IoT Security

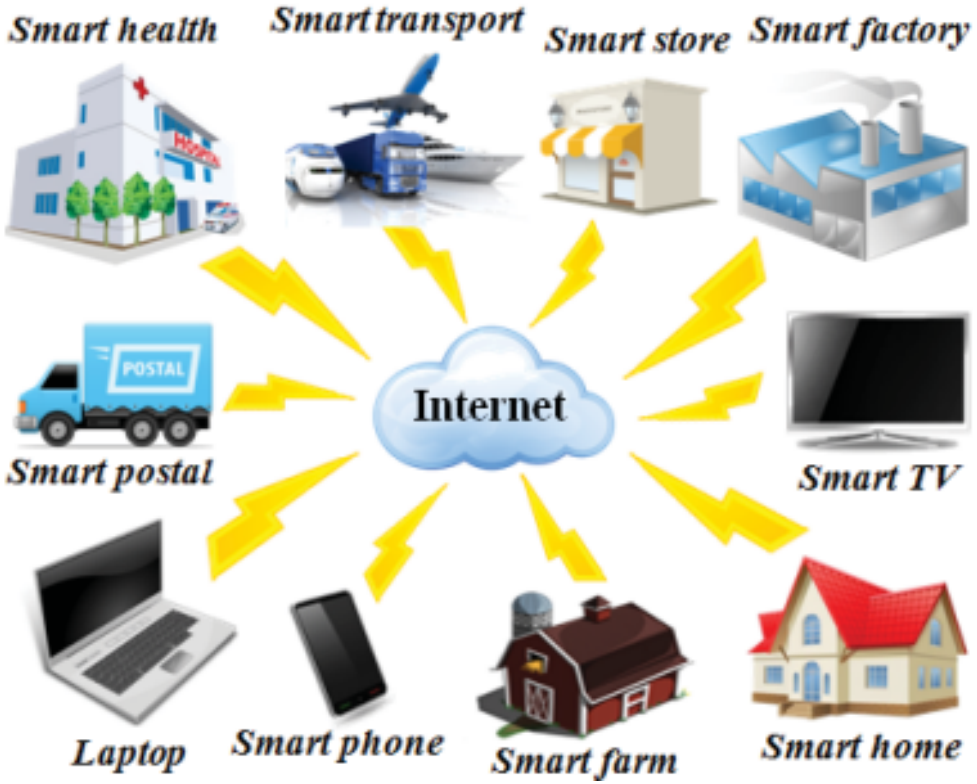
黃仁竑

Outline

- Introduction
- IoT vulnerable features
- IoT system security
- IoT application security
- Conclusion

Introduction

- IoT applications are emerging in our daily lives

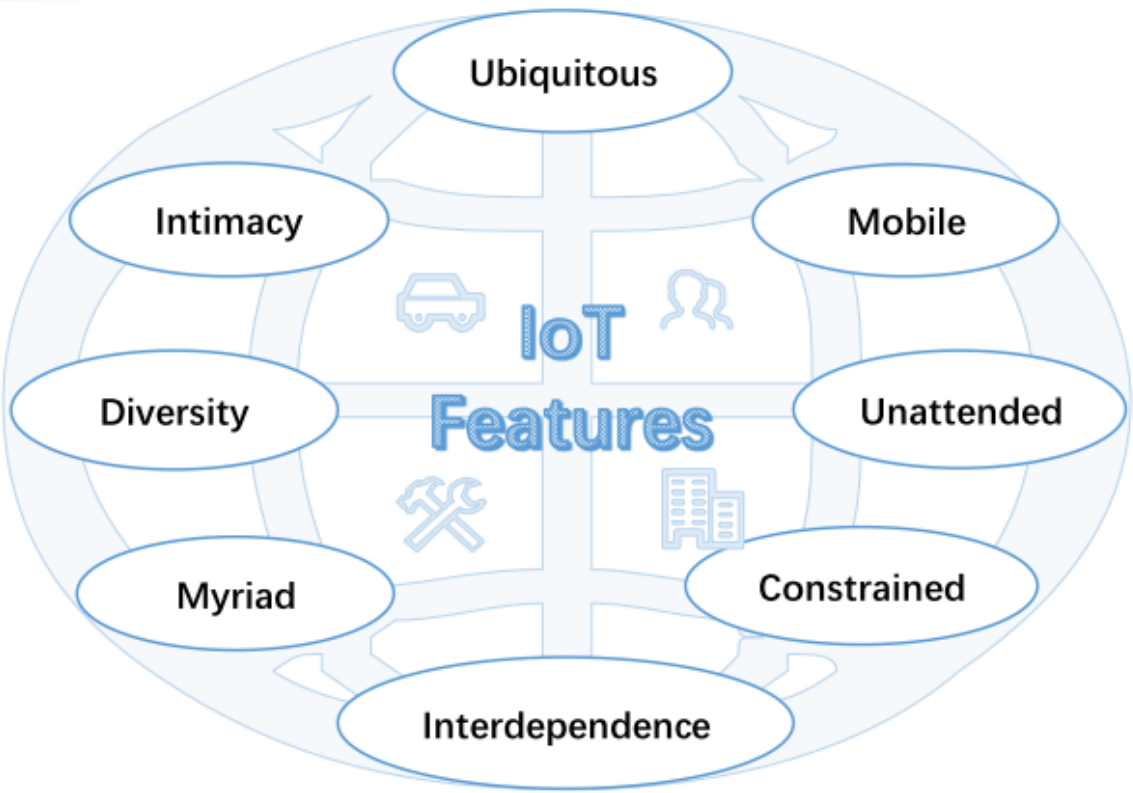


S Kraijak and P. Tuwanut, “A SURVEY ON IOT ARCHITECTURES, PROTOCOLS, APPLICATIONS, SECURITY, PRIVACY, REAL-WORLD IMPLEMENTATION AND FUTURE TRENDS,” 11th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM 2015), 2015.

Background

- IoT devices have become a powerful amplifying platform for cyberattacks
  - Large volume, pervasiveness, and high vulnerability
  - Increasing number of IoT devices (50 billions!!)
    - Good target for botnet
  - Processing power limited embedded system
    - Less secured system
  - Constantly connected to the Internet
  - Permeated with flaws
    - Naive security configurations
  - Vehicle for DDOS attacks

IoT Vulnerable Features



W. Zhou, Y. Jia, A. Peng, Y. Zhang, and P. Liu, "The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved," IEEE IoT journal, early access, 2018. (DOI 10.1109/JIOT.2018.2847733)

IoT Vulnerable Features

- Interdependence
  - Less human involved
  - IoT devices communicate with each other, and many of them could also implicitly controlled by other devices' behaviors or environmental conditions using smart rules.
  - Instead attacking the target device, the attackers could change other devices' behaviors or the surrounding environment, which have interdependence relationship with the target device.

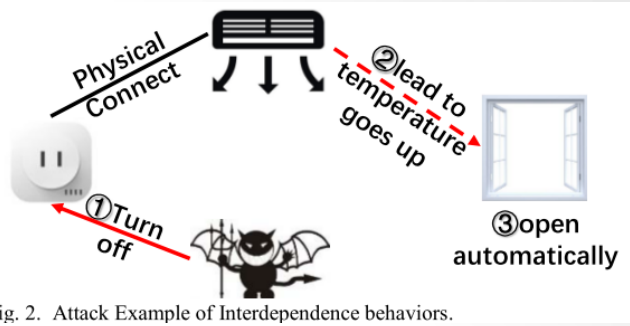
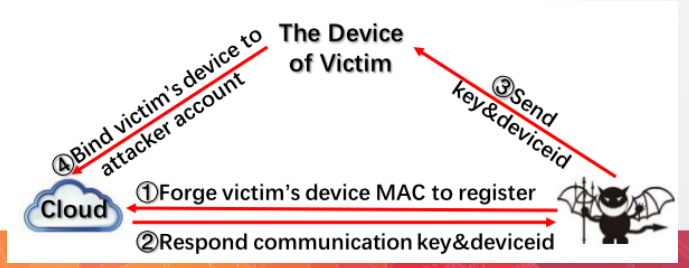


Fig. 2. Attack Example of Interdependence behaviors.

IoT Vulnerable Features

- Diversity
  - IoT devices are designed heterogeneously for different specific tasks and interact strongly with the different physical environment
  - May adopt different communication protocols
  - Ali mobile security team found more than 90% of IoT device firmware has security vulnerabilities and common Web security vulnerabilities
  - Due to lack of practical security experience for new IoT functions such as IoT device bootstrapping, new protocols usually have many potential security problems.



IoT Vulnerable Features

- Constrained
  - Many IoT devices have been designed to be lightweight and small.
    - have much less computing ability, storage resources, stringent requirements for power consumption
    - IoT devices used in vehicle systems, robot control systems and real-time healthcare systems must meet the deadline constraints of the real-time processes.
  - Due to constrained feature, most IoT devices do not deploy necessary defenses for system and network.

IoT Vulnerable Features

- Myriad
  - Enormous number of IoT devices will produce huge amount of IoT data
  - In 2016, the attack traffic of Mirai botnet which was composed of more than 1 million IoT devices, exceeded 1Tbps, which previous cyber-attacks have never been achieved. (large scale DDoS attacks)
  - The target of IoT botnets may no longer just be the website, but also the important infrastructures

IoT Vulnerable Features

- Unattended
  - Many IoT devices are long-time unattended
    - Smart meters, implantable medical devices (IMDs) and sensors in the special industrial, agricultural and military environment
  - Remote attacks targeted unattended devices are difficult to detect
    - As it is hard to physically connect an external interface to verify the state of these devices

IoT Vulnerable Features

- Intimacy
  - Some IoT devices not only collect our biology information including heart rate and blood pressure but also monitor and record our surrounding information and daily activities like the change of indoor temperature and the locations you have been.
  - The intimate relationships between users and IoT devices will certainly raise more serious and unnoticed privacy concerns.

IoT Vulnerable Features

- Mobile
  - Many IoT devices, such as wearable devices and smart cars are used in the mobile environment. These mobile IoT devices usually hop from one network environment to another and communicate with many unknown new devices.
  - Because mobile IoT devices usually join more networks, attackers tend to inject the malicious code into mobile IoT devices to accelerate its spread.

IoT Vulnerable Features

- Ubiquitous
  - IoT devices will become an indispensable part of people's daily lives.
  - IoT devices will be everywhere in our future lives.
  - The manufacturers do not pay enough attention to the security of their IoT products.
  - Most consumers lack the management and privacy protection awareness

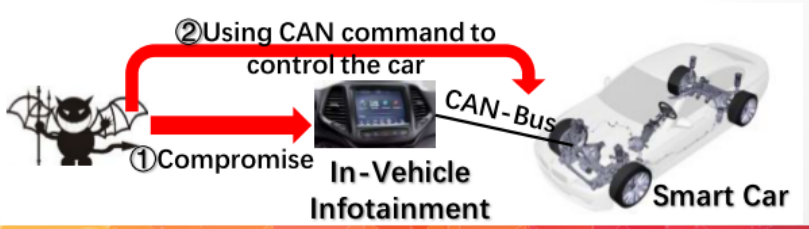


TABLE I

THREATS, CHALLENGES, AND OPPORTUNITIES OF EACH IOT FEATURES

Feature	Threat	Challenge	Opportunity
Inter-dependence	Bypassing static defenses, Overprivilege	Access control and privilege management	Context-based permission
Diversity	Insecure protocols	Fragmented	Dynamic analysis simulation platform, IDS
Constrained	Insecure systems	Lightweight defenses and protocols	Combining biological and physical characteristics
Myriad	IoT botnet, DDoS	Intrusion detection and prevention	IDS
Unattended	Remote attack	Remote verification	Remote attestation, Lightweight trusted execution
Intimacy	Privacy leak	Privacy protection	Homomorphic encryption, Anonymous protocols
Mobile	Malware propagation	Cross-domain identification and trust	Dynamic configuration
Ubiquitous	Insecure configuration	\	Safety consciousness

OWASP IoT Top Ten Project

- A holistic approach: all elements need to be considered
  - The Internet of Things Device
  - The Cloud
  - The Mobile Application
  - The Network Interfaces
  - The Software
  - Use of Encryption
  - Use of Authentication
  - Physical Security
  - USB ports

https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project

OSWAP IoT Top Ten Categories

- Insecure Web Interface
- Insufficient Authentication/Authorization
- Insecure Network Services
- Lack of Transport Encryption
- Privacy Concerns
- Insecure Cloud Interface
- Insecure Mobile Interface
- Insufficient Security Configurability
- Insecure Software/Firmware
- Poor Physical Security

OSWAP IoT Security Guidance

- Manufacturer IoT Security Guidance
  - e.g., Insecure Web Interface: Ensure that any web interface in the product disallows weak passwords
- Developer IoT Security Guidance
  - e.g., Insecure Web Interface: Ensure that any web interface coding is written to prevent the use of weak passwords
- Consumer IoT Security Guidance
  - e.g., Insecure Web Interface: If your system has the option to use HTTPS, ensure it is enabled

https://www.owasp.org/index.php/IoT_Security_Guidance

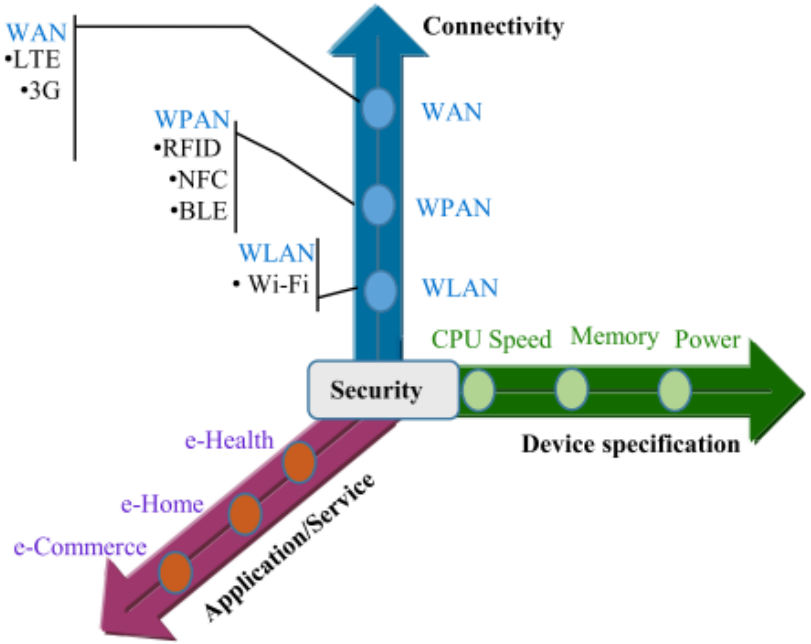
OSWAP IoT Framework Security Considerations

- Designing a secure IoT solution depends on a number of security considerations. One of the most important considerations is the use of a secure IoT framework for building your ecosystem.
- Framework evaluation criteria of typical IoT system archetypes
  - Edge
  - Gateway
  - Cloud Platform
  - Mobile

https://www.owasp.org/index.php/IoT_Framework_Assessment

IoT Security Landscape

- Connectivity: IoT protocol security
- System: IoT device security
- Application: IoT applications and services



Md. M. Hossain, M. Fotouhi, and R. Hasan, "Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things," 2015 IEEE World Congress on Services. (DOI 10.1109/SERVICES.2015.12)

IoT system security

C. Kolias, G. Kambourakis, A. Stavrou and J. Voas, “DDoS in the IoT: Mirai and Other Botnets,” IEEE Computer, Volume 50, Issue 7, pp. 80-84, 2017.

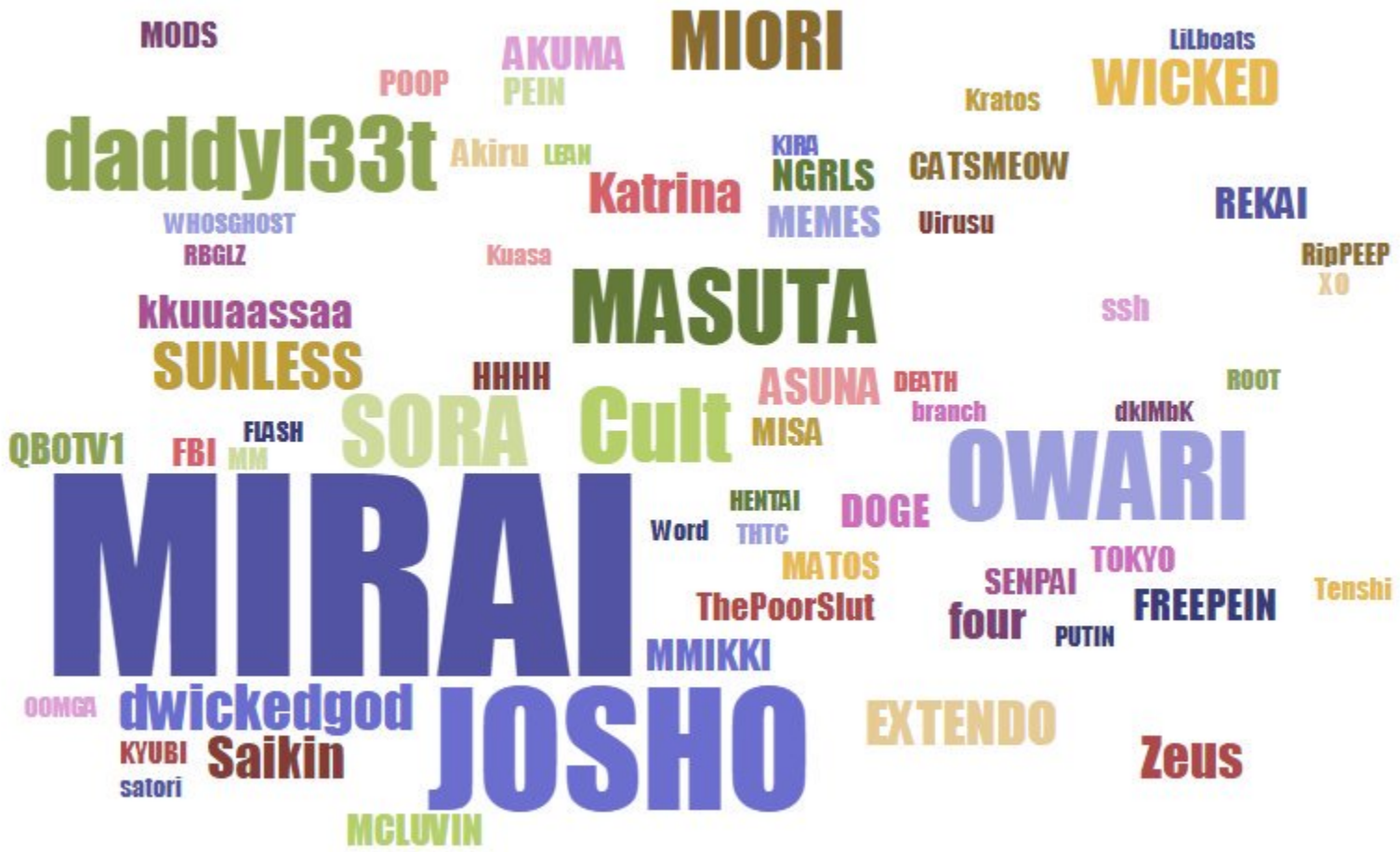
IoT Attack History

- Mirai botnet first identified in August 2016 by MalwareMustDie research group.
- In September 2016, the website of computer security consultant Brian Krebs was hit with 620 Gbps of traffic.
- At about the same time, an even bigger DDoS attack peaking at 1.1 Tbps, targeted the French webhost and cloud service provider OVH.
- In October 2016, DNS service provider Dyn was took down hundreds of websites, including Twitter, Netflix, Reddit, and GitHub, for several hours.

History

- In November 2016, Mirai variant knocked nearly a million Deutsche Telekom subscribers offline.
- In February 2017, a Mirai variant launched a 54-hour-long DDoS attack against a US college.
- Persirai is active since April 2017, another IoT botnet that shares Mirai's code base
  - Estimated 120,000 devices are vulnerable to Persirai
  - Exploiting a documented zero-day flaw that lets attackers directly obtain the password file.
  - DDoS attack based on UDP flooding

Word Cloud of Mirai



Mirai Variants

	Akiru	Katrina_V1	Sora	Saikin	Owari	Josho_V3	Tokyo
Successful infection	Akiru: applet not found	Katrina: applet not found	Sora: applet not found	Saikin: applet not found	Owari: applet not found	daddyl33t: applet not found	MIRAI: applet not found
Credential combination	40	11	36	80	26	34	37
Overlap with Mirai	4	No overlap	6	4	7	1	6
Killing ports	CCTV-DVR Systems : port 81 Netis Router port: 53413 Realtek SDK port: 52869	Netis Router port: 53413 Realtek SDK port: 52869 Huawei HG532 port: 37215	Netis Router 53413 Realtek SDK port: 52869 Huawei HG532 port: 37215	-	Netis Router 53413 Realtek SDK port: 52869 Huawei HG532 port: 37215	-	Netis Router 53413 Realtek SDK port: 52869 Huawei HG532 port: 37215
Targeted architecture	ARC RCE	-	-	ARC RCE	-	-	-
Decryption key	DF7ECADF	DEEDFBAF	DEDEFBAF	DEACFBEF	DEDEFBAF	DEDEFFBA	Default Mirai key

And many more …

- QBot
- Hakai
- Torii

New Business

- After open source of Mirai
  - hackers offered Mirai botnets for rent with as many as 400,000 simultaneously connected devices.

Basic Concept of Mirai

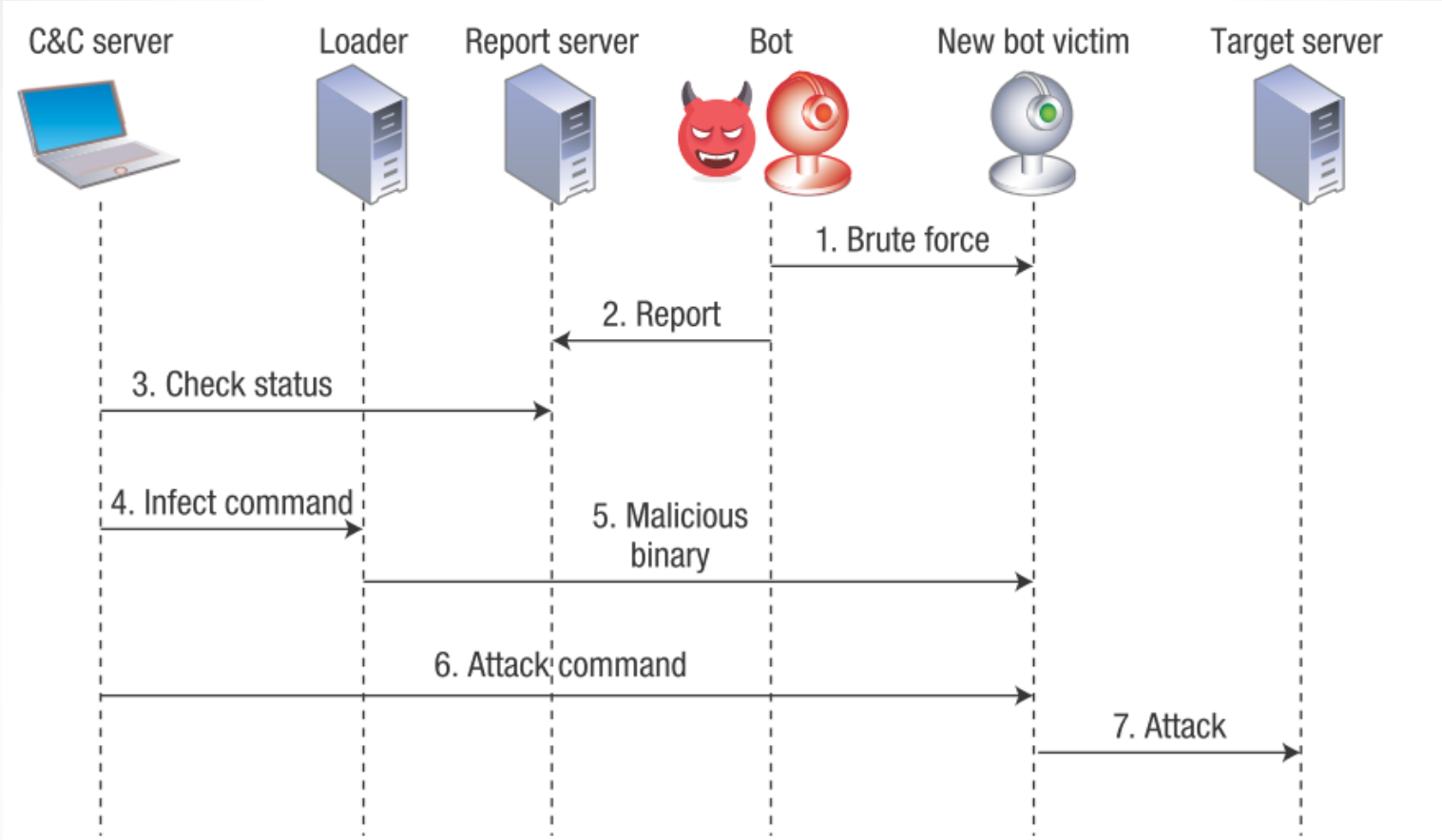
- Mirai primarily spreads by first infecting devices such as webcams, DVRs, and routers.

- It then deduces the administrative credentials of other IoT devices by means of brute force (by breaking username–password pairs using dictionary).

Main Components of Mirai

- Command and control (C&C)
  - The C&C server provides the botmaster with a centralized management interface to check the botnet's condition and orchestrate new DDoS attacks.
- Loader
  - The loader facilitates the dissemination of executables targeting different platforms (18 in total, including ARM, MIPS, and x86) by directly communicating with new victims.
- Report
  - The report server maintains a database with details about all devices in the botnet.

Mirai Botnet Operation and Communication



Constantinos Kolias, Georgios Kambourakis, Angelos Stavrou, Jeffrey Voas, "DDoS in the IoT: Mirai and Other Botnets," IEEE Computer, Volume 50, Issue 7, pp. 80-84, 2017.

Mirai Botnet Operation

- Initially, Mirai scans random public IP addresses through TCP ports 23 or 2323.
- The bot engages in a brute-force attack to discover the default credentials of weakly configured IoT devices (username–password pairs)
- Upon breaking the credentials and gaining a shell interface, the bot forwards various device characteristics to the report server through a different port.
- Via the C&C server, the botmaster frequently checks new prospective target victims as well as the botnet's current status by communicating with the report server.
- After deciding which vulnerable devices to infect, the botmaster issues an infect command in the loader.

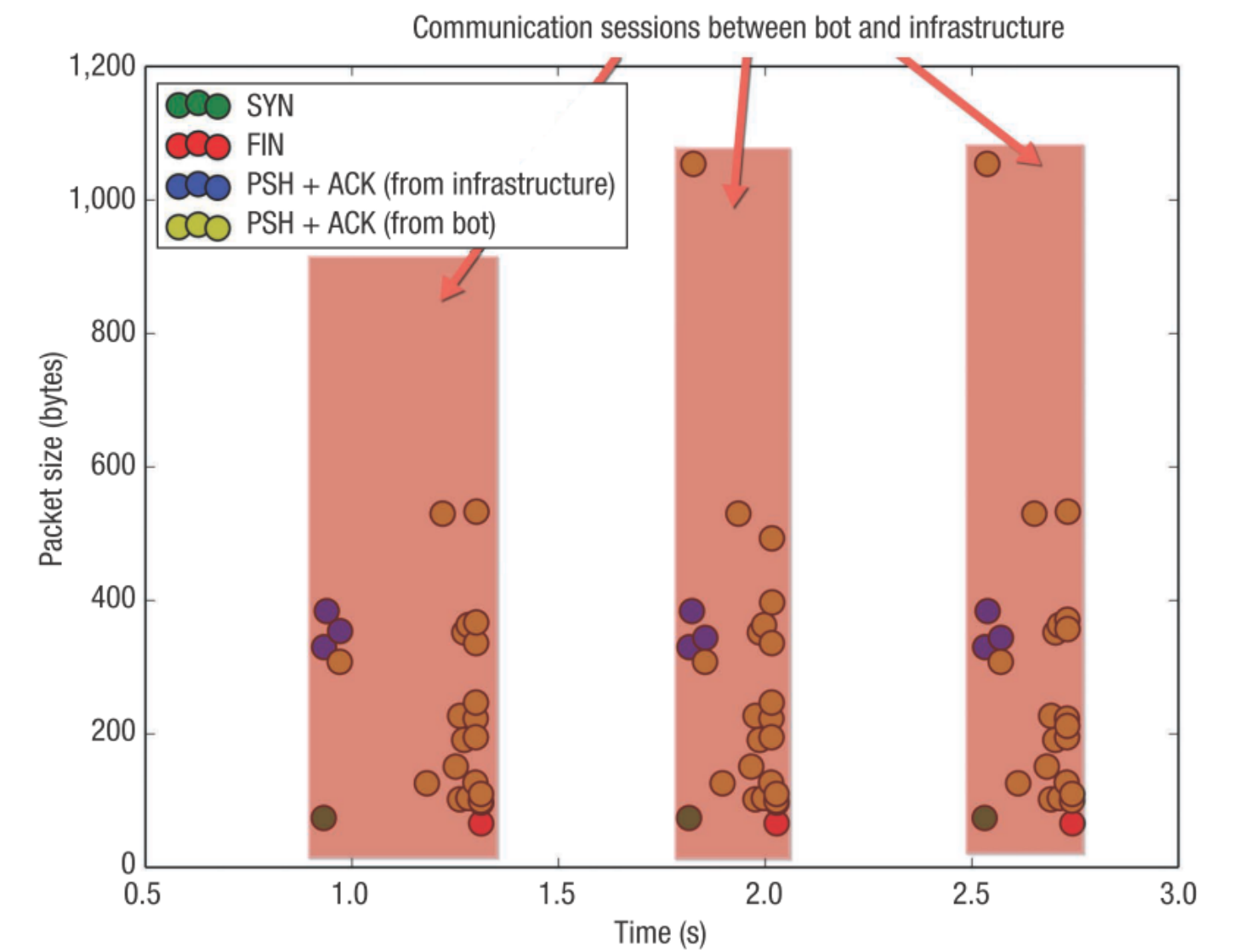
Mirai Botnet Operation

- The loader logs into the target device and instructs it to download and execute the corresponding binary version of the malware.
  - Wget www.gnu.org/software/wget/manual /wget.html
  - The newly recruited bot instance can communicate with the C&C server to receive attack commands.
- The botmaster instructs all bot instances to commence an attack against a target server.
  - Via port 7547, which ISPs use to remotely manage customers' broadband routers.
- The bot instances will start attacking the target server with one of 10 available attack variations such as Generic Routing Encapsulation (GRE), TCP, and HTTP flooding attacks.

Detecting Mirai

- Mirai signatures
  - sequentially testing specific credentials in specific ports
  - sending reports that generate distinctive patterns
  - downloading a specific type of binary code
  - exchanging keep-alive messages
  - receiving attack commands that have a specific structure
  - generating attack traffic with very few random elements

Communication Pattern of Mirai



Other IoT Bots

- LuaBot
  - Reported in August 2016, written in Lua programming language, encrypted C&C communication channel
- Hajime botnet
  - Discovered in October 2016, infection method similar to Mirai, used a centralized architecture (BitTorrent DHT), message is RC4 encrypted
- BrickerBot
  - Discovered in April 2017, leverage SSH service default credentials, misconfigurations, or known vulnerabilities, perform permanent denial-of-service (PDoS) (e.g., defacing firmware)

Comparison of IoT Bots

名稱	說明&特色	原始碼
Mirai	TB級的Iot Botnet，原始碼被公開在github中，利用預設帳號密碼進行感染。	有
TheMoon	針對路由器弱點進行攻擊(linksys、asus、tplink)	無
IoT-reaper	Mirai的變種、使用IoT設備漏洞進行感染提高攻擊效率。	無
adb miner	針對android相關設備的Iot攻擊(port: 5555)，主要是透過相關設備進行虛擬幣的挖掘。	無
Hajima	P2P Botnet，並且使用TR-069、GoAhead及DVR設備漏洞進行攻擊。	無

IoT system security: Lessons Learned

- Five main reasons IoT devices are particularly advantageous for creating botnets:
  - Constant and unobtrusive operation
  - Feeble protection
  - Poor maintenance
  - Considerable attack traffic
    - IoT devices are powerful enough and well situated to produce DDoS attack traffic
  - Noninteractive or minimally interactive user interfaces
    - infections are more likely to go unnoticed

IoT Application Security

Tips for Developing Secure IoT Apps

- Use Developers with Right Skills
- Use Proven IoT Application Platforms
- Watch IoT Device Firmware Security
- Ensure IoT Data is Secure from Physical Attacks
- Use Secure Hardware Components
- Apply Standard Security Best Practices

https://www.esecurityplanet.com/network-security/6-tips-for-developing-secure-iot-apps.html

IoT Application Protocols

Protocol	Protocol Features				
	TCP/UDP	Architecture	Security & QoS	Header Size	Maximum Length
MQTT	TCP	Pub/Sub	Both	2	5
AMQP	TCP	Pub/Sub	Both	8	-
CoAP	UDP	Req/Resp	Both	4	20
XMPP	TCP	Both	Security	-	-
DDS	TCP	Pub/Sub	QoS	-	-

Advanced Message Queuing Protocol (AMQP), Data Distribution Service (DDS)

- Support Authentication and encryption?
- Against sniffing?
- Against DOS or DDOS attacks?

IoT Application Security Goals

- Data confidentiality
  - The ability to ensure privacy for the user by providing a secure connection to only the permitted users.
- Data Integrity
  - Secure data so that data tampering cannot be done.
- Data Availability
  - The ability to provide data to its users, whenever needed.

Application Layer Disputes

- Malicious code injection
- Denial-of-service attack
- Phishing attack
  - The attacker gains credentials access of that victim and damage data.
- Sniffing attack
  - Could gain network information leading to system corruption or data leaking

Application Layer Security Problems

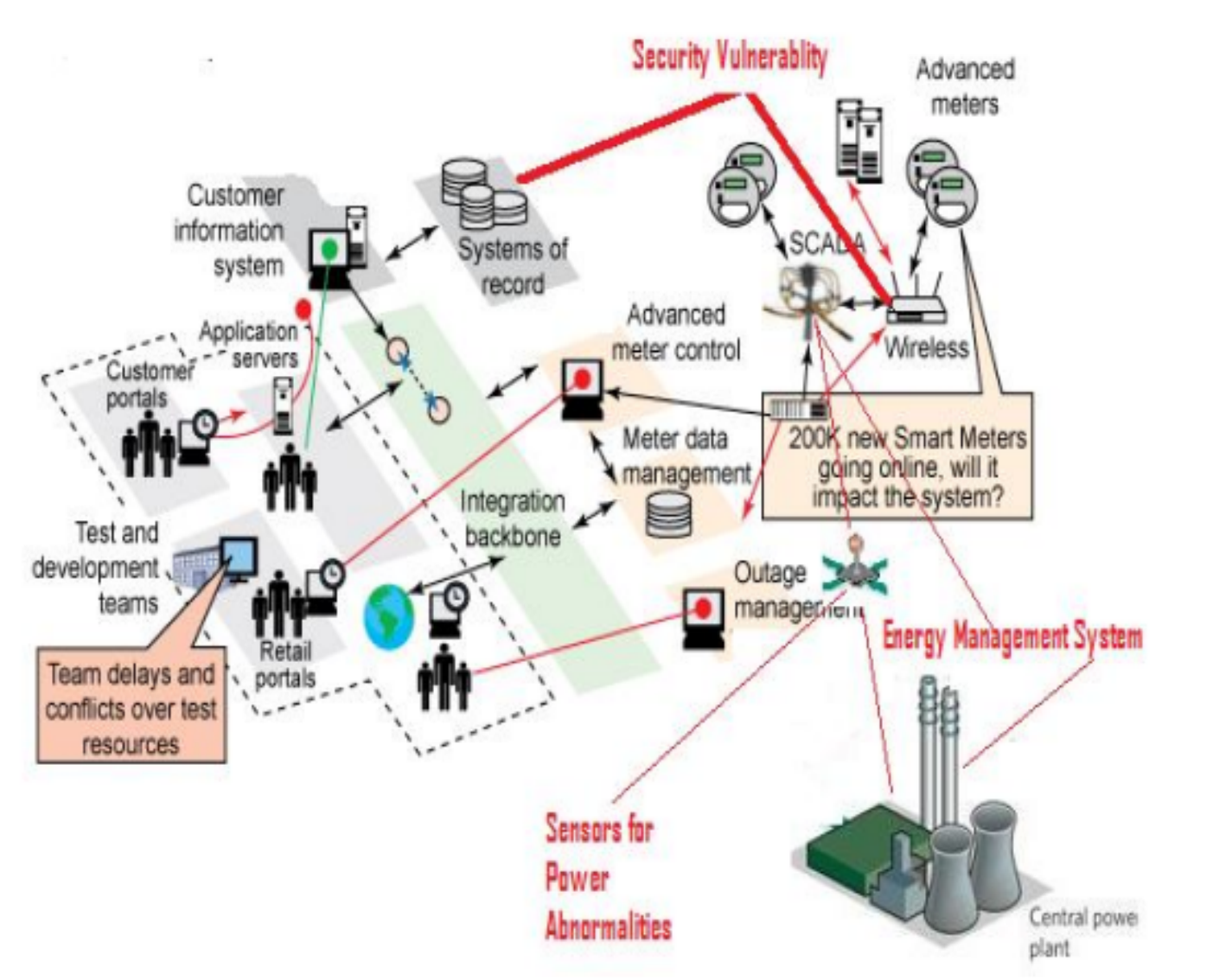
- Authentication of identity
  - Deploy proper authentication mechanism to prevent the illegal user getting into the system
- Data storage and recovery
  - Transmission involves the user privacy, integrity of data. Proper data storage and recovery should be incorporated during data transmission
- Handling huge data
  - Huge volume of data transmission involves data loss which in turn affect the efficient working of the network.
- Software vulnerabilities

Security Measures

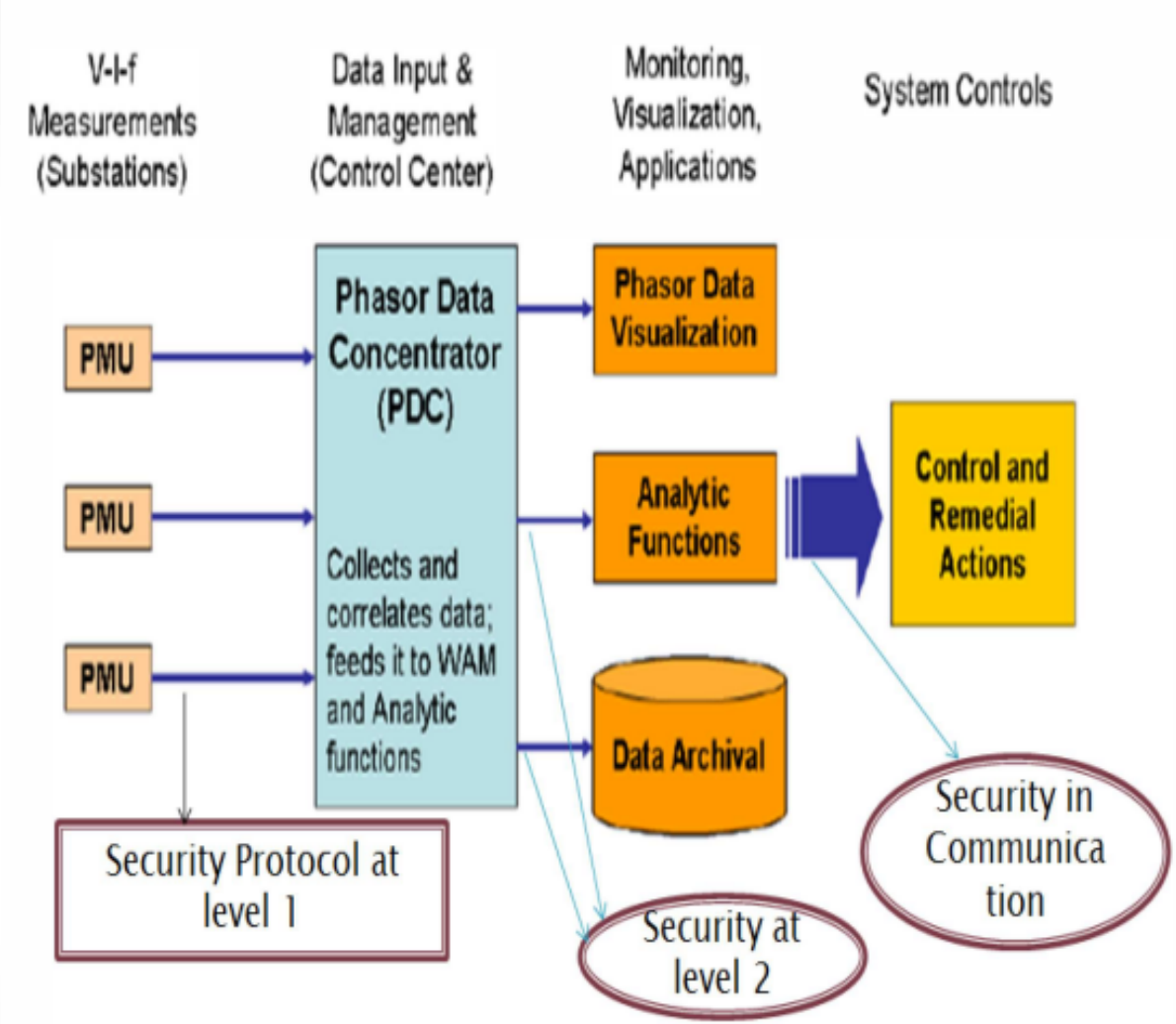
- Authentication
  - Cloud computing and virtualization are the main technology that are more prone to attacks.
- Intrusion Detection
- Risk Assessment
  - situation analysis, comparison of various standards and checks for risks acceptance level.
- Data security
  - encryption, anti-dos-firewalls, malwares, and spywares

IoT Application Security Case Studies

Security Vulnerability of Smart Grid



Calibrated Security for Smart Grid

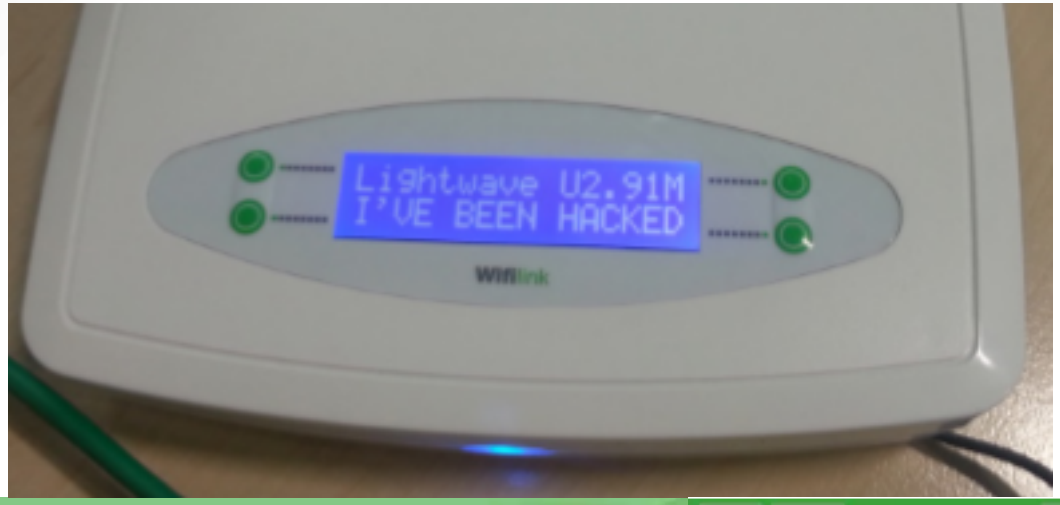


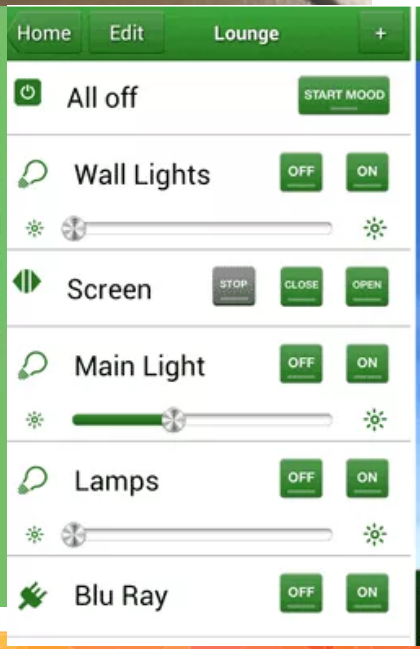
IoT Device Attack Case Study I

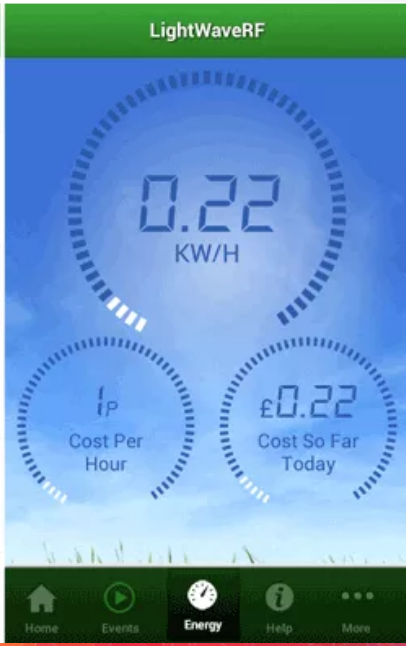
Smart Home Gateway

- LightwaveRF smart hub
  - 英國的無線家庭自動化品牌
  - 利用RF無線射頻技術，讓一般住家在無需配線的情況之下，也能增加一些自動控制的功能，實現家庭的自動化。
  - 可透過電腦或手機app來對設備進行遠端控制，目前能控制燈光開關、暖氣、插座、繼電器等設備。

LightwaveRF smart hub







Security Holes of LightwaveRF

- LightwaveRF smart hub checks for firmware updates every 15 minutes.
- It sends update check to a remote Trivial File Transfer Protocol (TFTP) server on the Internet.
- Since this connection is neither encrypted nor authenticated, it can easily be targeted by an attacker with access to the network, allowing them to conduct a man-in-the-middle (MITM) attack.

Firmware Update Attack

- Crack the Wi-Fi password
  - Easy since many people use weak passwords to protect their wireless network at home.
- Use Address Resolution Protocol (ARP) poisoning to redirect the smart hub's request to the attacker's TFTP server.
  - Since the firmware update is an unsigned blob in a raw format, it is easy to unpack and modify it.
  - Once the modified firmware update is served to the device and installed, the attacker gets full control over the smart hub device and could start attacking other connected devices from there.

https://www.symantec.com/content/dam/symantec/docs/white-papers/insecurity-in-the-internet-of-things-en.pdf

Man-in-the-middle Attack

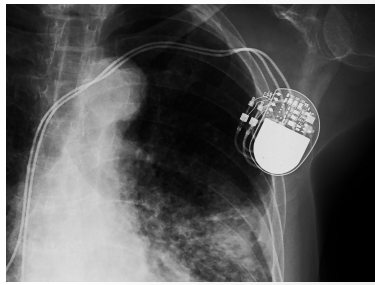
- Attackers can sniff the RF link for command packets and replay them.
  - With a smart hub that just turns devices on and off, it only receives a small number of different command packets.
  - As a result, the attackers don't need to worry about breaking any pairing if they are close enough to the device to inject spoofed packets.
  - This can allow them to take control of the targeted device.

IoT Device Attack Case Study II

https://www.theguardian.com/technology/2018/aug/09/implanted-medical-devices-hacking-risks-medtronic

駭客示範攻擊心律調節器

- Hackable implanted medical devices could cause deaths
  - A range of implanted medical devices with nine newly discovered security vulnerabilities
  - At the 2018 Black Hat information security conference, Jonathan Butts of QED Secure Solutions and Billy Kim Rios of Whitescope demonstrated the hacks in a live session
  - They remotely disabled an implantable insulin pump, preventing it from delivering the lifesaving medication, and then took total control of a pacemaker system, allowing them to deliver malware directly to the computers implanted in a patient's body.
  - The device is made by Medtronic.



胰島素幫浦(insulin pump) 心律調節器(Pacemaker)

Hacking Steps

- To take control of the pacemaker, Rios and Butts went up the chain, hacking the system that a doctor would use to program a patient's pacemaker.
- Their hack rewrote the system to replace the background with an ominous skull (骷髏頭), but a real hack could modify the system invisibly, while ensuring that any pacemaker connected to it would be programmed with harmful instructions.
  - Such as issue a shock or deny a shock
- Withholding treatment by the malware can be as damaging as active attempts to harm.

AI 物聯網安全防護平台

高教深耕109年度計畫成果

技術亮點

目標1

針對即時流量偵測能力，設計深度學習之封包檢測技術

改變文獻中要先把封包分類成不同的flow，才能對flow進行是否為攻擊流量的偵測方式，改以只看raw packet

目標2

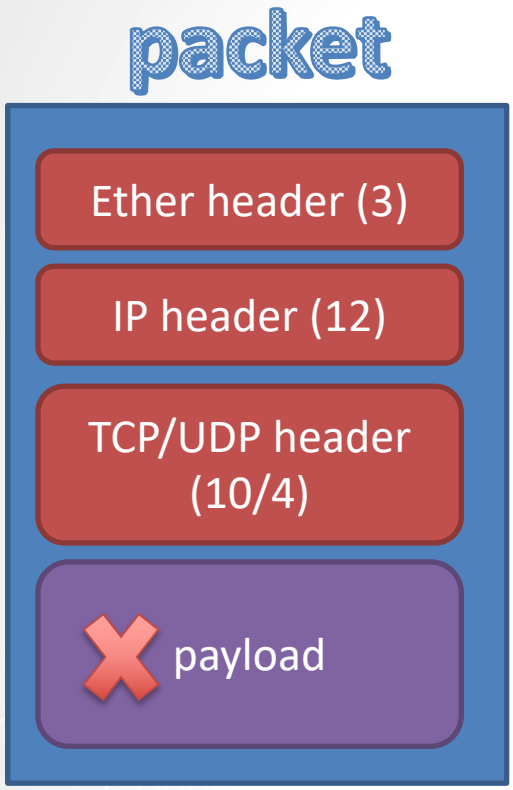
針對未知的新攻擊流量，設計無監督式深度學習之檢測技術

1. 以CNN提取流量特徵，避免正確特徵選取之因難
2. 以Autoencoder為無監督式深度學習模式，發展偵測未知的新攻擊流量技術

技術亮點一

技術名稱

長短期記憶模型對封包表頭格式之即時分析技術



特色

即時辨識每個封包屬於正常或惡意

raw packet detection

輕量長短期記憶網路訓練模型

field-based packet header word embedding

以欄位為字詞單位取代以位元組為單位，增加相對應欄位關聯性

packet labeling

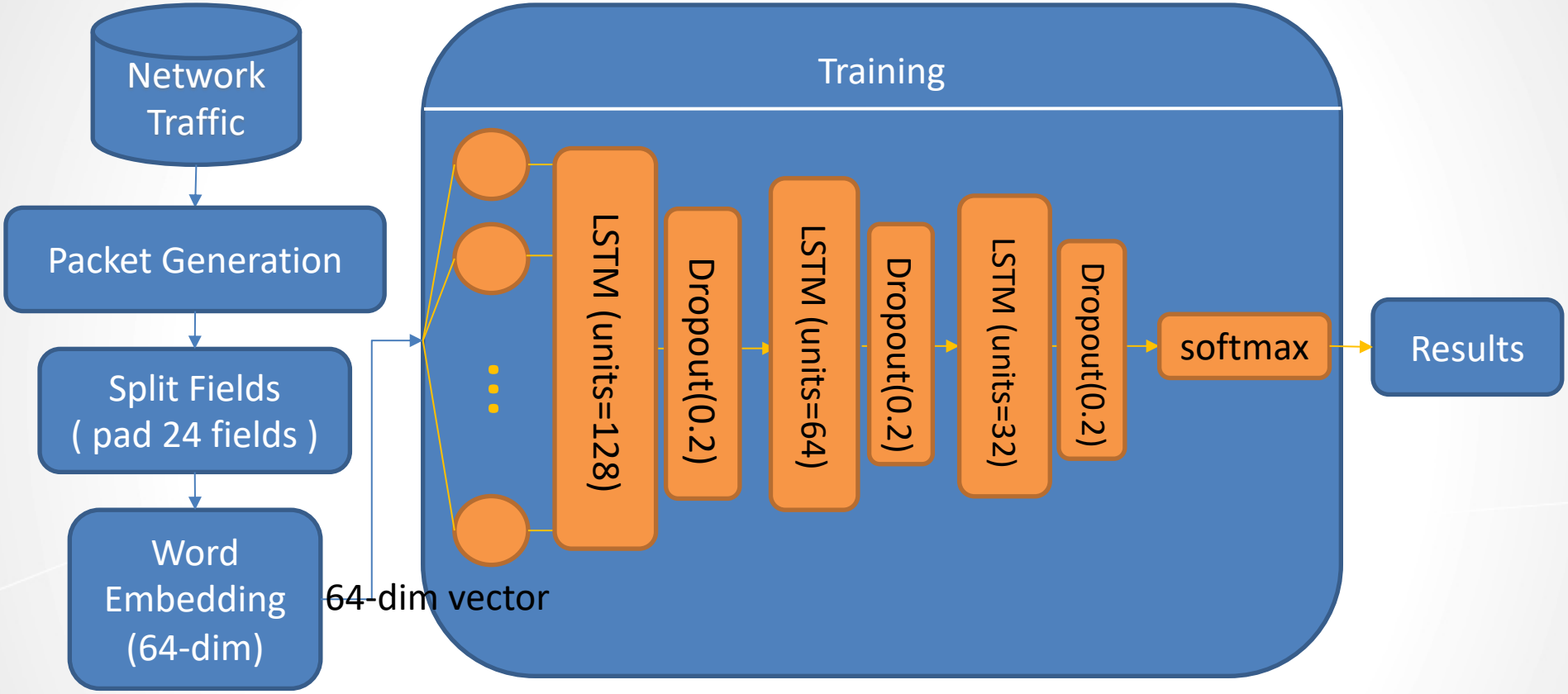
技術細節

ISCX2012-12jun / USTC-TFC2016

三層長短期記憶網路訓練模型

技術亮點一

偵測系統架構



技術亮點二

技術名稱

設計卷積神經網路之封包分類模型與惡意流量檢測技術

即時偵測能力

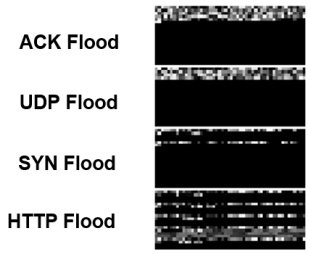
以流量之原始資料為輸入之模型，且大幅縮小資料大小。

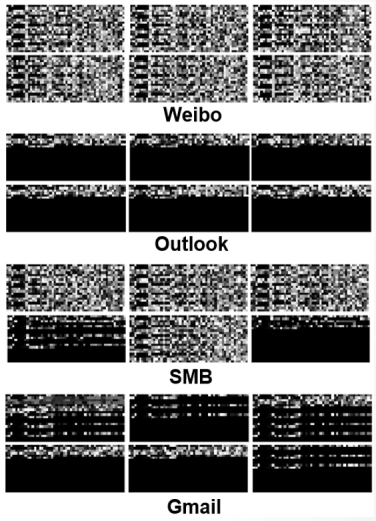
特徵提取

以卷積神經網路大幅減少特徵提取和特徵選擇之負擔。
以一維Filter提高特徵之適切性。

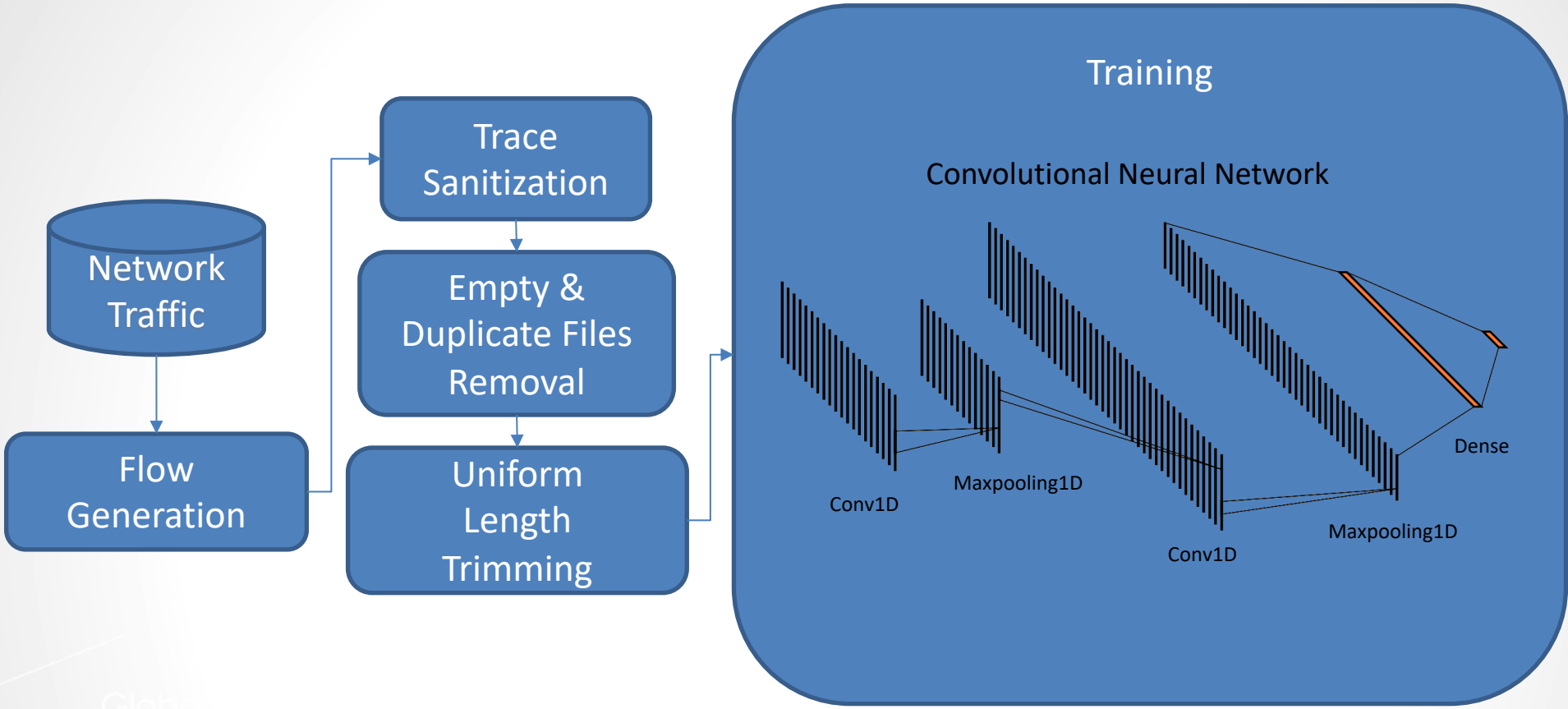
準確率

對每個flow的每個封包只截取固定長度。
實驗結果顯示截取每個Flow約100個位元組即可達到96%之準確率。





技術亮點二


Network Traffic
Flow Generation
Trace Sanitization
Empty & Duplicate Files Removal
Uniform Length Trimming
Training
Convolutional Neural Network
Conv1D
Maxpooling1D
Conv1D
Maxpooling1D
Dense

執行成果一

- Data used
  - ISCX-IDS-2012
    - remove 6/11, 6/16 data (only normal traffic in these two days)
  - USTC-TFC-2016
    - all data are used
  - Mirai Botnet
    - remove background traffic
  - Mirai traffic collected by ourselves
    - only contain malicious traffic
    - benign traffic taken from USTC-TFC-2016

執行成果一

- Data used
  - ISCX-IDS-2012
    - remove 6/11, 6/16 data (only normal traffic in these two days)
  - USTC-TFC-2016
    - all data are used
  - Mirai Botnet (from [1])
    - remove background traffic
  - Mirai traffic collected by ourselves
    - only contain malicious traffic
    - benign traffic taken from USTC-TFC-2016
- Training and testing
  - Balancing benign and malicious traffic
  - Testing: 10-fold auto select
- Validation
  - Original real traffic (randomly take 60-second traffic from the data set)

[1] C. D. McDermott, F. Majdani, A. Petrovski, “Botnet Detection in the Internet of Things using Deep Learning Approaches,” International Joint Conference on Neural Networks, 2018, pp. 1-8.

執行成果一

Testing Result

	USTC-TFC2016	ISCX2012-12	Mirai Botnet	Mirai + USTC-TFC2016
Accuracy	99.99%	99.99%	99.46%	100%
Precision	100%	99.98%	99.63%	100%
Recall	99.99%	99.99%	99.38%	100%
F1 score	99.99%	99.99%	99.51%	100%
FAR(False Alarm Rate)	1.1e-07%	7.46e-07%	0.026%	0%

執行成果一

Validation Result

	USTC-TFC2016	ISCX2012-12	Mirai Botnet	Mirai + USTC-TFC2016
Accuracy	99.88%	99.97%	99.36%	99.98%
Precision	99.99%	100%	99.49%	99.99%
Recall	99.86%	99.97%	99.27%	99.95%
F1 score	99.93%	99.98%	99.38%	99.97%
FAR(False Alarm Rate)	0.002%	0%	0.031%	0%

執行成果二

USTC-TFC2016 data set

Training	
類型	數量
BitTorrent	6000
Facetime	6000
FTP	6000
Gmail	6000
MySQL	6000
Outlook	6000
Skype	6000
SMB	6000
Weibo	6000
WorldofWarcraft	6000

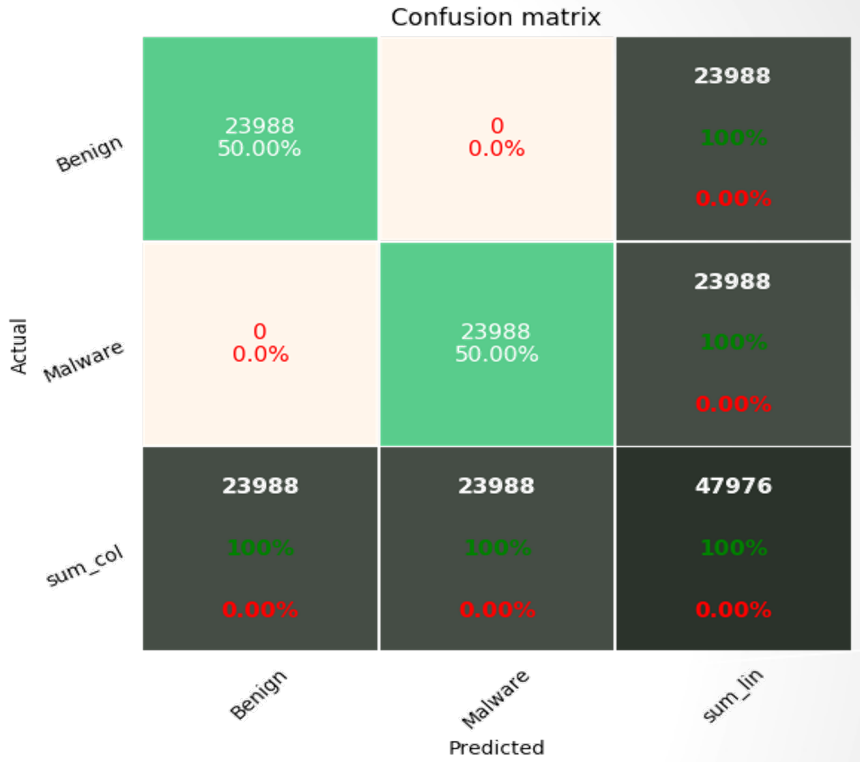
Testing	
類型	數量
BitTorrent	2398
Facetime	2398
FTP	2399
Gmail	2399
MySQL	2399
Outlook	2399
Skype	2399
SMB	2399
Weibo	2399
WorldofWarcraft	2399
ACK Flood	5997
SYN Flood	5997
UDP Flood	5997
HTTP Flood	5997

USTC-TFC2016之正常流量
+ Mirai之惡意DDoS流量

執行成果二

USTC-TFC2016 data set

Packet count	Packet Size(Bytes)				
	40	50	60	70	80
2	99.96%	100.00%	100.00%	100.00%	100.00%
3	99.99%	99.99%	100.00%	100.00%	100.00%
4	99.97%	99.95%	100.00%	99.99%	100.00%
5	99.98%	99.39%	99.99%	99.99%	100.00%



Malicious flow 辨識:
每個Flow取2個封包，每個封包取50位元組時，即可達到100%辨識率。

執行成果二

Mirai Botnet [1]

CNN training set	
類型	數量
Ack Flood	6600
Http Flood	120
Udp Flood	28816
Dns Flood	4312
Mirai	68200
Vse Flood	4432
Greip Flood	24712
Syn Flood	68200
Normal	68200

Training set for Autoencoder	
類型	數量
Normal	68200

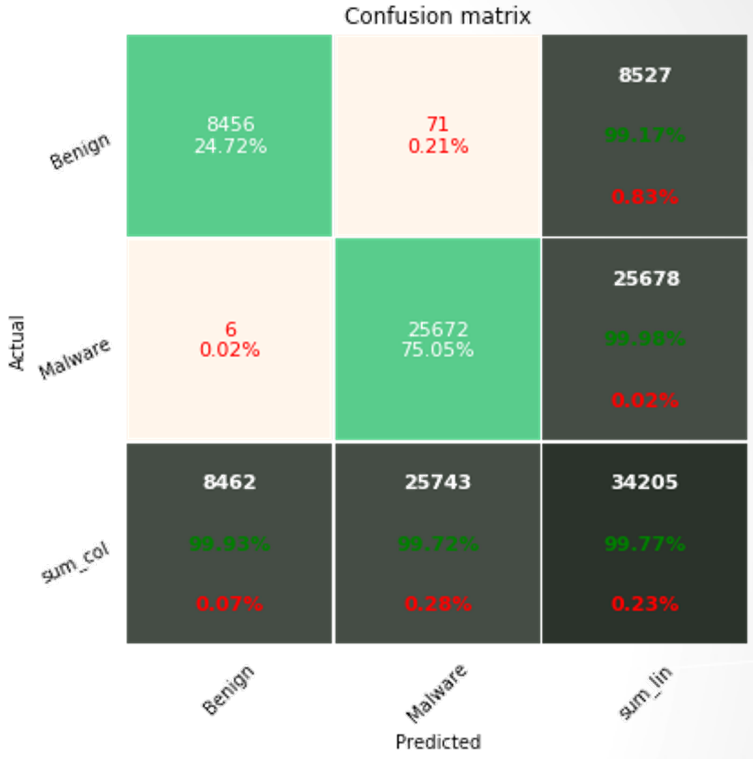
Testing	
類型	數量
Ack Flood	825
Http Flood	15
Udp Flood	3602
Dns Flood	539
Mirai	8525
Vse Flood	554
Greip Flood	3089
Syn Flood	8525
Normal	8525

[1] C. D. McDermott, F. Majdani, A. Petrovski, “Botnet Detection in the Internet of Things using Deep Learning Approaches,” International Joint Conference on Neural Networks, 2018, pp. 1-8.

執行成果二

Mirai Botnet [1]

Packet count	Packet Size(Bytes)				
	40	50	60	70	80
2	99.01%	99.11%	99.71%	99.76%	99.77%
3	97.88%	98.40%	99.67%	99.77%	99.77%
4	96.39%	97.60%	99.51%	99.71%	99.75%
5	95.54%	96.66%	99.38%	99.69%	99.73%



Malicious flow 辨識:
每個Flow取2個封包，每個封包取80位元組時，可達到99.77%辨識率。

Conclusion

- IoT devices are vulnerable
- Classification of IoT security issues
  - Connectivity: IoT protocol security
  - System: IoT device security
  - Application: IoT applications and services
- IoT system security
  - Mirai and its variants
- IoT application security
  - Security guidance for application developers
  - Protect data (confidentiality and privacy)

References

- S Kraijak and P. Tuwanut, “A Survey on IoT Architectures, Protocols, Applications, Security, Privacy, Real-world Implementation, and Future Trends,” 11th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM 2015), 2015.
- W. Zhou, Y. Jia, A. Peng, Y. Zhang, and P. Liu, “The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved,” IEEE IoT journal, early access, 2018. (DOI 10.1109/JIOT.2018.2847733)
- W. Zhou, Y. Jia, A. Peng, Y. Zhang, and P. Liu, “The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved,” IEEE IoT journal, early access, 2018. (DOI 10.1109/JIOT.2018.2847733)
- https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project
- Md. M. Hossain, M. Fotouhi, and R. Hasan, “Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things,” 2015 IEEE World Congress on Services. (DOI 10.1109/SERVICES.2015.12)

References

- C. Kolias, G. Kambourakis, A. Stavrou and J. Voas, “DDoS in the IoT: Mirai and Other Botnets,” IEEE Computer, Volume 50, Issue 7, pp. 80-84, 2017.
- https://www.esecurityplanet.com/network-security/6-tips-for-developing-secure-iot-apps.html
- S. N. Swamy, D. Jadhav, and N. Kulkarni, “Security Threats in the Application layer in IOT Applications,”International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC 2017), pp. 477-480.
- A. K. Koundinya, G.S. Sharvani, K. U. Rao, “Calibrated security measures for centralized loT applications of smart grids,” 2016 International Conference on Computational Systems and Information Systems for Sustainable Solutions, pp. 153-157.