ISSN : 2350-0743

www.ijramr.com

International Journal of Recent Advances in Multidisciplinary Research

Vol. 07, Issue 11, pp. 6397-6400, November, 2020

RESEARCH ARTICLE

FALSE DATA INJECTION ATTACK IN HEALTHCARE

***Hind Alshambari and Emad Alsuwat**

Department of Computer Science, College of Computers and Information Technology, Taif University

ARTICLE INFO

Article History:

Received 20th August, 2020
Received in revised form
16th September, 2020
Accepted 24th October, 2020
Published online 30th November, 2020

Keywords:

Software, Data Injection, Healthcare, Cybersecurity, False Data Injection Attacks.

ABSTRACT

The Internet of Things (IoT) has the potential to transform healthcare dramatically via changing the way hospitals, clinics, and other healthcare facilities collect and use data. IoT can bring together major technical and business trends related to mobility, automation, and data analysis to improve patient care delivery. IoT is the networking of physical objects such as on-board sensors, actuators, and other equipment that collect and transmit activity information in real-time across the network. The data collected from these devices can then be analyzed by the organization to improve patient care. That is, we can use the collected data to offer new services or improve the already existing services. IoT will enable health organizations to manage data in such a way that would make them able to differentiate themselves from their competitors. However, there are some vulnerabilities in practice that would make the use of IoT data infeasible such as False data injection attacks. In this paper, we aim to investigate false data injection attacks, its impact on healthcare, and how to detect and prevent such attacks.

INTRODUCTION

Security incidents related to the Internet of Things (IoT) in the medical field will experience a sharp increase in 2020. This alarm signal has just been raised by the American association HIMMS, working to improve care health using technology. The reason is simple: the number of connected objects explodes, and cybercriminals see them as opportunities to earn a lot of money. IoT technologies have been widely adopted and millions of connected devices will appear in key sectors such as health and medical care. According to a recent study by the national center of hospital expertise, the IoT represented more than 60% of innovation projects in the health sector in 2019. With these new connected objects, hospitals and medical offices want to improve the patient experience and reduce manual tasks. For example, a hospital in Los Angeles has built rooms with connected speakers to give patients a feeling of greater independence. In France, the Eure-Seine Hospital Center has installed a robot for pediatric emergencies to welcome children, reduce their stress and give them confidence. These two examples demonstrate the potential of medical devices and portable IoT devices to assist patients during their recovery. IOT has connect and erase barriers between the two worlds, the real and virtual world. Its success is due to the evolution of hardware equipment and communication technologies including wireless. IoT is the result of the development and combination of different technologies. It encompasses almost all areas of current information technology (IT) such as smart cities, machine (Machine to Machine), healthcare, wireless sensor networks (Wireless Sensor Networks (WSN)), etc. Widespread use of IoT can only be achieved when there is good security for objects and communication networks. It is essential to put in place a policy of security that prevents any malicious or unauthorized object from accessing IoT systems, to read their data, modify it by inject false data or forge it. This paper presents the issues caused through false data injection by compromised node in WSN in healthcare and some techniques to detect and prevent the FDI attack.

Healthcare attack background: This section explores how the healthcare sector while working to improve treatment and patient care withnew technologies has been introduces to several cyber security attackthat made criminals and cyber threat actors look to exploit the vulnerabilities.

Health organizations, prime target of hackers: Large-scale attacks, such as WannaCry and Not Petya ransom-ware, have already affected healthcare organizations using outdated software, and it is only a matter of time before another disastrous attack is revealed. WannaCry, for example, cost the UK's National Health Service, the NHS, about £ 100 million after it shut down hospitals and cancel 19,000 patient appointments (2).

***Corresponding author: Hind Alshambari,**
Department of Computer Science, College of Computers and Information Technology, Taif University.

As the number of healthcare organizations deploying IoT solutions increases, so too do security incidents due to the countless vulnerabilities of connected devices. The American association HIMMS explains in its study that almost 76% of healthcare establishments have suffered a cyber-attack in the past year, in particular very sophisticated attacks, APT (advanced persistent threats) and attacks originating from internal. Email is truly the main tool used by attackers to carry out their hacks, since 30% of attacks targeting health organizations, were initiated by a phishing email or spear phishing.

False data injection attack: False data injection that also known as a bad data injection, this attack exploits the vulnerability of the sensor nods whish are not tamper resistant and can easily compromised by the attacker. The attacker aims to inject malicious mensuration and change the state estimation results to cause disruption that lead to consequences in healthcare like violates the privacy and the integrity of data records of patients. FDIA is considered a major cyber-attack which can cause huge damage by altering sensitive data. Such an attack is also able to breakdown the system. There are many applications that depends on data sensor like healthcare, when these sensors attacked by FDIA that lead to wrong reports with false data. In healthcare the compromised node in network sensor due to the false data injection can lead to negative estimations and modify decision and many legitimate reports are dropped.

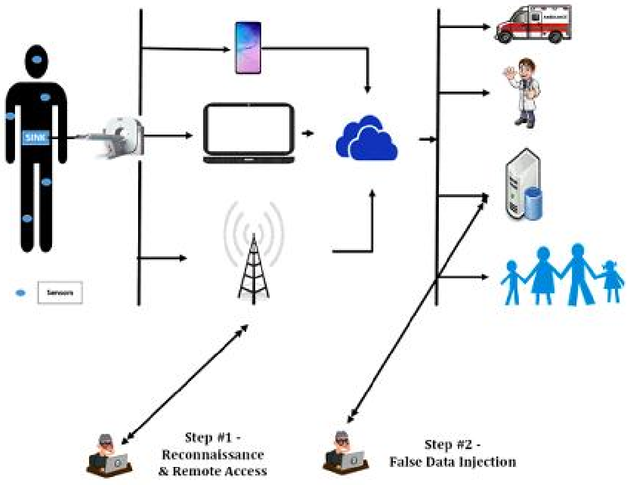

Figure 1. False Data Injection in Healthcare (3)

Healthcare attack detections

Detection of Intrusions In medical connected objects: One of the means used to acquire the information necessary for detection is the use of tracing techniques, which not only make it possible to have the list of system calls made, but also their arguments and information at different levels, when the we trace the kernel, like network information, the sequence of actions of the scheduler or even information on the use of the processor (4). Besides, Murtaza explains that the traces at the level of the nucleus make it possible to acquire much more useful information for the detection of intrusion. Tracing techniques are detailed in the corresponding section. However, the uses of intrusion detection systems have evolved with the arrival of new computer applications. Regarding cloud computing, Modi precisely describes the different intrusion detection techniques that can be used in this context.

The author explains that traditional systems (HIDS and NIDS) can be used, but that new systems have appeared. This is the case with distributed intrusion detection systems (DIDS) which are made up of several IDSs placed in a broad network and which correspond with each other (either with a main server or directly between them). These systems can combine both HIDS and NIDS. In addition, intrusion detection systems based on hypervisors of virtual machines have also been developed. Such systems thus make it possible to monitor the exchange of information between the virtual machines, between the virtual machines and the hypervisor and even with the hypervisor of the virtual network. Likewise, the democratization of smart phones, and in particular of the Android operating system, has created new threats for users. This justified various works on intrusion detection on such devices. Borek listed the different intrusion detection techniques used for objects running Android.

He explains that several works detect illegitimate applications according to their source code which can be used directly on the phone or on a server. In addition, dynamic analysis techniques have also been proposed, whether based on network information such as Ceroid or on information from the behavior of the. In addition, like traditional IDS, some works use tracking techniques to obtain system calls from the phone and thus be able to detect intrusions. This is the case for the solution proposed by Borek, but also for Copperdroid (Tam *et al*., 2015) and Crowdroid (Burguera and Nadjm-Tehrani, 2011)(5). These last two works are based respectively on an emulation of the Android system with Qemu and on events plotted directly on the phone but sent to a server for their analysis.

Detection of False Data Injection Attacks on medical connected objects: To detect attacks injecting false data into control systems, Wang *et al*. (6) propose an approach based on the relation of states. The proposed approach is a real-time system that monitors system states, detects inconsistent states and deduces the origins of attacks. Using the variable relationship graph, when an abnormal condition is detected, we can trace the chain of dependencies of the variable (s) in question and deduce the possible origin of the attack. The system architecture has three parts: a component analysis module which automatically analyzes the system variables to extract components and generate a graph describing the states of the valid system as well as another graph of relationships between variables. Here, alternation vectors that record the alternation relationships between two continuous states are also used to represent the real-time states of a component in normal operation. The second module is a detection module which uses the state graph to generate an invalid state alert if a new alternation vector is notfound in the state graph or an invalid transition alert if the current state could not be reached from a previous state. Finally, an origin inference module helps to locate the origin of or attacks by injection of false data. The system assessment by Wang *et al*. gives a detection rate of 95.83% and a false positive rate of (0.0125%). A device using a multi-algorithm intrusion detection approach for the Modbus TCP protocol was developed by Cheung *et al*.(7). This approach is based on a protocol level model, a model of expected communication patterns and a server and services detection model. The protocollevel model uses function codes, exception codes, implementation of Snort-based rules as well as the PVS language to formally specify a specific Modbus device. In the planned communication patterns model, the communication models between the different components of the SCADA network are created, and rules based on Snort are developed to detect deviations from these models. Note that here, the Snort rules are written to detect the "complement" of the models symbolizing the normal running. The last component which relies on learning to detect changes in the availability of the server or service consists of two detectors which are an EMERALD Bayes and EModbus sensor(8). Experiments show Monitoring SCADA networks is beneficial in the approach of model-based intrusion detection and this approach consider supportive for the approach of signature-based.(9).

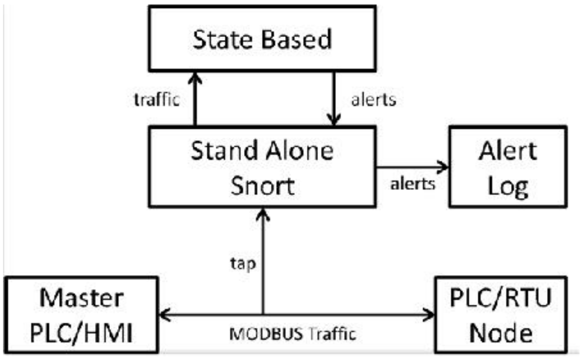

Figure 2. Intrusion Detection System Architecture (7)

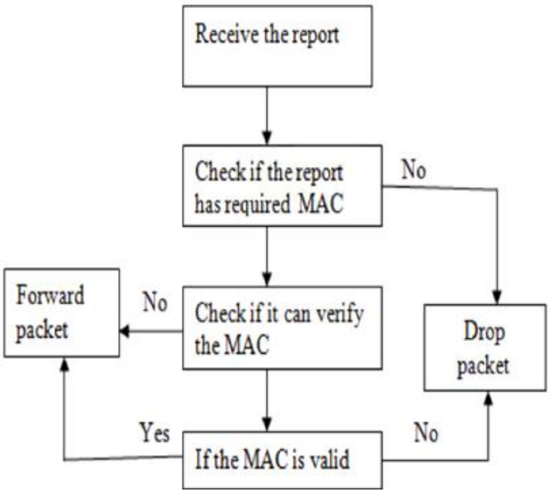

Figure 2. Flow diagram of en-route filtering process(15)

Solutions against False Data Injection Attacks in Healthcare: It is very Important to decrease the laying open area of objects connected to attacks and this is very complex task. To links between objects with the cloud, it demands knowing the value chain of architectural. We need more understanding of the objects themselves, its sensors and central processing unit, domestic and distant networks, protocols of all levels, then servers, their software and the data processing carried out there(10). The needs have been well known for years. Corporations to secure this part of the value chain suggests tools but they have been putting themselves for a brief time in connected objects.

Securing cloud: In terms of IoT security, there is obviously objects collecting data , then save it and compact in the servers and cloud to provide more privacy for data. This can be in the cloud of your connected object provider as well as in Apple's iCloud (for iHealth). Security for the user is in this case both a technical question.

Securing Wireless sensor: The approach adopted by many existing works to reduce the vulnerability of decentralized systems is to introduce the concept of trust. However, it is difficult to use these solutions in the case of wireless sensor networks, in particular because of the limitations on their energy and communication costs, imposed by the lightness of the hardware supports (11).

Boukerche, El-Khatib *et al.* (12) in propose an anonymous routing solution based on mixing networks as well as on a trusted authority which makes it possible to select only the trusted nodes for routing. Their solution called SDAR for Secure Distributed Anonymous Routing uses a trusted certification authority that generates private and public network keys. Unlike mixing networks, flow modification techniques are not used. Only the appearance is changed by encryption. A source node wishing to communicate with a destination node will first seek to establish the path to route its frame(13).

Hop-by-hop approach: Hop-by-hop is a security authentication approach that checks the integrity of the data by using pairwise key authentication. On other hand Hop-by-hop approach provide protection for wireless sensors network against FDIA(14).

En-route filtering schemes: False data injection attacks can be defeated by using En-route filtering. En-rout also used to enhance and improve the capability of filtering against the nodecomptonizations(15). En routing checks the destination node and the intermediate node authentication to prevent number of hops the false message travels to safe energy. The mechanism in En routing is to verify the MAC for each forwarding node, and it works by checks the integrity of the received report that comes from source node or lower associated node by verifying the MAC in received report. The report will be forward if the MAC verification is succeeds, otherwise it will be dropped.

Conclusion

Digital world made our daily lives much easier on several ways such as online shopping, banking, social media networking, and mailing services. However, this world has been exposed to much more cyber-attacks and data breaches that are occurring all the time especially medical institutions. Thus, these medical institutions need to be more careful in using and dealing with trending technology. Sensitive patients record which are collected by the trending technology need a back-up plan and servers to put back services in case these accords got hacked.

Security implements on medical institutions technologies need to be implemented in multiple layers and always training users by specialized IT departments. False data injection is considered one of the major cyber-attacks that can cause a huge damage by modifying the sensitive data. This kind of attack also can breakdown computer systems. This research paper has focused on false data injection in healthcare institutions, the impact of such attacks. We also discussed techniques and solutions used to detect and prevent such attacks, such as En-route filtering , anonymous routing, and intrusion detection systems.

REFERENCES

Ahmed, M. 2019. *False Image Injection Prevention Using iChain.* Applied Sciences, 9(20): p. 4328.

Axelsson, S. 2000. *Intrusion detection systems: A survey and taxonomy*. Technical report.

Boukerche, A., *et al*. 2004. *Anonymity enabling scheme for wireless ad hoc networks*. in *IEEE Global Telecommunications Conference Workshops, GlobeCom Workshops 2004*. 2004. IEEE.

Burguera, I., U. Zurutuza, and S. Nadjm-Tehrani. 2011. *Crowdroid: behavior-based malware detection system for android*. in *Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices*.

Choi, D.-H. and L. Xie. 2013. *Impact analysis of locational marginal price subject to power system topology errors*. in *2013 IEEE International Conference on Smart Grid Communications (SmartGridComm)*. 2013. IEEE.

Esmalifalak, M., *et al*., *Detecting stealthy false data injection using machine learning in smart grid.* IEEE Systems Journal, 2014. 11(3): p. 1644-1652.

Gao, W. and T.H. Morris, *On cyber attacks and signature based intrusion detection for modbus based industrial control systems.* Journal of Digital Forensics, Security and Law, 2014. 9(1): p. 3.

Goldenberg, N. and A. Wool, *Accurate modeling of Modbus/TCP for intrusion detection in SCADA systems.* International Journal of Critical Infrastructure Protection, 2013. 6: p. 63–75.

Haque, S.A., M. Rahman, and S.M. Aziz, *Sensor anomaly detection in wireless sensor networks for healthcare.* Sensors, 2015. 15(4): p. 8764-8786.

Initiative, I.o.T.G.S., *ITU.* Geneva, Switzerland, 2015.

Liu, Y., P. Ning, and M.K. Reiter, *False data injection attacks against state estimation in electric power grids.* ACM Transactions on Information and System Security (TISSEC), 2011. 14(1): p. 1-33.

Silva, R., *et al*. *A comparison of approaches to node and service discovery in 6lowPAN wireless sensor networks*. in *Proceedings of the 5th ACM symposium on QoS and security for wireless and mobile networks*. 2009.

Stajano, F., *Security for ubiquitous computing*. Vol. 1. 2002: Wiley Online Library.

Wang, Y., *et al*. *Srid: State relation based intrusion detection for false data injection attacks in scada*. in *European Symposium on Research in Computer Security*. 2014. Springer.

WSNs, I., *An Evaluation Of En-Route Filtering Methods For False Data Injection Attack.*

****