International Journal of Engineering Science Invention (IJESI)
ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726
www.ijesi.org ||Volume 7 Issue 12 Ver. IV || Dec 2018 || PP 69-72

A Survey on Security of Iot devices

Navya Shridhar C S, Dr Nagaveni V
Asst. Professor, Department of Computer Science, Don Bosco Institute of Technology
Associate Professor, Department of Computer Science, Acharya Institute of Technology
Corresponding Author: Navya Shridhar

Abstract: *IoT devices industry is rapidly growing with an ever-increasing list of manufacturers offering a countless number of smart devices targeted to enhance end-user's standard of living. Security is an after-thought in these devices resulting in vulnerabilities that have been successfully exploited. Many security problems can be mitigated through strong identification and authentication of devices, which enables administrators to enforce appropriate security controls on a particular device. As devices are plugged-in and removed from an IoT network, it is essential to identify the type of these devices and establish a behavioral baseline. Fingerprinting IoT devices is challenging due to the large variety of devices, protocols, and control interfaces, across the devices. An IoT device might respond to queries about its identity and type, which is a standard way of remotely learning about the device.*

Keywords: *Internet of Things, Encryption, Fingerprinting*

Date of Submission: 21-12-2018 Date of acceptance: 05-01-2019

I. Introduction

Internet of Things(IoT) represents a general concept for the ability of network devices to sense and collect data from the world around us, and then share that data across the Internet where it can be processed and utilized for various interesting purposes.

Internet of Things immediately triggers questions around the privacy of personal data. Whether real-time information about our physical location or updates about our weight and blood pressure that may be accessible by our health care providers, having new kinds and more detailed data about ourselves streaming over wireless networks and potentially around the world is an obvious concern. Supplying power to this new proliferation of IoT devices and their network connections can be expensive and logistically difficult. Portable devices require batteries that someday must be replaced. Although many mobile devices are optimized for lower power usage, energy costs to keep potentially billions of them running remains high.

IoT network security is a bit more challenging than traditional network security because there is a wider range of communication protocols, standards, and device capabilities, all of which pose significant issues and increased complexity.

Encrypting data at rest and in transit between IoT edge devices and back-end systems using standard cryptographic algorithms, helping maintain data integrity and preventing data sniffing by hackers. The wide range of IoT devices and hardware profiles limits the ability to have standard encryption processes and protocols. Moreover, all IoT encryption must be accompanied by equivalent full encryption key lifecycle management processes, since poor key management will reduce overall security.

Securing the data is not just enough for iot network. We should make sure that the communicating parties in the network is secured. Security solutions for IoT will need to take into account that IoT devices with unpatched vulnerabilities may often be present in the user's network and co-exist with other devices during their whole device lifetime. Since the iot devices are resource constrained, the iot network should be secured inorder to maintain the lifetime of the network devices.

II. General Security Analysis Of Iot Systems

The IoT extends the Internet to the physical world and thus poses many new security and privacy challenges. Some of the problems are due to the intrinsic characteristics of the IoT and its differences compared to traditional networks, while others arise as a result of the integration of the IoT and the Internet[2].

To protect against those attacks, it is important to examine the security problems according to the information flows and potential adversarial points of control. Below, we outline four security and privacy problems:

1.**Authentication and physical threats**: highlydistributed deployments of a large number of IoT devices, such as RFID tags and wireless sensors, will generally be deployed in public areas without any protection, which makes the devices difficult to manage and vulnerable to physical attacks. For example, an illegitimate sensor may register itself claiming that it is at one location while it is actually at a different location. Or a sensor installed in a room monitoring the room temperature is moved to another room by a malicious person. This introduces the challenge of authenticating IoT devices, which involves recognizing the device and verifying its association with a correct topological address.

2. Integrity: the unattended environment for IoT devices also makes data integrity a concern. Once deployed, most of these devices will operate in a self-supported manner. As with very limited maintenance or even no maintenance, tampering data is a much easier task than in a supervised wired network. Further, as a result of a natural loss of calibration or a deliberate perturbation of the measurement environment by an attacker, the data collected by IoT devices is quite likely to have low quality and might be corrupted at the environmental level. In short, IoT data may be noisy and easy to spoof and forge.

3. Confidentiality: the communication method between devices and the gateway is primarily wireless, which results in confidentiality risks. For example, eavesdropping is a major concern in wireless networks. Unfortunately, unlike many other wireless environments, such as cellular and Wi-Fi networks, it is difficult for IoT networks to provide confidentiality for data transmission due to the resource-constrained nature of low-end devices, which are a large fraction of IoT devices [3]. Different from typical devices in traditional wired and wireless networks, such as smartphones, tablets, PCs and routers, most of the devices in future IoT networks are active sensors or passive RFID tags, which have very limited resources and capabilities. Constraints on power, computational capability, storage and other aspects of an IoT device introduce a high barrier for it to perform the necessary operations to achieve data confidentiality, such as through encryption and key management.

4. Privacy: as an existing public concern for monitoring and interacting with the real world, the consequence of information leakage in local IoT networks becomes exacerbated when integrated into the global Internet. By connecting real world objects and information through the internet, data may become accessible to various organizations and domains across the Internet, instead of only being revealed to a small group, which makes it more likely to be exposed to sophisticated malicious parties and therefore increases the probability of being exploited and attack.

III. Related Work

A few kinds of existing schemes that are pertinent technique for IoT device security and used for protecting data transmission in IoT are discussed here.

Nhu-Ngoc Dao et al.in [6] "Achievable Multi-Security Levels for Lightweight IoT-enabled Devices in Infrastructureless Peer-Aware Communications" Author present SNAuth protocol is implemented on PACNET, that provides multiple security level based on number of utilized partial keys and PDs in the network have full abilities to manage their communications by themselves without any infrastructure entity. This approach provides a user convenience with reasonable resource consumption

A. B. Or´ue et al.in [7] "A lightweight Pseudorandom Number Generator for securing the Internet of Things" Author present a pseudorandom number generator algorithm is implemented in c++, which uses resource constrained devices.

Ou Ruan et al.in [8] "Provably Leakage-Resilient Password Based Authenticated Key Exchange in the Standard Model" proposed a PAKE protocol by combining Diffie-Hellman key exchange and the DF-LRS scheme, which is used to securely authenticate devices in insecure iot environment.

Fadi Al-Turjman et al.in [9] "Seamless Key Agreement Framework for Mobile-Sink in IoT Based Cloud-Centric Secured Public Safety Sensor Networks" proposed S-SAKA framework, this resolves the problem of mobile-sink and cluster-head. S-SAKA framework does not only solve some major security issues, but also ensures a seamless connectivity to reduce the computation and communication cost of the network systems.

Peng Xu et al.in [10] "Fast and Parallel Keyword Search Over Public-Key Ciphertexts for Cloud-Assisted IoT" proposed a new concept called searchable public-key ciphertexts with hidden structures (SPCHS) to accelerate the search performance. This approach saves the communication cost of the IoT devices to transfer ciphertexts, and improves the search performance of the cloud to retrieve the intended data.

Nhu-Ngoc Dao et al.in [11] "Adaptive MCS selection and resource planning for energy-efficient communication in LTE-M based IoT sensing platform" proposed an adaptive MCS selection and resourse planning algorithm, which works for low data rate devices especially when the transmission packet size is small.

Markus Miettinen et al.in[12] "IOT SENTINEL: Automated Device-Type Identification for Security Enforcement in IoT" Author presented an automated approach to identify the different types of iot devices connected to network gateway, which uses both classification and edit distance algorithm to identify the type of device. This approach provides protection for the user's network by enforcing network isolation where communications of potentially vulnerable devices are strictly controlled, thereby effectively mitigating security risks related to these devices.

Hang Guo et al.in [13] “IP-Based IoT Device Detection” proposed a novel approach to detect iot devices exchange traffic regularly with servers. For each specific type of device, author has tracked a list of device server names that device talks to. So, this requires prior knowledge of servers run by IoT manufacturers.

Nishadh Aluthge Helsinki et al.in [14] “IoT device fingerprinting with sequence-based features**”** Author proposed an approach based on capturing the initial communication behavior of a device during its setup and extracting the features related to a sequence of packets. This approach considers directionality of sequences as bidirectional and source-originated to define two sets of same feature types resulting in 90 features.

TABLE I. COMPARISION BETWEEN RELATED WORK

Ref. No	**Techniques Used**	**Pros**	**Cons**
[6]	SNAuth protocol for PACNET	Reduce the communication overhead	No central entity is used for control and management purpose, security is still a challenge for a dense PAC network. Communication cost is high.
[7]	pseudorandom number generator algorithm	Less computation with good performance	Very sensitive to initial condition and complexity of the initialization of parameter
[8]	Diffie-Hellman key exchange and the DF-LRS scheme	Confidentiality, Authentication	Doesn’t suite for all types of side channel attacks in hardware design of iot
[9]	S-SAKA framework	Reduces computation and communication cost	Results in increased relaying load and additional energy dissipation.
[10]	Searchable public-key ciphertexts with hidden structures (SPCHS)	Improves search performance	This work pays more attention to secure cloud data w.r.t uploading and retrieving data
[11]	adaptive MCS selection and resourse planning algorithm	Suitable for less computational device with small packet size	MCS is not suitable for different types of IOT devices with different data transmission requirement
[12]	classification and edit distance algorithm	Considered 23 features to identify the devices	More computational time
[13]	IP-Based IoT Device Detection	Suitable for limited device network	Prior knowledge of the servers run by IoT manufacturers
[14]	IoT device fingerprinting with sequence-based features using classification	14 % increase in the average prediction	The directionality of the traffic considering packets originated from source and packets between source and other entities. storage is an issue
[15]	Machine learning features for device profiling	Reduces false positives during device fingerprinting	monitor the device behaviour throughout its life time Computational time is high

IV. Challenges

Physical security is a most critical challenge in IoT because of some of IoT devices are likely to be deployed in places where physical security is difficult or impossible to achieve.

Another challenge is cryptography algorithms. Conventional cryptography algorithm is not suitable for constrained devices because of large key size like RSA. RSA is not suitable because of its large key size and high processing requirements.

Another challenge is how can generate the suitable small key in public-key cryptosystems that are secure the data transmission.

Another challenge is how can achieve Confidentiality + integrity + availability simultaneously.

Another challenge is how to keep the network safe from different types of attacks using device fingerprint.

V. Conclusion

In this review paper, we have focused on different lightweight encryption technique used in IoT for secure data transmission and different device fingerprinting approaches to secure the devices as well. Every technique the IoT network safe from attackers . Still security is a serious issue in IoT and it is hot research topic in IoT.

References

[1]. A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," IEEE Communications Surveys & Tutorials, vol. 17, pp. 2347-2376, 2015.

[2]. Somayya Madakam, R. Ramaswamy, Siddharth Tripathi, "Internet of Things (IoT): A LiteratureReview," Journal of Computer and Communications, 2015, 3, 164-173

[3]. Gerald, Josef,Christian and Josef Scharinger, "NFC Devices: Security and Privacy", ARES 08 proceedings of the 2008 Third International Conference on Availability, Reliability and Security, IEEE Computing Society, Washington, DC, USA, 2008

[4]. Want, R. (2006) An Introduction to RFID Technology. IEEE Pervasive Computing, 5, 25-33.

[5]. H. C. Chen, M. A. A. Faruque and P. H. Chou, "Security and privacy challenges in IoT-based machine-to-machine collaborative scenarios," 2016 International Conference on Hardware/Software Codesign and System Synthesis (CODES+ISSS), Pittsburgh, PA, 2016, pp. 1-2.

[6]. Nhu-Ngoc Dao, Yonghun Kim, SeohyeonJeong, Minho Park, Sungrae Cho,"Achievable Multi-Security Levels for Lightweight IoT-enabled Devices in Infrastructureless Peer-Aware Communications", 2169-3536 (c) 2017 IEEE.

[7]. A. B. Or´ue, Member, IEEE, L. Hern´andez-Encinas, A. Mart´ın and F. Montoya, "A lightweight Pseudorandom Number Generator for securing the Internet of Things", 2017 IEEE.

[8]. OuRuan, Jing Chen, Mingwu Zhang , "Provably Leakage-Resilient Password-Based Authenticated Key Exchange in the Standard Model", 2169-3536 (c) 2017 IEEE.

[9]. Fadi Al-Turjman 1, YoneyKirsal Ever2, Enver Ever 1, Huan X. Nguyen3, and DeebakBakkiam David1 , "Seamless Key Agreement Framework for Mobile- Sink in IoT Based Cloud-Centric Secured Public Safety Sensor Networks " Received September 21, 2017, accepted October 13, 2017, date of publication October 25, 2017, Digital Object Identifier 10.1109/ACCESS.2017.2766090 .

[10]. Peng Xu 1,2, (Member, Ieee), Xiaolan Tang1," Fast and Parallel Keyword Search Over Public-Key Ciphertexts for Cloud-Assisted IoT",Digital Object Identifier 10.1109/ACCESS.2017.2771301,IEEE 2017.

[11]. N.-N. Dao, M. Park, J. Kim, and S. Cho, "Adaptive MCS selection and resource planning for energy-efficient communication in LTE-M based IoT sensing platform," PloS one, vol. 12, no. 8, p. e0182527, 2017.

[12]. Markus Miettinen Ahmad-Reza Sadeghi, Samuel Marchal N. Asokan, IbbadHafeezSasuTarkoma, "IOT SENTINEL: Automated Device-Type Identification for Security Enforcement in IoT", 2017 IEEE 37th International Conference on Distributed Computing Systems.

[13]. Hang Guo, John Heidemann, "IP-Based IoT Device Detection", IoT S&P'18, August 20, 2018, Budapest, Hungary.

[14]. Nishadh Aluthge, IoT device fingerprinting with sequence-based features.

[15]. Bruhadeshwar Bezawada, Maalvika Bachani, Jordan Peterson, Hossein Shirazi, Indrakshi Ray, Indrajit Ra, IoTSense: Behavioral Fingerprinting of IoT Devices,arxiv1804.03852v11 Apr 2018.

Navya Shridhar" A Survey on Security of Iot devices" International Journal of Engineering Science Invention (IJESI), vol. 07, no. 12, 2018, pp 69-72