Security Threats for Short Range Communication Wireless Network on IoT Devices

Km Ujjawal[1]*, Sharvan Kumar Garg[2], Arif Ali[3], Deepak Kumar Singh[4]

Abstract

The Internet of Things (IoT) is becoming an advanced technology that is part of the daily activities of human life. The number of IoT devices is spending is predicted toincrease$ 1 trillion by 2022. Therefore, a large number of electronic gadgets connected to the Internet to transfer the data globally and other IoT devices use Bluetooth for short-distance data transfer because Bluetooth use low power and easily available on most of the devices but This creates a major challenge in the IoT field and one of the challenges is related to Bluetooth IoT devices Securities. User confidential information is transmitted between devices, and a few security issues such as privacy, confidentiality, integrity, and trustworthy issues need to be addressed. This paper provides an overview of the new attack vector affecting almost all connected devices. It influences about 5.3 billion gadgets across Android, home windows, Linux, and iOS. The new vector is known as BLUEBORNE ATTACKS. These attacks are effected all devices which are connected to Bluetooth. But in this paper, we are analysing BLUEBORNE ATTACKS and finding out what effect does this have on Bluetooth-connected devices, especially on Smartwatch. Also, we are analysing if hackers perform hacking activities by using BlueBorne attack and perform on smartwatch then what harmful activates are performed and also what advantages are taken.

Keywords: Internet of Thing, Smart Devices, Security threats, Bluetooth, Blue Borne Attacks

Doi Number: 10.4704/nq.2022.20.14. NQ880108 **NeuroQuantology 2022; 20(14):775-783**

1. INTRODUCTION

The Internet of Things is playing a very important role in the digital world and this is basically a combination of two words that is an internet of things, the internet is a type of global network that is used to connect devices and also help these devices globally com-munications to another device.

The other word is Thing which denotes the object. This technology basically enables things to talk to the internet is called the internet of things. According to its name that is the Inter-net of Things is basically work on a living thing as well as a non-living thing. Today these technologies are used in our everyday lifestyle such as at domestic, in public places, and within the place of work. A few items are audio system, TVs, cameras, doors, shutters, lighting, sensors, clocks, and many others [1]. This generation is innovative day by day and includes human life. inside the equal way, the existence of the individual is made easier however the demanding situations also are expanded and the very huge venture is safety, however these associated gadgets have emer-ged as appealing recommendations for at-tackers due to the fact their present day safety structure is often vulnerable or mis-taken, as shown via numerous threats such as Mirai, BlueBorne,

***Corresponding Author: -** Km Ujjawal
Address: - [1]*Research Scholar (Cyber Security), Subharti Institute of Technology & Engineering, Swami Vivekanand Subharti University, Meerut, E-mail:- Ujjwalmishra167@gmail.com
[2]Professor (CSE), Subharti Institute of Technology & Engineering, Swami Vivekanand Subharti University, Meerut
[3]Assistant Professor (CSE), School of Computer Science & Engineering, Dev Bhoomi Uttarakhand University, Dehradun
[4]Assistant Professor (CSE), School of Computer Science & Engineering, Dev Bhoomi Uttarakhand University, Dehradun
Relevant conflicts of interest/financial disclosures: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

DOS, and many others [2].

1.1 Bluetooth

In the section we discuss about Bluetooth, Bluetooth is a short-distance wireless network it was introduced in 1997 by Jim Kardach of Intel. The range of Bluetooth from 2.402 to 2.48 GHz it works on UHF radio waves in the Special Interest Group (ISM) band. It is also called a Personal Area Network. This tech-nology is basically used to connect one Bluetooth device to another Bluetooth device. The application of Bluetooth is used to transfer file, setting up the network, print, etc. also Bluetooth play very fundamentals role in booming technologies such as the Internet of Thing, Cloud Computing, Artificial Intelligence, etc [3]. On the internet of thing Bluetooth help to connect the objects which are short distance for example in a smart home, smart agricul-ture, smart hospital etc. there are number of an object are present and all object communicates with each other with the help of Bluetooth. If I talk about in Artificial Intel-ligence so Bluetooth also plays a very important role such as machine-to-machine communication etc. in cloud computing like sharing files, store files in virtually.

Bluetooth Classic and Bluetooth Low Energy cannot communicate, but both can be used on the same device. The device with Bluetooth technology notes has a dual-stack, which is a combination of both technological stacks. The control layer must have different layers of other technologies due to different radio specifications and coding, the Host layer allo-cate different layers and specific tech-nologies. Since Bluetooth Low Energy was designed for very low power consumption, it has a slower data rate compared to Bluetooth Classic. Bluetooth Classic can reach from 1Mb / s to 3Mb / s compared to the Bluetooth Low Energy data rate from 125Kb / s to 2Mb / s [4]. The main reason for using less energy to work in sleep mode, Bluetooth Low Energy is often in sleep mode and transmits data periodically. Bluetooth Classic and Low Power runs on the same 2.4GHz band. The difference lies in the layout of the channel. Bluetooth Classic has 79 channels with 1MHz bandwidth, while Blue - tooth Low Energy has 40 channels with 2MHz bandwidth and 3 channels defined as advertis - ing channels. In addition, both technologies have slightly different matching processes, authentication and encryption. The frequency hopping is in both technologies. The following section describes the Bluetooth Low Energy protocol stack, which is designed to fit devices designed for low power consumption. Although Blueborne may only be associated with Bluetooth Low Energy, it has been selected due to its growing popularity and significant similarity to the protocol layers and the Bluetooth Classic.

1.2 Bluetooth Low Energy specification

Bluetooth low energy was introduced in 2010 with a version of core speciation 4.0 [5]. Version 4.0 which separates Bluetooth intro-duces classic Bluetooth and Bluetooth Law Energy. The term Low Power was assigned later, indicating its limited use of energy. Previously it was marketed as a Bluetooth smart. From this point on, both agreements have distinguished development and are not mutually exclusive.

Like the Bluetooth Classic, Bluetooth Low Energy operates with a 2.4GHz licensed ISM band designed for industrial, scientific and medical purposes. The band is divided into 40 channels with 2MHz spaces between each channel. Three channels are used as adver-tising channels, in which devices in non-reversible mode transmit advertising packages. Some channels are data channels used to transmit data [4]. Frequency Hopping Spread Spectrum is used to reduce distortion and blurring, devices transmit each packet to a different channel. Communication between devices uses the primary / slave model, where one device is the connection launcher, the fore-man, and the other device is the slave.

The Bluetooth Low Energy protocol 2.1 stack consists of three main building blocks, Applica-tion, Host, and controller. The application is above the protocol stack and interacts with layers in the protocol stack. The Host layer is installed on top of the operating system, with the exception of the integrated devices, where the Hosting layer is integrated with the Control layer in a single microprocessor. The control layer is used within the hardware solution of the device. The interface between Host and Administrator provides the Host Controller

Interface (HCI). HCI provides similar access to Bluetooth Low Energy hardware components

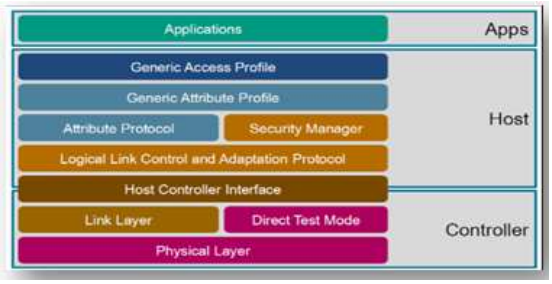


Fig: - 1 Bluetooth Low Energy Protocol Stack [6]

1.3 Bluetooth Low Energy stack controller layer

According to the Bluetooth Core Specification [4], the control layer refers to all the layers under HCI. The control layer controls the conversion of sensible data into data packets, ready for radio transmission. Provides reci - peent and transmitter, e.g. syncing both so that they are in the same channel. In addition, data encryption as well key production is done on the control layer without the need for a Hosting layer.

1.4 Physical Layer

The virtual layer, also called PHY [2], is responsible for transmitting and receiving packets at the body channel. This layer con - verts data transmission to and from baseband to him required formats. The radio operates on 40 channels from 2400MHz to 2485MHz, where channels with indexes 37, 38 and 39 advertise visual channels. They are spread out across all spectrums to reduce disruption to other networks, channel 37 is the first channel in the band, channel 39 is the last in the band, but the channel with index 38 is not.4 in the middle of the spectrum, located between Wi-Fi channels numbered 1 and 6 [7], which are the most widely used channels.

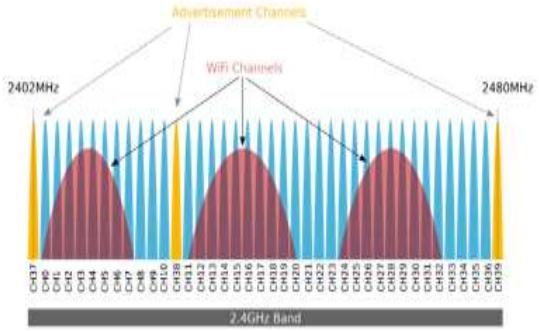


Fig:-2 Visible Bluetooth Low Energy channels and WiFi channel interference [7]

From version 5 of Bluetooth, Bluetooth Low Energy has 3 Physical Layer variants, LE 1M, LE 2M and LE Code. Each of them has a different advantage against the others. Each alternative uses Gaussian Frequency Shift Keying (GFSK) to transfer data via the wind. LE 1M is the same, used under Bluetooth version 5. It has a logo Mega 1 averages per second, equivalent to 1Mbs per data stream. LE Coded provides approximately four times the width compared to Bluetooth 4.0. Achieved with im-proved bit error detection and correction, which has the disadvantage of lowering the data rate. ILE 2M supports the level of 2 Mega symbols per second, while 1 symbol represents 1 lama. LE 2M supports data speeds of up to 2Mbs but reduces bandwidth. Important the profitability of LE 2M decreases power consumption because the maximum data rate is reduced transfer time. All of these data figures are not only theoretical.

1.5 Link Layer

Link Layer controls communication and send- ing or receiving packets. It acts as a state machine with different regions for each job 2.3. If the device wants to communicate with it another device, it enters the scanning mode for active scanning or scanning of the operation. in this case, the device listens to advertising channels of advertising packages from others devices. Those devices that distribute adver- tising packages are in an advertising environ- ment. That's right sending packages to individual advertising channels by any means and listening to feedback from devices that capture advertising channels. When the device master, advertising channels, has enough infor- mation from the slave device, to send adver-

tising packages, it starts connection. The connection status is the last state in this process.

In a connection status, both devices exchange data from time to time In Connection Events [8].In the first case, the primary device response to the advertising package containing the connection request package, when defining details about communication as an interval between each communication event or frequency hopping value. When the connection request package is accepted, both devices turn the situation into a connection. In the case of communication, the master and the slave exchanged data packets at every agreed time interval. If they do not have data to exchange, these packets are empty. When one device stops sending packets, connection is closed.

1.6 Bluetooth Low Energy stack handling layer

This protocol stack layer is defined as all layers above HCI and boils down to non-essential profiles in the Bluetooth Low Energy stack. These layers use contextual functions from the lower layer and the more important features, such as the separation and reassembly of the packages, multiplexing or service level. Often, they are called contracts, sometimes layers. Blueborne risk layers are not explored in this section.

1.7 Logical Link Control and Adaptation Protocol and Bluetooth Network Encapsulation Protocol

Logical Link Control and Adaptation Protocol, or L2CAP, is the lowest layer the handling side of the Bluetooth Low Energy stack. L2CAP is responsible for many services. Provides offline or offline-based services. This layer includes repetition, fragmentation and re-integration, control of each channel flow and error control. L2CAP data provides sensible channels for high protocols, ensuring that most protocols can use the same lower body layer [4].

L2CAP is pocket based but collaborative on channels. Channel identifier (CID) used to manage all these channels. The channel connects the remote address with end point on device. Some channels have a modified CID and work in the same way all devices. Static channels are used to send offline data, stream multiple, or establish related channels. The CID is governed by strength and independence from other connected devices. Recognition be-tween the same CID for connected variants devices are made to mimic CID with a sensible link, which is unique to all devices. The main connection between the devices is the dynamic channels. Splitting and reassembling makes transport of larger packets more limited baseband pack. This implementation separates the package from the top protocols to the smaller ones pieces, which can be transferred to the lower layer of the body. If the package comes from body parts, reassembled with hundreds of packets and transferred to higher protocols in stack.

In the connection process, both devices exchange configuration packs. Some of designned for L2CAP. Each stop request has only one option value. Among these options is the Maximum Transmission Unit (MTU), which is the highest payload data size high-end protocols, Quality of Service (QoS) option, which specifies the flow of communication as the average data rate or delay. I stopping is done in two steps. The first step involves the device sending the setting ask for a specific option. Upon receipt of a second machine configuretion request, this device responds with feedback. This reply message includes an agreement with prices or inconsistencies and default values

Bluetooth supports using the phone as an online modem between devices. This feature is provided by Bluetooth Network Encapsulation Protocol (BNEP). Packets come from a variety of networks protocols integrated into a Bluetooth-compatible packet format. These include packages provided to L2CAP via sen-sible channels focused on connectivity. BNEP data enables IP switch packets on WPAN 2 and is bound to L2CAP.

1.8 Generic Access Profile

Generic Access Profile (GAP) provides the definition and management of interactions and other devices. This includes tools available, streaming and establishing links. The GAP de - fines these key functions to ensure cohe-rence

all devices support Bluetooth Low Energy. GAP roles introduce device behaviour on the basis of physical objects.

- Central
- Observer
- Broadcaster
- Peripheral

Those roles form pairs, in which only rooted devices with pairs can communicate and the broadcaster and the viewer communicate through an advertising process and the broadcaster occasionally sends advertising packages and the viewer receives or scans those advertising packages. Peripheral and central role devices are also referred to as slaves and artisans. When the device in the peripheral role is enslaved and can links only accept, not establish. Its pairing device in the mid-range is also key begins to communicate with multiple devices [6].

In addition to device roles, GAP uses modes. GAP mode is a condition, which is describes its position against the pairing device. Those methods are divided into recovery methods connection methods [6].
GAP also controls Bluetooth Low Energy security by selecting security connection mode or by setting up encryption type. This defen-sive feature is not essential to Blue-borne's risk, so it is not analyzed in detail.

1.9 Security Manager Protocol

Security Manager Protocol (SMP) defines the process of matching and distributing keys between devices. The pairing process is carried out in 3 stages. In the first stage, the devices exchange information on their input and output capabilities. Based on their strengths determine which pairing method is used in the second phase. In the whole second phase one of the matching methods is developed.

1.10 Generic Attribute Protocol and Attribute Protocol

The Attribute Protocol (ATT) serves as a server for exposing local services to remote devices. Those local services are stored as a set of attributes. The ATT communication works as communication between client and server. The ATT client at a remote device can discover, read and write attributes at the ATT server.

The attribute has a universally Unique Identifier (UUID) identifier for individual services. ATT does not want to consider UUID, ATT server only retains UUID with additional values [4]. Generic Attribute Protocol (GATT) defines the data from the ATT protocol worked. GATT incorporates features from ATT to sensible groups. Each the group represents one service on the device and includes details about the service. These details they vary from service name to specific service function. Attribute format shown in Figure 2.4. The Properties Holder is used as an attribute address. Qualification Type, GATT can determine the type of data in the attribute, for example, of service (value 0x2800) or service element (value 0x2803) [6].

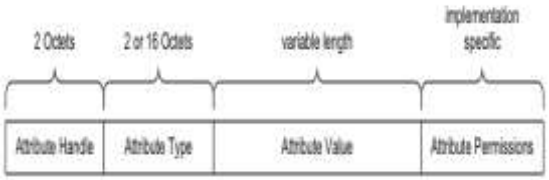


Fig:-4 ATT format attribute [8]

The number of use cases of Bluetooth increases similarly the number of vulnerabilities is also increasing in various forms the one of most concerning vulnerabilities is BlueBorne.

2 BlueBorne Attacks

This phase focuses first on system-related attacks targeted at IoT devices, and then discusses the BlueBorne attacks and other security measures proposed in associated work to address that attacks. In latest years, numerous attacks on conventional networks and online protocols exploiting vulnerabilities in IoT gadgets utilized in smart homes had been suggested [10]. A popular attack is a BlueBorne attack. The aim of the BlueBorne attack is to impact nearly every connected device. The BlueBorne is different from tra-ditional cyber-attacks because BlueBorne does not require clicking and downloading the malicious files even on the internet. It is spared through the air. It is basically a type of Bluetooth attack. In this attack, the hacker does not need to target

devices as well as pair to targeted devices. If Bluetooth is turned on then hackers can be connected the device takes control and spared through air and hacker can perform different hacking activities such as malware and ransomware and man in the mid-dle attack etc., which is completely un-detected by the user's imagination. It is also called airborne attach because it is spared through the air.

2.1 RISK OF BLUEBORNE

- It targeted weakest point in the network.
- It spreading from device to device through air
- it provides virtually full control over the device and also exploding those devices
- It serve various malicious objective such as ransomware, data theft and perform different hacking activities.
- It basically affected all the devices which is connect to the Bluetooth.

2.3. AFFECTED DEVICES

- Mobile Phone
- Smart Watch
- Smart TV
- Pumpkin Car Audio System

2.4. AVOID BLUEBORNE ATTACKS

- Use the BlueBorne Vulnerability Scanner.
- Update your device's operating system to the latest version.
- Turn off Bluetooth when not needed.
- Delete confidential information on your phone or back up your data.

3. LITERATURE SURVEY:-

According to Armis Labs, an eight-day risk profile that allows hackers to use a Bluetooth connection and take full control of the device. Depending on the wireless standard alone, it has the ability to infect desktops, laptops, cell phones, smart watches, and any other device that allows Bluetooth communication, without the need for pairing.

Armis also notes that BlueBorne affects devices running Google, Microsoft, and Apple applications. The security update was released to Android partners in early August and made part of the September episodes. Microsoft, on the other hand, has a risk-free update to all versions of its Windows 10 versions, with more details available here. Lastly, the vulner-ability had already been reduced by Apple on iOS 10. However, those using 9.3.5 and below remain at risk [12].

Bluetooth is a technology built on more than 20 years ago. The first version of Bluetooth appeared in 1994 while recently used as a data transfer method, in modern times this technology is one of the pillars of in modern times this technology is one of the pillars of Internet of Things (IoT). Over the years, the internet of Objects (IoT) has seen significant improvements in value transmission, sensors, automation, and smart devices. IoT is there extensive research into the use of many different types' areas, such as private and commercial, industrial and transport, or public sectors. In such areas, communication technology is available carefully considered as there are various needs. Because Cases of IoT usage, requiring a high level of communication, extra speed, and a larger volume of messages. Bluetooth 5.0 promises all these features and is presented to it The purpose of the IoT, because the number of IoT systems it has greatly expanded and reached the industries smart, smart home, and buildings .

The word Internet Material (IoT) was first used by Kevin Ashton in 1999 in context of supply chain management. Nowadays, IoT sites include covering a wide range of applications such as health care, transportation, and other resources, etc. IoT vision there anything in the physical world can be represented digitally and connected together to communicate. Interaction sensors, actuators, wireless communiations, people, and intelligent stuff creates significant improvements in IoT smart devices. [13]

In the current section, information about user behaviour while browsing the internet is collected to enrich the user online experience. As for IoT, the value of information collection is not limited to browsing the Internet behaviour; information about the daily user process as well collected so that the "Items" around the user interact to provide better services that meet your needs. Identity of collected infor-mation

that identifies the user to details, maintaining the privacy of collected data is a problem to be discussed in the event of a loss of personal information.[14]

4. REAEARCH GAP:-

Many researchers have explored aspects of different type of attacks such as DOS attacks, Man-in-the-middle, Password attack, Drive-by attack, Malware attack etc. and all these attacks to be performed by defaults human error, malicious software that is installed in your system without your consent but in this paper we discuss about one of the attack that is BLUEBORNE ATTACKS. This attack no need to click and download any malicious software as well as internet.

5. METHODLOGOY:-

1) In previous section (1) we have discuss about IoT technologies and their vulnerability in short range wireless devices.
2) In section (1.1) we have discuss about Bluetooth and its layer in details and also each layer describe different functionalities.
3) In section (1.2) we have discuss about blueborne attack and devices vulner-ability, and analyse how can affected in smart devices , one of the devices is we have selected smart watch and we have describe different usecase to analysis for blue borne attack in details.
4) Finally, the paper shows objective how blue borne attacks perform and then processes of avoiding it this attack.

6. ANALYSIS THE BLUEBORNE ATTACKS

Fig 1:-Steps to be Performed BlueBorne attack

According to this fig. Hacker is performing BlueBorne attack on one user called suspected user and that suspected user by default speared the different hacking activates to another user as well as smart object also. For example, Bluetooth is a short-range wireless network and it is used in all places whether at home, in hospital, banking sector, etc.it means critical places are also involved and by using Blue Borne hackers can take the confidential information and used its own purpose.

7. USE CASE OF BLUEBORNE ATTCKS PERFORMED THROUGH SMART WATCH

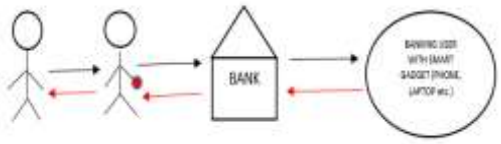


Fig 2:- BlueBorne attack performed in banking system

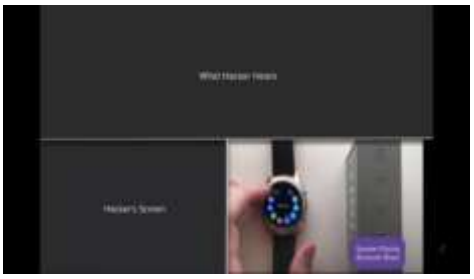
First Actor Shows as a hacker which is performed BlueBorne attack through a smart watch which is wearing by the second actor is called the suspected actor The hacker is to performs his hacking activities on the bank account through a smart watch which is wearing the second actor that connected to Bluetooth and through this smart gadget, hacker tack control the bank account and gather the confidential information of the banking system.

8. RESULT

PHASE:-1

(The first phase shows the hacker screen as well as the targeted device screen [12])

PHASE:-2



(Second phase hacker analysis the targeted device and user doing the different activities using Bluetooth. [12])

PHASE:-3

(Phase 3 hackers hack the targeted device which is smartwatch [12])

PHASE:-4

(Phase 4 is a final step and in this step, hacker is fully controlling the targeted device and still target user are unaware [12])

11. CONCLUSIONS

This paper has a concern about the security challenges and attacks that are BLUEBORNE ATTACKS faced by Digital devices such as Smartwatch, Smart TV, Mobile Phone, and other smart devices which are connected to Bluetooth. During BLUEBORNE ATTACKS perform on smartwatches we find out attackers can take control from one device to another device and potentially spared ransomware even more malware and gain access to critical system information In addition, the proposes of this paper is to study about BlueBorne attack and also how can avoid BlueBorne The research conducted during this study aims to provide new information on security attacks.

REFERENCES

Jang-Jaccard, J. and Nepal, S., 2014. A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences, 80(5), pp.973-993.

Mittal, S., Das, P.K., Mulwad, V., Joshi, A. and Finin, T., 2016, August. Cybertwitter: Using twitter to generate alerts for cybersecurity threats and vulnerabilities. In 2016 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM) (pp. 860-867). IEEE.

Zong, S., Ritter, A., Mueller, G. and Wright, E., 2019. Analyzing the perceived severity of cybersecurity threats reported on social media. arXiv preprint arXiv:1902.10680.

SIG, B. Bluetooth Core Specification, 5.1th ed., january 2019.

Zhang, Y., Weng, J., Dey, R. and Fu, X. B Bluetooth Low Energy (BLE) Security and Privacy. In:. October 2019, p. 13. DOI: 10.1007/978-3-319-32903-1298 – 1. *ISBN*978 – 3 – 319 – 32903 – 1

Microchip. Microchip Developer Help [online]. 2020 [cit. 2020-03-25]. Available at: https://microchipdeveloper.com/wireless:start.

Argenox. BLE Advertising Primer. Plano: Argenox, 2019. Available at: https://www.argenox.com/library/bluetooth-low-energy/ble-advertising-primer/.

https://stackoverflow.com/questions/28793182/smart-bluetooth-gatt-vs-att-what-are-the-differences-between-them

Hafeez, M. Antikainen, S. Tarkoma, Protecting iot-environments against traffic analysis attacks with traffic morphing, in: 2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), 2019, pp. 196–201. doi:10.1109/PERCOMW.2019.8730787.

Morris, D., Madzudzo, G. and Garcia-Perez, A., 2020. Cybersecurity threats in the auto industry: Tensions in the knowledge environment. Technological Forecasting and Social Change, 157, p.120102.

Seri, B. and Vishnepolsky, G. BlueBorne-Technical Report, 2017. 41 p. Available at:

https://go.armis.com/hubfs/BlueBorne%20Technical%20White%20Paper-1.pdf.

Armis. Blueborne. Armis, 2020. Available at: https://www.armis.com/blueborne/.

Sreenivas, Jathin. "A Survey on Bluetooth 5.0 for Internet of Things." In 2020.

Zhang, Zhi-Kai, et al. "IoT security: ongoing challenges and research opportunities." 2014 IEEE 7th international conference on service-oriented computing and applications. IEEE, 2014.

K. Li, X. Yu, H. Zhang, L. Wu, X. Du, P. Ratazzi, M. Guizani, Security mech- anisms to defend against new attacks on software-defined radio, in: 2018 Inter- national Conference on Computing, Networking and Communications (ICNC), 2018, pp. 537–541. doi:10.1109/ICCNC.2018.8390381

M.Almiani,A.Razaque,L.Yimu,M.J.khan,T.Minjie,M.Alweshah,S.Atiewi, Bluetooth application-layer packet-filtering for blueborne attack defending, in: 2019 Fourth International Conference on Fog and Mobile Edge

Computing (FMEC), 2019, pp. 142–148. doi:10.1109/FMEC.2019.8795354.

O. Stan, R. Bitton, M. Ezrets, M. Dadon, M. Inokuchi, O. Yoshinobu, Y. Tomo- hiko, Y. Elovici, A. Shabtai, Extending attack graphs to represent cyber-attacks in communication protocols and modern it networks, IEEE Transactions on De- pendable and Secure Computing (2020) 1– 1 doi:10.1109/TDSC.2020.3041999

W. Iqbal, H. Abbas, M. Daneshmand, B. Rauf, Y. Abbas, An in-depth analysis of IoT security requirements, challenges and their countermeasures via software-defined security. IEEE Internet Things J. https://doi.org/10.1109/JIOT.2020.2997651

F. Rasapour, E. Serra, H. Mehrpouyan, Framework for detecting control com- mand injection attacks on industrial control systems (ics), in: 2019 Seventh International Symposium on Computing and Networking (CANDAR), 2019, pp. 211–217. doi:10.1109/CANDAR.2019.00035

N.M. Karie, N.M. Sahri, P. Haskell-Dowland, IoT threat detection advances, challenges and future directions, in 2020 IEEE Workshop on Emerging Technologies for Security in IoT (ETSecIoT), (2020), pp. 22–29. https://doi.org/10.1109/ETSecIoT50046.2020.00009