Acharige *et al. J Surveill Secur Saf* 2021;2:26-41
DOI: 10.20517/jsss.2020.17

Journal of Surveillance, Security and Safety

Original Article

Open Access

Check for updates

A security study of Bluetooth-powered robot toy

Kavintha M. Acharige[1], Otávio de P. Albuquerque[2], Marcelo Fantinato[2], Sarajane M. Peres[2], Patrick C. K. Hung[1]

[1]Faculty of Business and Information Technology, Ontario Tech University, Oshawa, Ontario L1G 0C5, Canada.
[2]School of Arts, Sciences and Humanities, University of São Paulo, São Paulo, SP, 03828-000, Brazil.

Correspondence to: Prof. Patrick C. K. Hung, Faculty of Business and Information Technology, Ontario Tech University, Oshawa, 2000 Simcoe Street North Oshawa, Ontario L1G 0C5, Canada. E-mail: patrick.hung@ontariotechu.ca

How to cite this article: Acharige KM, de P. Albuquerque O, Fantinato M, Peres SM, Hung PCK. A security study of Bluetooth-powered robot toy. *J Surveill Secur Saf* 2021;2:26-41. http://dx.doi.org/10.20517/jsss.2020.17

Received: 6 May 2020 **First Decision**: 17 Nov 2020 **Revised**: 25 Nov 2020 **Accepted**: 21 Dec 2020 **Available online:** 25 Feb 2021

Academic Editors: Athanasios Vasilakos, Haris Mouratidis **Copy Editor**: Xi-Jun Chen **Production Editor**: Yue-Yue Zhang

Abstract

Aim: A smart toy robot has its intellect with circuits on board. It has a built-in microprocessor, sensors of one or more types, a mechanical system including moving parts, and some firmware to control and tie the parts together. The embedded sensors and devices help to create their functionality. These devices include wireless communication for data transfer. One such device for wireless communication is Bluetooth, which can be dangerous due to attack vulnerabilities, especially on Bluetooth Low Energy (BLE) devices.

Methods: In addition to discovering vulnerabilities in Bluetooth communication, common issues have been identified, including related attacks, threats, malware, and vulnerabilities. To identify specific attacks for Bluetooth devices used in smart toys, this study adopted Qoopers, a robot capable of integrating different devices into its model. Qoopers was tested using security frameworks to simulate attacks.

Results: We found that devices with BLE are more susceptible to attack. Qoopers was exposed to security frameworks used in restricted conditions, demonstrating that they can be hacked using a man-in-the-middle (MITM) attack and eavesdropping on data transfer. This paper also discusses solutions to prevent Bluetooth attacks.

Conclusion: Bluetooth communication is vulnerable to different attacks, including MITM. This happens even with Qoopers robot when it is reprogrammed with customized applications with less security. These smart toy robots are used mainly by children under 16, who can make mistakes by ignoring security, focusing only on functionality, increasing the risk of personal information theft and other threats.

Keywords: Smart toy robot, Bluetooth, security, man-in-the-middle attacks

1 INTRODUCTION

Twenty-first-century children are born into the world of technology. Generation Alpha starts from the year where the iPad was introduced. Born into a technological world, children possess higher computer literacy and understand the gamification of learning. Thus, ordinary toys are not of their interest. Smart toys have been introduced as playmates for both Generations Z and Alpha. For this reason, these toys, which are called "smart", are omnipresent in houses with children. A toy can have a variety of purposes, including education, leisure, and socialization[1]. Toys offer several benefits to the child, including cognitive, motor, social, and linguistic development[2]. A smart toy is defined as a physical toy component that connects to mobile services through Wi-Fi[3]. It is an intelligence product with onboard circuitry. Smart toys can learn, act according to a pattern, and change their behavior based on the environmental stimulus. Typically, the smart toys present today have an embedded microprocessor, sensors of one or more types, a mechanical system to comprehend moving parts, and some firmware to control and tie the pieces together[4].

The smart toy Qoopers is an interactive robot package that can be classified as a Science, Technology, Engineering, and Mathematics (STEM) product[5]. STEM products aim at training, emotion, and learning. Various STEM toys are available, and they concentrate on key topics of programming, electronics, chemistry, robotic toys, etc. Although Qoopers does not have all the typical features/functions (e.g., chatbot) in other smart toys such as Mattel's Hello Barbie, its package consists of electronic modules, main programming board, wheels, hardware, tools, etc., along with the application, which facilitates drag and drop programming, something that not all smart toys have. It offers the ability to build a robot with the use of the given components. It has a large capacity for "*Do It Yourself*" and possesses an attractive look.

The use of Bluetooth in toy robots is helpful because toy robots' original purpose is to educate children regarding robotics, and the days are made to work in close range. Moreover, toys should not be directly connected to the Internet, making them more complicated in both functional and security aspects. Bluetooth serves this purpose when compared to the Internet of Things (IoT) technologies. However, when it comes to security, the shortcomings depend on how Bluetooth technology is used. IoT is a continually growing area, with smart devices being implemented everywhere using computing artifacts called embedded systems. Most smart devices have a Real-time Operating System (RTOS), which is used to develop embedded systems, as it assists in building a reliable system. IoT requires that most of these connected devices be operated for long periods, but they are constrained in power, memory, and storage. In smart toy robots, embedded communication technologies may include wireless communication using Wi-Fi, RFID, Bluetooth, and NFC[6]. As IoT systems require communication between electronic devices over the Internet platform, it and its operating system become more vulnerable to malicious attacks from third-party intruders. Therefore, various encryption techniques are implemented for the security of these operating systems[7].

The Roboblock company, Qoopers' creator, provides sensors be integrated with the Arduino board. The default program in the robot and mobile application uses security constraints when communicating. However, that infrastructure is vulnerable to a Denial of Service (DoS) attack, during which an authorized mobile application cannot initiate communication with the robot until it is rebooted. An example of concern is a user attaches a video capturing or sound recording device with Qoopers, but the inter-device communication is not secured. Then, an attacker can exploit this type of vulnerability and steal personal information. Personally Identifiable Information (PII) is any information about an individual maintained by an organization that can be used to distinguish or trace an individual's identity, including any information linkable to an identifiable individual[8]. Compared with other IoT related attacks, for Bluetooth attacks, the attacker should be in close range of the vulnerable Bluetooth devices, but very specific tailored attacks can be made and exploited even if there are physical barriers, so security matters any cost.

Smart toy robots such as the Qoopers will be the next generation of the market. A survey by Juniper Research[9], a UK-based company specializing in market research within the digital ecosystem, reported that smart toys are the new key market for toy companies, and sales would grow from the US $2.8 billion in 2015 to the US $11.3 billion by 2020. The last year's trend has been smart toys embedding more devices and sensors into their structure, bringing more risks, such as attacks on Bluetooth devices and leakage of data. The leakage of data can be a dangerous risk, especially if they are personal data such as a PII, e.g., capturing location data and identifying documentation, and attacks such as blackmail and kidnapping can happen. Therefore, taking better precautions to make these toys more secure by introducing a proper framework is the next issue that needs to be addressed.

This paper discusses possible security vulnerabilities, mainly in Bluetooth devices, presents the functionality of Qoopers, and discusses why these features are worthy of attention. The rest of the paper is organized as follows. Section 2 addresses the background of smart toy robots and related IoT technologies. Section 3 discusses the literature review of related security issues. Section 4 discusses the security attacks on Qoopers. Section 5 focuses on strategies aligned with preventing Bluetooth attacks. Section 6 discusses the primary outcomes of this study. Section 7 includes the conclusion and future work.

2 BACKGROUND

This section presents a brief overview of Internet-connected toys (smart toys), their interactions with users, personal information manipulation, and Bluetooth connections and sensors.

2.1 Smart toys and robots

A smart toy is a toy with intelligent functionalities that a child can interact with. Technologies such as Artificial Intelligence (AI), machine learning, speech recognition, etc., are used in this kind of toy where children get personalized responses when they play. In this context, a smart toy can be effectively considered IoT with AI functionalities that can provide Augmented Reality (AR) experiences to users[3]. Many toy robots on the market are made by many corporations of various sizes, and they can be classified in different ways, such as software-enabled toys, which comprises all smart toy robots and subcategories defined through their different structures and purposes. Such robots have a limited type of functionality and simple programming software that can be developed without the need to have high-end knowledge. The common abilities of such robots include running, walking, flipping, or dancing. Most of these robots are available as a packaged kit and need to be assembled by the customer.

A common type of robot is humanoid, which refers to those that can completely represent the human body shape, face, hands, feet, and human characteristics. They have been developed to the point that they can show their emotions, think about their feelings, and learn by watching the events that happen around them. Their other features include walking ability, voice communication, and facial conversation[10]. Having stated previous advantages, some disadvantages associated with these humanoid robots: First, each movement is limited to their Degree of Freedom (DoF). In humans, muscles help maintain movement, but, in robots, an electric motor, a gear that does not have any backlash, and a controller with a top decrease ratio are used to maintain such an act. Second, they all have a problem with power resource restriction. Third, there is a lack of real-world usage of such humanoid robots on production lines. Therefore, it is a costly process to develop them considering the features that they provide.

With the development of new technologies and methods, two-legged robots may be able to perform more tasks and take more responsibility, e.g., service applications, dangerous tasks, space applications, *etc*. Two-legged walking, also called biped walking, can be considered the best walking method as it allows moving without any surface limitation in contract with wheeled and chained robots. Legged robots can work

in situations that no other robots can, including climbing and jumping over obstacles. They can also be adapted to mobile applications and work close to each other[11].

Toy robots can be grouped by their characteristics, including height, weight, controller or processing unit, operating system, type of power supply, type of power capacitor, the rate of freedom, the variety of the sensors, and the type of connection they use to connect to the user. These characteristics can fall into different groups: Robotainment, usually small and lightweight, includes robots designed for containment, entertainment, and education[12]. They can also facilitate various sensors and be programmed by many usual programming languages such as C/C++, Python, Java, or even scientific languages such as MATLAB. A simple programming medium can also be used for children to program such robots. Another group is Infoassistance, which includes robots mainly developed to communicate with humans and bring information to help them. The term "Infoassistance" represents the goal of assisting people. Their size is small to average, so they will operate in the usual human environment without disrupting anyone. They can recognize body language and facial expressions, understand language, and communicate with people.

The next group is called Rescue[13]. The main purpose is to perform in dangerous environments that are hazardous for humans or even help in natural disaster situations. They have many advanced sensors for temperature, humidity, identifying human bodies, and observing any chemical exposures. In this group, the robots are made up of light material that can be aluminum. The main disadvantage of this group is its high price. The last group is Intelligent robots, which possess a mixture of human portability and artificial intelligence. This group aims to help people without any human intervention. They need to move similar to humans since they need to be adored by humans and not scare them.

2.1.1 Qoopers

To study Bluetooth attacks, this research adopted a smart toy robot called Qoopers[14]. It is a programmable metal robot kit introduced to the industry of toys by Robobloq. It usually comes in a disassembled pack with all the metal parts separated. Users must assemble it by integrating different parts and creating different models, including sensors as per the requirement.

Qoopers robots can be run and coded under the Raspbian Operating System by coding languages such as Arduino Integrated Development Environment (IDE), Python, and JavaScript. It is compatible with any Raspberry Pi with Universal Serial Bus (USB) ports: Raspberry Pi 3 Model A, Raspberry Pi 3 Model B, and Raspberry Pi 3 Model B+. The robot has two application development methods: using the standalone application, to program functionalities or running and coding in Raspbian OS with languages such as Arduino IDE, Python, and JavaScript. Robobloq is compatible with any Raspberry Pi with USB ports: Raspberry Pi 3 Model A, Raspberry Pi 3 Model B, and Raspberry Pi 3 Model B+.

Apart from basic programming, Qoopers allows integrating different sensors associated with programming functions. Its package comes with an ultrasonic sensor with the following specifications: operating voltage, DC 5 V; detection angle, less than 20°; and detection distance, 5-250 cm. The sensor can be attached to the Arduino board using an RJ45 cable. Sensor output can be used to avoid obstacles in programming flow, and the standalone platform supports this type of operation. Robobloq provides application programming interfaces (APIs) for programming through a high-level language such as Python. Qoopers can be reprogrammed by erasing the default program written on the Arduino board or modified using the programs provided by Qoopers website or coding with C or C++ language.

To communicate with a mobile phone through Bluetooth, AT commands can be used. Once the program is set to communicate with a mobile application, it can either use an existing mobile application such as a Bluetooth terminal to communicate with the device or create a new application from scratch using a mobile

platform's APIs. For Android, many APIs can be used, while Apple iOS has separate APIs. Here, users can usually use available mobile applications to connect with Qoopers through Bluetooth technology, with the application initializing a connection before it communicates with the robot. This communication is secure to a certain extent but still vulnerable to DoS attacks. Qoopers can block further connections by attaching a proxy to it. Qoopers comes with a built in Bluetooth board, and, when programming, it can be used to connect with the computer/mobile application.

2.2 Bluetooth network connection and sensor

Bluetooth is used to connect two devices or network by connecting several devices together. For two Bluetooth devices to communicate, a procedure called "pairing" must first be conducted. Two trusting devices become eligible to be a pair and build a link key that is eventually used to generate a data encryption key for each session. This technology can be used to access one device using remotely. Bluetooth technology is becoming increasingly popular for short-range wireless communication. Most mobile devices are equipped with Bluetooth to share or link to peripherals such as headphones, speakers, *etc*. Nearly four billion Bluetooth-enabled devices were shipped around the world in 2019[15]. Bluetooth is a short-range wireless network usually found between two or more closely located devices within a range of ≤ 10 m and a Wi-Fi Local Area Network (LAN) equivalent to 2.4 GHz. The Bluetooth protocol operates on several layers. The lowest layer is the Logical Link Control (LLC) and Adaptation Protocol (L2CAP), which constructs the security layer of Bluetooth. This is followed by Radio Frequency Communication (RFCOMM), which emulates the serial communication profiles over Bluetooth. Next, Object Exchange (OBEX) provides services for file transfer[16].

Mobile devices with Bluetooth come with these functions, such as the limitation of the links to previously "paired" devices or to turn network invisible to other devices, the default settings have it turned off, which makes the device visible to the Bluetooth neighborhood. Thus, users who are not familiar with the devices, or have less knowledge of the existing security and privacy issues they are vulnerable, use their devices' default settings without enabling these provided basic security measures.

Bluetooth is a semi-open standard for short-range and ad hoc communications such as Wireless Personal Area Networks (WPAN). Its peer-to-peer, low-cost, and low-power characteristics make it possible for Bluetooth to create small-scale ad-hoc networks-piconets. The Bluetooth piconet can support eight devices, one master and the rest as slaves. As Bluetooth is a wireless transmission network, risks exist where data could be purposely blocked or disrupted, or incorrect or altered content could be transmitted to piconet phones[17].

3 RELATED WORK

Although there is a growing demand for Bluetooth devices, the security and privacy issues were not discussed extensively until recently. As a result of rare discussions regarding these topics, there have been many exploits published in the past couple of years. As per the study of similar literature, it was identified that, although there are fundamental security measures such as invisibility, authentication, and encryption, they are seldom used effectively[18]. Bluetooth makes use of Frequency Hopping Spread Spectrum (FHSS) software for its interaction to minimize signal noise in such a crowded section of the frequency spectrum[19]. Not only does FHSS reduce the chance of other signals interfering with Bluetooth signals, but it also offers a minimal degree of transmission protection by continually changing frequency. This minimal protection makes it easier for a malicious node to find the device's exact frequency and eavesdrop on contact information, which provides chances to vulnerabilities to privacy and safety threats.

Considering the radio link power control and communication range, Bluetooth devices can measure the received signal strength and alert their neighbors to increase or decrease the transmitting power. For

small mobile phones, this technology is particularly useful to save limited power and extend battery life. Depending on the type of power management, the communication range of Bluetooth devices is 1-91 m. While the transmitting capacity of a Bluetooth device can be changed, considerable differences exist among different devices' power levels. power control is not considered a safety device. It aids in reducing the risk of being attacked since the existence of opponents should be within the contact range to begin an attack[17]. Considering the data rate and versions, the speed at which a Bluetooth device can transmit information depends on the Bluetooth standard version it supports[17]. The transmission rate is up to 1 Mbps for Bluetooth 1.1 and 1.2 and up to 3 Mbps for versions 2.0 + Enhanced Data Rate (EDR) and 2.1 + EDR. "Bluetooth over Wi-Fi" is supported by Bluetooth 3.0, with a transmission rate of nearly 24 Mbps[19].

Ad hoc and infrastructural are the two network architectures supported by Bluetooth. A Bluetooth Access Point (AP) allows interaction between connected devices in an infrastructural network, whereas Bluetooth devices create direct connections in ad hoc networks without intermediaries. It is possible to architecturally split a Bluetooth device into two usable parts: the host and the host controller. The host is the base unit, such as a computer connected to the Bluetooth network. Its functions include introducing protocols in the upper layer, such as LLC and L2CAP, and Service Discovery Protocol (SDP)[19]. The host controller, usually mounted in a USB dongle or incorporated as an embedded device, is responsible for the lower layer functions such as signaling, baseband, and Link Manager Protocol (LMP)[19]. Host and host controllers are combined into one unit in many handheld devices such as smartphones and even smaller units such as Bluetooth headsets. The properties of Bluetooth security are (1) information privacy; (2) system encryption; and (3) authorization. Information privacy relates to the avoidance of illegal disclosure of confidential data. Encryption requires the confirmation of the identification of the Bluetooth device engaged in the interaction. Authorization usually occurs following efficient verification, where the aim is to guarantee that a machine is granted permission to make use of a service. Unlike other forms of networks, Bluetooth is not specific for user authentication.

A study on the security and privacy risks in smart toys with wireless connections[20] shows the need for care, mainly to protect the pairing and the connections used in them. The authors evaluated 11 smart toys available on the market and their possible security and privacy flaws, including threats of unauthorized physical, near, or remote access to the smart toy. Unsafe Bluetooth practices were identified, such as using a static MAC address, making the physical space and the child potentially traceable, and accepting an unauthorized connection, which can allow toys to be hacked and thus attackers to take control of the toy's behavior and intercept data transmitted from the toy to the application.

4 Security issues

Bluetooth enabled devices are mostly used as personal devices where sensitive data are stored. Exposing these sensitive data can be an issue for a person's safety.

Haataja *et al.*[21] classified threats into Bluesnarfing attack, PIN crunching, offline PIN recovery attack, offline encryption key recovery attack, Blueprinting attack, etc, [Table 1]. These are categorized under disclosure threats, while reflection attacks and backdoor attacks are grouped as integrity threats. DoS is identified as another category of threats. In contrast, the rest of the threats, such as Bluebugging, Blooovering attack, HelloMoto attacks, and online PIN cracking, are categorized as multi-threats, as Haataja *et al.*[21] argued these attacks could not be categorized under a single category of threats.

Several possible threats have been identified against different layers of Bluetooth. Furthermore, some standard and device-specific attacks have also been identified. These threats are reported to leverage unreliable or ineffective implementations [Table 2].

Table 1. Bluetooth related attacks

Attack	Description	Ref.
Bluejacking	It consists of sending a message by Bluetooth to visible devices. The most popular bluejacking method works by submitting a digital business card, a good feature at business meetings or trade shows	[22,23]
Bluesnarfing	An opponent can link to a mobile phone without alerting the user, capturing personal data such as phone books or calendar files. The connection is made by Object Exchange (OBEX), e.g., directly to the specific file containing the phone book. It opens an OBEX File Transfer Protocol (FTP) connection to the target device with full interactive access to its file system	[21,24]
Bluebug	Allowing a mobile device to be taken over nearly absolutely by setting up an interface secretly for remote control of certain devices. This may include modifying or reading mobile content such as address book, calendars, schedules, Short Message Service (SMS) and remotely manipulating the device by making calls, sending text messages, *etc.*	[22,23]
Denial of Service (DoS)	DoS refers to the scenario where a few repeated requests for contact are received on the device, making it impossible to use. DoS attacks like sending multiples packets that cause the phone to crash the Bluetooth stack and the service request power, which is battery exhaustion by Wi-Fi connection	[22,25]
Cracking PIN	Bluetooth packets are captured by a sniffer and can decipher the packets to evaluate the data they hold. If the collecting packets are involved in authenticating two Bluetooth devices, it can use that packet information to determine the client's PIN. The packet data include PIN-derived information instead of the PIN itself	[21,22,23]
Blueprinting	It is used to evaluate the target device's maker, computer type, or firmware version. It is an attack that can use to produce information on the manufacturers and models of Bluetooth devices to figure out Bluetooth security issues	[21,22]

Table 2. Bluetooth related threats

Threat	Description	Ref.
Association threat	Bluetooth device vendors may connect the specific Bluetooth identifier to the owner's identification. While there is currently no consolidated database containing such information, there is a database connecting unique identifiers of mobile phones to individuals	[15]
Location threat	Bluetooth devices can be used to recognize and monitor neighboring people and the positioning of Bluetooth-enabled objects as smartphones and satellite navigators	[26]
Preference threat	Radio Frequency (RF) identification tags specifically recognize the producer and product type of the labeled objects and expose an element's unique identity. Such data can be collected and used to establish an individual's preference profile and even assess these items' monetary value	[26]
Constellation threat	Devices with Bluetooth typically generate a virtual background that can be controlled and recorded. The attack consists of extracting person-to-people associations and identifying a group of people and their actions to infer this group's properties	[26]
Transaction threat	Through analyzing shifts in constellations, transactions between individuals can be monitored. When an object activated by Bluetooth travels from one constellation to another, they may decide that there has been a transfer between those individuals	[15]
Breadcrumb threat	A client can be continuously connected to the Bluetooth products they own due to the connection risk. When the consumer discards certain objects, this relationship does not automatically dissolve and the data are not completely deleted	[26]

There are several types of Bluetooth malware. Each type of malware has its method of infecting, spreading, and intention. Within the identified malware list, the ones that exploit the information or cause financial damage to the victim are known as malware of high severity. Malware that paralyze a computer or cause the victim to be distracted are known as malware of low severity. The latter malware are mainly categorized into trojans and worms [Table 3].

The above gives a clear idea of possible privacy and security threats when using Bluetooth. It can be deduced that the overall security of Bluetooth networks is based on the Bluetooth medium's security, the security of Bluetooth protocols, and the security parameters used in Bluetooth communication[27].

Research carried out regarding Bluetooth devices' security and privacy issues has identified a set of causes that contribute to Bluetooth vulnerabilities. According to Berrehili and Belmekki[16], the common causes identified are visibility, vulnerability to eavesdropping, deficiencies in encryption mechanism, weaknesses in PIN code selection, weaknesses in association models of System Software Package (SSP), and weaknesses in the device configuration[21][Table 4].

5 Bluetooth attacks prevention

Solutions for prevent or mitigate those risks cited previously are developed on the literature of security and privacy related to Bluetooth connections, from the simplest ones that common users can make to complex

Table 3. Bluetooth related to malware

Malware	Description	Ref.
Trojans	Is a malware type that exploits the client to access the system or execute harmful tasks. A trojan cannot spread itself, but it can capture critical information and give the offender access to sensitive data	[27]
Skull	Is a type of Trojan that renders all mobile apps worthless and displays a skull's blinking animation when any request is accessed. It spreads by Bluetooth and Short Message Service (SMS)	[27]
Steal War	When a device is infected, it shows that some untrusted source is attacking the device and that some files need to be installed to restore the system. Once the user clicks on the install button, the trojan is installed in the system. It can be transmitted through Bluetooth as well as Multimedia Messaging Service (MMS)	[27]
Drever	A Trojan that tricks the victim by displaying the existence of an upgrade to Symbian OS, enforcing to download the change, being sent as a system folder to the setting document. Once infected, it can infect others and disable Symbian antivirus through Bluetooth	[27]
Worms	Spread to other devices due to their ability to self-replicate. Infected devices delete files or send information through email. Bluetooth worms often infect Symbian OS	[27]
Cabir	Once a device becomes tainted, it continually searches for neighboring Bluetooth devices and spreads via Bluetooth files to other devices. The user receives pop-ups telling them to install it, and Cabir resends and blocks the User Interface (UI) until the request for installation is accepted	[27]
Mabir	Like Cabir. The only difference is that it replicates via both Bluetooth and MMS	[27]
Beselo	It is a self-replicating worm that spreads via Bluetooth links and communications from MMS. The victim acknowledges that it is a media archive that includes pictures, audio, and video clips with common file extensions, e.g., jpg, mp3, and mp4	[27]

Table 4. Bluetooth related vulnerabilities

Vulnerability	Description	Ref.
Visibility	The default Bluetooth device configuration is being visible to the public, with the undiscoverable mode option. The existence of undiscoverable gadgets can be found by searching the Bluetooth address domain by brute force	[16,24]
Vulnerability to eavesdropping	As Bluetooth is a wireless RF transmission system that primarily uses omnidirectional antennas, it is less likely to identify an eavesdropper. Eavesdropping tools can be set up in a long distance of the communication system, facilitating access to unencrypted information through Bluetooth	[16,21]
Deficiencies in encryption mechanism	Despite the many benefits of Bluetooth encryption, it also has some drawbacks. One of the most significant weakness happens when it is difficult to use 128-bit authentication	[16,21]
Weaknesses in PIN code selection	The use of weak PIN codes to access Bluetooth devices is common. Simple four-digit passwords are generally used, making it easier for an eavesdropper to use brute-force attacks to identify the right code combination	[16,21]

mechanisms provide by the advancement of the technology.

According to Ihamäki and Keljakka[18], simple steps such as downloading resources from trusted websites, using an antivirus application, keeping applications up-to-date, and keeping track of unusual behavior in devices, battery usage, etc. can also be taken to prevent security and privacy issues which occur due to Bluetooth communication. For SSP enabled Bluetooth devices, the report proposes several possible countermeasures, as discussed below[16].

The simplest and cheapest intervention to fight MITM attacks is to compel devices to recognize only authenticated connection keys[28,29]. The definition of a secure database is a registry that includes an entry for each system and the security requirements of that company. Bluetooth protocol stacks typically have this security database method. One of the security requirements is that the device demands an authenticated link key. If this criterion is not met, access is restricted[21]. SSP MIMT assaults can be avoided at the user interface level as well. An additional window should pop up asking whether the pairing device is trusted or not. Devices that cannot enforce the use of authenticated link keys employ the approach mentioned above of a new window at the user interface level; employ another appropriate method; apply protection in the same manner as older Bluetooth devices; or do not use Bluetooth safety at all[21].

Summing up the content of related studies, the following are identified as the most important facts. The cumulative reliability of Bluetooth networks focuses on the safety of the Bluetooth medium, the safety of Bluetooth protocols, and the criteria used for ensuring security during Bluetooth interactions. The weaknesses that have been identified in the Bluetooth medium protocols and Bluetooth safety criteria can significantly compromise the privacy and security of Bluetooth networks.

Table 5. Commands to install the BtleJuice framework

sudo yum install bluez bluez-libs bluez-libs-devel npm
sudo npm install -g btlejuice

Table 6. Command to launch the proxy and start the core server in the host machine

sudo btlejuice-proxy
sudo service bluetooth stop
sudo hciconfig hci0 up
sudo btlejuice -u <Proxy IP address> -w

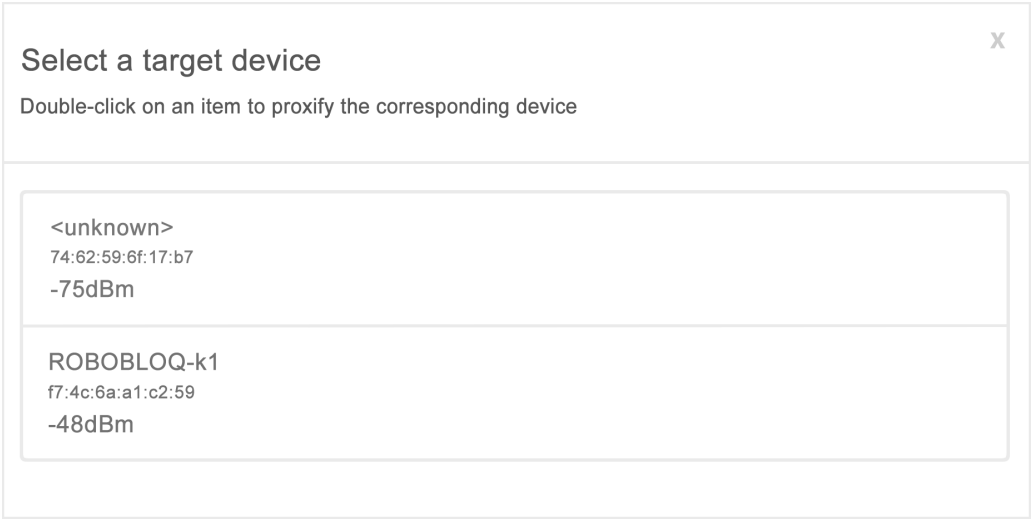

Figure 1. BtleJuice vulnerable device selection to the proxy.

6 ATTACKS ON QOOPERS

The experiment discussed in this section is compliant with the International Organization for Standardization "ISO/IEC 27002:2013: Section 6.2 Mobile devices and teleworking" to ensure the security of teleworking and use of mobile devices[30]. Since Qoopers runs on Bluetooth 4.0 LE, it is susceptible to Bluetooth attacks and mainly the MITM attacks discussed in the following.

6.1 BtleJuice MITM

BtleJuice is a framework that can perform a MITM attack on Bluetooth low energy platforms. It gives a dedicated web interface to interact with the attacked device. The framework is built on top of Python and Node.js bindings. BtleJuice is composed of two main components: an interception proxy and a core. These components are required to run on independent machines to operate two Bluetooth 4.0+ adapters simultaneously. A virtual machine can be used as the proxy, and the host machine can be used as the core. Once the Bluetooth adapters are set up through hciconfig and BtleJuice is installed [Table 5], we can launch the proxy from the virtual machine, and then it can start the core server in the host machine [Table 6].

When the target button is clicked, a dialog popup presents the available BLE devices [Figure 1]. The user can select the device by double-clicking. Once the selection is made, the web user interface is populated with connected device information, and the proxy as a dummy is ready to connect with mobile applications [Figure 2]. All the intercepted Generic Attribute Profile (GATT) operations are then displayed with the corresponding services and Universal Unique Identifier (UUID) characteristics and the data associated with them.

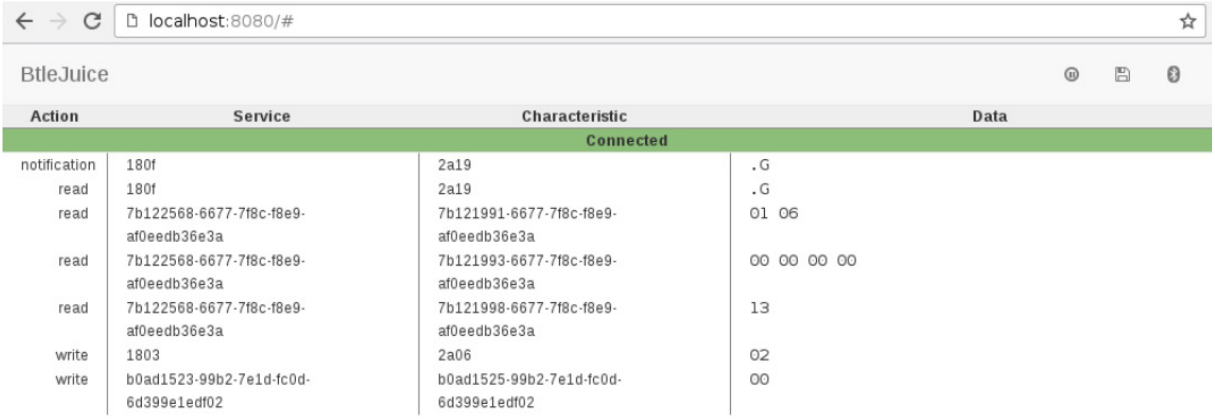

Figure 2. The Connected device on BtleJuice web interface.

Table 7. Configure config.env and set Bluetooth adapter device ID

NOBLE_HCI_DEVICE_ID: noble ("central", ws-slave) device
BLENO_HCI_DEVICE_ID: bleno ("peripheral", advertise) device
WS_SLAVE: IP address of ws-slave box
DEVICES_PATH: path to store json files

Table 8. Command to start the central device

sudo node ws-slave
node scan
node scan <peripheral>
node advertise -a <advertisement_json_file> -s <services_json_file>

6.2 GATTacker

GATTacker is a framework for MITM attacks on Bluetooth Low Energy devices built on top node.js[31]. To install this framework two modules must be installed before node.js: Noble[32] and Bleno[33] are supportive frameworks that make it easier to set up a core and a proxy to perform the attack. After that, the "config. env" file must be configured with Bluetooth adapters, so Bluetooth adapter device IDs should be countable accordingly, and the attributes should also be set to run the platform [Table 7]. The next step is to start the central device, and, from the slave, available BLE devices can be found through scanning. Finally, the peripheral device can be created and connected with the vulnerable device [Table 8].

6.3 Bluefruit LE Sniffer

Bluefruit LE Sniffer is a Bluetooth Low Energy packet sniffer developed by Adafruit[34]. This device can be used to sniff Bluetooth data packets in the open air and be integrated with Wireshark[35]. To use the device, first, the relevant drivers must be installed. For the latest version of a sniffer, CP2104 Driver developed by Silicon Labs must be installed. They provide an application with Wireshark configuration, which is publicly available to download. Otherwise, it is necessary to integrate the given libraries (plugin) with the existing Wireshark platform and start capturing packets [Figure 3].

To run the application, Python 2 should be installed first, in which there is nrf_sniffer.bat that can be used to run on Windows platforms. Suppose it is necessary to sniff data being exchanged between two Bluetooth LE devices. In that case, a connection between the original device and a second Bluetooth LE device needs to be established. The nrf-sniffer firmware can listen to all the exchanges that happen between these devices, but it cannot connect with a BLE peripheral or central device (i.e., it works in passive mode). However, the communication is encrypted correctly, it is hard to crack the secrets and extract actual data.

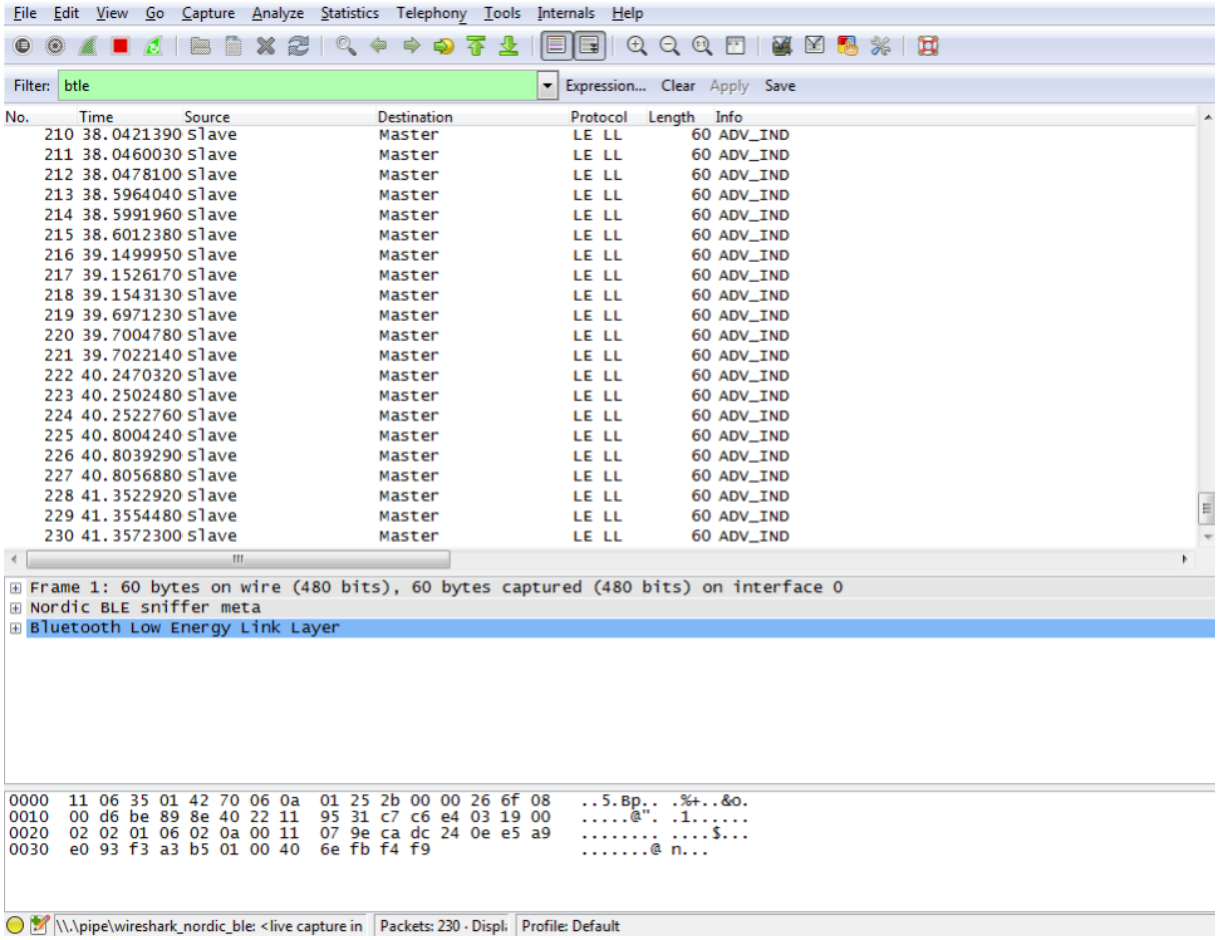

Figure 3. Wireshark packet capture using Bluefruit LE Sniffer.

7 PREVENTING BLUETOOTH ATTACKS

Research has been carried out to take countermeasures for Bluetooth attacks. Some methodologies that have been implemented and proposed are discussed below.

Monitoring the communication between devices is one method that can be used to prevent these attacks. Having a keen eye on the communication between devices makes it possible to identify any unusual behavior in the communication pattern. Some researchers have developed a set of rules based on this unusual communication behavior detected in Bluetooth devices. An intrusion detection and prevention system has been created to address certain Bluetooth attacks. When an intruder is observed, the protocol analyzer immediately warns the network manager that the Bluetooth network is under threat[21]. This manual organizational intrusion mitigation can be used in all instances independent of the strengths of the authorized Bluetooth devices. A small application runs on all genuine Bluetooth devices that allows programs to be installed on respective devices. These devices must run this application to receive warning messages from the IDS. When an alert message is received, phones under attack may immediately detach or reject any further Bluetooth connections. This solution does not apply to all types of Bluetooth attacks, as the security capability of Bluetooth devices is limited.

Another solution that has been initiated is RF fingerprints[36]. Although the same company manufactures many Bluetooth devices, they can be identified separately by using the slight differences in signal variations.

Table 9. Best practices to enhance user awareness

Update default settings to achieve optimal standards.
Ensure devices are in and remain in a secure range.
Use long and random PIN codes, which makes the codes less susceptible to brute-force attacks.
Change the default PIN for devices and frequently updating this PIN.
Set devices to the undiscoverable mode by default, except when pairing.
Turn off a device's Bluetooth when not needed or in use, especially in certain public areas.
Be cautious when prompted to enter the PIN in unexpected events.
Frequently update drivers to have the most recent product improvements and security fixes.
It is recommended that users refrain from using non-supported or not secure Bluetooth-enabled devices or modules, including Bluetooth versions 1.0 and 1.2.
Users should use SSP instead of legacy PIN authentication for the pairing exchange process when it is possible. This will help mitigate PIN cracking attacks.
All lost or stolen Bluetooth devices should be unpaired from devices they had previously been paired.
Users should never accept transmissions from unknown or suspicious devices, and they should only be accepted from trusted devices.
All devices that are paired should be removed immediately after use.
Devices should be monitored and kept at close range.

Variations are most noticeable when the system is triggered or when it tries to access the network because there is a brief intermittent period in the signal. The transient period only lasts just 2-10 ms; however, significant changes in rate, duration, and temperature happen during the transient stage. From this part of the signal, the RF fingerprint can be generated. As all devices have an RF fingerprint, legitimate devices can be differentiated from illegitimate devices. Then, Bluetooth equipped devices can detect legitimate devices before initiating a connection.

Following the above solutions, this paper suggests deactivating the function for a predefined period. Users can directly deactivate the Bluetooth functionality on their devices by pressing a button, switching the device off, or configuring Bluetooth to operate in "Stealth" mode. The first two solutions completely stop Bluetooth communication, while the third allows known devices to communicate with the owner's device. There are two issues related to this solution. Most people today rarely suspend or deactivate Bluetooth functionality due to the lack of knowledge on using these devices. The second approach that has been put forward is to rename unique identifiers occasionally. However, this is a complicated process to carry out with Bluetooth devices. Here, the renaming of both entities should take place. For this approach to operate for Bluetooth, every system should keep track of the renaming process on all other gadgets with which it communicates and vice versa. Another approach is to allow users to adjust the range of the signal in the device. Implementation of a controller that would dynamically adjust the Bluetooth signal's intensity would enable users to expand their signal as much as is needed.

The current level of protection available in most Bluetooth devices is inadequate. Many types of Bluetooth devices have short, mostly only four-digit, fixed PIN codes. This has been identified as a major problem for security. Bluetooth manufacturers should, therefore, deeply consider the security concerns. Client awareness of security issues is overly critical for personally identifiable information from eavesdroppers and hackers. Most people have no idea how to customize the privacy settings on their Bluetooth devices correctly. Therefore, above all the proposed solutions, device users should be informed of the privacy and security issues and the impacts of their personal information being exposed to the public. Furthermore, they should be made aware of the basic countermeasures that can be taken to address or, more importantly, prevent the probable issues [Table 9].

Device makers should adopt a clear and understandable goal for common user's privacy policies to provide information about what data can be collected and stored and with whom those data can be shared. Furthermore, materials such as frequently asked questions should be provided to present the main questions and their answers and show the risks of the environment to help with security and privacy decision-making. Bluetooth protection is based on creating a set of events linked together where all the

events should take steps to prevent exposing sensitive raw data to the eavesdropper. All occurrences must happen in a specific security chain to be set up effectively.

In addition to user awareness, it is important to enforce these constraints on a technological framework. For Qoopers, it is better to remove the custom programming ability and expose a tested framework to do programming and all other alterations. This is important because, by doing this, children's actions are not going to affect the security countermeasures while serving the purpose of STEM.

Toy and robot companies also need to implement mechanisms to prevent security risks in their smart robot toys, such as common attacks (e.g., DoS and MIMT). This goes beyond using a newer version of the device and firmware or using PIN authentication. Given the large data collection and storage capacity that a toy can have, as well as the related risks, it is necessary to adopt security requirements that address both the old and new problems of attacks on devices, sensors, and systems (databases and mobile services) connected to a robot and the current issues of the IoT environment. Considering robot toys as an IoT device, the authentication solutions often used in the IoT environment can easily be adopted by toymakers.

Mechanisms of authentication and validation of devices, sensors, and data collection and storage by them are necessary to prevent and resist attacks, specially the MIMT experienced on the Qoopers. Different authentication solutions, not just password-based ones, are presented in the literature. Solutions such as mutual authentication based on blockchain receive more attention recently due to their efficiency in the face of security properties such as anonymity, integrity, and confidentiality of data[37,38]. Cloud-based authentication is used to create secure communication between external parties (legit mobile services) and the embedded devices (e.g., Bluetooth) in the robot toys, providing access to data stored on the cloud server, generating a secure session key between them for future communication[39,40]. Besides ensuring the security desired by parents and the entire experience based on the toy's functionalities wished by the child.

8 DISCUSSION

The emerging trend of smart toy robots creates many opportunities for children. In education, children receive many benefits, but there are possibilities of privacy breaches and other damages without appropriate controls. This paper mainly focuses on Bluetooth powered devices and toy robots. Bluetooth devices are susceptible to different threats and vulnerabilities based on the Bluetooth version.

Qoopers robot was introduced for learning, but it can be upgraded into a powerful device that can record video (by attaching a camera), record sounds (by attaching a microphone), *etc*. The important thing is children can program this robot in any way they want using provided APIs, or they can erase everything and use their programs and connect with the robot using Bluetooth. This is dangerous because if they do not use a secure channel when interacting with the robot, there is a possibility of being hacked, and private data may get breached. We used Qoopers for the experiments, but these risks exist in all smart toys that use Bluetooth devices, so the security risks are a great concern of parents and toy makers/Bluetooth manufacturers as the users are children. At present, Bluetooth security vulnerabilities tend to be the biggest issue with Bluetooth protection.

MITM attacks are common these days, and Bluetooth platforms are also susceptible to such attacks. BtleJuice and GATTacker are frameworks that can be used in MITM attacks. Qoopers were exposed to BtleJuice and GATTacker in restricted conditions, and the results show that Qoopers can also be hacked using a MITM attack and transferring data can eavesdrop. Since these robots are used inside houses, there is a high chance that personal data can be retrieved without permission using a Bluetooth attack. The only requirement here is that attackers need to be in close range to perform an attack, but with high-

tech devices, an attack can be launched in a reasonable range. Rather than publicly attacking devices, a specifically tailored attack can be launched with the right toolset.

Therefore, device users should be informed on privacy and security issues and the impacts of their personal information being exposed to the public. Furthermore, they should be made aware of the basic countermeasures that can be taken to address or, more importantly, prevent the probable issues. Bluetooth protection is based on creating a set of events linked together where all the events should take steps to avoid exposing sensitive raw data to the eavesdropper. Therefore, all occurrences must happen in a specific security chain to be set up effectively.

Contributions

This works contributes to the secure area related to smart toys, showing the frequent types of attacks on Bluetooth devices, as well the attacks they are susceptible to, which are used in many IoT devices, including on smart toy robots. In addition, a set of best practices for users and toy makers or Bluetooth manufactures to prevent certain Bluetooth attacks and to mitigate secure risks is presented. Bluetooth manufacturers should deeply consider the security concerns. Client awareness of security issues is extremely critical for the defense of personally identifiable information from eavesdroppers and hackers. Therefore, device users should be made aware of the security issues and the impacts of their personal information being exposed to the public, as well as the basic countermeasures that can be taken to address or, more importantly, prevent the probable issues.

Limitations

The experiments were made only on Qoopers that uses the Bluetooth 4.0 Low Energy device in its structure, which is susceptible to MITM and other attacks. Using other smart toys robots with more modern Bluetooth devices would be appropriate for comparing different devices' security levels. In addition, the risks related to privacy were not included in this study, being it did not delve into the subject of threats such as the interception of sensitive data, among others.

In conclusion, Bluetooth is an important device present in smart toy robots used for wireless communication. This device can be dangerous due to attack vulnerabilities, especially on devices with Bluetooth Low Energy. In this study, we addressed vulnerabilities in Bluetooth communication and common Bluetooth issues, including related attacks, threats, malware, and vulnerabilities. To identify specific attacks for Bluetooth devices used in smart toys, this study adopted Qoopers, a robot capable of integrating different devices into its model. Qoopers was tested using security frameworks to simulate attacks.

We found that devices with BLE are more susceptible to attack. Qoopers was exposed to security frameworks used in restricted conditions, demonstrating that it can be hacked using a MITM attack and eavesdropping on data transfer. This paper also discusses solutions to prevent Bluetooth attacks. Bluetooth communication is vulnerable to different attacks, including MITM. This happens even with Qoopers robot when it is reprogrammed with customized applications with less security. These smart toy robots are used mainly by children under 16, who can make mistakes by ignoring security, focusing only on functionality, increasing the risk of personal information theft, among other threats.

As for future work, Qoopers can be further investigated when children program the Arduino board. This is important because Robobloq provides a programmable Arduino board. If children try to program with ad-hoc programs on the Internet without knowing their purposes, this sort of device can be used as a small component or bot for larger botnets that retrieve personal information.

DECLARATIONS

Authors' contributions

Made substantial contributions to the study's conception, design, performed data analysis, and interpretation: Acharige KM, and Albuquerque O. de P.

Performed data acquisition and provided administrative, technical, and material support: Hung PCK, Fantinato M, Peres SM

Availability of data and materials

Not applicable.

Financial support and sponsorship

None.

Conflicts of interest

All authors declared that there are no conflicts of interest.

Ethical approval and consent to participate

Not applicable.

Consent for publication

Not applicable.

REFERENCES

1. Rafferty L, Hung PCK. Introduction to toy computing. Mobile Services for Toy Computing. Springer; 2015. pp. 1-7.
2. Frost JL, Wortham SC, Reifel RS. Play and child development. [S.l.]: Merrill: Prentice Hall; 2001.
3. Hung PCK, Iqbal F, Huang S, Melaisi M, Pang K. A Glance of Child's Play Privacy in Smart Toys. In: Sun X, Liu A, Chao H, Bertino E, editors. Cloud Computing and Security. Cham: Springer International Publishing; 2016.
4. Intel Technology Journal. Developing smart toys - from idea to product. Available from: https://www.intel.com/content/dam/www/public/us/en/documents/research/2001-vol05-iss-4-intel-technology-journal.pdf. [Last accessed on 20 Feb 2021]
5. White DW. What is stem education and why is it important? In: Florida Association of Teacher Educators Journal; 2014. pp. 1-8. Available from: http://stembestpractice.com/what-is-stem-education-and-why-is-it-important/. [Last accessed on 20 Feb 2021]
6. Albuquerque ODP, Fantinato M, Kelner J, de Albuquerque AP. Privacy in smart toys: Risks and proposed solutions. *Electronic Commerce Research and Applications* 2020;39:100922.
7. Henson M, Taylor S. Memory encryption: A survey of existing techniques. *ACM Computing Surveys* 2014;46:1-26.
8. Guide to protecting the confidentiality of personally identifiable information (PII). National Institute of Standards and Technology, USA. Available from: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=904990. [Last accessed on 20 Feb 2021]
9. Juniper Research. Smart toy revenues to hit $2.8bn this year, driven by black Friday & Christmas holiday sales. Available from: https://www.juniperresearch.com/press/press-releases/smart-toy-revenues-to-hit-2-8bn-this-year. [Last accessed on 18 Apr 2020]
10. Shasha S, Mahmoud M, Mannan M, Youssef A. Playing with danger: A taxonomy and evaluation of threats to smart toys. *IEEE Internet of Things Journal* 2019;6:2986-3002.
11. Kopacek, P. Supplemental ways for improving international stability SWIIS. *IFAC Proceedings Volumes* 2008;41:5257-61.
12. Linert J, Kopacek P. Humanoid robots Robotainment. *IFAC-PapersOnLine* 2018;51:220-5.
13. Liu Y, Nejat G. Robotic urban search and rescue: A survey from the control perspective. *J Intell Robot Syst* 2013;72:147-65.
14. Qppoers - Robobloq Co. Ltd. Available from: https://www.robobloq.com/product/qoopers. [Last accessed on 20 Feb 2021]
15. Babar S, Mahalle P, Stango A, Prasad N, Prasad R. Proposed security model and threat taxonomy for the Internet of Things (IoT). In: Meghanathan N, Boumerdassi S, Chaki N, Nagamalai D, editors. Recent Trends in Network Security and Applications. Berlin: Springer Berlin Heidelberg; 2010. pp. 420-9.
16. Berrehili FZ, Belmekki A. Privacy Preservation in the Internet of Things. Advances in Ubiquitous Networking 2. Singapore: Springer Singapore; 2017. pp. 163-175.
17. Chen L, Cooper P, Liu Q. Security in Bluetooth networks and communications. Wireless Network Security. Berlin: Springer Berlin Heidelberg; 2013. pp. 77-94.

18. Ihamäki P, Heljakka K. Smart, skilled and connected in the 21st century: education promises of the Internet of Toys (IoToys). Honolulu. 2018. pp. 5-8. Available from: https://www.researchgate.net/publication/322136955_Ihamaki_P_Heljakka_K_2018_Smart_Skilled_and_Connected_in_The_21st_Century_Educational_Promises_of_the_Internet_of_Toys_IoToys. [Last accessed on 20 Feb 2021]
19. Chen L, Ji J, Zhang Z. Wireless network security: theories and applications. Beijing Heidelberg: Higher Education Press; 2013.
20. Mascheroni G, Donell H. The Internet of Toys: A report on media and social discourses around young children and IoToys; DigiLitEY. 2017. Available from: http://digilitey.eu/wp-content/uploads/2017/01/IoToys-June-2017-reduced.pdf. [Last accessed on 20 Feb 2021]
21. Haataja K, Hyppönen K, Pasanen S, Toivanen P. Bluetooth Security Attacks: comparative analysis, attacks, and countermeasures. Heidelberg: Springer Berlin Heidelberg; 2013.
22. Lonzetta A, Cope P, Campbell J, Mohd B, Hayajneh T. Security vulnerabilities in Bluetooth technology as used in IoT. *JSAN* 2018;7:28
23. Legg G. The bluejacking, bluesnarfing, bluebugging blues: Bluetooth faces perception of vulnerability. Available from: http://www.eetimes.com/document.asp?doc_id=1275730. [Last accessed on 20 Feb 2021]
24. Caldwell L, Ekerfelt S, Hornung A, Wu JY. The art of Bluedentistry: current security and privacy issues with Bluetooth devices. 2006. Available from: https://www.semanticscholar.org/paper/The-art-of-Bluedentistry-%3A-Current-security-and-Caldwell-Ekerfelt/f727a7ae513f7ce5035bf4459c17fd586dfaccfd#citing-papers. [Last accessed on 20 Feb 2021]
25. Huang Y, Hong P, Yu B. Design of Bluetooth DOS attacks detection and defense mechanism. 4th ed. China: IEEE International Conference on Computer and Communications (ICCC); 2018. pp. 1382-7.
26. Kostakos V. The privacy implications of Bluetooth. 2008. Available from: https://arxiv.org/abs/0804.3752. [Last accessed on 20 Feb 2021]
27. Hassan SS, Bibon SD, Hossain MS, Atiquzzaman M. Security threats in Bluetooth technology. *Computers & Security*. May 2018;74:308-22.
28. Sandhya S, Devi KAS. Contention for man-in-the-middle attacks in Bluetooth networks. International conference on computational intelligence and communication networks; 2012 Nov 3-5; Mathura, India: IEEE; 2012. p. 700-3.
29. Kügler D. "Man in the middle" attacks on Bluetooth. In: Wright R.N. editors. International Conference on Financial Cryptography; 2003; Springer, Berlin, Heidelberg; p. 149-61.
30. ISO/IEC 27002:2013 Information technology - Security techniques - Code of practice for information security controls. The International Organization for Standardization (ISO), Edition 2, October 2013. Available from: https://www.iso.org/standard/54533.html. [Last accessed on 20 Feb 2021]
31. Securing/gattacker. GitHub. Available from: https://github.com/securing/gattacker. [Last accessed on 20 Feb 2021]
32. A Node.js BLE (Bluetooth Low Energy) central module. Available from: https://github.com/sandeepmistry/noble. [Last accessed on 20 Feb 2021]
33. A Node.js module for implementing BLE (Bluetooth Low Energy) peripherals. Available from: https://github.com/sandeepmistry/bleno. [Last accessed on 20 Feb 2021]
34. Adafruit Bluefruit LE Sniffer. Available from: https://www.adafruit.com/products/2269. [Last accessed on 20 Feb 2021]
35. Wireshark 2.1. Available from: https://www.wireshark.org/docs/wsdg_html_chunked/index.html. [Last accessed on 20 Feb 2021]
36. Lin C, He D, Huang X, Choo KR, Vasilakos AV. BSeIn: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0. *Journal of Network and Computer Applications* 2018;116:42-52.
37. Ureten O, Serinken N. Wireless security through RF fingerprinting. *Canadian Journal of Electrical and Computer Engineering* 2007;32:27-33.
38. Jangirala S, Das AK, Vasilakos AV. Designing secure lightweight blockchain-enabled RFID-based authentication protocol for supply chains in 5G mobile edge computing environment. *IEEE Transactions on Industrial Informatics*. 2020;16:7081-93.
39. Wazid M, Das AK, KVB, Vasilakos AV. LAM-CIoT: Lightweight authentication mechanism in cloud-based IoT environment. *Journal of Network and Computer Application* 2020;150:102496.
40. Das AK, Wazid M, Kumar N, Vasilakos AV, Rodrigues JPC. Biometrics-based privacy-preserving user authentication scheme for cloud-based industrial Internet of things deployment. *IEEE Internet of Things Journal* 2018;5:4900-13.