# Project 1 Network security for IOT devices

1. Problem statement

First of all, what are IOT devices? From Wikipedia we get a statement as follows: “The Internet of Things (IoT) describes physical objects (or groups of such objects), that are embedded with sensors, processing ability, software, and other technologies, and that connect and exchange data with other devices and systems over the Internet or other communications networks.” In a word, anything that could connect to the internet can be regard as IOT device, for example: smartphones, smart home, and smart cars…… And the variety kinds of IOT devices are mostly divided into consumer, commercial, industrial, and infrastructure spaces.

After defining IOT, we want to know why its network security matters. The IoT paradigm has experienced immense growth in the past decade, with billions of devices connected to the Internet. It’s quite obvious that the safety of such huge number of devices need to be guaranteed, imagine when everything around us is connected to the internet without any protection and completely exposed to attack, your door can be easily cracked and all your private documents can be accessed by hackers, such harmfulness could be even worth than crime in the real world. So, with the development of IOT, the corresponding protection and detection methods of IOT network security should also be placed in the center of our view.

1. Applications

As mentioned above, IOT devices are mostly divided into consumer, commercial, industrial, and infrastructure spaces, I’ll show applications from each of these areas. For example, smart homes make it convenient to control devices at home remotely or automatically, including lighting, heating and air conditioning, media and security systems, and camera systems; Medical and healthcare also occupies an important position in IOT, The Internet of Medical Things (IoMT) is an application of the IoT for medical and health related purposes, data collection and analysis for research, and monitoring. IOT also helps a lot for agriculture in many ways: collecting data on temperature, rainfall, humidity, wind speed, pest infestation, and soil content. One more example for infrastructure applications is metropolitan scale deployments. There are several planned or ongoing large-scale deployments of the IoT, to enable better management of cities and systems like parking management, improving water and air quality, digital city agenda...

A large number of IOT applications have been used in various purpose to create a better environment for us, more and more IOT devices will be occupying an increasingly important part in our lives. Correspondingly, network security applications of IOT devices are also under development.

For example the IBM provides the X-force Red offensive security service as a solution, it provides a global teams of hackers to break into organizations and uncover risky vulnerabilities that attackers may use for personal gain. The Xage security gives your users OT access from any device in any location. Block attacks against unterminated desktop and OT protocols, vulnerable jump boxes, VPN exploits, ill-managed workstation accounts, insecure passwords and open firewall ports. There are also other kinds of firewalls, safety manager applications from IT companies helps you defending network attacks.

1. Interested area of topic

For me, the infinity possibility of IOT devices is really attractive, however without powerful enough security measures, all the advantages and convenience it brings could be relatively harmful. I remember in the movie “the Terminators”, in the future when everything is connected to the internet and become IOT devices, including military equipment, than once we lost control to those devices the consequences can be devastating. So I want to mostly focus on the security applications part in this project.

1. Literature review

Internet of Things is considered as the third industrial revolution. Nowadays, IOT objects are used almost in all fields, there’s no doubt about the importance of IOT. Whats more, the potential danger exposed by these smart devices are not only affect the security of IoT systems, but also the complete eco-system including Web-sites, applications, social networks and servers. Consequently, we should pay more attention to study and analyze how to defend attacks towards IOT.

Several approached have been proposed by companies and researchers for network security of IOT. F. Chen *et al* reviewed data mining (DM) for IoT in knowledge, technique and application points of view[1]. The authors study big data algorithms and challenges when deployed in IoT environment. Tsai *et al* survey both, features of data for IoT and features for data mining for IoT with a discussion about changes, potentials, open issues, and future trends[2]. However, Cui *et al*. provide an overview of the application of machine learning in IoT domain[3]. This survey is very concentrates on progresses in machine learning techniques for IoT applications. Finally, Mahdavinejad *et a*l. present a taxonomy of machine learning algorithms while discussing how they can be applied to the data in order to extract higher level information[4].

1. Open-source resource

For online open-source resources, I mostly focus on a github project called PENIOT, which is basically a penetration testing tool for Internet of Things (IoT) devices. It helps you to test/penetrate your devices by targeting their internet connectivity with different types of security attacks. In other words, you can expose your device to both active and passive security attacks.

One thing that come into attention is that its extensibility, it’s now supporting: Advanced Message Queuing Protocol, Bluetooth low energy, Constraint Application Protocol, and Message Queuing Telemetry Transport four protocols, however you can extend already existing protocols with your newly implemented attacks.

This license is listed under the MIT license: A short and simple permissive license with conditions only requiring preservation of copyright and license notices. Licensed works, modifications, and larger works may be distributed under different terms and without source code.Basically, you can do whatever you want as long as you include the original copyright and license notice in any copy of the software /source. I think this kind of licence are easy for our further use and research

As for the participants of this project: Berat Cankar,Bilgehan Bingöl,Doğukan Çavdaroğlu, Ebru Çelebi and is supervised by Pelin Angın.

1. Reference

[1]F. Chen et al., “Data mining for the Internet of Things: Literature review and challenges,” Int. J. Distrib. Sensor Netw., vol. 11, no. 8, Aug. 2015, Art. no. 431047. [Online]. Available: https://doi.org/ 10.1155/2015/431047

[2] C.-W. Tsai, C.-F. Lai, M.-C. Chiang, and L.-T. Yang, “Data mining for Internet of Things: A survey,” IEEE Commun. Surveys Tuts., vol. 16, no. 1, pp. 77–97, 1st Quart., 2014.

[3] L. Cui et al., “A survey on application of machine learning for Internet of Things,” Int. J. Mach. Learn. Cybern., vol. 9, no. 8, pp. 1399–1417, Aug. 2018. [Online]. Available: https://doi.org/10.1007/s13042-018- 0834-5

[4] M. S. Mahdavinejad et al., “Machine learning for Internet of Things data analysis: A survey,” Digit. Commun. Netw., vol. 4, no. 3, pp. 161–175, Aug. 2018. [Online]. Available: http://www.sciencedirect. com/science/article/pii/S235286481730247X

Github:https://github.com/yakuza8/peniot

Wikipedia:https://en.wikipedia.org/wiki/Internet\_of\_things