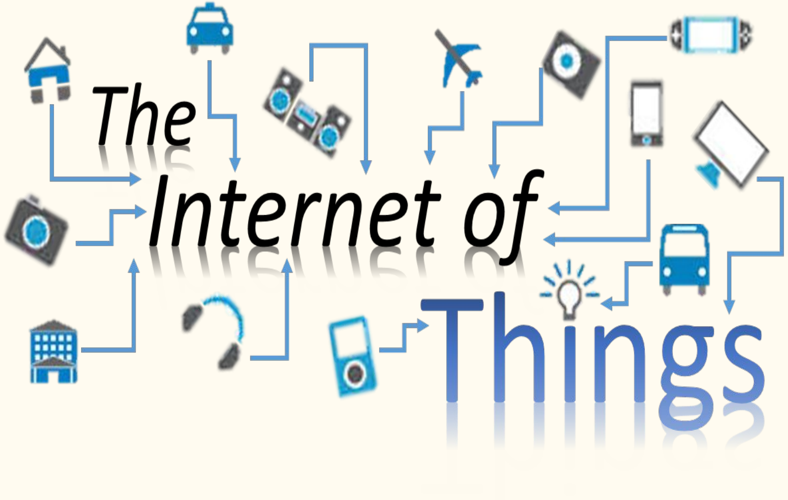
IoT Security

By: Risheed Malatombee, Julian Park, Wook Cho

What is IoT and IoT Devices?

"The Internet of Things (IoT) refers to the billions of physical devices connected to the internet, collecting and sharing data"

- IoT devices are components of :
  - Information Technology (IT)
  - Operational Technology (OT)
- Explicitly, IoT devices are a convergence of :
  - cloud computing
  - mobile computing
  - embedded systems
  - big data
  - low-price hardware
  - other technological advances



"There are about 7 billion internet-connected devices"

Applicability of IoT devices

- IoT devices can be applied to every sector, namely:
  - Transportation
  - Healthcare
  - Office work
- As consumers, we use IoT devices sometimes unknowingly, namely:
  - Kitchen appliances
  - Thermostats
  - Home security cameras
  - Door locks
  - Light bulbs
- All of these components help to make up a “smart” environment!

IoT Device Privacy Risks

- **Protect device security:**
  - Prevent a device from being used to conduct attacks.
- **Protect data security:**
  - Protect the confidentiality, integrity, and availability of data.
- **Protect individuals' privacy:**
  - Protect individuals' privacy impacted by PII processing beyond risks managed through device and data security protection.

Challenges associated to IoT security

- Understand the IoT device risk considerations to mitigating privacy risks.

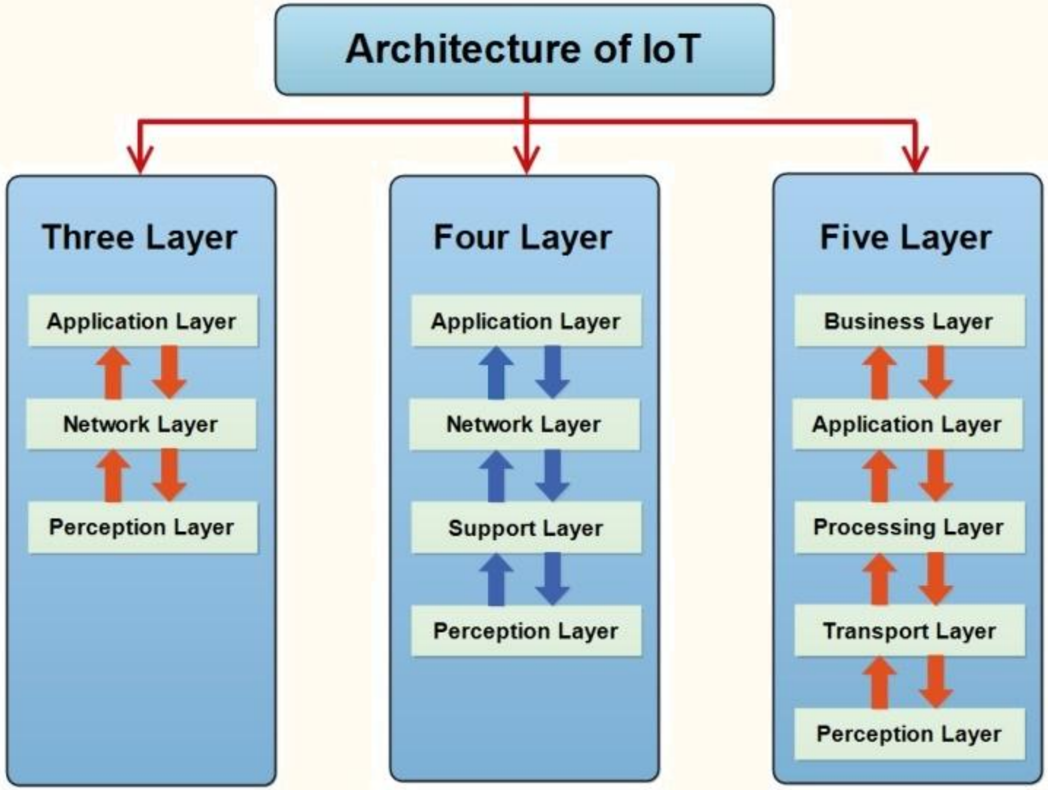
- Adjust organizational policies to address the privacy risk mitigation challenges.

- Implement updated mitigation practices.

Standard IoT Architecture layer & Protocol

Technical challenges in applying TCP/IP to the IoT environment

- Power constraint
- Mesh network
- scalable routing mechanism
- reliable and in-order byte stream delivery
- Security

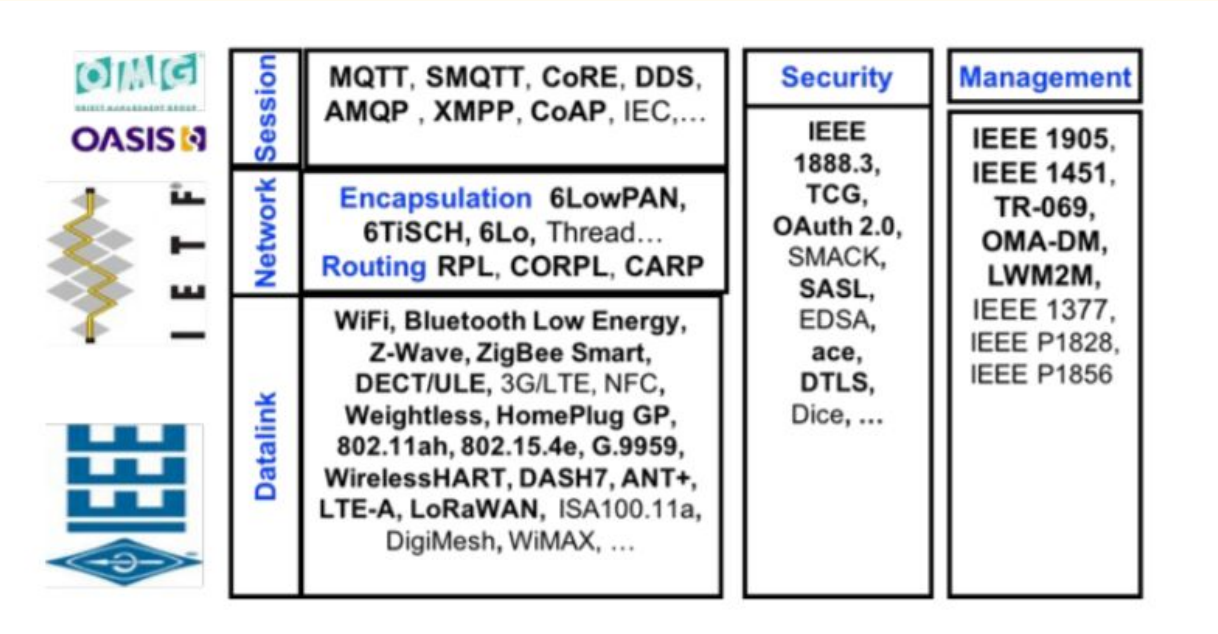


Common Security Threat and Problem

Business Layer	● Business Logic Attack ● Zero Day Attack	
Application Layer	● Cross site Scripting ● Malicious Code Attack	● The ability of dealing with Mass Data
Processing Layer	● Exhaustion ● Malware	
Transport (Network) Layer	● DoS attack ● Man-in-The-Middle (MiTM) Attack ● Storage Attack	
Perception Layer	● Eavesdropping ● Node Capture ● Timing Attack	● Replay Attack ● Fake Node and Malicious

IoT Protocols

- Mobility
- Reliability
- Scalability
- Management
- Availability
- Interoperability
- Cost and complexity
- Power harvesting



Session
MQTT, SMQTT, CoRE, DDS, AMQP , XMPP, CoAP, IEC,...

Network
Encapsulation 6LowPAN, 6TiSCH, 6Lo, Thread...
Routing RPL, CORPL, CARP

Datalink
WiFi, Bluetooth Low Energy, Z-Wave, ZigBee Smart, DECT/ULE, 3G/LTE, NFC, Weightless, HomePlug GP, 802.11ah, 802.15.4e, G.9959, WirelessHART, DASH7, ANT+, LTE-A, LoRaWAN, ISA100.11a, DigiMesh, WiMAX, ...

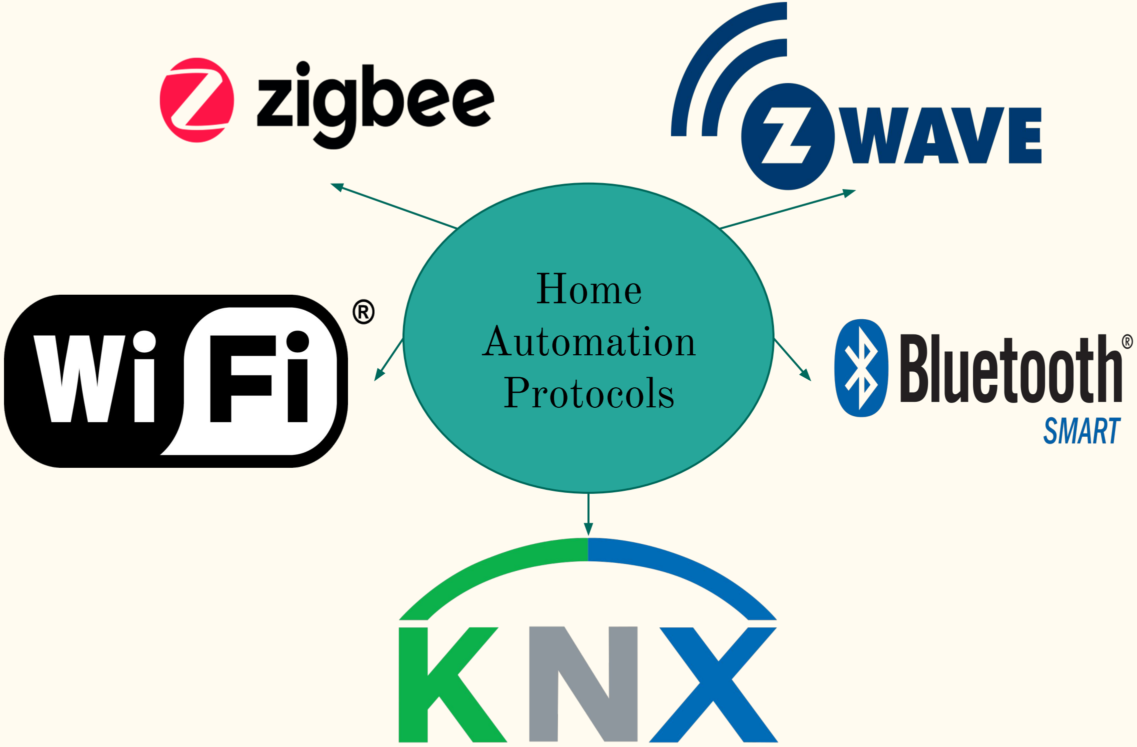
Security
IEEE 1888.3, TCG, OAuth 2.0, SMACK, SASL, EDSA, ace, DTLS, Dice, ...

Management
IEEE 1905, IEEE 1451, TR-069, OMA-DM, LWM2M, IEEE 1377, IEEE P1828, IEEE P1856

Most popular Smart Home Protocols

Aspects consistent with Smart Home Protocols:

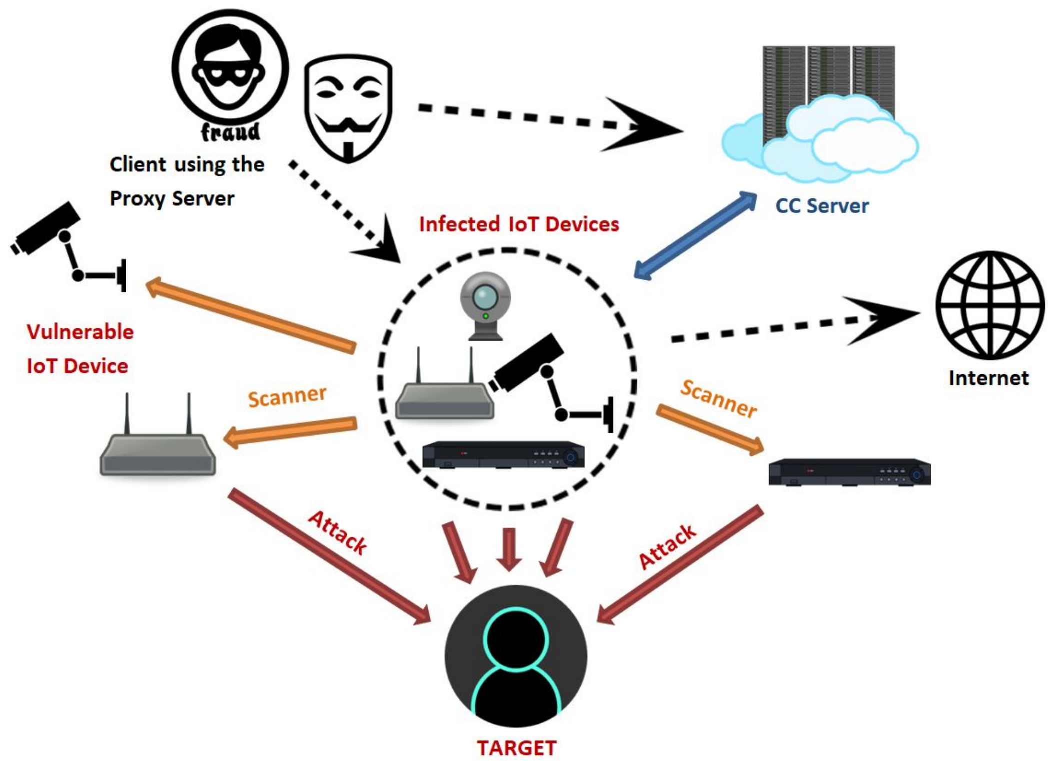
- Low Power
- Low-Cost
- Mesh Network
- Decentralized
- Flexible network



Home Automation Protocols

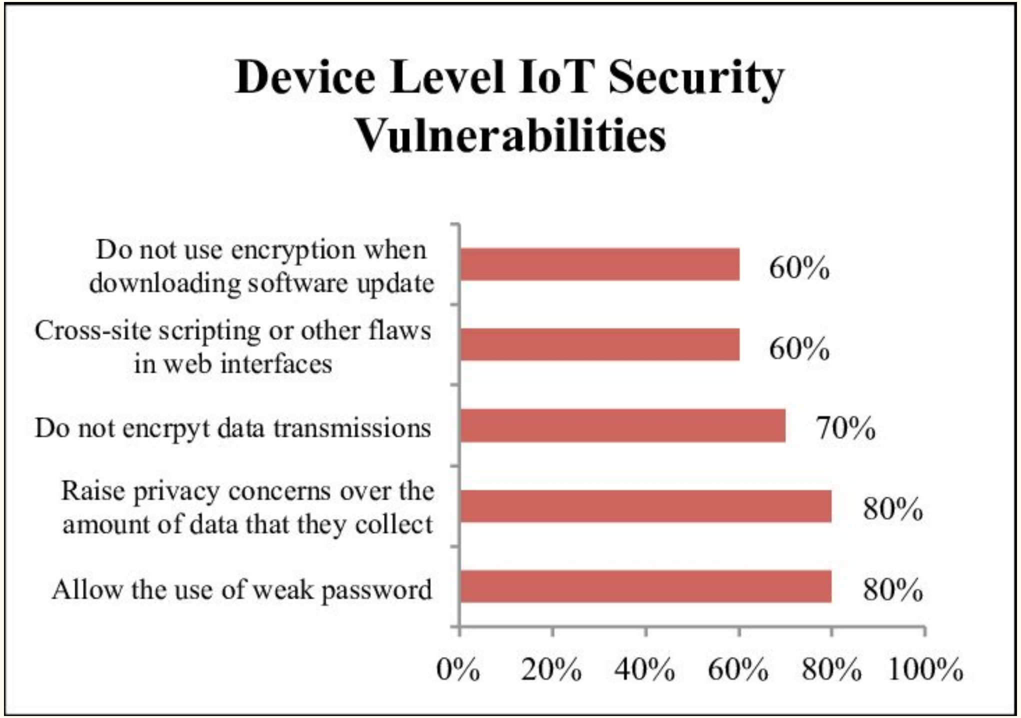
Mirai Botnet DDoS attack on IoT Devices

- Mirai: Malware(Trojan)
- Botnet: Malware infected Internet Connected Computers
- Distributed Denial-of-Service: Malicious attack on target by disruption normal traffic



Vulnerabilities of IoT Devices

- Lack of computing power due to size
- Default factory setting not changed by users
- Weak authentication technique
- Difficult in updating the software



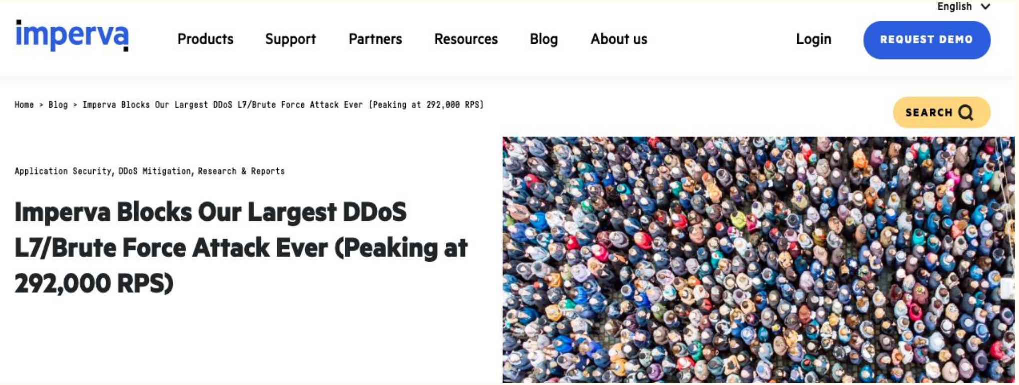
Mirai Botnet DDoS on IoT Devices(Case Study)

- Lasted 13 days : Apr 23, 2019 - May 5, 2019

- Search for open Telnet port, using set of default password combinations

- Peak flow: 292,000 RPS(Requests per Second)

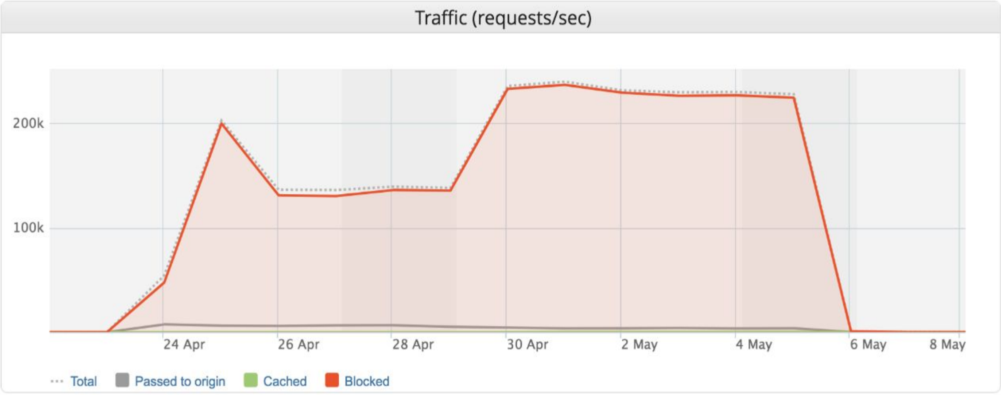
- 402,000 different IP addresses



Home > Blog > Imperva Blocks Our Largest DDoS L7/Brute Force Attack Ever (Peaking at 292,000 RPS)

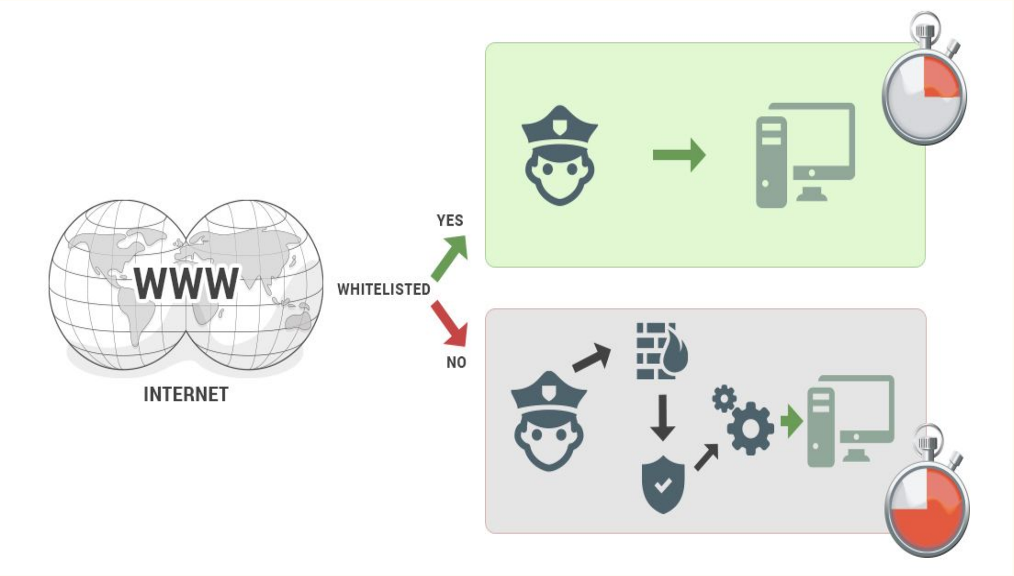
Application Security, DDoS Mitigation, Research & Reports

Imperva Blocks Our Largest DDoS L7/Brute Force Attack Ever (Peaking at 292,000 RPS)



Possible Solutions

- Change default setting (change password, etc.)
- Set up firewalls
- Whitelisting: only authorized applications can be accepted. Block unauthorized applications



Questions

What are the 3 kind of risks that are imposed on IoT devices?

What kind of common security threats does perception layer (sensors) pose?

What's one of IoT devices' vulnerabilities for Mirai Botnet DDoS attack?

Bibliography

https://techjury.net/blog/how-many-iot-devices-are-there/

https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8228.pdf

https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8371556

https://www.fortinet.com/blog/threat-research/omg--mirai-based-bot-turns-iot-devices-into-proxy-servers.html

https://www.cloudflare.com/learning/ddos/glossary/mirai-botnet

Gamundani, Attlee & Phillips, Amelia & Muyingi, Hippolyte. (2018). An Overview of Potential Authentication Threats and Attacks on Internet of Things(IoT): A Focus on Smart Home Applications. 10.1109/Cybermatics_2018.2018.00043.

T. S. Gopal, M. Meerolla, G. Jyostna, P. Reddy Lakshmi Eswari and E. Magesh, "Mitigating Mirai Malware Spreading in IoT Environment," 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Bangalore, 2018, pp. 2226-2230. doi: 10.1109/ICACCI.2018.8554643
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8554643&isnumber=8554361

Bibliography

https://www.bankinfosecurity.com/massive-botnet-attack-used-more-than-400000-iot-devices-a-12841

T. S. Gopal, M. Meerolla, G. Jyostna, P. Reddy Lakshmi Eswari and E. Magesh, "Mitigating Mirai Malware Spreading in IoT Environment," 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Bangalore, 2018, pp. 2226-2230.doi: 10.1109/ICACCI.2018.8554643
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8554643&isnumber=8554361

https://securebox.comodo.com/whitelisted/

Burhan, Muhammad et al. "IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey." Sensors (Basel, Switzerland) vol. 18,9 2796. 24 Aug. 2018, doi:10.3390/s18092796

Ramya, T. and K. Anitha. "Challenges in IoT Networking via TCP / IP Architecture." (2017).

Pallavi Sethi and Smruti R. Sarangi, "Internet of Things: Architectures, Protocols, and Applications," Journal of Electrical and Computer Engineering, vol. 2017, Article ID 9324035, 25 pages, 2017. https://doi.org/10.1155/2017/9324035.

Salman, T., & Jain, R. (2017). A survey of protocols and standards for internet of things. Advanced Computing and Communications, 1(1), 1–20.