Project Proposal: Internet-of-Things Hacking

Student Name: DHARMENDAR

Introduction:

(Beale, S.S. and Berris, P., 2017) internet of things system rapidly growing to meet the requirement of smart system, IOT internet enabled system which easily hacked by hacker, needs to improve the IOT system security and data confidentiality with more recursive manner. Since IOT system easily visible to smart phones and smart devices, IOT control house appliances, electronics controls and smart energy management system, various other industrial control applications exists, smart industrial system executes rapidly by implementation of IOT system. Since it has been investigated that hackers have control on car, aero planes, train and dams and some researcher suggest might be commercial flight is on risk, smart flight system also managed by IOT system by connectivity of smart passenger control with over the span of source to destination. Recent studies show that Twitter and Netflix data has been hacked and misused by hackers, computer crime act and cybercrime acts implement in these types of activities, but the issue is that hacker does not share their locations and IP address. (Serror, M., Hack, S., Henze, M., Schuba, M. and Wehrle, K., 2020.) Since IOT connected consumer devices, the industrial 4 revolution changed the system, so needs to secure the consumer IOT system as well as secure the industrial IOT system. Various challenges and issues exists in the development of security features in IOT system. This research going to present the state of the art solution to secure the IOT system at consumer level and industrial level. (Westerlund, O. and Asif, R., 2019),drone hacking with raspberry PI 3, drone system used for security purposes designed with IOT enabled system, drone easily crashed and hacked by opponents and hacker. Since WIFI enabled drone vulnerabilities captured easily and does not able to hide the WIFI system. These attacks happened in IOT system as follows:

IOT Hacking Attack:

1. Denial of service
2. Man in the middle attack
3. Untheorized root access
4. WIFI attack
5. Internet attack

Hacking Technique

10 common hacking technique, various hacker using various hacking technique to prevents hacking in IOT system. Simple hacking and complex hacking prevent both might be same time. Common hacking technique might be occurred such as Phishing DDOS, Clickjacking, hackers might be able to capture the personal data in an unauthorized way.

1. Bait & Switch

Using the bait and switch hacking method in which attacker buy advertising switches on websites, in which the user might be able to click on particular website ad, and might be able to redirect on the web page in which the infected and malware could be installed. Hackers can executes malware program in the IOT system which stop the internal working of system and disable sometime.

2. Cookie theft

Cookie store personal data in browser history, such as user name, password of IOT, once the hacker get to access to cookie which can unauthenticated himself on browser, most common hacking attack in which the IOT IP address easily captured by using the browser cookies technique, hacker enable the user IP packets to capture the IOT system, the cookie theft also recognized as session hijacking attack and sidejacking attack.

3. Clickjacking attack

Clickjacking attack which consider UI reader interface in this attack hacker hides the real actual user interface and display own user interface by reading them some content, user interface in which user can

easily capture the link and desktop system location. Movies streaming and torrent website in which the advertising common method used to steal the data & information.

4. DDOS Attack

(N. Vlajic and D. Zhou, 2018) the internet of thing devices composed of several internet link in which the intended the common denial of service attack (distributed denial of service attack) needs to protect the IOT from these such hacking attack, this research suggest some firewall protection based solution in which the vulnerable future direction has been added.

Hacking Advantages & Disadvantages

(Hamza, A.A., Abdel-Halim, I.T., Sobh, M.A. and Bahaa-Eldin, A.M., 2021.) The survey and program analysis taxonomy for IOT platforms, hacking addressed in some critical issues by the mean of such critical issues supporting attack. IOT system become the open invitation in which various serious security issues has been addressed and mitigated, hacking might be destroyed the IOT system processing and working, might be able to crash the internal storage system, hence program analysis is method which focused on defensive in contradiction of the hacking attack. Systematic literature review analyzed the various security issues in IOT system, examining the security analysis, hence program analysis method classify the method which has created & examined by the security analysis system which detects various malware applications. (Matre, M.O. and Kvåle, E.L., 2020) carrier advantages and disadvantages of IOT cargo tracking system, hence technology has changed the lives of human industries have been pressured towards the innovation and shipping market should be followed the product tracking service, product tracking service implemented by various industries to control and manage the overall industrial production control system, product purchased and transported by the purchase office, product tracking control logistic process including shipping control, IOT tracking is novel technology production in which real time cargo update, so IOT is hacked during product tracking which major loss of product during production so needs to fixed them.

Since ethical hacking is only option to predict and verify the real time hackers that appear in real time situation that capture the IOT system, since IOT system would be able to connected on android phone and windows operating system, ethical hacking might be able to identify the hacking attack might be able to stop the hacking. Ethical hacking is possible through Kali Linux Operating system and Parrot Security.

How hacking is prevent in IOT system

IOT hacking might be prevent and stop by ethical hacking system, there are common two types of hacking.

1. Hacking
2. Ethical Hacking

Ethical hacking is the way to train the administrator by giving some hacking tips and method, which enable to view the DDOS attack, session hijacking attack, firewall attack and internet attack. Kali Linux and Parrot operating system which is common platform of ethical hacking, backend the IOT system connected and completed program analysis platform has been developed. Hacking is basically system program which executed in IOT system through internet protocol mechanism, but ethical hacking is the way to identify the common attack and stop them in real time.

Project Plan

This project plan goal is to achieve the IOT hacking system method and prevention by planning systematic literature review and identify the literature research gap and fulfill the research gap by doing this project.

Statement of Work

1. Technical and systematic literature Review → (2015-2021)
2. Methods of IOT hacking
3. Ethical Hacking Programming
4. IOT SECURITY FIRWALL
5. Python programing

Project Schedules-→ Project Action Plan Timeline 2022

Tasks	Objectives	Success Criteria	Time Frame	Resources
Project Introduction	Thesis intro, ethical hacking on IOT	• Unauthenticated Access • Weak Authentication. • Hidden Backdoors. • Encryption Keys.	July 1sth to 8th July 2022	1. Google Scholars 2. IEEE Sites. 3. ScienceDirect
Research Technical Literature	Thesis literature finding	• Finding research gap • Studying technical literature from 2011 to 2021. • Writing technical review on this.	July 9th To 18th July 2022	1. Google Scholars 2. IEEE Sites. 3. ScienceDirect 4. ACM Library 5. IEEE Xplore 6. MDPI
Research Methods	Thesis methods on IOT Hacking	Ethical Hacking tools on IOT IOT Security Firewall Python programing methods IOT security methods	18th July 2022 to 22nd July 2022	1. YouTube 2. GitHub 3. Kaggle 4. Google Scholars
Ethical Hacking Tool	Thesis Tool	Python programming tool	23rd July 2022 to 25th July 2022	1. Python Sites 2. Tutorial 3. Research finding 4. Python Notebook 5. Dataset Kaggle
Result & Analysis Python Programming	Thesis Result & Analysis	• Critical Evaluation of results to other researchers works • Comparison with other researcher	26th July 2022 to 27th July 2022	1. Google Scholars 2. IEEE 3. ACM 4. Science Direct 5. MDPI
Research Ethics	Ethics on research	Follows the rules and instruction conducting research criteria	28th July to 30th July 2022	• Google Scholars
Discussion & Conclusion	Discussion	Critical validation and evaluation with other researcher	31st July 2022	1. IEEE Xplore 2. IEEE Sites 3. ACM

Methods of Research

(Kagita, M.K., Thilakarathne, N., Gadekallu, T.R., Maddikunta, P.K.R. and Singh, S., 2021.) the success of IOT would not ignored due to ease the life of human, in previous research various security method has deployed but the successful method is not applied yet, so far the research gap exists to secure the IOT system from hacker and vulnerable attack. Since cyber security method needs to revised them various countries having week cybersecurity methods, since antivirus and malware tools is not sufficient to secure them.(Williams, P.A. and McCauley, V., 2016,) security issues exists in medical and health devices which designed by the IOT system, patient confidential personal data needs to secured, hacker might be able to capture the real time patient health and able to destroy them. Limited security with low power design and limited storage capacity.

This research going to design the following solutions as follows:

1. Safe and protected enable data transfer system
2. Security system of WIFI
3. Securing the internal IOT system with Firewall
4. Securing the IOT devices by virtual private network
5. Securing internet service provider system

Result & Analysis

1. Ethical Hacking Programming
2. IOT SECURITY FIREWALL
3. Python programing

References

Beale, S.S. and Berris, P., (2017). Hacking the Internet of things: Vulnerabilities, dangers, and legal responses. *Duke L. & Tech. Rev.*, *16*, p.161.

Serror, M., Hack, S., Henze, M., Schuba, M. and Wehrle, K., (2020). Challenges and opportunities in securing the industrial internet of things. *IEEE Transactions on Industrial Informatics*, *17*(5), pp.2985-2996.

Westerlund, O. and Asif, R., (2019), February. Drone hacking with raspberry-pi 3 and wifi pineapple: Security and privacy threats for the internet-of-things. In (*2019) 1st International Conference on Unmanned Vehicle Systems-Oman (UVS)* (pp. 1-10). IEEE.

Kagita, M.K., Thilakarathne, N., Gadekallu, T.R., Maddikunta, P.K.R. and Singh, S., (2021). A review on cyber crimes on the Internet of Things. *Deep Learning for Security and Privacy Preservation in IoT*, pp.83-98.

Williams, P.A. and McCauley, V., 2016, December. Always connected: The security challenges of the healthcare Internet of Things. In *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)* (pp. 30-35). IEEE.

N. Vlajic and D. Zhou, (2018)"IoT as a Land of Opportunity for DDoS Hackers," in *Computer*, vol. 51, no. 7, pp. 26-34, July (2018), doi: 10.1109/MC.2018.3011046.

Hamza, A.A., Abdel-Halim, I.T., Sobh, M.A. and Bahaa-Eldin, A.M., (2021). A survey and taxonomy of program analysis for IoT platforms. *Ain Shams Engineering Journal*, *12*(4), pp.3725-3736.

Matre, M.O. and Kvåle, E.L., 2020. *What are the carrier advantages and disadvantages of IoT cargo tracking?* (Bachelor's thesis, NTNU).