Analysing Smart Home Security Using Packet Tracer Simulation Software

Nur Najihah Abdul Aziz , Rizzo Mungka Anak Rechie , Batrisyia B Mohd Bakry,
Ruhani AB. Rahman, Yusnani Mohd Yussoff
College of Engineering
University Technology MARA (UiTM)
Shah Alam, Selangor, Malaysia.
yusna233@uitm.edu.my

2021 IEEE 11th IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE) | 978-1-6654-0338-2/21/$31.00 ©2021 IEEE | DOI: 10.1109/ISCAIE51753.2021.9431781

Abstract* – The advancement in the Internet of Things for electronic devices and applications has attracted people, especially younger generations, to move into the interconnected world. A smart home is an example of an application that is highly in demand. Together with the rise is cybersecurity issues. By being connected, many users are exposed to security threats without their knowledge. This paper presents a security analysis on the smart home environment using Packet Tracer Simulation Software. A testbed of a basic smart home set consisting of electronic appliances, gadgets, and surveillance system is set up in the Cisco Packet Tracer software version 7.1. Possible vulnerabilities issues were simulated at the network and application layers. The vulnerabilities and possible attacks on the smart home network environment were successfully identified. Mitigation techniques on the attack were proposed to reduce the probability of the network attacks. *Keywords- Internet of Things, security, Packet Tracer

I. INTRODUCTION

Over the years, the use of IoT devices has been varying and increasing. Gartner, Inc. forecasts that "the enterprise and automotive Internet of Things (IoT) market will grow to 5.8 billion endpoints in 2020, a 21% increase from 2019" [1]. Furthermore, according to Joe O'Halloran in the Computer Weekly article, dated 3rd November 2020, the industrial IoT sectors will reach 37 billion in 2025 [2]. In 2020, over 50 billion devices are connected to the internet [3]. These are some related articles that show the future trend and demand for IoT applications. The significant increase of IoT applications is contributed by the advancement of wireless technology, including cellular and satellite technology. It is undeniable that the COVID-19 lockdown has disrupted the investments in the Internet of Things. However, a larger number are planning to increase their investment in IoT implementations to reduce the operating costs [2].

The rebranding of Wireless Sensor Network to the Internet of Things has accelerated and widened the range of interconnected applications. IoT applications nowadays are very broad, ranging from the shortest wireless range such as in personal area networks to the longest wireless range which is in the wide-area networks. The applications now cover all aspects of our life. The benefits from IoT can be the internal and external focus. Examples of internal or direct focus are safety and security improvement in the factory, asset optimization, expenses reduction, and resources conservation. On the other hand, the external benefits of IoT can be improving well-being through integrated and online health management systems, service enhancement by specific authorities, and increased engagement in society.

According to the analysis done and published by iot-analytics.com [4], the highest IoT applications currently is in the area of industrial or manufacturing. This is followed by transportation, energy, retail, and healthcare. Furthermore, there is 620 IoT platform available in 2019 to support the users with AWS and Azure being the top spots [4].

Despite the advantages of IoT applications and the readiness of technology to support IoT advancement, security issues are one of the important challenges that developers have to consider. As more people are digitally connected, users become more vulnerable to cyber threats [6]. It is easier to exploit and manipulate data that is exchanged over the internet as the connectivity increases. As stated by the World Economic Forum (WEF), cyber-attacks need to be addressed as a global risk and are ranked at the 5th place for threat and 7th place for impact in the WEF top 10 Global Risks [7]. It can be said that as more Internet of Things (IoT) devices are connected to the Internet, cyber threats increases. This is due to the unavailability of common security standards addressing the security issues in IoT devices [8].

IoT architecture can be presented in the form of layers. The basic three layers consisting of perception layers consisting of sensors and actuators. Network layer that connects the devices through routers and gateways and finally the application layer that consists of cloud or servers and serve as the interface to the users. Understanding the details of each layer is very important in securing the IoT applications as threats can exist in every single layer due to the vulnerabilities.

This paper will first discuss on the security issues in the IoT applications focusing on smart homes network. The methodology section will then present the work conducted to identify vulnerabilities in the smart home using packet tracer

Authorized licensed use limited to: American International University Bangladesh. Downloaded on December 30,2024 at 06:15:13 UTC from IEEE Xplore. Restrictions apply.

simulation software. Following that, the result section will discuss the attacks found followed by the proposed mitigation technique.

II. IoT Security Issues

As mentioned in the introduction section, security issues in IoT applications exist at every layer in IoT architecture. Figure 1 depicts the three basic layers in IoT architecture.

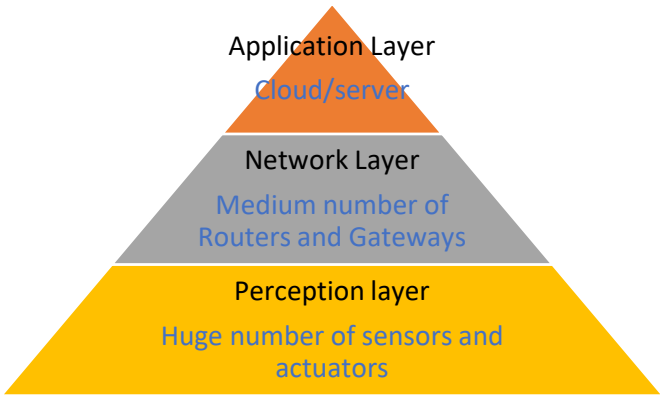


Fig 1. Layers in IoT Architecture

A. Perception Layer

The perception layer consists of sensors and actuators connected to a specific location or place. Depending on the applications, the number of devices can vary from below 10 to millions of connected devices. For smart home applications, these sensors include a camera for a surveillance system, Home Digital Voice Assistant (HDVA) such as Alexa and echo dot, entrance system, temperature and humidity sensors, and finally electrical appliances such as light, fan, television, and few more. Few articles have discussed the security issues on the HDVA that is gaining popularity [9-18]. Vulnerabilities at this layer basically lie at the hardware design and will not be covered in this paper.

B. Network layer

One of the vulnerabilities that exist in the smart home network is through a gateway. A simulation study conducted by a group of a researcher using few network analysis tools such as Wireshark, Cain & Abel and NetworkMiner based on Kampung Wi-Fi network has shown the vulnerability of the gateway that enables attackers to further conduct another attack such as brute-force and identify open ports on the network [19]. Home router and gateway is also vulnerable to authentication and password attack especially when the owners are using default device password and never change the password for a long time after sharing it with visitors. Considering the two types of attacks which are service interruption and information gathering, the impact of the second type of attack is much brutal compared to the first. Information gathering attacks will lead to a far more serious consequence where the attacker might be able to get into the house network and expose the privacy of the homeowner.

C. Application Layer

Another source of vulnerabilities is cloud servers and mobile devices that are used to remote control and monitor the home. Communication between mobile apps, servers, and sensors increases the security challenges [20]. Mobile apps are directly exposed to the public network, which makes it one of the vulnerable points for the smart home system. Therefore, the encryption for outbound and inbound of sensitive data flows in and out of the app is very crucial. DDOS attacks, Man-In-The-Middle (MITM) attacks, session hijacking are examples of attacks at the application layer.

D. Cisco Packet Tracer

Packet Tracer has been used widely by instructors and students in teaching and learning networking related courses. Cisco Packet Tracer version 7.2 comes with IoT functionalities that allow user to configure IoT devices and simulate IoT automation on this software [21]. In the same release, a low-level IoT simulation using Single Board Computer (SBC) and sensors were provided. Smart devices, sensors, actuators, and microcontrollers are included in this software. Smart devices are devices to connect via wired or wireless technology which can be used to quickly set up the behavior manually in the packet tracer tab. The sensors include intelligent lighting systems, air-conditioning systems, coffee makers, alarms, RFID, and a wide range of other sensors, such as carbon dioxide, humidity, temperature, water level sensors, etc.

The following section presents the steps involved in the development of the smart home applications and analysis on the vulnerabilities that exist in the smart home network using packet tracer simulation software.

III. Methodology

This section presents a smart home development using packet tracer tools. A smart home network consisting of smart devices, routers, gateway, remote user and cloud services are designed and configured to imitate real smart home services that allow remote monitoring and automation.

Figure 2 presents the overall diagram of the smart home implemented in packet tracer software. The design consisting of few smart home devices such as light, fan, garage, alarm, RFID and few more devices. All the devices were then linked to the wireless router installed in the accessible range in the house. The router is connected to the gateway and linked to the internet that consist of servers and cloud storage. In general, the design can be classified into four sections which are sensors and actuators, router and gateway, cloud service provider and finally user interfaces that allow remote monitoring and controlling of the smart home. This design is consistent with the three-layer IoT architecture concept presented in section 2.

Authorized licensed use limited to: American International University Bangladesh. Downloaded on December 30,2024 at 06:15:13 UTC from IEEE Xplore. Restrictions apply.

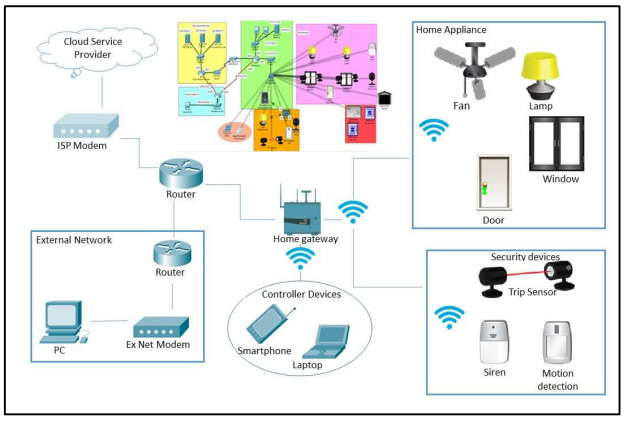
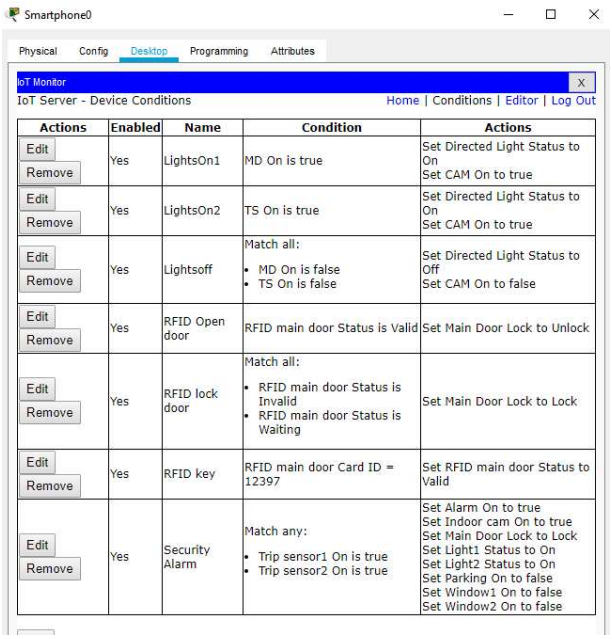


Fig 2. Smart home network

Following the design, all devices need to be configured properly. Fig.3 tabulates the pre-set conditions that are available in the packet tracer tools. As an example, there are four conditions set, which is MD (motion detection) is True, TS (trip sensor) is True, RFID information is Valid and Security alarm is True.



Actions	Enabled	Name	Condition	Actions
Edit Remove	Yes	LightsOn1	MD On is true	Set Directed Light Status to On Set CAM On to true
Edit Remove	Yes	LightsOn2	TS On is true	Set Directed Light Status to On Set CAM On to true
Edit Remove	Yes	Lightsoff	Match all: • MD On is false • TS On is false	Set Directed Light Status to Off Set CAM On to false
Edit Remove	Yes	RFID Open door	RFID main door Status is Valid	Set Main Door Lock to Unlock
Edit Remove	Yes	RFID lock door	Match all: • RFID main door Status is Invalid • RFID main door Status is Waiting	Set Main Door Lock to Lock
Edit Remove	Yes	RFID key	RFID main door Card ID = 12397	Set RFID main door Status to Valid
Edit Remove	Yes	Security Alarm	Match any: • Trip sensor1 On is true • Trip sensor2 On is true	Set Alarm On to true Set Indoor cam On to true Set Main Door Lock to Lock Set Light1 Status to On Set Light2 Status to On Set Parking On to false Set Window1 On to false Set Window2 On to false

Fig 3. Pre-set condition for smart home

A. *Gateway layer*

The smart home requires internet access to allow real time remote monitoring and automation. The smart things layer is linked to the gateway to support the automation packages. Gateway transfers these data via Wi-Fi (IEEE802.11n) to the cloud layer from the smart things layer. The Cisco switch (2960-24TT) connects the wired connection from the smart home gateway through the fast ethernet cable. The PT modem is used for the Internet communication of the home network. The Internet Service Provider (ISP) router takes the IP address of the getaways layer via DHCP service configuration. Figure 3 depicts the connection to the gateway through wireless router from the smart home. The switches and personal computer attached is for the purpose of analysing the complexity of the smart home network. However, detailed configuration is not going to be discussed in this paper.

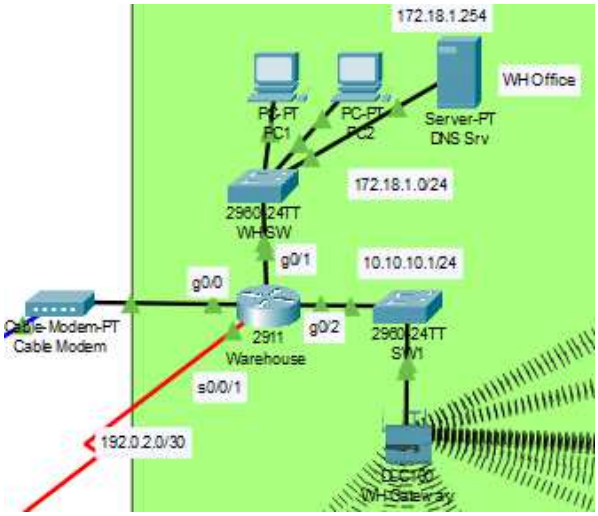


Fig 4. Connection on Gateway Layer

B. *Cloud Service Provider Layer*

All information about the smart things is stored at this layer in the registration server. This layer will be the most crucial layer for researchers to add network security services. Access control list was configured to restrict traffic between the lab IoT devices and the cloud service provider. Without ACL, any traffic is allowed to enter and exit, making it more vulnerable to unwanted and dangerous traffic. To make sure the web communication is secure, HTTPS protocol is used as a security measure.

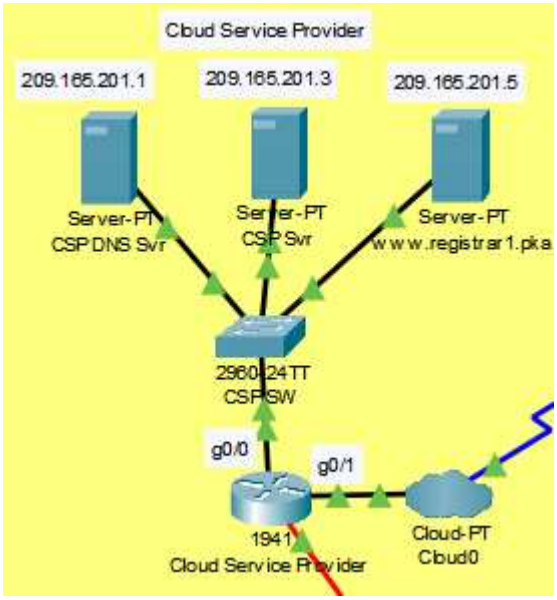


Fig 5. Cloud service provider layer

Authorized licensed use limited to: American International University Bangladesh. Downloaded on December 30,2024 at 06:15:13 UTC from IEEE Xplore. Restrictions apply.

C. End-User

Finally, remote users were set up to simulate remote monitoring. Any smart device such as tablet, laptop, and smartphone are configured with detailed information such as username and password to the home network. In this implementation, only a laptop and a smartphone are used.

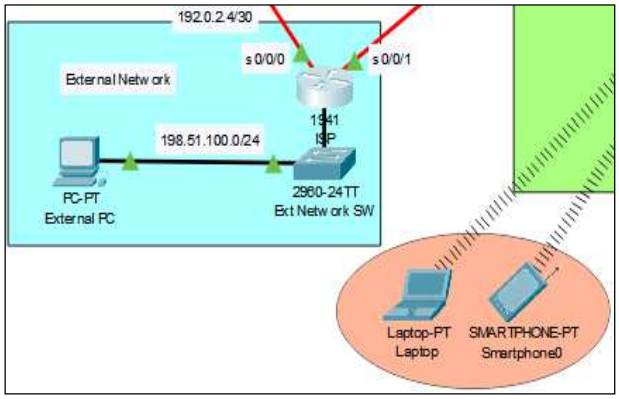


Fig 6. End-devices

IV. Result and Analysis

Analysis of the vulnerability was done using tcpdump and Wireshark software. The tcpdump will capture the packets traversing through the network and the results were screened out on Wireshark. Figure 7 shows the data that was captured when the user login to the internet server. Since the transmission is not encrypted, the packet tracer was able to view the username and password entered by the user. This attack is known as a spoofing attack and can easily be done by an amateur attacker. This type of attack is possible if the attacker managed to get into the home network using a valid username and password. Once the attacker gets the username and password, they will try it on another valuable websites such as banking. If they are lucky, they will successfully transfer the money.

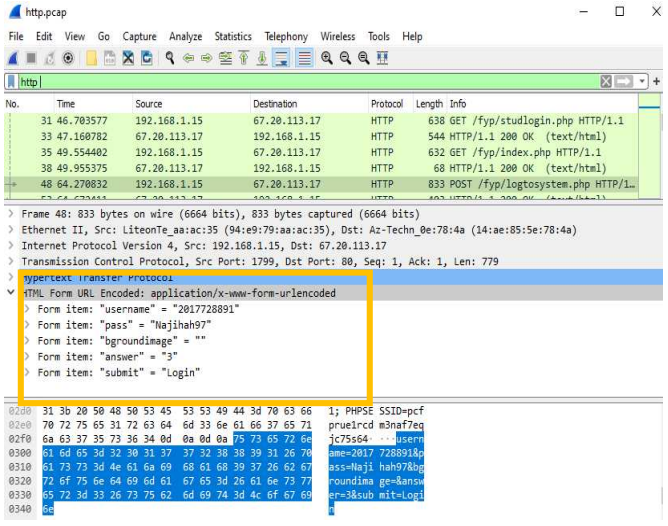


Fig 7. Vulnerabilities in the HTTP protocol

The easiest way to mitigate this type of attack is by closing the http port shows in figure 8. However, this might not be a practical method. In real life, users from the smart home still need to access the http website.

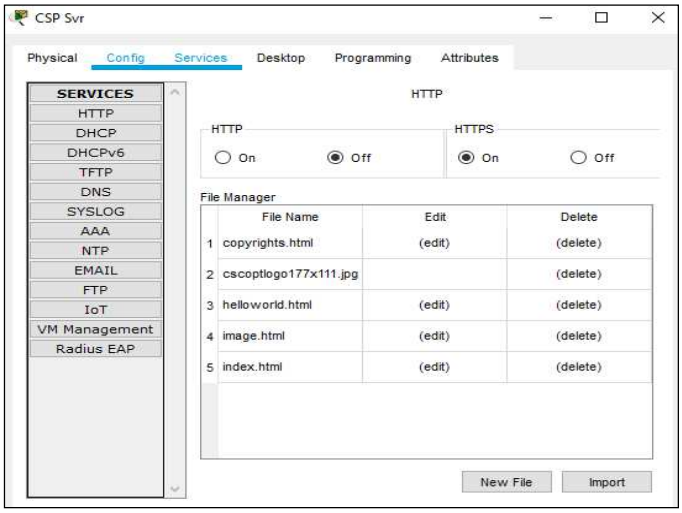


Fig 8. HTTP port off

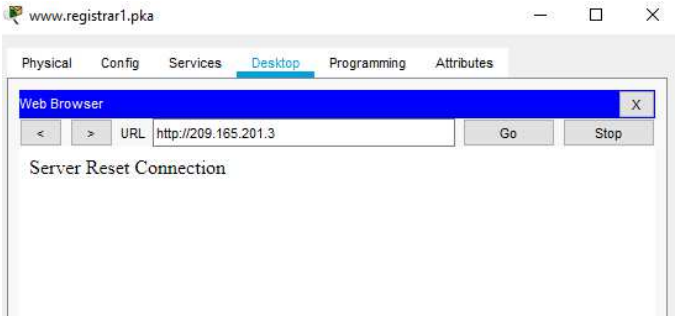


Fig 9. Server cannot reach the web using HTTP protocol

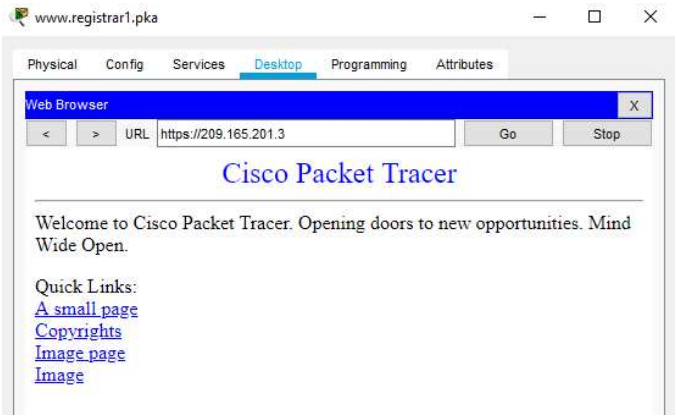


Fig 10. server can reach the web through HTTPS protocol

Figure 9 and Figure 10 show the result when the HTTP port is closed and the HTTPS port opens in the packet tracer. Figure 11 shows the output of using the HTTPS protocol, which is the data entered by the user were in encrypted data. The username and password are no longer visible.

Authorized licensed use limited to: American International University Bangladesh. Downloaded on December 30,2024 at 06:15:13 UTC from IEEE Xplore. Restrictions apply.

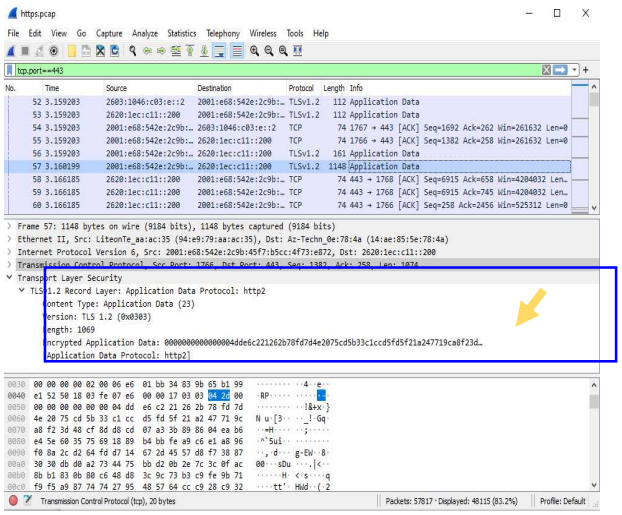


Fig 11. Encrypted application data using HTTPS protocol

Figure 12 shows the smart things that were connected to the IoT server. Any devices that can reach this IoT server can change the condition set. As mentioned earlier. System disruption is another possible type of attack. Although it does not expose the user credentials, it will disrupt the smart home services. Imagine, a remote user was not able to control his house due to system interruption. If the surveillance system was interupted, the user might not be able to ensure the safety of his house.

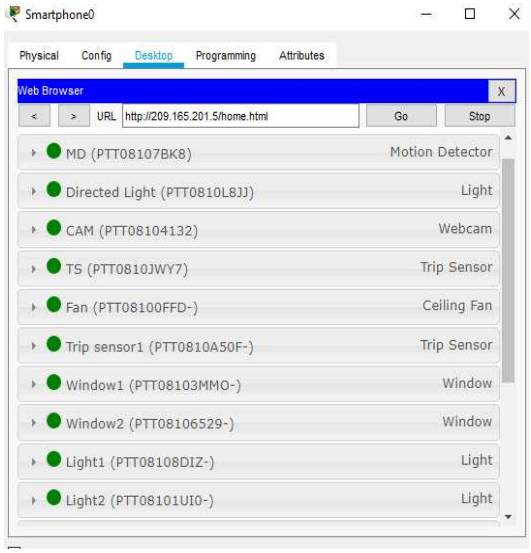


Fig 12. Things connected to the IoT server

An example of the above attack is DoS attacks. It is growing stronger and sophisticated. This attack will happen when hackers are able to flood an IP address with hundreds or thousands of messages that lead to system disruption.

To mitigate this attack, Access Control List protocol was used to filter the incoming and outgoing traffic. All the traffic flowing through the home network will be compared with the ACL statement which will either block or allow. In these cases, the external network had been blocked to enter the IoT devices server to avoid overload traffic. Figure 13 shows the traffic from the external network that had been blocked and cannot reach the IoT server.

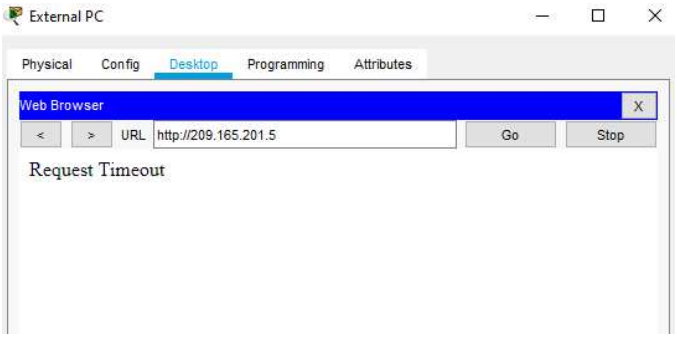


Fig 13. External PC cannot reach the server

Only some remote device that were allowed to reach the IoT device Server as shown in figure 12.

Fig 14. smartphone allows to reach the IoT server

V. Conclusion

In conclusion, the demand for IoT applications will continue to grow with the advancement in wireless technology and smart devices. Together with AI and data analytic technology, the development of IoT applications will significantly increase. However, the security issues will be high and the effects on users and the company should not be underestimated. The design of IoT applications should consider security features from the very beginning which is at the perception layer. This paper has proved the existence of vulnerabilities at the network and application layers. There are many other types of attacks that can be demonstrated and analysed using packet tracer simulation software. An Access Control List is a practical solution in securing home network. Besides preventing DOS attack, it can act as a firewall to the network. As COVID-19 shows no sign of declining, the outcome from this work will indirectly contribute to the teaching and learning activities in the networking and security class. Students will be able to design, configure, simulate the IoT network and analyse the security issues in the network as in the real environment.

ACKNOWLEDGMENT

The authors of this paper would like to acknowledge and thank School of Electrical Engineering, College of Engineering, Universiti Teknologi Mara for supporting this research work.

Authorized licensed use limited to: American International University Bangladesh. Downloaded on December 30,2024 at 06:15:13 UTC from IEEE Xplore. Restrictions apply.

REFERENCES

[1] Gartner, "Gartner Says 5.8 Billion Enterprise and Automotive IoT Endpoints Will Be in Use in 2020," Gartner, 29 August 2019. [Online]. Available:https://www.gartner.com/en/newsroom/pressreleases/2019-08-29-gartner-says-5-8-billion-enterprise-and-automotive-io. [Accessed 3 February 2021].

[2] J. O'Halloran, "Industrial IoT connections to reach 37 billion by 2025," ComputerWeekly.com, 3 November 2020. [Online]. Available:https://www.computerweekly.com/news/252491495/Industrial-IoT-connections-to-reach-37-billion-by-2025. [Accessed 3 February 2021].

[3] McKinsey&Company, "The Internet of Things:Mapping the Value Beyond the Hype," McKinsey Global Institude , 2015.

[4] P. Scully, "Which are the hottest application areas for the Internet of Things right now?" IoT Analytics, 8 July 2020. [Online]. Available: https://iot-analytics.com/top-10-iot-applications-in-2020/. [Accessed 3 February 2021]

[5] M.Hung, Leading the IoT, Gartner; https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf. . [Accessed 3 February 2021

[6] F. Meneghello, M. Calore, D. Zucchetto, M. Polese and A. Zanella, "IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices," in IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8182-8201, Oct. 2019, doi: 10.1109/JIOT.2019.2935189.

[7] S. Shiaeles, N. Kolokotronis and E. Bellini, "IoT Vulnerability Data Crawling and Analysis," 2019 IEEE World Congress on Services (SERVICES), Milan, Italy, 2019, pp. 78-83, doi: 10.1109/SERVICES.2019.00028.

[8] A. Shakdher, S. Agrawal and B. Yang, "Security Vulnerabilities in Consumer IoT Applications," 2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS), Washington, DC, USA, 2019, pp. 1-6, doi: 10.1109/BigDataSecurity-HPSC-IDS.2019.00012

[9] X. Lei, G. H. Tu, A. X. Liu, C. Y. Li, and T. Xie, "The insecurity of home digital voice assistants - Vulnerabilities, attacks and countermeasures," 2018 IEEE Conf. Commun. Netw. Secur. CNS 2018, pp. 1–9, 2018, doi: 10.1109/CNS.2018.8433167.

[10] W. Haack, M. Severance, M. Wallace, and J. Wohlwend, "Security Analysis of the Amazon Echo," Massachusetts Inst. Technol., pp. 1–14, 2017.

[11] D. Overstreet, H. Wimmer, and A. T. Modeling, "Penetration Testing of the Amazon Echo Digital Voice Assistant Using a Denial-of-Service Attack," 2019 SoutheastCon, pp. 1–6, 2019.

[12] R. Leong, "Analyzing the Privacy Attack Landscape for Amazon Alexa Devices," p. 13, 2018.

[13] I. Clinton, L. Cook, and S. Banik, "A Survey of Various Methods for Analyzing the Amazon Echo," 2016.

[14] A. Alhadlaq, J. Tang, A. Korolova, and M. Almaymoni, "Privacy in the Amazon Alexa Skills Ecosystem," 2015.

[15] W. Diao, X. Liu, Z. Zhou, and K. Zhang, "Your voice assistant is mine: How to abuse speakers to steal information and control your phone," Proc. ACM Conf. Comput. Commun. Secur., vol. 2014-Novem, no. November, pp. 63–74, 2014, doi: 10.1145/2666620.2666623.

[16] N. Zhang, X. Mi, X. Feng, X. Wang, Y. Tian, and F. Qian, "Dangerous skills: Understanding and mitigating security risks of voice-controlled third-party functions on virtual personal assistant systems," Proc. - IEEE Symp. Secur. Priv., vol. 2019-May, pp. 1381–1396, 2019, doi: 10.1109/SP.2019.00016.

[17] H. Feng, K. Fawaz, and K. G. Shin, "Continuous authentication for voice assistants," Proc. Annu. Int. Conf. Mob. Comput. Networking, MOBICOM, vol. Part F1312, pp. 343–355, 2017, doi: 10.1145/3117811.3117823

[18] G. Cho, J. Choi, H. Kim, S. Hyun, and J. Ryoo, "Threat modeling and analysis of voice assistant applications," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 11402 LNCS, pp. 197–209, 2019, doi: 10.1007/978-3-030-17982-3_16.

[19] S. Fahmy, A. Nasir, and N. Shamsuddin, "Wireless network attack: Raising the awareness of Kampung WiFi residents," 2012 Int. Conf. Comput. Inf. Sci. ICCIS 2012 - A Conf. World Eng. Sci. Technol. Congr. ESTCON 2012 - Conf. Proc., vol. 2, pp. 736–740, 2012, doi: 10.1109/ICCISci.2012.6297124.

[20] E. Ruiz, R. Avelar, and X. Wang, "Poster: Protecting remote controlling apps of smart-home-oriented IOT devices," Proc. - Int. Conf. Softw. Eng., pp. 212–213, 2018, doi: 10.1145/3183440.3195101.

[21] PacketTracerNetwork, "What's new in Cisco Packet Tracer 7.2?" Packet Tracer Network, 31 March 2018. [Online]. Available: https://www.packettracernetwork.com/features/packettracer-72-newfeatures.html. [Accessed 4 February 2021].

Authorized licensed use limited to: American International University Bangladesh. Downloaded on December 30,2024 at 06:15:13 UTC from IEEE Xplore. Restrictions apply.