TEST Engineering & Management

January - February 2020
ISSN: 0193 - 4120 Page No. 4858 - 4862

A State of Art on Security Issues and Countermeasures in IoT

C. Santhosh Kumar, Assistant Professor in the Department of Computer Science & Engineering at Priyadarshini Engineering College, Vaniyambadi.
K. Vishnukumar, Associate Professor in Computer Science and Engineering Department at KPR Institute of Engineering & Technology, Coimbatore, Tamilnadu, India.

Article Info
Volume 82
Page Number: 4858 - 4862
Publication Issue:
January-February 2020

Article History
Article Received: *18 May 2019*
Revised: *14 July 2019*
Accepted: *22 December 2019*
Publication: *23 January 2020*

Abstract:

The Internet of Things (IoT), which is projected to deliver end-to-end services as a transformative approach. Handheld smart devices become a key component of IoT. In addition, IoT advertising has contributed to issues of public safety, including individual privacy problems, organized crime risk, and cyber attacks. First, we describe briefly the well-known IoT reference model and its layers in order to achieve this goal. Secondly, we are discussing the feasible IoT applications and the probable motivations of the attackers targeting the intelligent environment. Thirdly, in each layer, we are discussing various security attacks. Fourth, we describe these attacks as possible countermeasures. We conclude with the present two budding security challenges that have not yet been explained in detail in earlier reviews.

Keywords:*Privacy, Integrity, Security, Vulnerability*.

I. INTRODUCTION

The Things Internet (IoT) has no precise definition. A broad understanding of IoT, however, is that it offers any information services across the World Wide Web by facilitating interaction between things-to-thing, human-to-thing, human-to-human, and things-to-things [1]. IoT interconnection of heterogeneous objects, such as sensors, humans or anything feasible that can act as a service request / response [2]. The novelty of different communication protocols, hardware improvements, offers the possibility of changing an isolated system into a communicating object. The smart device's storage capabilities, computing power, and energy capacity have significantly improved and its sizes have been reduced. The measure of emerging threats and attacks against an object or an individual's safety has grown tremendously as a side effect. The significant development in secure smart devices will authorize people with a variety of services, ranging from health care to smart infrastructure, where very different things, such as temperature sensors, medical sensors, and light sensors, can communicate with each other or with a person handling smart devices, such as cell phones, tablets, or laptops, etc.

The researchers are presently working to identify potential threats and present budding solutions. This paper summarizes in detail the IoT security issues and countermeasures. The aim of the survey is to provide readers with an awareness of the types of attacks and how they have been resolved, and what threats are still awaiting.

A. IoT Reference Model

In industrial and academic publications, the IoT reference models have been widely discussed. Fig. 1 shows the seven-level model of Cisco and its various levels. CISCO's seven-level model may be standardized, creating a widely accepted IoT reference model [3]. The information flow in this model is generally bi-directional. The predominant data flow path, however, depends on the applications.

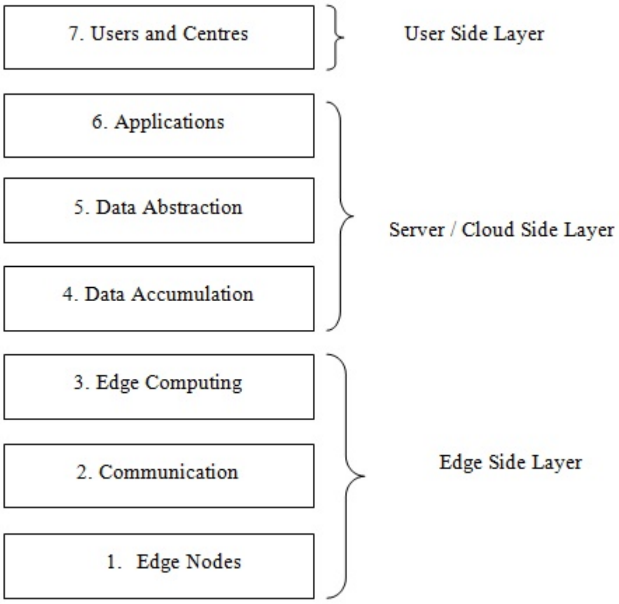


Fig 1. Cisco’s seven level Reference model [3]

Level 1-Edge devices: This reference model's first dimension typically consists of computer devices, such as RFID scanners, sensors, smart controllers, etc., and various versions of RFID tags. From this level, information integrity and privacy must be taken into account.

Level 2-Communication: it includes all mechanisms that allow command or information to be transmitted: I first-level device communication, (ii) second-level component communication, and (iii) first-level and third-level data transmission (edge computing).

Level 3-Edge computing: It originates from simple data processing. This is important to reduce the higher level computational load as well as to provide an earlier response.

Level 4-Data abstraction: It becomes more efficient and simpler to process. At this level, the regular tasks of entities include standardizing, deformalizing, consolidating and indexing data into one spot.

Level 5-Applications: The application delivers understanding of information where programming cooperates with levels of data abstraction and data accumulation. IoT uses are abundant and can vary considerably across the business and industrial needs sectors.

Level 6- canters and users: The smart users are located at this top level. Users use their analytical data and applications.

The spectrum of IoT systems and attackers is discussed in Section 2. In particular, we identify the IoT security requirements. We then define possible attacks against IoT in Section 3. In Section 4, we outline countermeasures to these attacks. We are addressing two new security challenges in Section 5. Lastly, in Section 6, we include with conclusions and recommendations for future research.

II. Background

A. Scope of Applications

1. Smart vehicles: Small IoT-based systems can provide remote locking/unlocking of vehicles, access to traffic information and download of roadmaps. Besides, Internet-connected car gives significant security against theft**.**

2. Smart buildings:Remote control devices receive **and get** direction from users to perform activities in the residential building.

3. Health monitoring: The future of healthcare systems based on IoT lies in the development of personal health monitoring to allow early detection of diseases.

4. Construction management: Significant IoT implementations are the control and maintenance of modern infrastructure, such as traffic lights, bridges, railway tracks and buildings [4].

5. Environmental monitoring: Having smart things with embedded sensors allows emergency situations to be tracked in the area, e.g. a flood requiring quick response. Therefore, IoT-based devices will analyze the quality of air, water, humidity and temperature [5].

6. Production and management: Smart systems make it possible to produce new products and control / monitoring systems quickly [6]. In contrast, methodologies for intellectual management use real-time measurements, which permits power efficiency and safety management.

B. Probable attackers and their Intentions

Probable attackers may hack IoT devices for the purpose of stealing sensitive information, such as location data, credit / debit card numbers, health information, financial accounts, passwords. We may also attempt to compromise IoT systems, such as launching attacks on a third-party organization, edge nodes. Also, **attackers** may be concerned in compromising smart devices to target against a group.

C. The scope of IoT against Security

Next, in the field of IoT, we define two of the most commonly used terms: a security attack and a safe thing. It is imperative to understand the attributes that define security while defining a secure thing.

III. IOT VULNERABILITIES

Edge compute nodes*:* We instigate attacks on the edge compute nodes, such as detectors, RFID readers, and lightweight nodes. Equipment Trojans have developed as a major coordinated circuit wellbeing alarm [8]–[12]. Trojans are commonly separated into two kinds dependent on their systems of triggering [13]. The intruder can extract cryptographic information with a physical contact to the computer, alter the software, or change the OS. Physical attacks on the nodes of the edge can lead to complete destruction. The major intention is therefore to collect information for future reference, such as discovering the common key.

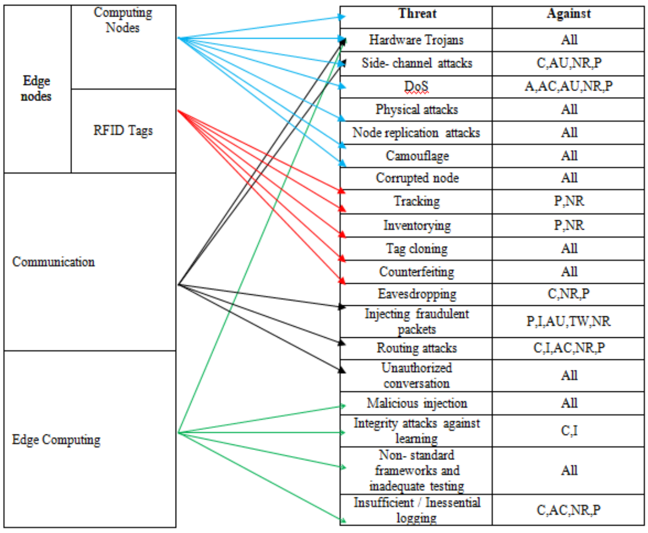
Inventorying: Explicit kinds of labels convey significant data about the articles to which they are associated. Therefore, a person with an EPC tag is obligated for inventorying, for example a label peruser can break down the person's items. This risk prompts genuine inquiries regarding privacy. For instance, the gatecrasher can realize what kinds of therapeutic hardware, for example, wearing a patient, an insulin siphon, and in this way what illnesses he experiences, for example, diabetes.

IV. COUNTERMEASURES

In this section several countermeasures for security issues and each defence in edge nodes level are discussed.

A. Computing nodes

Policy-based approaches are the effective methods at this stage of IoT to address privacy and security issues. An IDS can be used to consistently experience the brutality of critical policies. An IDS ensures that there is no need to violate general standards. Policy-based approaches are consistent in dealing with deprivation attacks of sleep and battery-draining by identifying unusual node requests. In an integrated circuit, a PUF is a noisy function. When a challenge is queried, a PUF produces a reaction based on both and the unique characteristics of the device's physical properties. It is believed that PUF is physically unclonable, visible, and unpredictable. PUFs authorize unique device authentication and identification and provide mechanisms for Trojan recognition.



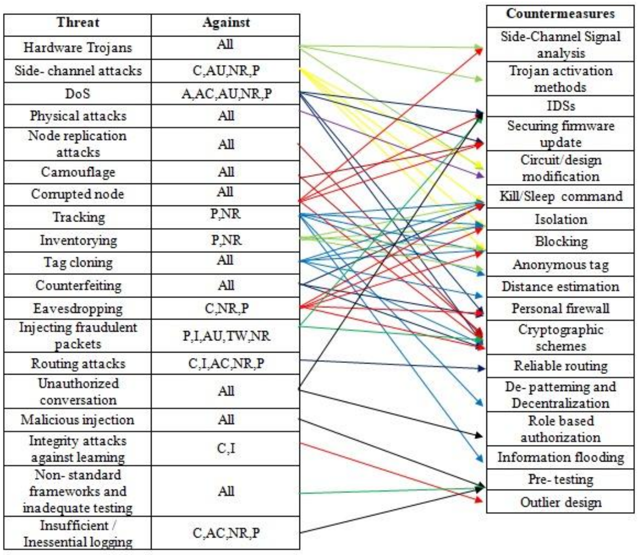
Threat	Against
Hardware Trojans	All
Side- channel attacks	C,AU,NR,P
DoS	A,AC,AU,NR,P
Physical attacks	All
Node replication attacks	All
Camouflage	All
Corrupted node	All
Tracking	P,NR
Inventorying	P,NR
Tag cloning	All
Counterfeiting	All
Eavesdropping	C,NR,P
Injecting fraudulent packets	P,I,AU,TW,NR
Routing attacks	C,I,AC,NR,P
Unauthorized conversation	All
Malicious injection	All
Integrity attacks against learning	C,I
Non- standard frameworks and inadequate testing	All
Insufficient / Inessential logging	C,AC,NR,P

Fig. 3 a) Summary of attacks

B. RFID tags

a) Anonymous tag: Kinoshita has suggested a unique idea based on the visualization of the look-up table. The real ID and each tag's anonymous ID are mapped and stored. Remember that an RFID tag produces the anonymous ID that does not have useful intrinsic data, it can allow spam time tracking. So, the anonymous ID can be generated periodically to address the tracking issue.

b) Personal firewall: A private RFID firewall checks the tag requests of all users. The firewall that allows high processing facilities can be installed in a system and sufficient storage capacity, such as a mobile. it allows complex policies to be built. For example, if the user is not within 50 meters of workplace, "the tag will not miss its sensitive data."



Threat	Against
Hardware Trojans	All
Side- channel attacks	C,AU,NR,P
DoS	A,AC,AU,NR,P
Physical attacks	All
Node replication attacks	All
Camouflage	All
Corrupted node	All
Tracking	P,NR
Inventorying	P,NR
Tag cloning	All
Counterfeiting	All
Eavesdropping	C,NR,P
Injecting fraudulent packets	P,I,AU,TW,NR
Routing attacks	C,I,AC,NR,P
Unauthorized conversation	All
Malicious injection	All
Integrity attacks against learning	C,I
Non- standard frameworks and inadequate testing	All
Insufficient / Inessential logging	C,AC,NR,P

Countermeasures
Side-Channel Signal analysis
Trojan activation methods
IDSs
Securing firmware update
Circuit/design modification
Kill/Sleep command
Isolation
Blocking
Anonymous tag
Distance estimation
Personal firewall
Cryptographic schemes
Reliable routing
De- patterning and Decentralization
Role based authorization
Information flooding
Pre- testing
Outlier design

Fig. 3 b) Summary of countermeasures

V. EMERGING CHALLENGES

We have summarized numerous attacks along with countermeasures on smart objects security. Next, we talk about two budding security challenges that have not yet been explained in detail in the earlier reviews. Most smart applications are based on Small battery-powered, low-storage devices and computing resources Over the past few years, some research has attempted to study the unpredicted uses of data from environment or an individual through internet-connected devices.

VI. CONCLUSION

Over the past decade, the emergence of the Internet of Things paradigm has exponentially lead to numerous threats and probable attacks on things or individuals ' security or privacy. This survey attempted to condense a level-by-level fashion against several IoT security attacks or concerns and countermeasures. This paper's primary goal is to provide an opportunity to the researchers to investigate which threats have been propelled and addressed, and which threats stay behind unaddressed. Furthermore, due to the tremendous growth of smart applications, both industrial / academic research communities and manufacturers should proactively and aggressively address these threats.

REFERENCES:

[1] Singh, Dhananjay, Gaurav Tripathi, and Antonio J. Jara. "A survey of Internet-of-Things: Future vision, architecture, challenges and services." 2014 IEEE world forum on Internet of Things (WF-IoT). IEEE, 2014.

[2] Atzori, Luigi, Antonio Iera, and GiacomoMorabito. "The internet of things: A survey." Computer networks 54.15 (2010): 2787-2805.

[3] Guth, Jasmin, et al. "Comparison of IoT platform architectures: A field study based on a reference architecture." 2016 Cloudification of the Internet of Things (CIoT). IEEE, 2016.

[4] Lazarescu, Mihai T. "Design of a WSN platform for long-term environmental monitoring for IoT applications." IEEE Journal on emerging and selected topics in circuits and systems 3.1 (2013): 45-54.

[5] Fleisch, Elgar. "What is the internet of things? An economic perspective." Economics, Management, and Financial Markets 5.2 (2010): 125-157.

[6] Tajima, May. "Strategic value of RFID in supply chain management." Journal of purchasing and supply management 13.4 (2007): 261-273.

[7] Bhunia, Swarup, et al. "Hardware Trojan attacks: threat analysis and countermeasures." Proceedings of the IEEE 102.8 (2014): 1229-1247.

[8] Salmani, Hassan, and Mark M. Tehranipoor. "Vulnerability analysis of a circuit layout to hardware Trojan insertion." IEEE Transactions on Information Forensics and Security 11.6 (2016): 1214-1225.

[9] Wehbe, Taimour, et al. "A novel approach to detect hardware Trojan attacks on primary data inputs." Proceedings of the WESS'15: Workshop on Embedded Systems Security. ACM, 2015.

[10] Milosevic, Jelena, Alberto Ferrante, and Francesco Regazzoni. "Security challenges for hardware designers of mobile systems." 2015 Mobile Systems Technologies Workshop (MST). IEEE, 2015.

[11] ManikantanShila, Devu, and VivekVenugopal. "Design, implementation and security analysis of hardware trojan threats in FPGA." Proceedings of the 2014 ACM/SIGDA international symposium on Field-programmable gate arrays. ACM, 2014.

[12] Tehranipoor, Mohammad, and FarinazKoushanfar. "A survey of hardware trojan taxonomy and detection." IEEE design & test of computers 27.1 (2010): 10-25.

[13] Tanaka, Hidema. "Information leakage via electromagnetic emanations and evaluation of tempest countermeasures." International Conference on Information Systems Security. Springer, Berlin, Heidelberg, 2007.

[14] Vuagnoux, Martin, and Sylvain Pasini. "Compromising Electromagnetic Emanations of Wired and Wireless Keyboards." USENIX security symposium. 2009.

[15] Nia, Arsalan Mohsen, et al. "Physiological information leakage: A new frontier in health information security." IEEE Transactions on Emerging Topics in Computing 4.3 (2015): 321-334.

[16] Martin, Thomas, et al. "Denial-of-service attacks on battery-powered mobile computers." Second IEEE Annual Conference on Pervasive Computing and Communications, 2004. Proceedings of the. IEEE, 2004.

[17] Khouzani, M. H. R., and Saswati Sarkar. "Maximum damage battery depletion attack in mobile sensor networks." IEEE Transactions on Automatic Control 56.10 (2011): 2358-2368.

[18] Agah, Afrand, and Sajal K. Das. "Preventing DoS attacks in wireless sensor networks: A repeated game theory approach." IJ Network Security 5.2 (2007): 145-153.

[19] Vasserman, Eugene Y., and Nicholas Hopper. "Vampire attacks: draining life from wireless ad hoc sensor networks." IEEE transactions on mobile computing 12.2 (2011): 318-332.