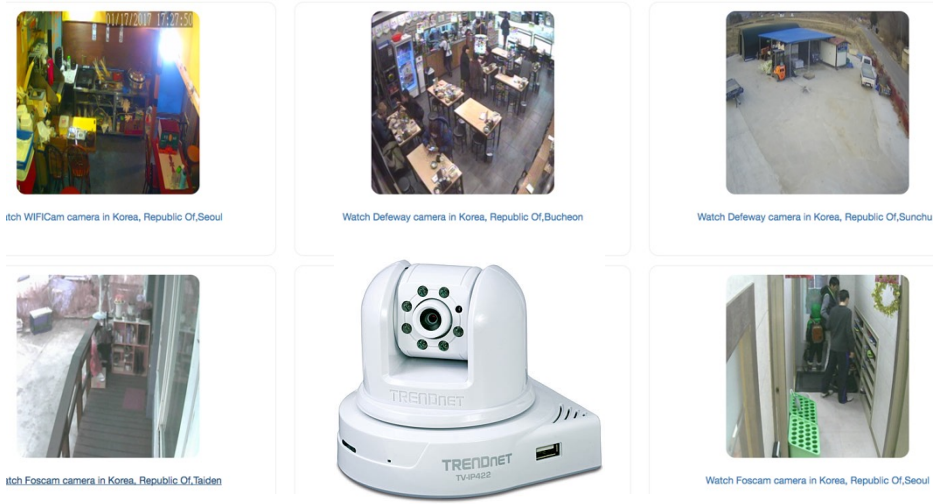
Camouflage graffiti and art stickers cause a neural network to misclassify stop signs as speed limit 45 signs or yield signs.

Reference: https://www.blackhat.com/docs/us-15/materials/us-15-Sandvik-When-IoT-Attacks-Hacking-A-Linux-Powered-Rifle.pdf

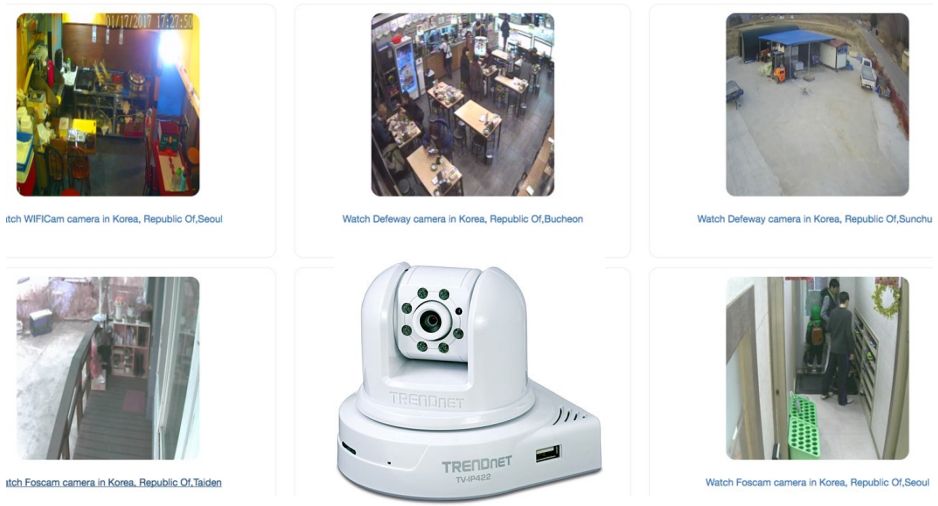
Larger Scale: Billions of hackable devices

Reference: https://www.wired.com/story/mirai-botnet-minecraft-scam-brought-down-the-internet/
M. Antonakakis et al., “Understanding the Mirai Botnet,” in USENIX Security, 2017.

Larger Scale: Billions of hackable devices



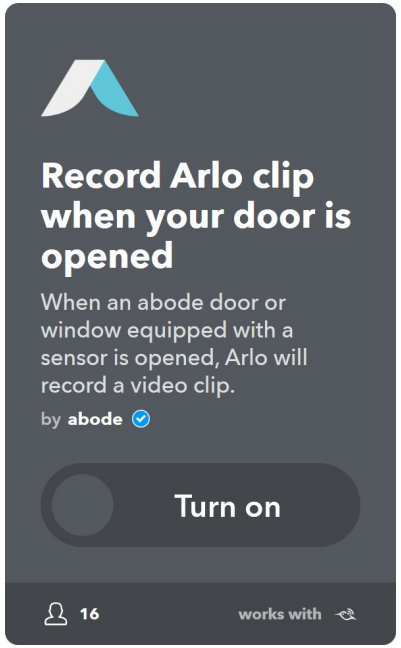
Larger Scale: Billions of hackable devices

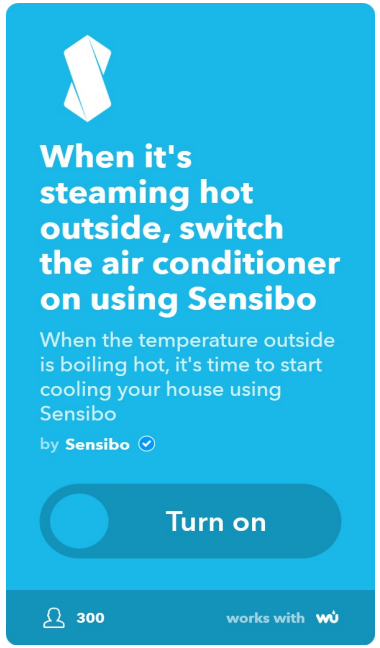


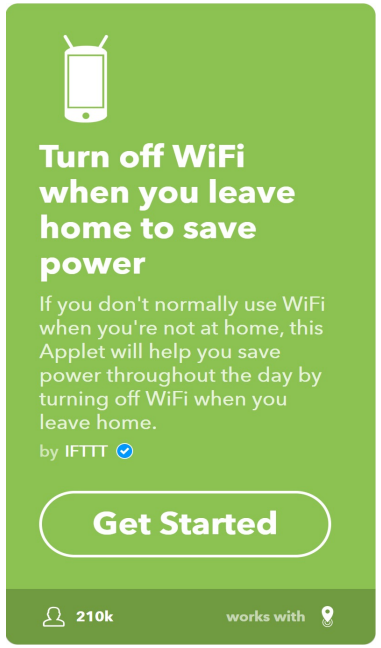
Reference: https://www.bbc.com/news/technology-42853072

Example of our research direction: security and privacy risks of IoT trigger-action platforms

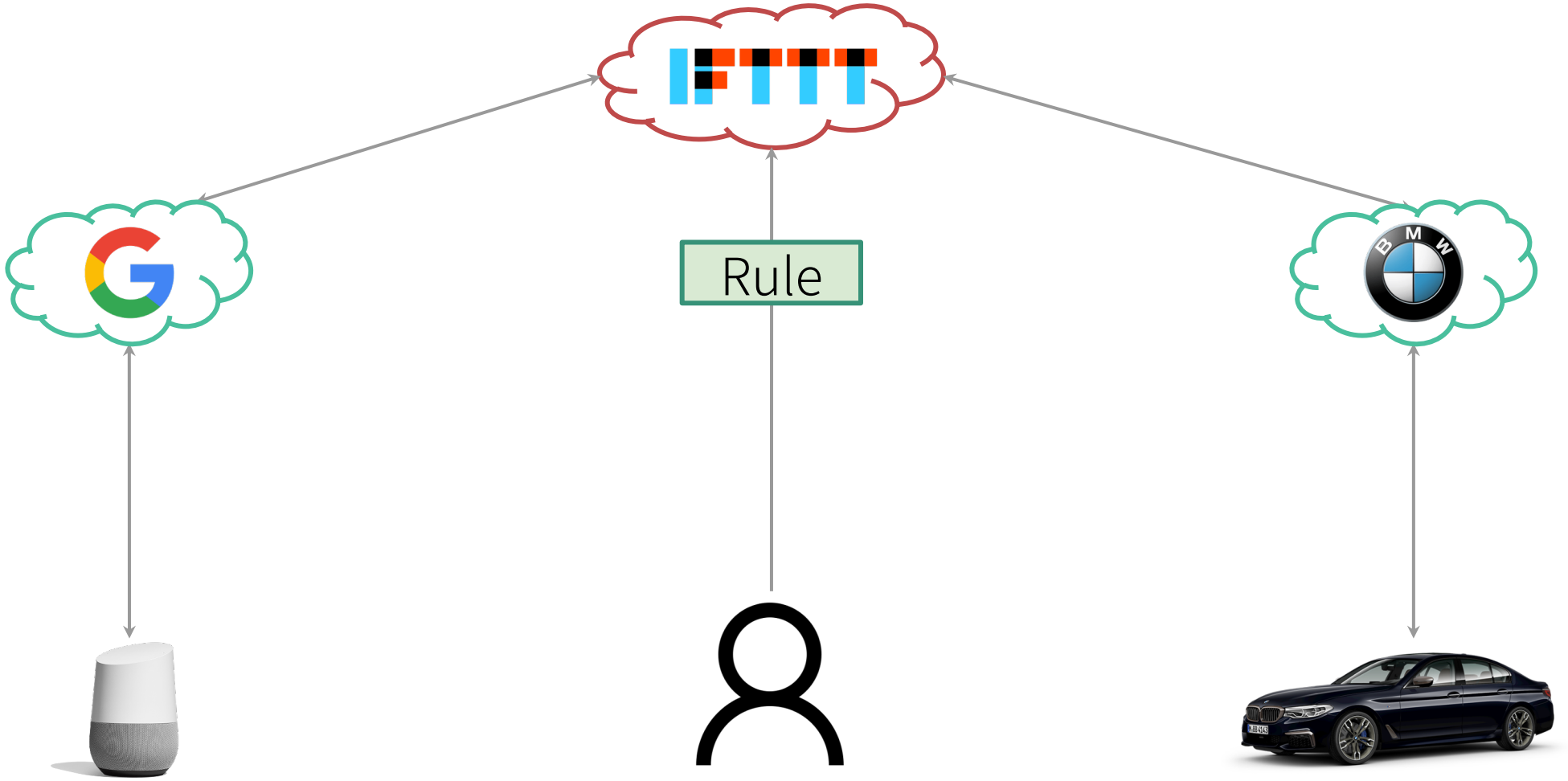
- Emerging trigger-action platforms empower users to setup automation rules
  - Connects devices via rules in the form of "If some trigger happens, then do some action."
  - Popular platforms includes IFTTT, Zapier, Microsoft Power Automate, Stringify, etc.





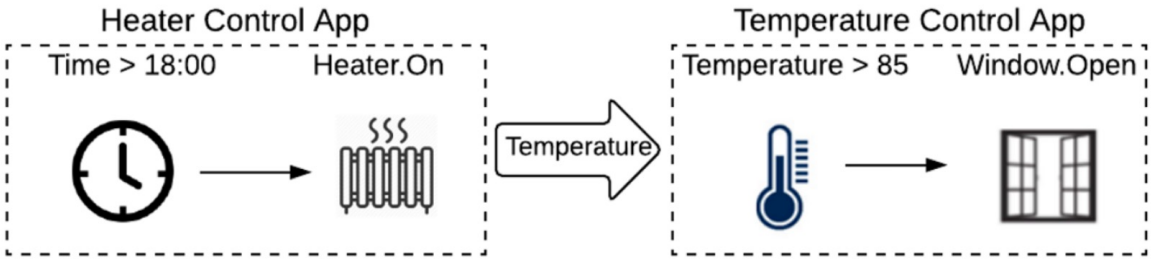


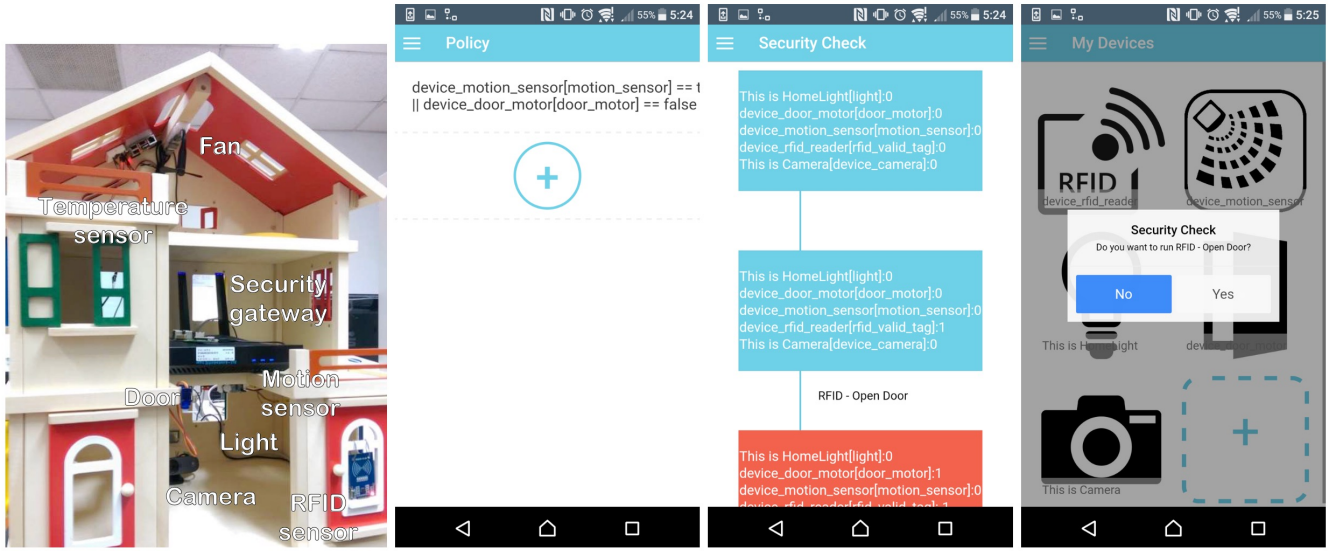
IFTTT Ecosystem



Example of our research direction: security and privacy risks of IoT trigger-action platforms

- Unexpected interaction between IoTs via physical environments



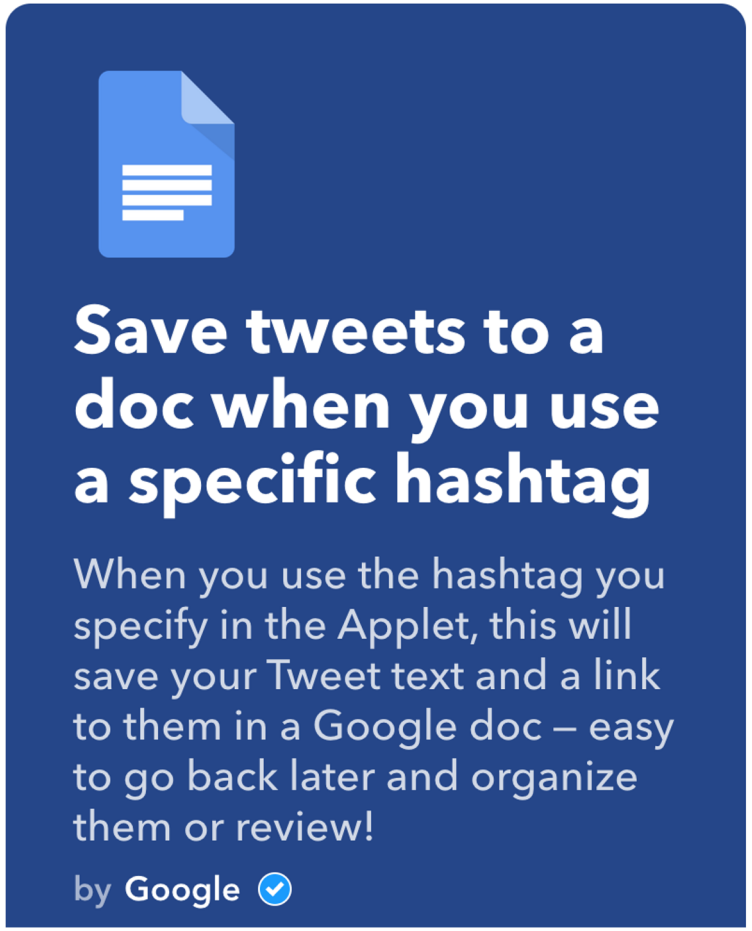


(a) A toy house (b) Security policies (c) Check result (d) Security alarms

On the Safety of IoT Device Physical Interaction Control, CCS 2018
SAFECHAIN: Securing Trigger-Action Programming from Attack Chains, IEEE Transactions on Information Forensics and Security, 2019

Example of our research direction: security and privacy risks of IoT trigger-action platforms

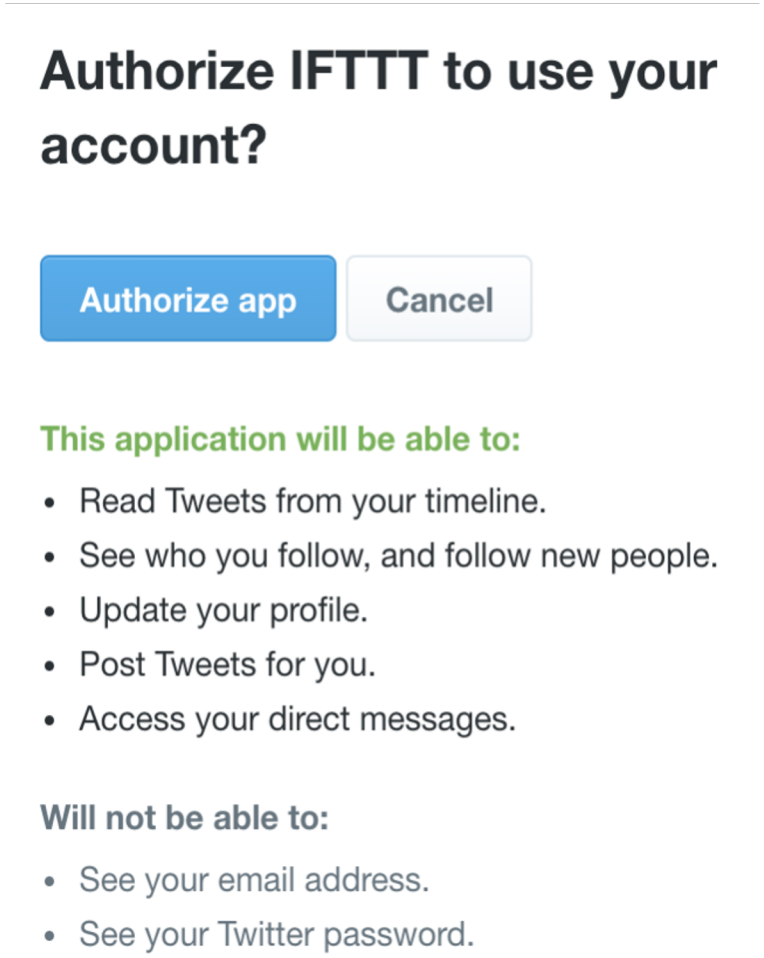
- Over-privileged access tokens
  - Online services are not designed to support only trigger-action platforms
  - Coarse-grained OAuth scopes
- What privileges will this applet request to access your twitter account?



Reference: “Decentralized Action Integrity for Trigger-Action IoT Platforms,” NDSS 2018.

Example of our research direction: security and privacy risks of IoT trigger-action platforms

- Many of them are not necessary to complete the task
- User is only given an all-or-nothing choice

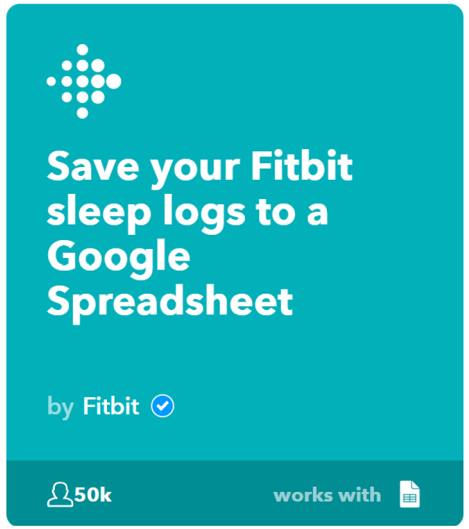


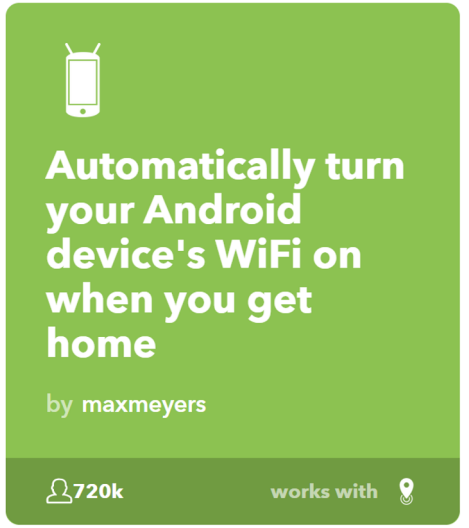
Reference: “Decentralized Action Integrity for Trigger-Action IoT Platforms,” NDSS 2018.

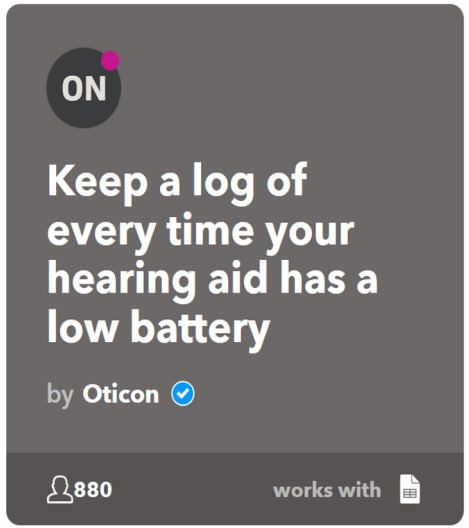
Example of our research direction: security and privacy risks of IoT trigger-action platforms

Table 1. Sources of Leakages (n = 500)

	Data	Presence	Ownership
# of triggers	456	127	2
percentage	91.2%	25.4%	0.4%



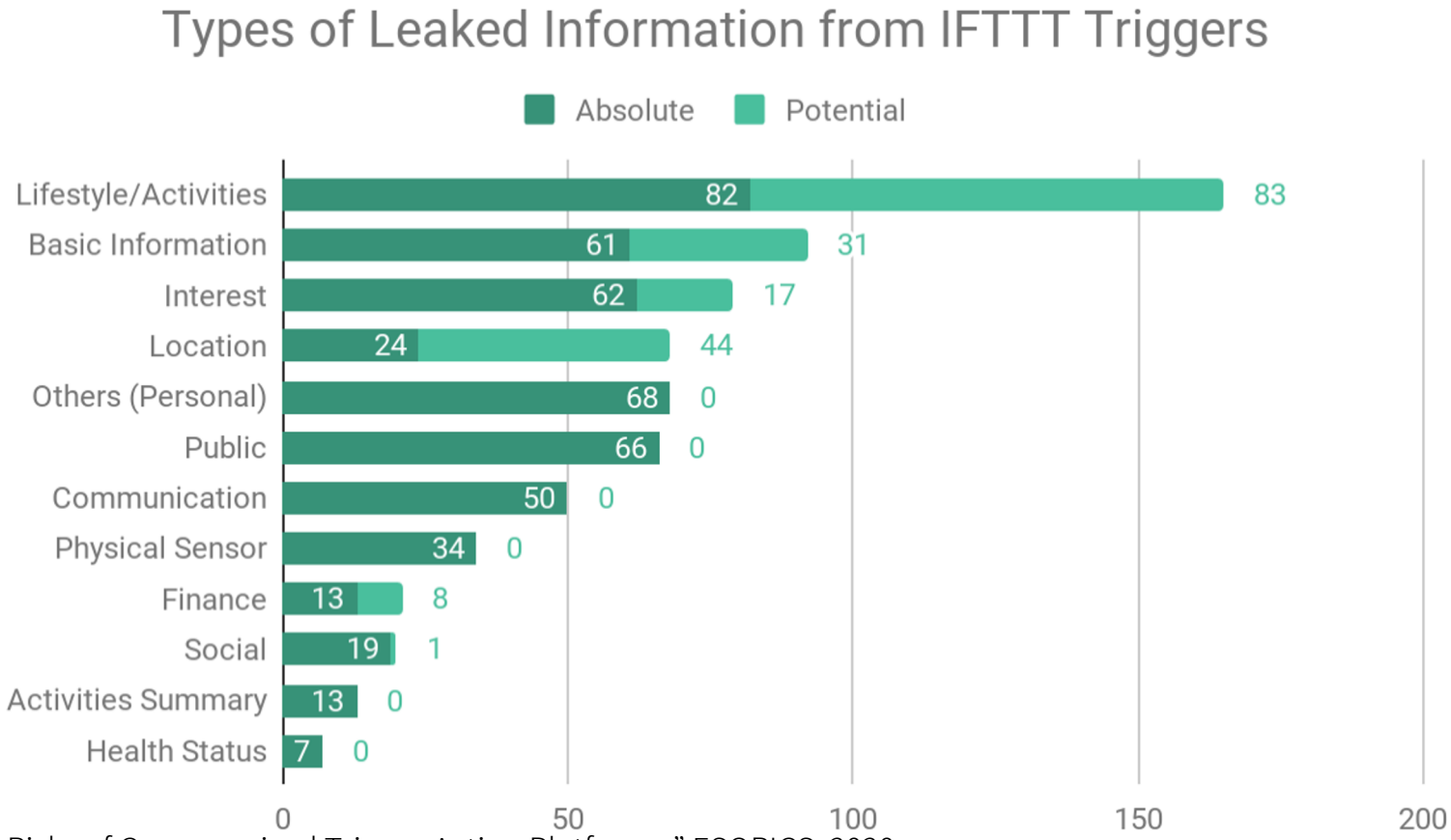




Reference: “On the Privacy Risks of Compromised Trigger-Action Platforms,” ESORICS, 2020.

Example of our research direction: security and privacy risks of IoT trigger-action platforms

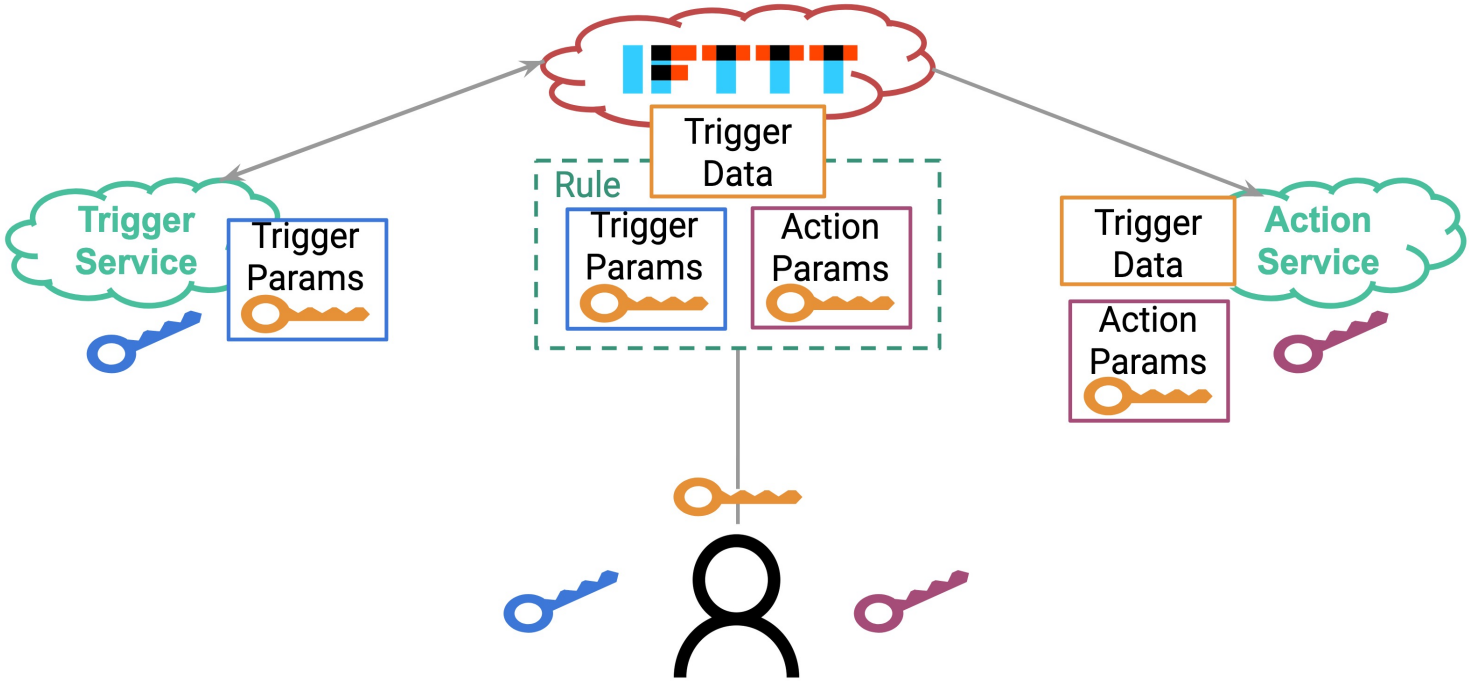
- A wide range of information can be known by IFTTT!



Reference: "On the Privacy Risks of Compromised Trigger-Action Platforms," ESORICS, 2020.

Example of our research direction: security and privacy risks of IoT trigger-action platforms

- Privacy-preserving trigger-action platforms



Reference: “On the Privacy Risks of Compromised Trigger-Action Platforms,” ESORICS, 2020.

Two-week Agenda

- Security 101 – 什麼是資訊安全？
- 進階主題
  - 高可用性網路 – 網路被癱瘓了連不上？
  - 物聯網安全 – 按個鍵就控制紅綠燈、汽車、電網？
  - 資安與社會 – 資安離我很遙遠？
  - 網路隱私 – 為什麼廣告都知道我喜歡什麼？
  - 自動化漏洞挖掘 – 打 001011 就能入侵電腦、盜走上億元？
  - 資安與倫理 – 研究的再現性與道德駭客
- 如何選擇資安這條路

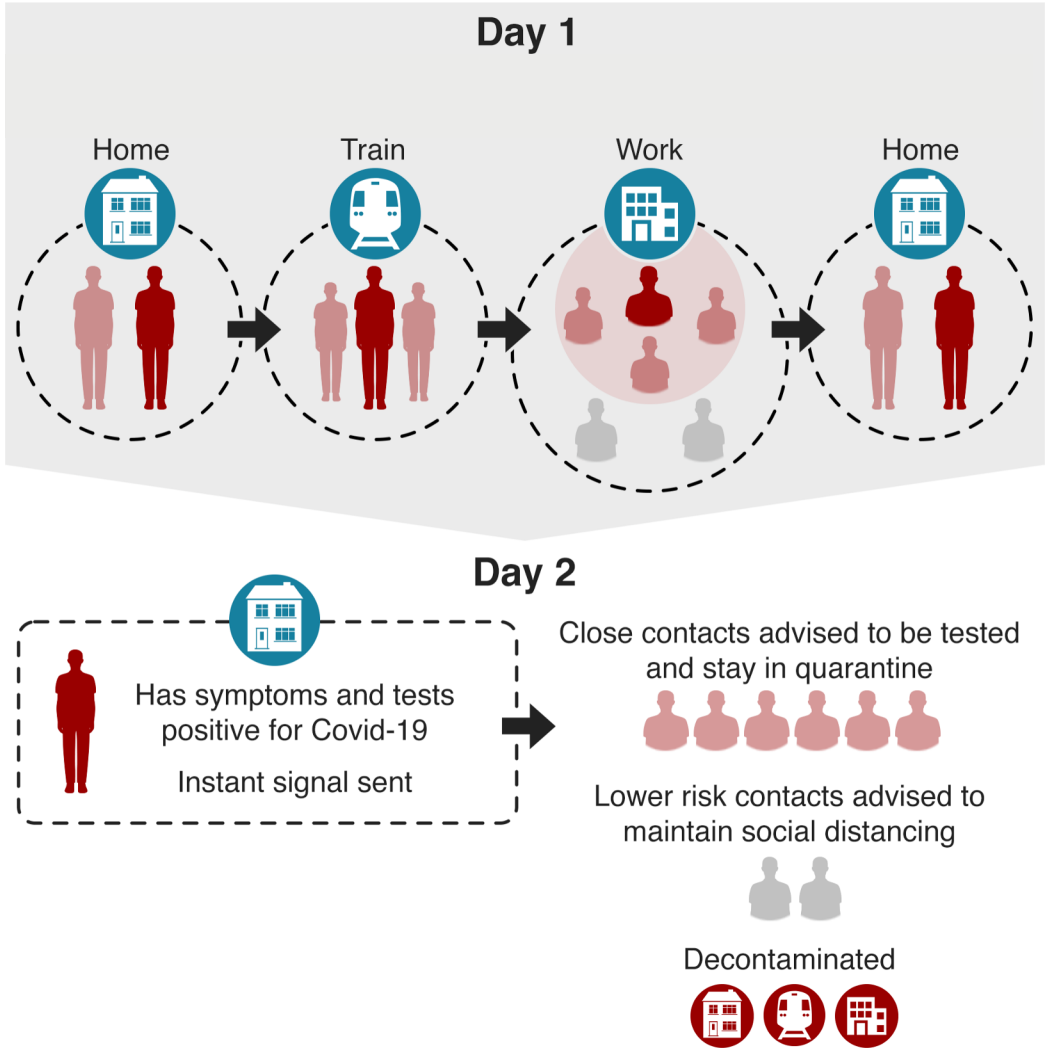
Privacy-preserving Contact Tracing

Privacy-preserving Contact Tracing

- Theory - what is privacy-preserving contact tracing?
- Empirical evaluation – how accurate it is in realistic settings?
- Practice – deployment in the world and Taiwan

Privacy-preserving Contact Tracing

- Theory - what is privacy-preserving contact tracing?
- Empirical evaluation – how accurate it is in realistic settings
- Practice – deployment in the world and Taiwan



Contact Tracing

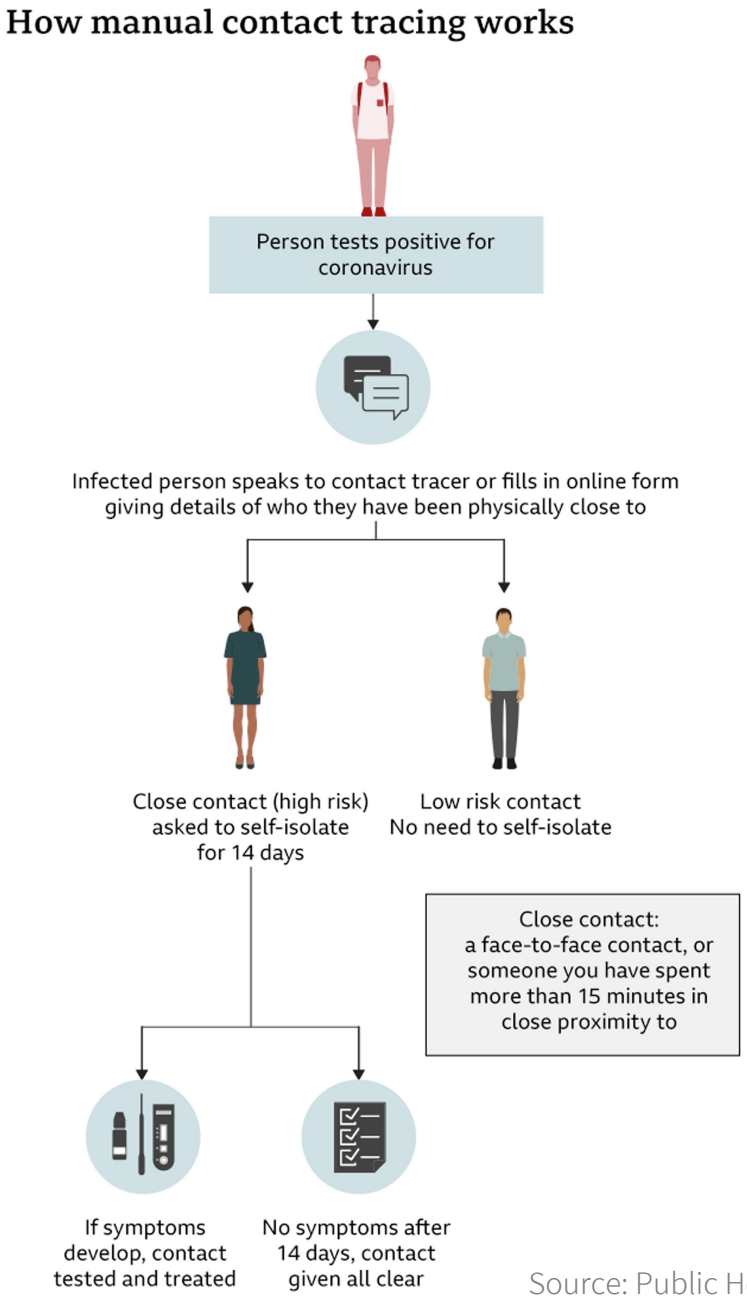
A well-known method for controlling the spread of infectious diseases

Identifies those who were...

- in close proximity with an infected person
- for long enough time
- during likely transmission period

* **Covid-19**: within 2m for > 15 minutes in past 14 days

Source: https://www.electronicsweekly.com/news/business/conflicted-approach-bluetooth-contact-tracing-2020-04/ (modified)



Limitations of Manual Contact Tracing

- Overwhelmed when the number of confirmed cases is high
- Relies on human's memory and self-report
- Unable to identify contacts with strangers

Source: Public Health England (https://www.bbc.com/news/explainers-52442754)

Digital Contact Tracing

- Identifies contacts between two people via digital logs

Digital Contact Tracing

- Identifies contacts between two people via digital logs
- Two types: logging location or proximity

Digital Contact Tracing – Logging Location

- E.g., via GPS, QR code, cellular-tower history
- Each person's trajectory may be exposed to a central authority
- Concerns about mass surveillance and privacy violation

Location log

```
10:30 Taipei Main Station
13:00 Taipei 101
13:30 Convention Center
…
```

Digital Contact Tracing – Logging Proximity

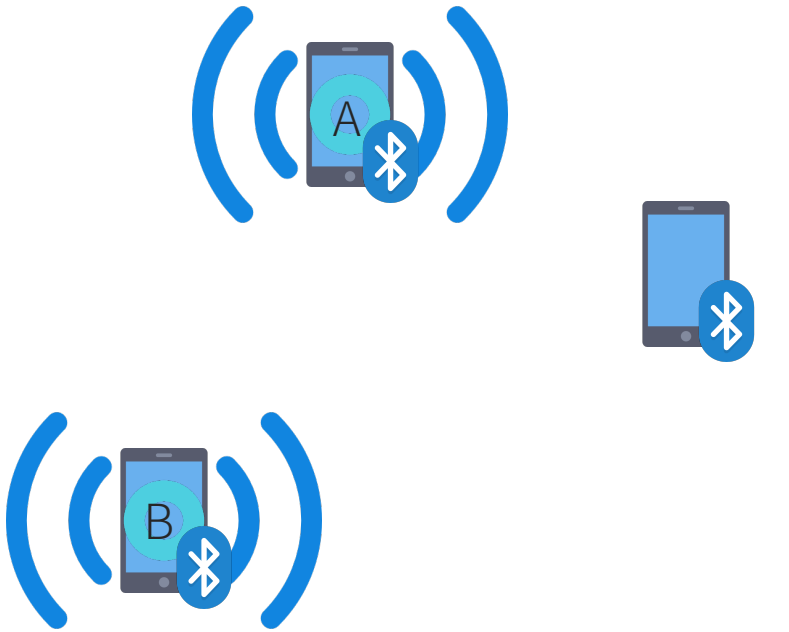
- Logging proximity instead of location improves privacy
- Proximity can be easily detected in a decentralized manner using short-range communication, such as Bluetooth, further improving privacy

Proximity log

```
10:30 10 meters from device A
10:30 5 meters from device B
13:00 2 meters from device C
13:30 1 meter from device D
…
```

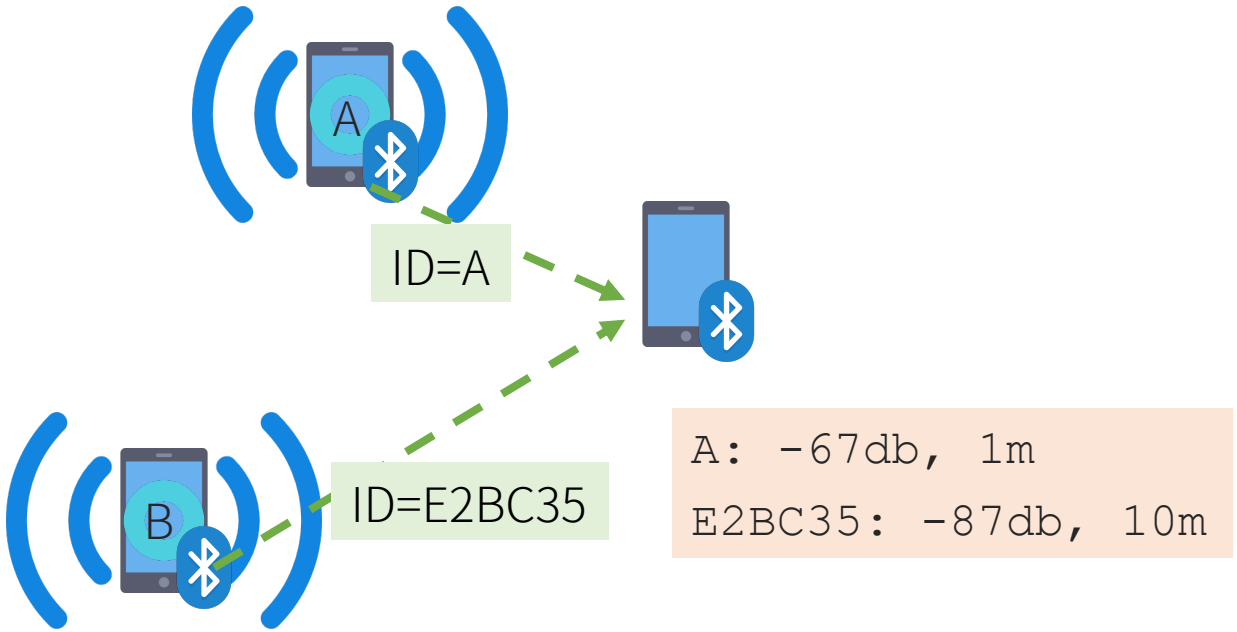
Privacy preservation via Bluetooth and decentralization

Assumption: devices in proximity will receive Bluetooth tokens and can estimate distance via received signal strength indication (RSSI)



Privacy preservation via Bluetooth and decentralization

Assumption: devices in proximity will receive Bluetooth tokens and can estimate distance via received signal strength indication (RSSI)

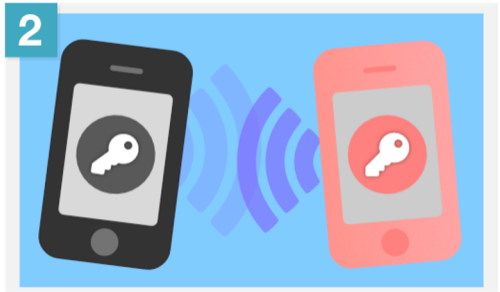


$$RSSI = -10N \log d + R$$

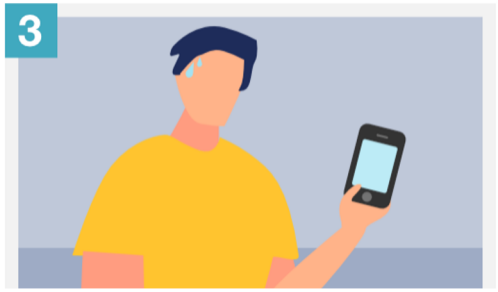
Distance-RSSI mapping when $N = 2$ (environmental factor), $R = -67$ (reference RSSI at 1m):

distance (m)	10	2	1	0.5	0.1
RSSI (dB)	-87.0	-73.0	-67.0	-60.9	-47.0

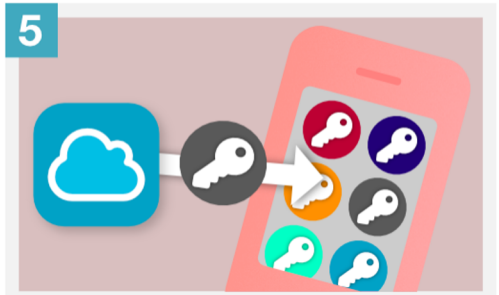
Workflow of Privacy-preserving contact tracing apps



Exchange anonymized and frequently-changing tokens with each other



Upload owned tokens if tested positive



Download tokens to see if contacted with someone infected

Source: https://www.expressnewspoint.com/apple-and-google-collaborate-on-covid-19-contact-tracing-technology/

Privacy-preserving Contact Tracing

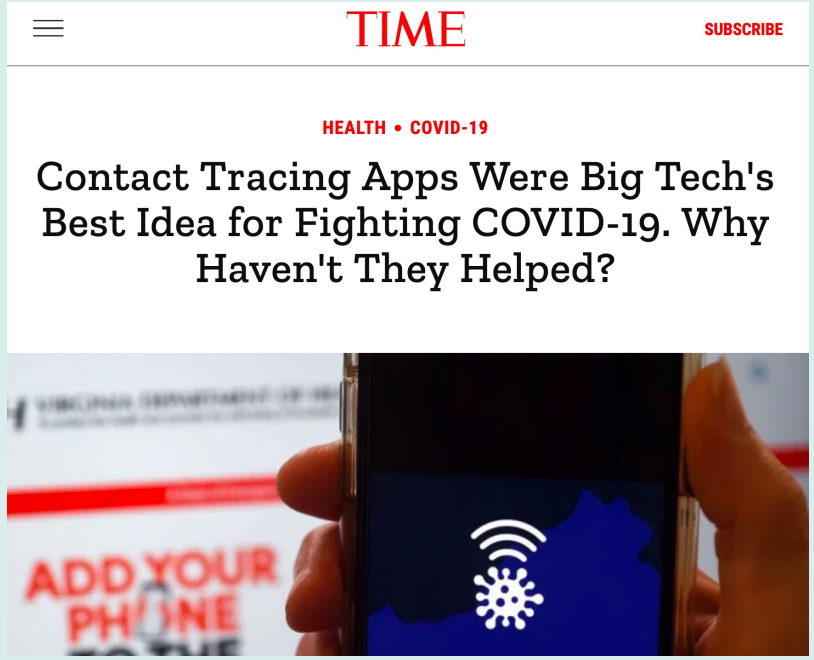
- Theory - what is privacy-preserving contact tracing?
- Empirical evaluation – how accurate it is in realistic settings?
- Practice – deployment in the world and Taiwan

Significant Attention on:

- Investigating advanced security and privacy issues and their countermeasures
- Developing apps and pushing for adoption
- Simulation-based evaluation

Little do we know:

The effectiveness of Bluetooth-based proximity detection in real-world settings



Source: https://time.com/5905772/covid-19-contact-tracing-apps/

Little do we know: the effectiveness of Bluetooth-based proximity detection in real-world settings

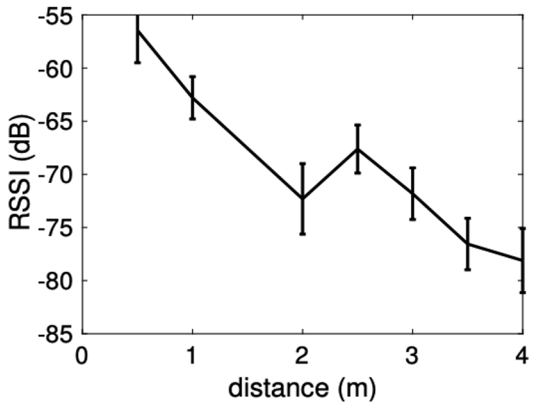
More empirical studies are needed to answer

- Can it accurately estimate distance based on RSSI?
- Can it accurately detect contact events?
- What are its potentials and limitations?

- So that we can better use this tool, in combination with others, to combat Covid-19

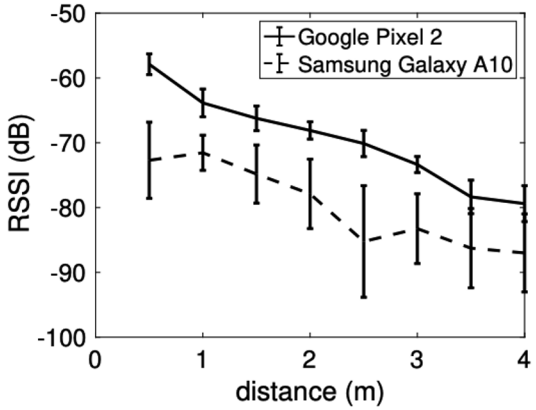
Empirical Studies by Leith and Farrell

- Measuring RSSI between two phones indoor and outdoor
- **Finding**: RSSI need not decrease with increasing distance
- **Implication**: Bluetooth RSSI may be unreliable for estimating distance



(a) RSSI vs distance

(b) Indoor location



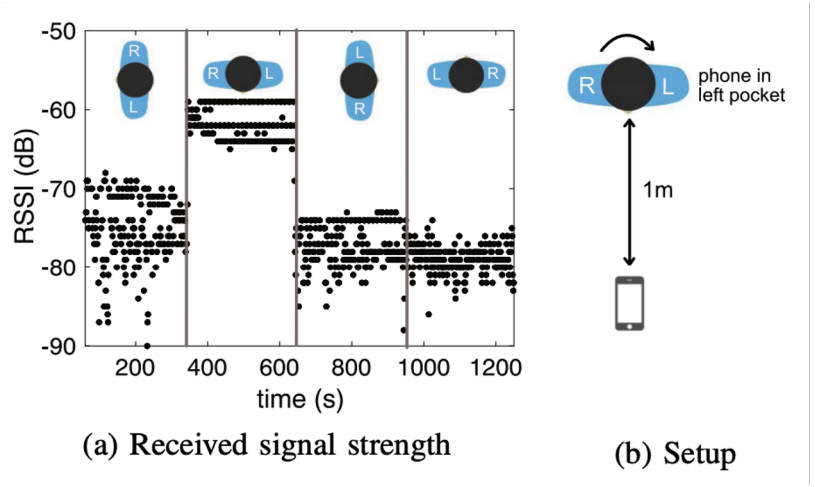
(a) RSSI vs distance

(b) Garden location

[1] "Coronavirus Contact Tracing: Evaluating The Potential Of Using Bluetooth Received Signal Strength For Proximity Detection," May 2020.

Empirical Studies by Leith and Farrell

- Measuring RSSI under different phone positions and orientations
- **Finding**: Signal attenuation by human body and orientation
- **Implication**: Other factors affecting RSSI should be taken into consideration

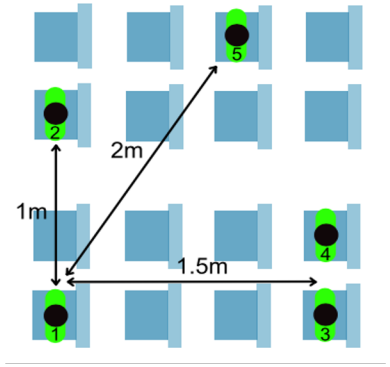


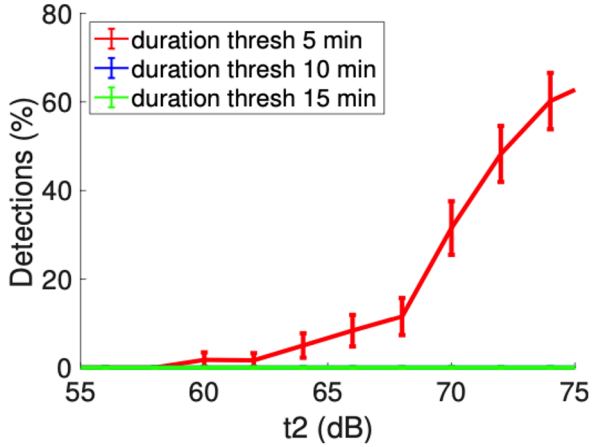
(a) Received signal strength (b) Setup

[1] "Coronavirus Contact Tracing: Evaluating The Potential Of Using Bluetooth Received Signal Strength For Proximity Detection," May 2020.

Empirical Studies by Leith and Farrell

- Estimating contact detection via RSSI on public transportation such as buses and trams
- **Finding**: Low detection rate, possibly due to interference and reflection by metal surface
- **Implication**: Users should be aware of possible false negatives



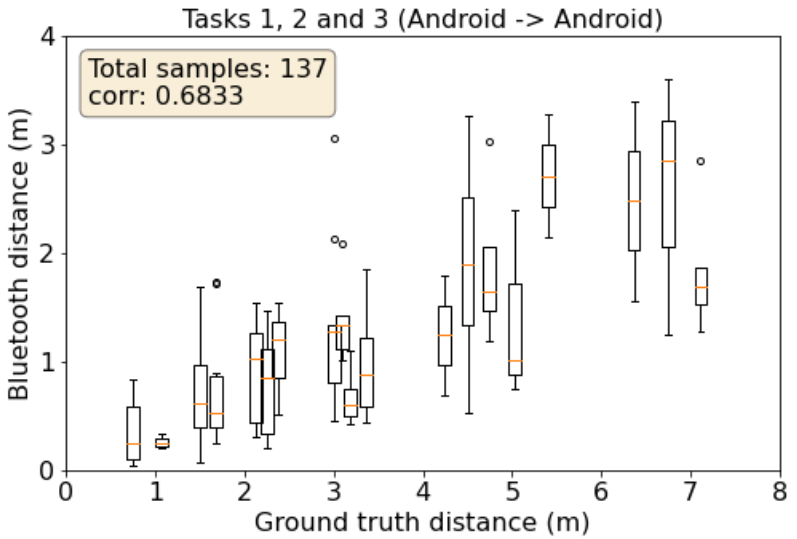


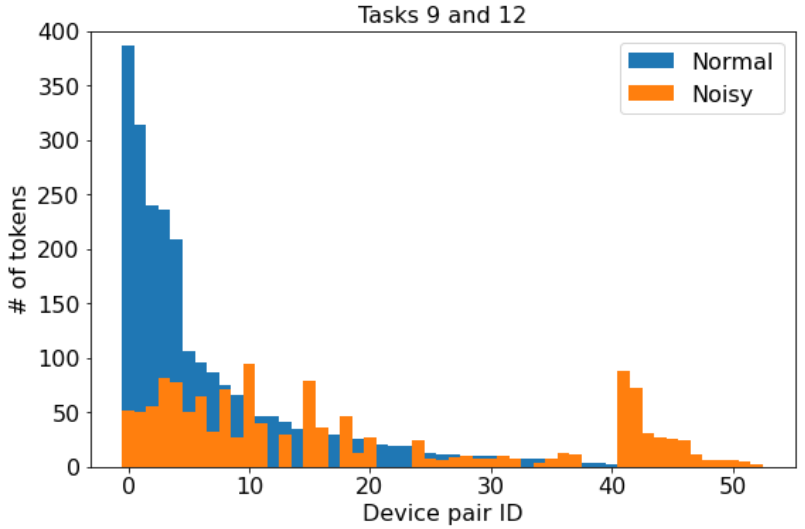
[1] "Coronavirus Contact Tracing: Evaluating The Potential Of Using Bluetooth Received Signal Strength For Proximity Detection," May 2020.

Our empirical Studies

- Measuring RSSI between phones in crowds with different sizes and densities
- **Finding**: RSSI is unreliable for estimating distance, and worsens when crowded or jammed
- **Implication**: May be least useful when it is most in need (e.g., in crowds)

30 participants: 14 Android; 16 iOS





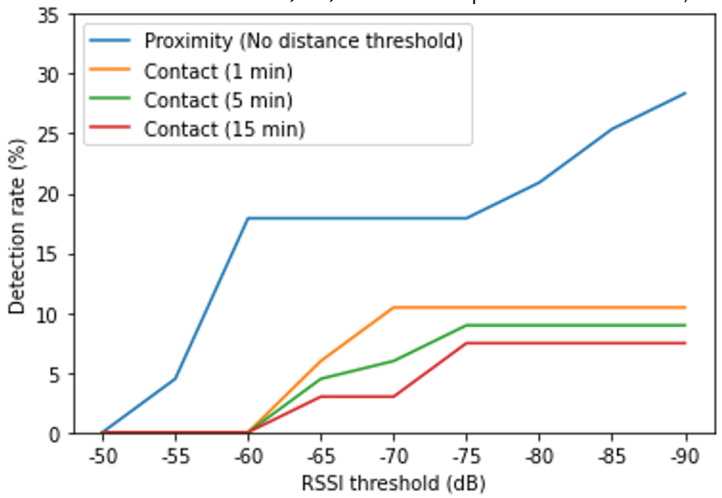
[2] Hsu-Chun Hsiao, Chun-Ying Huang, Bing-Kai Hong, Shin-Ming Cheng, Hsin-Yuan Hu, Chia-Chien Wu, Jian-Sin Lee, Shih-Hong Wang, Wei Jeng, "An Empirical Evaluation of Bluetooth-based Decentralized Contact Tracing in Crowds." *arXiv preprint arXiv:2011.04322*, 2020.

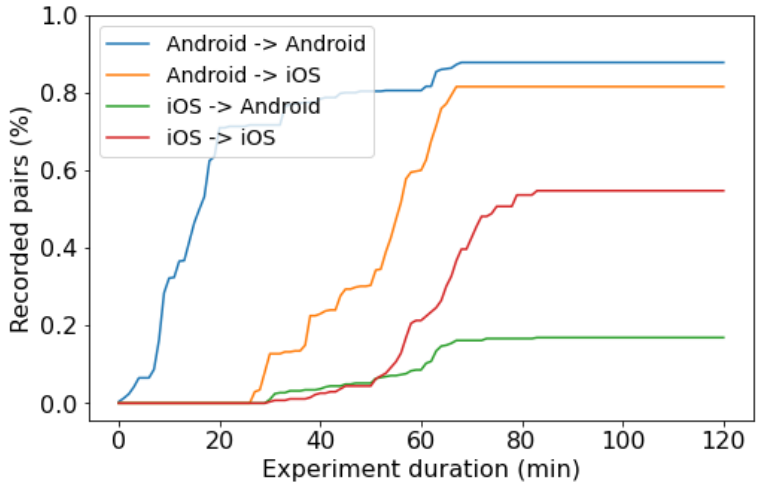
Our empirical Studies

- Estimating contact detection via RSSI in crowds
- **Finding**: Failed to capture most contact events, but detection rate increases with time duration and distance: 63% of contact events were detected over a 90-min period.
- **Implication**: Useful for detecting coarse-grained contact events, e.g., within 20m for an hour

50 participants: 24 Android; 26 iOS

Contact event (in proximity at the beginning and end of a 1-, 5-, 15-min exposure duration)



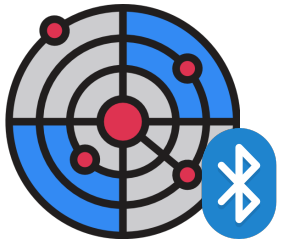


[2] Hsu-Chun Hsiao, Chun-Ying Huang, Bing-Kai Hong, Shin-Ming Cheng, Hsin-Yuan Hu, Chia-Chien Wu, Jian-Sin Lee, Shih-Hong Wang, Wei Jeng, "An Empirical Evaluation of Bluetooth-based Decentralized Contact Tracing in Crowds," *arXiv preprint arXiv:2011.04322*, 2020.

Privacy-preserving Contact Tracing

- Theory - what is privacy-preserving contact tracing?
- Empirical evaluation – how accurate it is in realistic settings
- Practice – deployment in the world and Taiwan

Privacy-preserving contact-tracing apps in the wild



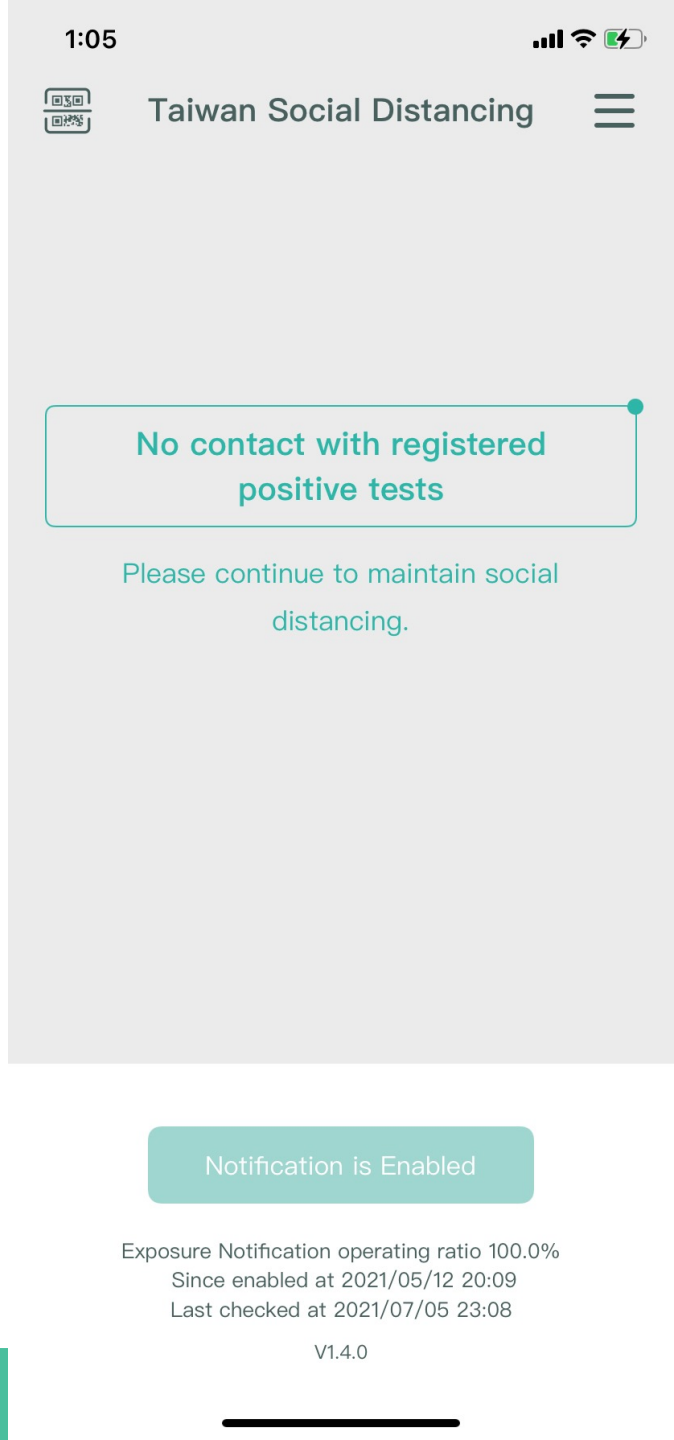
- Most are based on Bluetooth for decentralized proximity detection
- Adoption as of Nov. 2020: 37 countries and 22 U.S. states [3]
  - Switzerland's SwissCOVID, Germany's Corona-Warn-App, Arizona's Covid-Watch, etc.
- Apple and Google jointly developed the GAEN API for creating national apps, and later released Exposure Notification Express for national health authorities
- Recent analysis of UK's app suggests it helps contained the spread of Covid-19 [4]
  - Used regularly by 16.5 million users (28% of the total population)
- Question: Identifying true positives vs. cost of false positives and false negatives?

[3] Mosoff, R., Friedlich, T., Scassa, T., Bronson, K., & Millar, J. (2020). Global Pandemic App Watch (GPAW): COVID-19 Exposure Notification and Contact Tracing Apps. Retrieved from https://craiedl.ca/gpaw/
[4] https://www.nature.com/articles/s41586-021-03606-z

Case Study: Taiwan

- A privacy-preserving contact-tracing app launched in May 2021, about 4 million (about 17% of the total population) downloads in a month
  - Only 183 people (2% of the confirmed cases) uploaded their data by the end of May

- Issues hurting the adoption and trust on the app
  - False negatives caused confusions and reduced trust
  - Panics due to lack of information and support
  - Many didn't understand this technology



Case Study: Taiwan

- People prefer using a QR-code based solution (which is less private)
  - Privacy might not be a primary concern for some people when dealing with an outbreak?
  - No app installation required
  - The technology is easier to understand
- **Take away**: accessibility and scientific communication are important

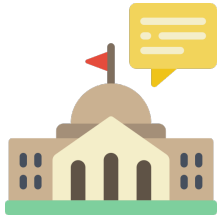
Unpredictable and Unbiased Randomness Generation

Randomness generation

- Unpredictable and unbiased randomness enables fair distribution of limited resources in democratic societies
  - E.g., 樂透、抽公宅、抽疫苗殘劑、各式各樣的振興券

Assuming a trusted authority?

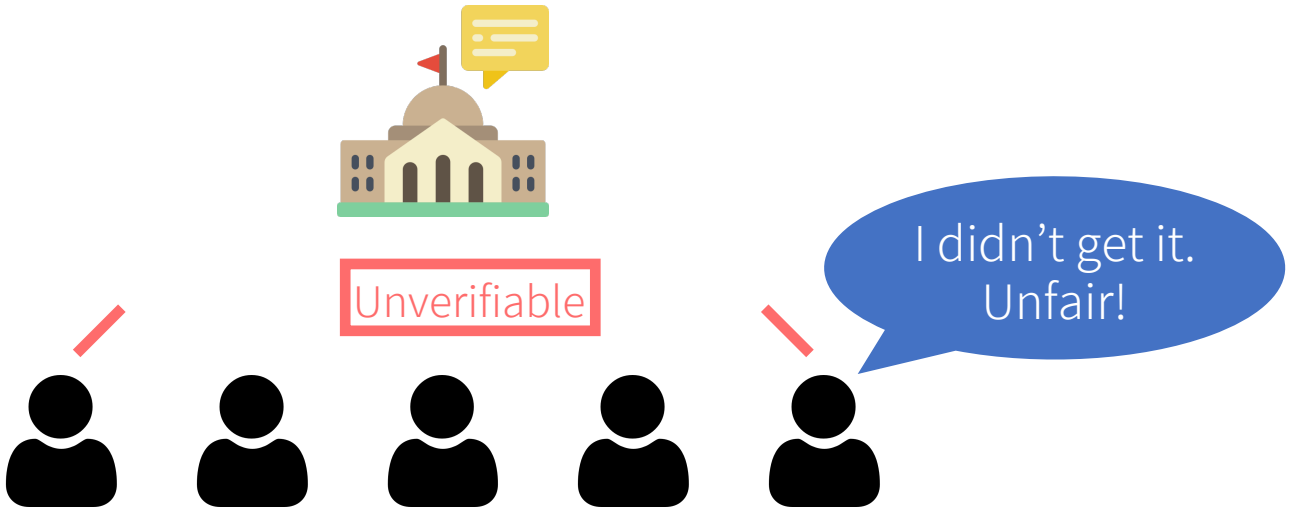
- Unpredictable and unbiased randomness enables fair distribution of limited resources in democratic societies



Random Selection

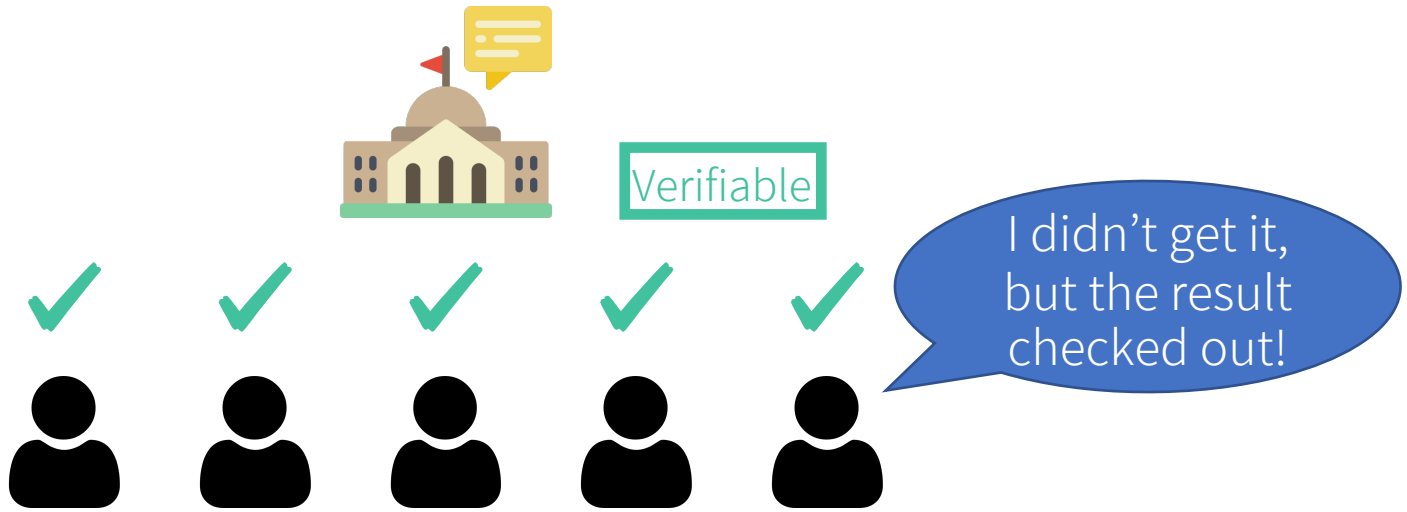
Assuming a trusted authority?

- Unpredictable and unbiased randomness enables fair distribution of limited resources in democratic societies



Without a trusted authority

- Unpredictable and unbiased randomness enables fair distribution of limited resources in democratic societies



Without a trusted authority

1. Participant i contributes randomness x_i

2. Server generates a number R based on x_is, along with a proof

3. Participant verifies R and the proof

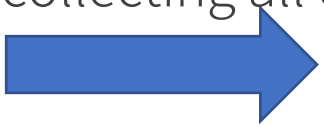
- Goals:
  - Everyone can efficiently verify server's computation
  - No one can predict or bias the number
- Assumption: at least one participant is honest

Related Work: Commit-and-reveal

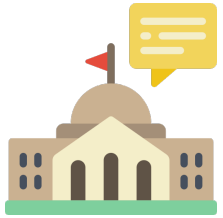
- Cryptographic hash function: computationally hard to compute the inverse

Commit

After collecting all commits



Reveal



R <- rand(r_1, r_2, r_3, r_4, r_5)

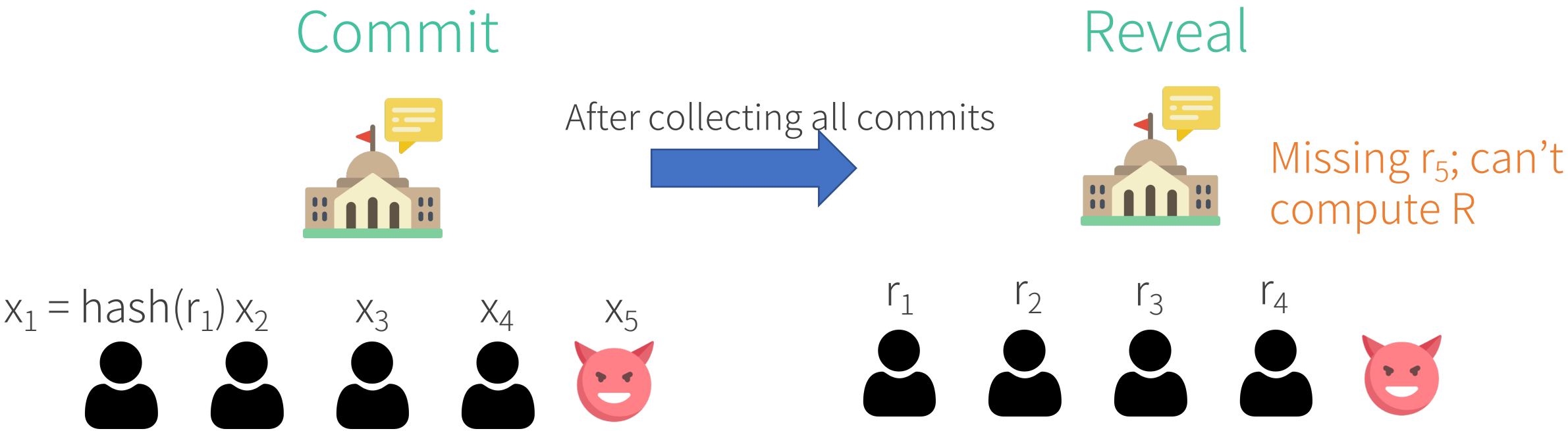
x_1 = hash(r_1) x_2 x_3 x_4 x_5

r_1 r_2 r_3 r_4 r_5

* Everyone can verify r_1, r_2, r_3, r_4, r_5 and R by recomputing hash() and rand() and instantly.

Related Work: Commit-and-reveal

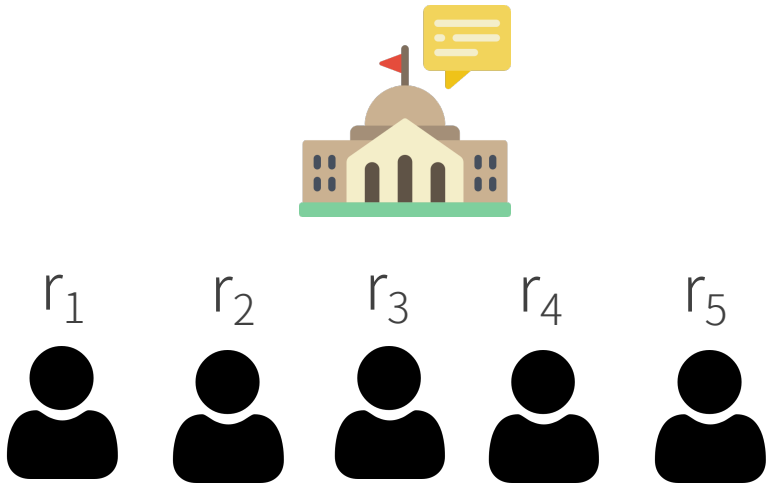
- Vulnerable to denial of service

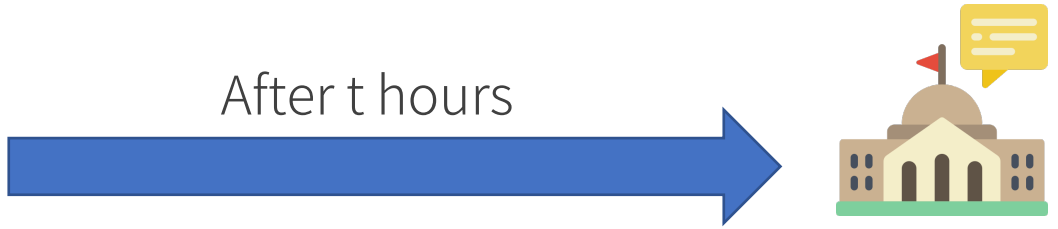


Related Work: Using a delay function

- Delay function: moderately hard to compute (e.g., taking hours to compute)
- Both evaluation and verification are very slow: linear to the randomness contribution phase

Randomness Contribution





Output
R <- delay(t, r_1, r_2, r_3, r_4, r_5)

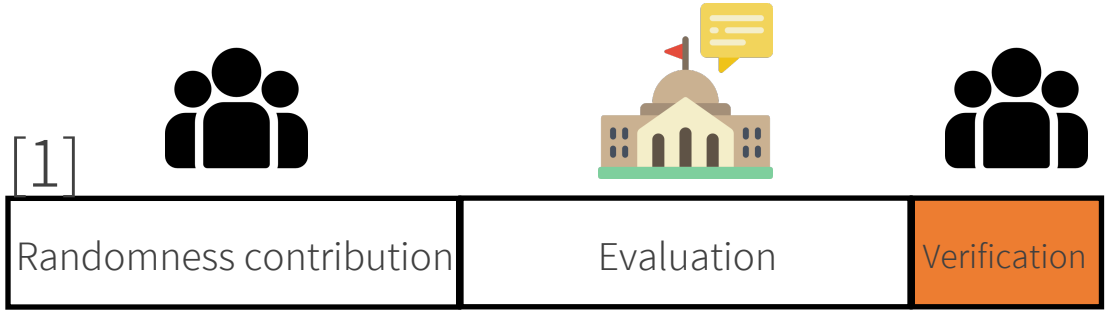
* t should be at least as long as the randomness contribution phase

* Everyone knowing t, r_1, r_2, r_3, r_4, r_5 can verify R by recomputing delay(), which takes t hours.

Our solution: in a nutshell (3/3)

Prior work:
Use a delay function

Our work:
Use a verifiable delay function [1]



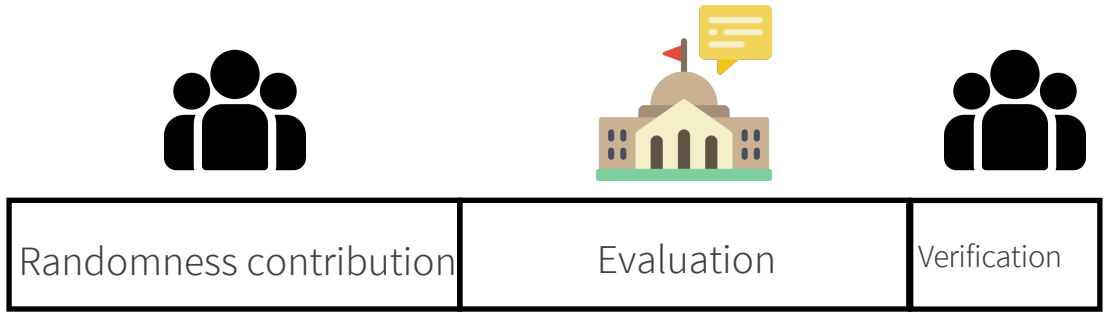
=> Reduce verification cost from linear to constant

[1] Dan Boneh, Joseph Bonneau, Benedikt Bünz, and Ben Fisch. Verifiable delay functions. In Annual international cryptology conference, pages 757–788. Springer, 2018.

Our solution: in a nutshell (3/3)

Our work – basic scheme:

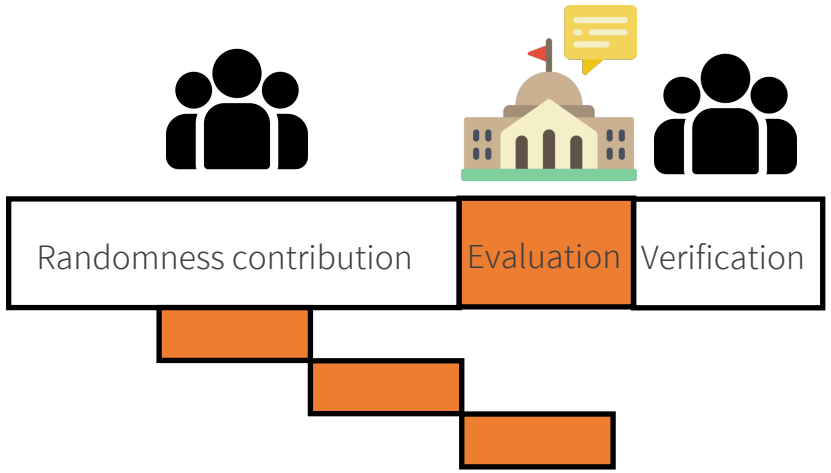
- Use a verifiable delay function (VDF)



Our work – improved scheme:

- Use a VDF
- Pipeline contribution & evaluation
- Aggregate VDF proofs
- Better implementation

=> Reduce evaluation cost by a factor

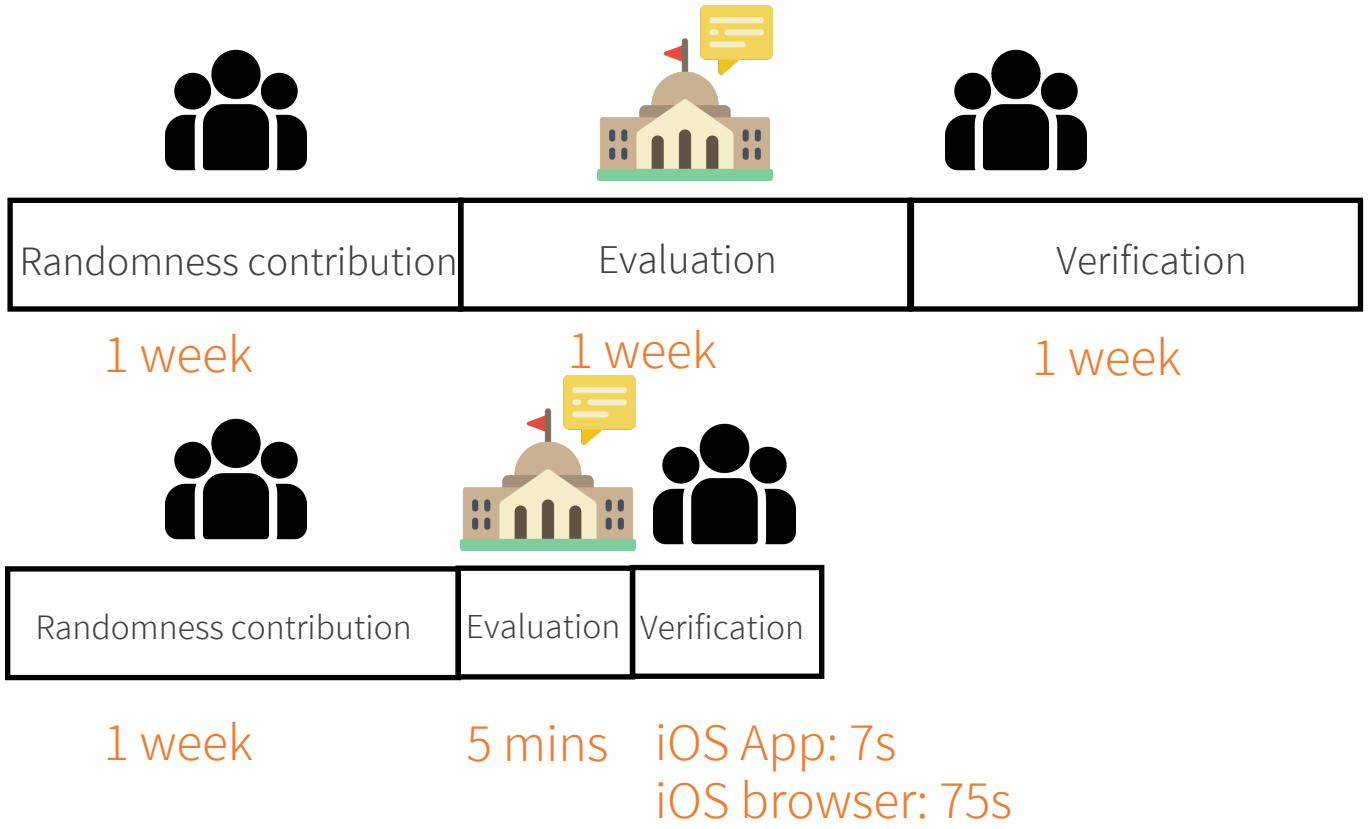


Our solution: in a nutshell (3/3)

Prior work:
- Use a delay function

Our work – improved scheme:
- Use a VDF
- Pipeline contribution & evaluation
- Aggregate VDF proofs
- Better implementation

=> Reduce evaluation cost by a factor



Summary

- Security 101 – 什麼是資訊安全？
- 進階主題
  - 高可用性網路 – 網路被癱瘓了連不上？
  - 物聯網安全 – 按個鍵就控制紅綠燈、汽車、電網？
  - 資安與社會 – 資安離我很遙遠？
  - 網路隱私 – 為什麼廣告都知道我喜歡什麼？
  - 自動化漏洞挖掘 – 打 001011 就能入侵電腦、盜走上億元？
  - 資安與倫理 – 研究的再現性與道德駭客
- 如何選擇資安這條路

Security requirements: e.g., CIA
Principle #1: Defining a reasonable threat model
Principle #2: Security is only as strong as the weakest link