International Journal of Scientific Research and Engineering Development-– Volume 2 Issue 5, Sep – Oct 2019

Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Unauthorized Access Detection in IOT using Canary Token Algorithm

Jijin Godwin. J*, Narender Malishetty**, Raghul.R***

*(Department of ECE,Velammal Institute of Technology Chennai, India Email: jijingodwin.j@gmail.com)

**(Department of ECE,Velammal Institute of Technology Chennai, India Email: narender.malishetty@gmail.com)

***(Department of ECE,Velammal Institute of Technology Chennai, India Email: raghulecevit@gmail.com)

Abstract:

IoT is the rapidly growing field after the Internet and Smartphones. In the era of the connected world it is clear that almost all devices and things in the near future will be connected to the Internet. When any new technology comes it also comes with a variety of vulnerabilities which is ready to be exploited. Even though Iot has been around for the past few years there is something which hinders it from becoming a global thing, one among such thing is the security. Conventional widely used authentications based on single password or pin can be compromised with side channel or dictionary attacks. So it is always good to have an Intrusion Detection System (IDS) such as Canary Tokens which is being deployed natively on the users itself, thereby even if the server is compromised and somehow it goes undetected still the users can be warned and their valuable data can be protected.

Keywords—**IoT Security, IDS, Canary tokens.**

I. INTRODUCTION

The growth of the Internet evolving rapidly, which once considered as impossible or impractical now becoming reality. Internet of Things (IoT) is a recently evolved technology that has taken the world by a storm. Basically, an IoT system consists of several interrelated computing devices, sensors, RFID tags, etc. that are connected to the main server through the internet enabling transfer of data and information without human intervention. Iot relies mainly on the Internet hence the devices of the systems need not be in the close proximity with each other The tremendous growth of the internet has enabled IoT's rapid growth and today IoT systems find applications in a variety of fields such as home automation systems, military, surveillance systems, sustainable agriculture, healthcare, manufacturing, smart cities and so on. The tremendous expansion of the Internet related applications and gadgets over the past decade was given a huge blow to worldwide communication systems, nearly 60% of the internet connection now happens through wireless devices such as smartphones. This tremendous growth has also led to the development of IoT.

Due to its open nature, new devices that enter the network are configured automatically in the IoT network and moreover, the interconnected devices need not be homogeneous this leaves such networks prone to a lot of attacks. More and more generic devices getting connected together in the network making it a hierarchical IoT network(HIoTn) which is a special kind of generic IoT network, which is composed of various nodes such as gateway nodes, cluster head nodes and sensing nodes organized in a hierarchy [1]. With all the advancements that have been made in the field of IoT over the past years' security issues have been a major concern that has hampered the usage of IoT systems in certain critical fields such as warfare, military surveillance, etc. Since they are built on top of the internet, IoT systems are extremely vulnerable to malicious attacks Most of the IoT based systems are heavily deployed in critical processes where sensitive data passed between devices in the network and must not fall into malicious hands.Apart from all these the most

 ©IJSRED: All Rights are Reserved

vulnerable part of the IoT is considered to be the physical layer where the devices can be accessed by anyone which again poses a major threat. The absence of a dedicated protocol for the communication of IoT devices along with the grouping of heterogeneous devices in IoT applications it is necessary to encrypt the information End to End, but due to the low computational power and less data rate for processing, it cannot be easily implemented in IoT without having some tradeoffs. Modified versions of many cryptographic hash algorithms have been presented but even they can be compromised with side channel attacks.

A Canary token is a type of Honeypot; Honeypot is a kind of system which can be used to attract the potential malicious person who seeks to gain unauthorized access to the system. It is mainly used to study system securities, traces left by the hacker and even can be used to analyze and improve the securities in the current system. In general, Honeypot acts as a decoy by taking the position of the data, computers, and application by simulating their actual behaviors. Usually when there is a security breach it will be mostly concentrated on the server side where huge client data is available, thus in time of breach most of the data is inaccessible due to DDoS (Dynamic Denial of Service) and there are no methods to safeguards these data unless the provider makes a best solution at that time. Instead of that canary tokens which are self-hosted on the client can work as Intrusion Detection System (IDS) even when the server is compromised.

II. EXISTING WORK

Providing authentication and security measures for IoT is not the same as that of providing it to other similar Internet-based services. Many global level attacks are daily targeted over IoT but due to its staggered nature, it won't make it to the mainstream. Mirai malware is the first globally targeted IoT based malware which turned all networking computers into botnets turning them into devices which used in DDoS attacks. A collaborative PHY-aided technique for end to end authentication of IoT devices was proposed by Peng Hao*et all* [2] which combines the conventional asymmetric, cryptography-based E2E IoT device authentication with D2D PHY fingerprinting.Honeypot are extensively being used in the field of security researches, the use of roaming honeypots for mitigating Denial of Service (DoS) attack had been proposed by Sherif M. Khattab*et al*[6].A new security authentication scheme for HIoTNs have been presented,the formal security using the widely accepted ROR model and also informal security analysis for various known attacks including the sensing nodes capture attack are thoroughly examinedby Mohammed Wazid*et all* [1]. Mario Frustasi*et all* studiedvarious critical security loopholes of the IoT and proposed that the most vulnerable level of the IoT system model is the Perception Layer due to the physical exposure of IoT devices on the Interconnected systems [3].Amitav Mukherjee reviewed several security techniques for distributed detection and communication scenarios in an IoT context and it is concluded that there is a clear need for a theoretically well-founded and holistic approach for incorporating complexity and energy constraints into physical-layer security designs [4]. Finally making the IOT to be satisfying for the TIPPSS (Trust, Identity, Privacy, Protection, Safety, and Security) considering and ensuring TIPPSS for IoT can enable a safer, more secure world for all of humanity is proposed by Florence D. Hudson [5].

III. CANARY TOKENS

As we already mentioned canary token is a type of production honeypot which is being extensively used in the field of security researches. It is usually deployed as a decoy for the original system so that attacker misunderstood it for the original system and deploy his attack there. But canary tokens cannot be used for such purposes instead it can be used to track the record made by the attacker, it works on the following way.

Initially, the canary token will be natively deployed in the service of the user, each canary token comes with unique id so all of them are easily traceable. Next, the canary token will be tightly integrated along with the native service of the user. When a user makes a call to the actual service our token will also get executed, when requested it returns a 1x1 pixel image to the user

 ©IJSRED: All Rights are Reserved

thus from the attacker perspective only original service will be executed but actually, the canary token is also executed. Canary tokens usually consist of a set of python codes which when executed returns the source IP, user agent, time and some other useful information to the user.

IV. PROPOSED MODEL

In Proposed model, the system works as depicted by the block diagram shown below,

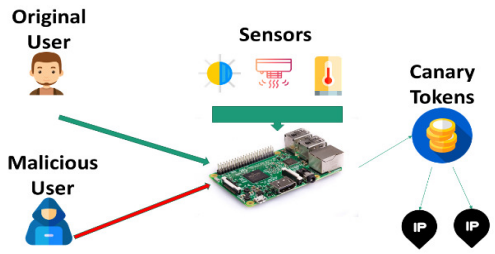

Figure.1

Fig.1 shows all the login requests for the IoT server of the raspberry pi are logged via canary tokens, this monitors and triggers (example: When a user requests the login for the IoT via a specific url canary tokens tracks the ip and triggers the user via E-mail/ any provided warning methods) in real time.The canary token is an open source honeypot solution provided by canarytokens.org, from them we pull dns request based token and recompiled it based on our need and hosted it in our custom domain, we created a python code which initiates the booting of the canary service. Now whenever a new http/get request made to the login page of the IoT service we will receive the time, source ip, user agent of the person even if the login fails.

We are using Cayenne IoT platform for maintaining our IoT, it comes with bundled sensor installations for various default sensors and also supports integrating generic analog and digital sensors along with actuators, it can even support MQTT based services. By default, the platform can monitor various parameters of the raspberry pi in real time such as CPU usage, available RAM, available memory, Soc temperature and even has a toggle to remotely power on/off the Raspberry Pi.

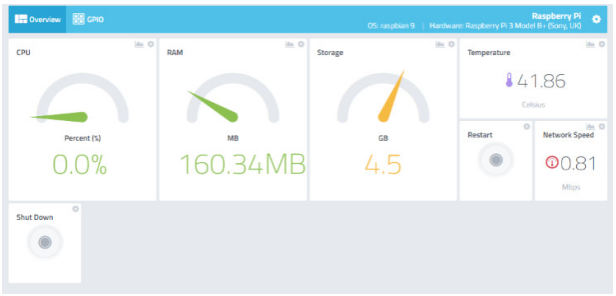

Figure. 2

Fig. 2 shows the interface of Cayenne IoT platform in which the Raspberry Pi is managed, as we can see from the above image that the parameters of the Raspberry Pi are coming directly from the device in live feed which can also be used to show the output of the sensors both in formatted and unformmated versions.

V. RESULT

On the back end runs our Canary token server, which is actively tracking all the login requests for our IoT system, the advantage of this is it runs natively on the platform itself moreover it won't be visible to the attacker.

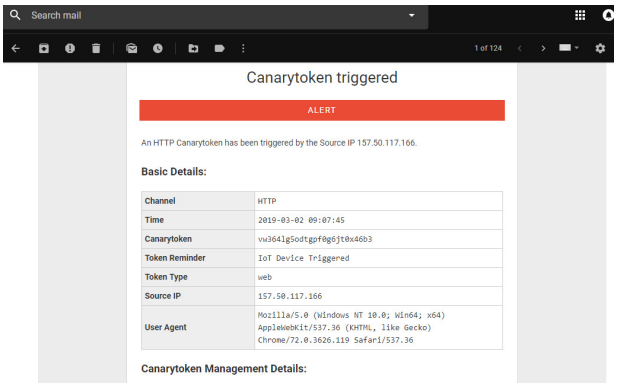

Figure.3

Fig. 3 shows the mail triggered output from our canary token for the IoT monitoring system.

As we can see from the triggered mail that the channel in which the request is made, its time, source ip address for the HTTP request along with the user agent which shows from which medium the request is made (In this case it is from a chromium based web browser which runs on a windows x64 machine) all can be gathered. All the above parameters can be cross checked with

 ©IJSRED: All Rights are Reserved

the actual user and if any discrepancies are to be found then the user can be warned directly.

VI. CONCLUSION

The main reason for the lack of security in IoT is the absence of cryptographic protocols especially made for IoT's.Even though there are methods like use of modified hash algorithms have been proposed the absence of native hardware support for the encryption function always kept IoT with less number of choices. Thus we have implemented an Intrusion Detection System (IDS) natively on the client itself thus we will always be warned even when there is a breach in the server.But the scenario is going to change soon as Google introduced a new encryption algorithm "Adiantum" [7] which is mainly targeted for low-end Android devices. The use of AES on these devices are quite painful because it will take huge time to encrypt and decrypt device information on the go, thus conventional methods such as XTS or CBC-ESSIV modes of operation, which are length-preserving is commonly used. To address this issue Google has created Adiantum, which allows us to use the ChaCha stream cipher in a length-preserving mode, by adapting ideas from AES-based proposals for length-preserving encryption such as HCTR and HCH.This does require some computational power to encrypt and decrypt but it will be satisfied by any IoT easily. Thus in the future, we are in thought of adding Adiantum to our IoT along with our existing Canary Tokens.

VII. ACKNOWLEDGEMENT

The authors would like to thank Velammal Institute of Technology for providing facilities in their research lab and the staff members for providing proper guidance.

VIII. REFERENCES

[1] Mohammad Wazid, Ashok Kumar Das, Vanga Odelu, Neeraj Kumar, Mauro Conti, Minho Jo ".Design of Secure User Authenticated Key Management Protocol for Generic IoT Networks", IEEE Internet of Things Journal Vol.5, issues.1, February 2018.

[2] Peng Hao, Xiabin Wang, Weiming Shen, "A Collaborative PHY-Aided Technique For End-to-End IoT Device Authentication", IEEE Access Volume. 3.2018.

[3] Mario FRUSTACI, Pasquale PACE, Gianluca ALOI, Giancarlo FORTINO, "Evaluating critical security issues of the IoT world:Present and Future challenges" IEEE Internet of Things Journal Vol. 5, issue. 1 February 2018.

[4] Amitav Mukherjee, "Physical-Layer Security in the Internet of Things: Sensing and Communication Confidentiality Under Resource Constraints", Proceedings of the IEEE vol.103 issue.10 October 2015.

[5] Florence D. Hudson ,"Enabling Trust and Security: TIPPSS for IoT", IT Professoionals Vol.20 issue.2 March 2018.

[6] S.M. Khattab, C. Sangpachatanaruk, D. Mosse, R. Melhem, T. Znati "Roaming honeypots for mitigating service-level denial-of-service attacks", IEEE Proceedings 2004.

[7] https://security.googleblog.com/2019/02/introducing-adiantum-encryption-for.html

 ©IJSRED: All Rights are Reserved