International Journal For Technological Research In Engineering
Volume 8, Issue 4, December-2020 *ISSN (Online): 2347 - 4718*

Security Issues in the Internet of Things (IoT): A Comprehensive Study

[1]Kunal Yadav, [2]Aryaveer Singh, [3]Yuvraj Rajput, [4]Prof.Indu Khatri
[1,2,3] Students, [4]Guide
Department of Computer science
Bhagwan Mahaveer College of Engineering and Management, Sonipat, Harayana

ABSTRACT:- The Internet of Things (IoT) has fundamentally changed the way information technology and communication environments work, with significant advantages derived from wireless sensors and nanotechnology, among others. While IoT is still a growing and expanding platform, the current research in privacy and security shows there is little integration and unification of security and privacy that may affect user adoption of the technology because of fear of personal data exposure. The surveys conducted so far focus on vulnerabilities based on information exchange technologies applicable to the Internet. None of the surveys has brought out the integrated privacy and security perspective centered on the user. The aim of this paper is to provide the reader with a comprehensive discussion on the current state of the art of IoT, with particular focus on what have been done in the areas of privacy and security threats, attack surface, vulnerabilities and countermeasures and to propose a threat taxonomy. IoT user requirements and challenges were identified and discussed to highlight the baseline security and privacy needs and concerns of the user. The paper also proposed threat taxonomy to address the security requirements in a broader perspective. This survey of IoT Privacy and Security has been undertaken through a systematic literature review using online databases and other resources to search for all articles that meet certain criteria, entering information about each study into a personal database, and then drawing up tables summarizing the current state of literature. As a result, the paper distills the latest developments in IoT privacy and security, highlights the open issues and identifies areas for further research.

1. INTRODUCTION

The Internet of Things (IoT) has attracted considerable attention during the past few years. The concept of IoT was firstly proposed by Kevin Ashton in 1999. Due to rapid advancements in mobile communication, Wireless Sensor Networks (WSN), Radio Frequency Identification (RFID), and cloud computing, communications among IoT devices has become more convenient than it was before. IoT devices are capable of cooperating with one another. The World of IoT includes a huge variety of devices that include smartphones, personal computers, PDAs, laptops, tablets, and other hand-held embedded devices. The IoT devices are based on cost-effective sensors and wireless communication systems to communicate with each other and transfer meaningful information to the centralized system. In general, the term **IoT** (Internet of Things) refers to the rapidly growing number of digital devices – the quantity is now billions – these devices can communicate and interact with others over the network/internet worldwide and they can be remotely monitored and controlled. The IoT includes only smart sensors and other devices. On the operational level of IoT, for example weather data is collected. IoT offers new opportunities for cities to use data to manage traffic, cut pollution, make better use of infrastructure and keep citizens safe and clean.

The IoT has successfully integrated the fictional space and the real world on the same platform. The major targets of IoT are the configuration of a smart environment and self-conscious independent devices such as smart living, smart items, smart health, and smart cities among others. Nowadays the adoption rate of IoT devices is very high, more and more devices are connected via the internet. According to appraisal, there are 30 billion connected things with approximately 200 billion connections that will generate revenue of approximately 700 billion euros by the year 2020. Now in China, there are nine billion devices that are expected to reach 24 billion by the year 2020. In future, the IoT will completely change our living styles and business models. It will permit people and devices to communicate anytime, anyplace, with any device under ideal conditions using any network and any service. The main goal of IoT is to create Superior world for human beings in the future.

On every day, The IoT devices are targeted by attackers and intruders. An appraisal discloses that 70% of the IoT devices are very easy to attack. Therefore, an efficient mechanism is extremely needed to secure the devices connected to the internet against hackers and intruders.

2. SECURITY PROBLEMS AND CONSIDERATIONS

The IoT is an ecosystem of physical objects that are connected and accessible through the Internet. With a single application on a smartphone, IoT devices can be efficiently managed and monitored, and, in general, they work smoothly. But they are not secure in an era of relentlessly growing cyber-attacks. One reason is that IoT devices are not plug-and-play. Many are delivered with simple password authentication. And some organizations have implemented these devices without altering the factory settings. This is a

major risk. Once a hacker knows the default credentials, which typically exist in thousands of similar devices, it's easy for him or her to gain access to IoT systems and a back door into a corporate network—or into somebody's smart home. Smartphones—also, of course, wireless devices—have had few problems blocking viruses and other types of malware.

The newer smartphones and tablets were not only designed for a connected world but also molded by developers who applied lessons learned from the desktops preceding them. Unfortunately, this doesn't mean that IoT manufacturers will find it relatively easy to improve security. Because the IoT remains a relatively young market, many product designers and manufacturers appear more interested in getting their products to market quickly than in taking the required steps to build in good security from the start.

There are few steps that companies or smart home owners or both can take to help mitigate security vulnerability:

Consider implementing loosely coupled IoT systems.

This would require creating a separate service set identifier (SSID) and virtual LAN and having the capacity to route that traffic through a firewall. The network, meanwhile, would be configured and managed from a centralized location.

This can help ensure that the failure of a single device doesn't lead to widespread failure. This partial solution, of course, would need to be implemented in such a way that it blends organization-specific operational capabilities with multilayered cyber risk management techniques.

Insert security into the supply chain.

Start relationships with supply chain managers that lead to an agreement mandating no approval for any IoT purchases unless a security team has signed off on them.

Control access within an IoT environment.

First, organizations should identify the behaviors and activities deemed accepted by connected devices, and then put in controls that account for this. This should mitigate malicious or unauthorized activities.

Limit the ability of IoT devices to initiate corporate network connections.

Instead, IoT devices should connect to networks only through network firewalls and access control lists. This would not prevent adversaries from attacking systems that have direct network connections. It would, however, limit their ability to laterally move within networks.

End users must make a point of embracing their own security precautions.

This includes changing passwords and implementing stronger ones, installing patches when available, checking the device manufacturer's website regularly for firmware updates and, of course, using Internet security software.

Conduct research before purchasing devices.

Make sure you know what types of data they collect, how it is stored and protected and whether it's shared with third parties. Also review policies or protections regarding data breaches.

Notwithstanding a lack of guidance, business and technology leaders should recognize that essentially they have little choice but to develop and implement their own global cyber risk standards. They should also try to share them with other entities. Formal standards are highly likely to become a reality at some point, but this won't occur for years.
If major IoT users partner with others and operate cooperatively, significant value can be created. It's true—in lieu of formal standards—that major hiccups could become an issue in the early-going.

3. ENHANCING IOT SECURITY

Run security tests IoT source code:To build better security into IoT, organizations should start with the smallest component in their network infrastructure—the code.
The majority of IoT devices are very small Therefore, the source code tends to be written in the 'common tongue'—C or C++ and C# languages which frequently fall victim to common problems like memory leaks and buffer-overflow vulnerabilities. These issues are the network equivalent of the common cold.
Security and IT administrators can also use stack cookies. These are randomized data strings that applications are coded to write into the stack just before the Instruction Pointer Register, to which data overflows if a buffer overflow occurs. In the event a buffer overflow does occur, the stack cookie gets overwritten.
The application will be further coded to verify that the stack cookie string will continue to match how the code was initially written. If the stack cookie doesn't match, the application terminates.

Deploy Access Control System: Organizations should first identify the behaviors and activities that are deemed acceptable by connected things within the IoT environment, and then put in place controls that account for this but at the same time don't hinder processes.
Instead of using a separate VLAN [virtual LAN] or network segment which can be restrictive and debilitating for IoT devices, implement context-aware access controls throughout your network to allow appropriate actions and behaviors, not just at the connection level but also at the command and data transfer levels. This will ensure that devices can operate as

planned while also limiting their ability to conduct malicious or unauthorized activities.

Need IoT gear to meet all security standards: Organizations as a matter of course hire all kinds of service providers, and in some cases those services are provided through equipment that's placed on the customer's premises. In the age of

IoT, there's a good chance the machinery will be connected and therefore vulnerable to hacking and other intrusions. Make sure it's clear who's responsible for updates and the lifecycle of the equipment, as well as if you'll have access to it in case of an incident. Those same vendors would push back on routine patching responsibilities or upgrades to operating systems.

In some way the hardware OEMs and the software companies now all expect to be held accountable to identify and quickly resolve weaknesses in their products, so too should the companies that provide us the IP cameras, medical devices, printers, wireless access points, refrigerators, environmental controls and the untold number of other IoT devices upon which we increasingly rely. Companies should apply the controls outlined in common security frameworks to IoT devices. For example, include security functional requirements in your contracts; request recent vulnerability scans or assert the right to scan them yourself; obligate the vendors to provide timely updates to address identified weaknesses; and rescan the devices after any firmware updates to ensure that identified issues have been resolved and that no new issues have been introduced.

Stopping IoT identity spoofing: Hackers and their techniques have become more proficient over the years, and this can represent a big threat for IoT security.

They continually up their game like counterfeiters and forgers. The exponential increase in IoT devices means that the attack surface or the attack vector has increased exponentially.

All IoT devices must have a unique identity. In the absence of a unique identity, an organization is at high risk of being spoofed or hacked from the microcontroller level to the endpoint devices at the network edge to the applications and the transport layer.

Denying IoT devices initiate network connections: Enterprises can also force connections to IoT devices to go through jump hosts and/or network proxies. By proxying the connection in a funnel point, an organization can then inspect network traffic prior to coming from and to IoT devices, and interrogate (the traffic) more effectively. That enables it to determine if the traffic and the payloads it carries are appropriate for the IoT device to be receiving or transmitting.

Give IoT a network of its own: Many types of control devices, such as thermostats and lighting controls, connect via wireless. However, most enterprise wireless networks require WPA2-Enterprise/802.1x, but Most of those devices do not support WPA2-Enterprise So, Developing a more secure device would be ideal. However, if the environment supports it you could put those devices on their own wireless network, segregated from the production network and allowing Internet access only. That would require creating a separate service set identifier (SSID) and virtual LAN and having the capacity to route that traffic through a firewall, then put them on our guest network, which is segregated from production.

Also, avoid public Wi-Fi networks. You might want to manage your IoT devices through your mobile device in a coffee shop across town. If you're on public Wi-Fi generally not a good idea one should a VPN

4. CONCLUSION

In this paper, we analyzed the solutions currently available for the implementation of urban IoTs. The discussed technologies are close to being standardized, and industry players are already active in the production of devices that take advantage of these technologies to enable the applications of interest. In fact, while the range of design options for IoT systems is rather wide, the set of open and standardized protocols is significantly smaller. The enabling technologies, furthermore, have reached a level of maturity that allows for the practical realization of IoT solutions and services, starting from field trials that will hopefully help clear the uncertainty that still prevents a massive adoption of the IoT paradigm. A concrete proof-of-concept implementation, deployed in collaboration with the city of Padova, Italy, can be a relevant example of application of the IoT paradigm to smart city.

REFERENCE

- J. S. Kumar and D. R. Patel, "A survey on internet of things: Security and privacy issues," International Journal of Computer Applications, vol. 90, no. 11, 2014.
- M. Abomhara and G. M. Køien, "Security and privacy in the internet of things: Current status and open issues," in Privacy and Security in Mobile Systems (PRISMS), International Conference on. IEEE, 2014
- Privacy and security of Internet of Things ,Author "Markb Mbock " ,"Ogonjia George" ,"Okeyob Joseph "MuliaroWafulaa".
- Castellani, S. Loreto, A. Rahman, T. Fossati, and E. Dijk, Best practices for HTTP-CoAP mapping implementation, draft-castellani-core-http-mapping-07 (work in progress), s.l.: IETF 2013. [Online]. Available: https://tools.ietf.org/html/draft-castellani-core-http-mapping-02.
- S. Deering and R. Hinden, Internet Protocol, Version 6 (IPv6) Specification, RFC2460, s.l.: IETF Dec. 1998. [Online]. Available: https://www.ietf.org/ rfc/rfc2460.txt.
- G. Montenegro, N. Kushalnagar, J. Hui, and D. Culler, Transmission of IPv6 packets over IEEE 802.15.4 networks, RFC4944, s.l.: IETF Sep. 2007. [Online]. Available: http://tools.ietf.org/html/rfc4944.
- J. Hui and P. Thubert, Compression format for IPv6 datagrams over IEEE802.15.4-Based Networks,

RFC6282, s.l.: IETF Sep. 2011. [Online]. Available: http://tools.ietf.org/html/rfc6282.

- K. Rose, S. Eldridge, and L. Chapin, "The internet of things: Anoverview," The Internet Society (ISOC), pp. 1–50, 2015.
- H. Ning, H. Liu, and L. T. Yang, "Cyberentity security in the internet of things," Computer, vol. 46, no. 4, pp. 46–53, 2013.

