IoT Devices Security and Privacy Threats Defense Strategies using Bluetooth Low Energy

Rashmi Priya[1], Mashhod Siddiqui[2]
[1]MTech Scholar, [2]Assistant Professor
[1]Department of Computer Science Engineering, RKDF College of Engineering, Bhopal, India
[2]Department of Computer Science Engineering, RKDF College of Engineering, Bhopal, India
rashmipriya20jangmail.com[1] mash.czar@gmail.com[2]

Abstract: With the exponential growth of the Internet of Things (IoT) and the ease of use of Bluetooth Low Energy (BLE) connection protocols, defense strategies for IoT BLE sensors need to be developed. While there are papers on qualitative IoT research, quantitative IoT experiments using BLE sensors still need to be worked on. Compare the raw pre-test to the post-test applying the Bluetooth security check as a processing variable to determine if the results are statistically significant. Using experimental design and testing tools, researchers demonstrated that two of the seven threat categories provide some level of protection against known vulnerabilities; However, the null hypothesis was rejected, claiming that NIST control would provide some protection against known attacks.

Keywords: Internet of Things, Bluetooth Low Energy, NIST, security controls

I. Introduction

Although the definition of the Internet of Things has been contradictory, the technology is one that aggregates everyday things connected to sensors into heterogeneous networks. According to [1], the IoT has limited human intervention. Technology to shine in the environment of technology and cyberspace. Physically, data was exchanged by collecting, generating, or processing data relevant to their role in cyberspace. The sensors collected sensitive consumer security or privacy data.This may affect legal concerns of . [1] Additionally, the authors stated that software development or configuration control on IoT sensors could impact cybersecurity concerns on this host network. manufacturers were held back by security regulations and recently had government interventions related only to IoT cybersecurity [2]. Government agencies have feared the harshness of the industry in enforcing the regulations, and the United States government has encouraged safe development, which has been adopted by an accepted vendor for future work [2]. The Bluetooth wireless communications industry has evolved to a place where the technology is integrating the sensor into many devices, including mobile devices, wearables, and vehicles. There have been many technology integrations and security updates including version 4.2 of Bluetooth Low Energy (BLE), including Bluetooth Low Energy (BLE) version 4.2. Focused on increasing security posture for the low power requirements of channel hopping and earlier, BLE was a communication protocol for IoT communication protocol [3]. The IOT device maker includes BLL with BLE technology and integrated IOT sensors. For the paper experiments, the BLE protocol used version 4.2. Background of IoT BLE Experimental Study source used by IoT sensors started with device level attack and attacker abused usability in code and firmware bugs [4]. The attacks leveraged the IoT sensor through a heavy-duty Bluetooth attack. The strategy requires user intervention to disable Bluetooth when not in use. According to [5], IoT middleware sensors act as a bridge between physical and virtual resources that do not have equal control over security.due to low consumption and lack of code [5] exploitation is due to poor implementation criteria or lack of strict configuration control [5]. The attackers implemented a variety of problems with a large number of vulnerable sensors [5]. a bridge between middleware and memory-related vulnerabilities, triggered a buffer overflow attack against a specific sensor. By exploiting memory, an attacker allows a memory executable to serve malicious content, container code, or vulnerable sensors. By executing malicious code, an attacker can monitor or deploy software on a targeted IoT sensor [3].According to [6], Commands and Controls (C2), where sensor nodes create complex networks through agent-based self-organization models by implementing predefined rules, the result is an agent-based model that integrates expected behavior and uncovers opportunities. implement penetration testing tools [6]. Self-organization that is not controlled by external sources is formed through the creation of complex sensory networks [6]. If there is a sensor change, it adapts to the newly defined rules. The attacker has a set of malicious rules that override the predefined steps to force phishing to create a sensor. Fake IoT variables [6], problem for BLE IoT sensors A common problem is that IoT sensors are vulnerable to cyber attacks [3]. The specific problem is that IoT sensors have many security issues due to the BLE encryption vulnerability, resulting in cybersecurity attacks [3] UK Ministry of Digital Culture, Media and Sport, 2018) a problem as these vulnerabilities expose IoT sensors to attacks. The network is publicly accessible.(2018) presented 20 known attack vectors using IoT sensors with BLE communication protocol to exploit vulnerabilities in their implementation. IoT devices lag behind security controls and lack standard security monitoring (UK. Department for Culture, Media and Digital Sport, 2018).

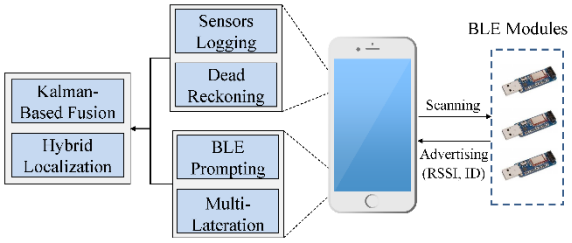

Figure:1 Improved BLE Indoor Localization

The Purpose of IoT BLE Defensive Study

The purpose of this quantitative experiment is to create a defense strategy framework to solve the security issues of IoT sensors that use BLE vulnerabilities. The experimental test design utilizes the National Institute of Standards and Technology (NIST) security guidelines, which test the industry's current baselines in an innovative test environment. The recommendations of this work show a detailed threat model, which contains quantitative statistics and defense strategies to mitigate the attack vectors of IoT sensors using BLE, and add the results to the defense framework of IoT.

Table 1. Threats and Well-Known Bluetooth Attacks

Type of Threat	Threats to Bluetooth	Well-Known Attacks	Type of Threat
BDADDR attacks, spoofing gained	Bdaddr (Device Address)	Bluetooth Mac Spoofing Attack #1	BDADDR attacks, spoofing gained
knowledge of the target address to	BTClass (Class of Device)	Bluetooth Pin Cracking Attack #2	knowledge of the target address to
exploit the BLE sensor further.	HCIConfig (Device Name, Class of	BluePrinting Attack #9	exploit the BLE sensor further.
Some attacks required BDADDR to	Device)	BlueBorne Attack #11	Some attacks required BDADDR to

The Nature of the IoT BLE Research Experiment

The nature of this study was a quantitative experience [7].The study method has been a measurable experimental design that uses the BLE vulnerability to test the IOOT sensor. The association of technology which lists the 20 well-known attacks,tools or technologies used to operate Bluetooth, Table 1, is shown in Table 1. The attack method defined in Table 1 is used to analyze the model of Defense for the IOOT sensor using ble.The theoretical basis of multiple variable methods revealed the deviation from the current industry and recommendations of the current industry, or with various vulnerabilities for the capacity to secure IoT sensors using BLE . It was to test the available IOT sensors. Well-known attacks and basic sensor configurations provide starting points to handle test cases equally. The focus on all sensors in the population and the results are presented in Figures 1 and 2.

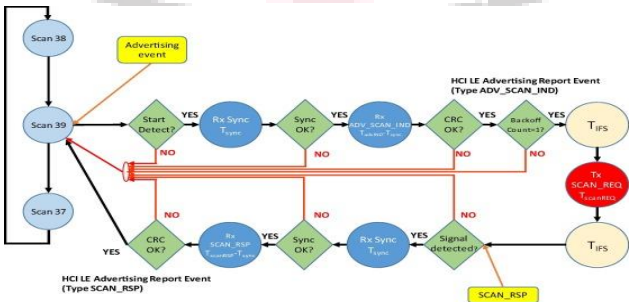

Figure:2 Low-cost test measurement setup for real IoT BLE sensor device

The world's view of this study focuses on the postpositivist approach [7].During this experience, the intention was to focus on closed-door laboratory networks using best practices, test plans, test cases and best practices, test plans, cases of Test and results models for the declaration and declaration of the following considerations.“Network of Things,” NIST Special Pub 800-183 for sensor management;“IoT Trust Concerns” NIST cybersecurity whitepaper for 17 trust areas incorporated into IoT deployments .“Guide to Bluetooth Security,” NIST Special Publication 800-121, Revision 2 for Bluetooth Vulnerabilities, Threats, and Countermeasures [8]

NIST Mobile Threat Catalogue and Mitigations

NIST maintained the Mobile Threat Catalogue (MTC), where some of the well- known attacks had mitigations for Bluetooth devices [9]. The MTC developed by NIST to identify threats, mitigations, and countermeasures to mobile computing devices (NIST, 2016x). When completing a search through the threat categories, there were 5 of 12 threat areas directly related to Bluetooth vulnerabilities and countermeasures. The Authentication (AUT), Global Positioning Systems (GPS), Local/Personal Area Networking (LPN), Supply Chain (SPC), and Stack (STA) categories had a direct relation to the well-known vulnerability list; however, it was not all-inclusive.

Table 2. Mapping Bluetooth Attacks to NIST

Well-Known Bluetooth Attack	**Mobile Threat Catalogue**
BlueBugging	LPN-10
Brute-Force BD_ADDR	LPN-11
BlueJacking	LPN-14
BluePrinting	LPN-6
Bluecasing War Nibbling	LPN-7
Bluesmack	LPN-8
Bluetooth Denial of Service	LPN-8, GPS-0
Bluetooth Snarfing	LPN-9
Bluetooth Backdoor	SPC-21
BlueBump	N/A
BlueDump	N/A
Blueover	N/A
MultiBlue	N/A

II. LITERATURE REVIEW

The first titles searched included “Securing the IoT Bluetooth Low Energy,” “Defensive Strategies for the IoT Bluetooth Low Energy,” and “Self-organized IoT devices to defend against cyber threats.” Keyword searches completed the literature review documented in Appendix A and Table 3. The following hypothesis and research question guided the literature review. The application of NIST security controls and best practices for the IoT sensors using BLE would not adequately protect the devices from exploitation, leveraging well-known Bluetooth attacks.

Additionally, the null hypothesis was applying NIST security controls, and best practices for securing IoT sensors using the BLE device would mitigate well-known Bluetooth attacks. The historical documentation, research articles, journals, and publications suggested there are significant problems within the IoT and lead the researcher to answer “Will the application of NIST recommended security controls and best practices mitigate the success of well-known attack vectors on IoT sensors using BLE?”

Historical and Legal Overview

According to the Internet of Things: Privacy & Security in a Connected World (Federal Trade Commission, 2015), security risks included disclosure of Personally Identifiable Information (PII), attacks critical infrastructure, and risks to personal security were concerns in emerging IoT technology. Storing account and financial information on Smart TVs during internet browsing could expose users to information disclosure (Federal Trade Commission, 2015). According to the Federal Trade Commission (2015),trust relationships and interconnection of the IoT sensors were a concern because vulnerable sensors create vulnerabilities for protected IoT nodes.

IoT – Sensors

The "Internet of Things: a security point of view" . conducted an extensive qualitative study on the software vulnerabilities in IoT and concluded there would need to be a future study on defensive strategies to build a framework. The study established a framework modeling four-layers focusing on sensors, communication, network, and software security .. The researchers stated within an enterprise where IoT sensors exist, and it may be vulnerable to data breaches. Li concluded the review by generalizing the need for defensive framework experimentation in IoT [10]. Within the evaluation, communication occurred through HTTP or an unencrypted link susceptible to information disclosure [10].

Bluetooth Low Energy Technical Review

"A Guide to Bluetooth Security" [8]provided information on security capabilities and provided security recommendations for Bluetooth communications. Bluetooth beacons designed to run on battery power and deployed for use during an extended period [8] . Beacons maintained up to a 30- meter (100 foot) range to establish a connection [8] .BLE operated on 40 channels and used AES-CCM for authentication and encryption [8] .In BLE, a Piconet was set up for the local Wireless Personal Area Network (WPAN) [8] . Piconets have the highest device limit of 7 active sensors; however, they can have 255 stored sensors [8] . Slave sensors of one Piconet can be the master of another, creating a network chain [8] . BLE sensors can send connectionless broadcast data to all nodes within the Piconet [8] .

Well-Known Bluetooth Attacks

While there were many different types of attacks for Bluetooth, an important note to take is the version of the sensor [3]. An outdated Bluetooth sensor places the entire Piconet at risk for exploitation [3] Secure BLE sensors communicating with weak sensors would not protect the connection and is as strong as the weakest device [4] documented well known Bluetooth attacks from a holistic view from early Bluetooth implementation to the present-day risks represented spoofing, pin cracking, eavesdropping, unauthorized disclosure of data, configuration software management and physical security. NIST security guidance and control documented countermeasures of some attacks through the Mobile Threat Catalogue.

Securing Software Defined Networks for Bluetooth Low Energy

In "Securing the Internet of Things: Challenges, Threats and Solutions" [11] defended the software-defined network for an IoT network had limitations when deploying Security Information and Event Management (SIEM) technologies; due to the amount of data processing it did, effective monitoring and alerts on malicious traffic produced a large number of alerts [11]. In "Shielding IoT against cyber-attacks: An event-based approach using SIEM"[12]stated Intrusion Detection System (IDS) solutions which reported security incidents to a SIEM had issues with limited hardware resources on IoT sensors, their protocol stack, and generating massive amounts of data. Accurate reporting of security incidents with an IDS did not use Bayesian inference to filter data for processing [12]. Therefore, the researchers evaluated multiple open-source IDS products to perform Incident Response, including Suricata, OpenVAS, and Kismet IDS, sending IoT alerts to OSSIM [12]. contributed static correlational rules for IoT security architecture used with Incident Response. The rules addressed the mapping of software vulnerabilities, security events, and attack surfaces to specific IoT devices and sensors [12].

Mitigation Strategies

In HACKING IoT: A Case Study on Baby Monitor Exposures and Vulnerabilities [13] described the IoT sensors lacked a reasonable vulnerability management path once it left the Manufacturer. The authors cited patches, and poor configuration management were substantial factors of reported flaws in IoT [13].The purpose of the whitepaper was to examine 10 IoT vulnerabilities found by Rapid7 and communicated to customers, vendors, and CERT in baby monitors [13]. Over half of the flaws represented remote code execution (RCE), which allowed an attacker to gain access to the device from the Internet [13]. Remote shell or backdoor access was possible due to hardcoded passwords and unencrypted URLs [13].

IoT Threat Modeling

In “High-probability and wild-card scenarios for future crimes and terror attacks using the Internet of Things” [10] created a cause and effect model to exhaust all possibilities using the IoT to build scenarios for future crimes and terror attacks. The problem connected IoT to many everyday things, financial, medical, power plants, vehicles, and many more [10]. The study weighed out potential threats against their potential impact [10].

Current Findings

The Federal Trade Commission (2015) was a business case for IoT risk management, where many of the recommendations were available in other NIST and Defense Information Systems Agency (DISA) related guidance. The report stated that they did not want to create regulation because it would stifle IoT emerging markets and development (Federal Trade Commission, 2015). With the mass proliferation of IoT, roughly 25 billion vulnerable sensors could execute a massive botnet by nefarious individuals (Federal Trade Commission, 2015).[14] raised points about targeting high-value people or things through IoT at a specific event using GPS proximity. Targeting included an executive meeting or a hospital to disable IoT sensors [14]. [4] stated that secure IoT sensors using BLE flashing is not possible on a large scale. It needs an automated process and careful development process to protect against well-known Bluetooth vulnerabilities and additional adaptive triggers to alert monitoring systems of a security change 12] monitoring IoT BLE was possible with manual intervention by static categorization of all available options on an IoT device. Alerts, when a value changed and monitored specific values or conditions, would be possible with manual IoT categorization [12].

Pre-Test between IoT BLE Sensors

The pre-test between sensors discovered changes between the pilot study, which used one sensor, and pre-test conditions used two new sensors to evaluate the Threats to Bluetooth. With the pre-test conditions set, each tool executed from the Kali Linux virtual machine. Each Threat to Bluetooth ran and the level of access calculated by using the CVSS base score in Table 4 and added local environmental conditions during the pre- test experiment. The calculations adjusted using the base scores calculated from the category where each tool was evaluated by itself using the CVSS v3.1 calculator. Any tools resulting in a zero score did not receive further evaluation. The test discovered changes from the Pilot study and base score; however, each test condition remained the same between the two IoT BLE sensors.

According to Satam BLE data analysis used a Wireshark sniffer configured with Bluetooth filters to target Bluetooth traffic. Wireshark was configured with 20 specific filters focused on BLE traffic between the Kali Linux VM and the IoT BLE sensor. Wireshark was used to capture, and filter large amounts of network traffic stored in PCAP files . In Table 6, 20 Wireshark filters were used during the experiment to match monitoring criteria for the NIST Security Controls and Recommendations checklist.

The BlueZ testing tools were administrative and debugging tools misused during the experiment. Gatttool was a Linux command-line utility used to interact with BLE devices and connected directly to a known Bluetooth MAC address to display all profile characteristics. Additionally, Gatttool set a security level to communicate with a BLE device. HCITool, HCI Config, and HCIdump were administrative utilities to scan, configure, and receive debugging information from a BLE device. A separate program Bluetoothctl was a command-line configuration utility and scanned and paired with BLE devices.

III. RESEARCH METHODOLOGY

The study was a single-subject, multi-facility experimental design using a control group. According to [7], individual studies require multiple chronological steps, including observed behavior without intervention, baseline conditions without intervention, and provision of intervention measures to monitor behavior over time. The baseline consists of two sensors where the features of both sets have no processing variables independent of NIST security checks to assess whether the results produce the same pre-processing baseline. Then, in the intervention phase, the adoption of the NIST Bluetooth guidelines and best practices was applied to a new set of sensors and baselines that show the difference between NIST pretreatment and intervention. In addition, prior to conducting experimental or pilot studies, the researcher purchased six Mpression sets and randomly selected two unpackaged sets for the experiments, with the remaining sets used to replicate the experimental research.A pilot study validated the experimental procedure and detection methods outlined in the Study Type section, using a BLE-IoT sensor to perform instrument tests. After completing the experimental study, the researcher confirmed that the data collection analysis yielded the correct measurements and imported the results into the IBM SPSS v26 database. The pilot study sensor was decommissioned after use and should not be reused unless further calibration is required. A further calibration is done by adjusting the experimental procedure and the assumptions made when creating the fields in the IBM SPSS database.

During this test, the goal was to focus on a closed laboratory network that uses industry guidelines in the "Type of Investigation" section, where the test plan, test cases, and outcome model for the test are developed, statistical analysis, and reporting.In the "Nature of Research" section, the well-known vulnerability classification and Bluetooth testing tools

have compiled test cases from the "Common Bluetooth Attacks" and "Classification" sections. Bluetooth Attacks" [3]. Results provided a dataset to analyze the statistical likelihood of an attack, the discovery of mitigation techniques, and the existential risk of IoT BLE sensors configured with control measures. NIST security clearance.

Design adequacy

When investigating a quantitative research design, a single-subject multibase design is most suitable for the experiment [15]. According to [7], all subjects were treated the same in repeated measurement attempts. Individual project designs do not require a large population and can apply incremental changes to each reference simultaneously [15]. Researchers made changes to the baseline, observed the impact of a change, and made any necessary changes to assess the effectiveness of NIST controls on

BLE, and implemented security and mitigation measures to secure the configuration. IoT sensors.Due to the small sample size of the test, a sensor is used as a control to show the difference between before and after the test showing the difference between treated subjects or the effect of the change due to the hole. Compared to the chosen research method, a qualitative case study does not provide the necessary insight into the effects of changing a variable [7]. In comparison, quantitative research

tested one hypothesis and one null hypothesis, while qualitative research focused on answering survey questions [7]. In contrast, answering qualitative questions from case studies did not have the same effect on the pre-existing sample [7]. Therefore, choosing a quantitative experiment is the most appropriate for the study.Sampling The experiment uses a unique and measurable test design to test defense strategies for IoT sensors using BLE [7] One sensor is used as control variable

and the second sensor as processing group; there are many steps that have completed the best design and after testing; A test plan, test cases and results model created a database with statistical analysis and quantified reports for each threat type, Bluetooth threat and repeated measurement results. Because of this test case model, the test case generation comes from a list of known attacks from known Bluetooth exploit vectors [3]. Panels are compared using CVSS Calculator v3.1 using

known risk weights and formulas. Results identified a code review where developers did not follow a cybersecurity development model [10].Data Analysis Creswell recommended quantitative studies using software to help the researcher generate statistics. The IBM SPSS database software was suggested as a tool. IBM SPSS is well known for producing statistical data for analysis among researchers. provided tools to help researchers use IBM SPSS for data analysis. Descriptive and comparative statistics of RMANOVA results were the two types of data analysis used to analyze the data collected during the experiment.The analysis used RMANOVA for the following research question: Research Question 1 (RQ1). Will NIST enforcement, recommended security controls, and best practices mitigate the success of known attack vectors on IoT sensors using BLE? RMANOVA = Repeated Measures for Analysis of a Variance Dependent Variable = Existing IoT BLE Sensor Vulnerabilities Independent Variable = BLE Security Controls NIST Tutorial SPSS Repeated Measures ANOVA (2019) provided a step-by-step process for analyzing a population within the subject where there are two measurable ones and linear outcome variables. The first variable measures the current state of the IoT BLE sensor, regardless of whether a vulnerability is present or not. The second variable measured the IoT BLE sensor with the -NIST control applied to test the null hypothesis H0. By applying NIST security controls and best practices to protect IoT sensors with the BLE device, known Bluetooth attacks could potentially be mitigated. In comparison, if there were no changes, what countermeasures could reduce the likelihood of an attack on BLE-IoT sensors?The last variable compared the results of changing the variable testing hypothesis H1. Applying NIST security controls and best practices secured IoT sensors with the BLE device and failed to mitigate known Bluetooth attacks.

IV . RESULTS

This research focuses on the results obtained from quantitative experiments using RMANOVA and the defined experimental procedure. A pilot study validated the SPSS v26 database acquisition method, the experimental variables, and the initial CVSS v3.1 score used to present the results. Results. Next, two previously measured sensors with the same results and adjusted CVSS 3.1 assessment presented environmental and status considerations.

The researcher evaluated the best data and adjusted the Wireshark application's network traffic display filter, and then implemented security controls. The Wireshark application is a passive monitoring tool and works in parallel with the traffic and does not affect the test. Network filters allow investigators to collect data directly related to the NIST Security Recommendations and Controls Checklist. The security check test was conducted from January 31, 2020 to February 9, 2020.Repeated NIST measurement results must be verified before proceeding with the risk reduction assessment.

The risk mitigation assessment requires a technical and theoretical review of risk mitigation strategies in the literature to limit exposure to BLE-IoT sensors. pieces of information collected from conference papers over the last 24 months were used to develop effective countermeasures for BLE-IoT sensors. Ultimately, the charts developed a visual representation of the test results, and the researcher provided updates to the NIST Bluetooth security guidelines to mitigate attacks. BLE-IoT Test Equipment and Procedures The test methodology follows a step-by-step process to ensure each part of the test is captured.After the pre-test is completed, the results are calculated using the CVSS calculator and reported in Table

7. The calculated results are used as the measurement results of the pre-test. The investigator then applies NIST security controls and best practices. The NIST Bluetooth Guide and the Mobile Threat Directory were used as references in developing the checklist. After the security checks have been performed, a second test of each configuration is performed and recorded in Table 7 for sensors X and Y.The test results are encrypted and entered into the SPSS database. Code analysis of each configuration and firmware then completed the final risk mitigation analysis.

Steps to complete the test:

Step 1. Configure the BLE dongle and Wireshark to capture all traffic during the test.

step 2.All profile settings have been applied to both IoT BLE sensors.

Step 3. Each Bluetooth threat is tested on BLE-IoT sensor X and Y. Step 4. Completed the BLE-IoT sensor test and stopped all collections.Step 5. Repeat step 14 for each Bluetooth threat.

Step 6. Enter Results and End Run

Equipment Tools Required tools and materials

During testing, the equipment required to obtain the results included the monitoring software loaded on the Apple iPad and USB Bluetooth dongles for recording the results. Requires the IoT BLE test kit with smartphone, Android app, software compiled by Mpression website for each personality, firmware for the IoT BLE sensor and power supply from a USB source.The Bluetooth tools in Table 6 were loaded into Kali Linux Distribution and is used throughout the test.

Empirical test conditions According to [16], the calculation of the CVSS is based on quantitative and qualitative factors to determine the severity and the risk through the CVSS score. The CVSS score itself does not determine the concrete environmental conditions or the probability of success of the deployed instruments [16]; The base score does not change with the environment or the chances of success; Therefore, each threat category was presented in Table 4 with a CVSS reference value of 3.1 [16]. According to [17], the remote attacker does not need an account on the attacked platform and with IoT BLE as the wireless technology, all tests use the remote attacker methodology.The researcher restricted authentication and key pairing during testing with the BLE IoT sensor. Three factors were observed during the experiment: 1) no transmission range limitation, 2) encryption was not configurable, and 3) IoT BLE sensor detection was not disabled.

Pre-Test Conditions

Used a subset of vulnerability test data, manual analysis, and an understanding of exploits on sensors through testing. A pre-test was conducted on the IoT BLE sensors sequentially and equally with the subset of tools from the pilot study. In Table 4, the CVSS calculator results formed the base score, where each category was adjusted to the Threat to Bluetooth during the pre-test. The sensor, category of threat, and threats to Bluetooth calculated the CVSS Score for a threat. Scores were adjusted during the experiment to match the conditions of each tool and test condition. When all of the conditions were met, the measurement was calculated for the final result for the pre-test. Test results entered into Table 7 Pilot to Pre-test Sensor Findings, and Table 8 CVSS Calculations reflected the calculated measurements.

Pre-Test between IoT BLE Sensors

The pre-test between sensors discovered changes between the pilot study, which used one sensor, and pre-test conditions used two new sensors to evaluate the Threats to Bluetooth. With the pre-test conditions set, each tool executed from the Kali Linux virtual machine. Each Threat to Bluetooth ran and the level of access calculated by using the CVSS base score in Table 4 and added local environmental conditions during the pre-test experiment. The calculations adjusted using the base scores calculated from the category where each tool was evaluated by itself using the CVSS v3.1 calculator. Any tools resulting in a zero score did not receive further evaluation. The test discovered changes from the Pilot study and base score; however, each test condition remained the same between the two IoT BLE sensors.

The “Equipment required Tools and Hardware” section defined systems and hardware to test threats to Bluetooth in Table 5.

Table 5. Pilot Sensor Findings

Threats to Bluetooth	**Pilot**
Base Score	8.2
SDP Tool	0
Bluetooth CTL	8.2

Reconnaissance HCIDump	8.2
HCI Tool	8.2
Eavesdropping Blueprinting	n/a
Bluesniff	n/a
BT Audit	n/a
Base Score	7.6
Spooftooph	0
Base Score Device	7.6
Man in the Bthidproxy	n/a
Base Score	9.6
L2Ping	0
Battery Exhaustion	n/a
Denial of BlueJacking	n/a
Blueper	n/a
BlueSYN	n/a
Base Score	8.3

In Table 6, the BLE filters coincided with the NIST security controls checklist items. The filters were used during the experiment to identify the current settings for theIoT BLE sensor kit. The Wireshark filter reference for "bthci_evt" was used to compile the list.

Table 6. BLE Filters

Wireshark Filter	**Description**
Bthci_evt.encryption_enable	Encryption Enable
Bthci_evt.adv_handle	Advertising Handle
Bthci_evt.adv_phy	Advertising PHY
Bthci_evt.advertising_sid	Advertising SID
Authetication	Bthci_evt.auth_enable
Bthci_evt.auth_requirements	Authetication Requirements

Bthci_evt.bd_addr	BD Addr
Bthci_evt_code	Bluetooth Event Code
Bthci_evt.current_mode	Current Mode
Bthci_evt.device_name	Device Name
Bthci_evt.encryption_mode	Encryption Mode
LE General Discoverable Mode	Bthci_evt.le_flags_general_disc_mode
LE Limited Discoverable Mode	Bthci_evt.le_flags_limit_disc_mode
Bthci_evt.link_key	Link Key
Periodic Advertising	Bthci_evt.le_features.periodic_advertising
Pin Type	Bthci_evt.pin_type
Bthci_evt.cte_rssi	RSSI Value
Frame_epoch_time	Timestamp stored in Wireshark

In Table 7, the pilot to pre-test sensor findings compiled the test results for one pilot sensor and two pre-test sensors for each tool. The CVSS score from pilot to pre-test was adjusted due to environmental conditions during the test. Adjustments were made using the online CVSS v3.1 calculator and operational considerations of the tool.

TABLE 7. PILOT TO PRE-TEST SENSOR FINDINGS

Category of Threat Threats to Bluetooth	**Pilot**	**Pre-Test Sensor**	**Pre-Test Sensor**
		X	Y
Base Score	8.2		
SDPTool	0	0	0
Reconnaissance Bluetooth ctl	8.2	8.3	8.3
HCIConfig	7.6		
Eavesdropping HCIDump	8.2	7.9	7.9
HCITool	8.2	7.9	7.9

In Table 8, the CVSS calculations were adjusted from the base scores noted in Table 4. When the researcher executed each of the tools, operational changes, and environmental considerations were used to populate the CVSS v3.1 calculator. The final result in the base, temporal, and environmental metrics are represented in the CVSS score and calculator results.

Table 8. CVSS Calculations

Category of Threat	CVSS	CVSS Calculator Results
Active Reconnaissance and Eavesdropping		
HCItool	7.9	AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:F/RL:W/RC:C/CR :M/IR:M/AR:M/MAV:A/MAC:L/MPR:N/MUI:N/MS:U/MC:H /MI:H/MA:L
hcidump	7.9	AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:F/RL:W/RC:C/CR :M/IR:M/AR:M/MAV:A/MAC:L/MPR:N/MUI:N/MS:U/MC:H /MI:H/MA:L
bluetoothctl	8.3	AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:F/RL:W/RC:C/CR :H/IR:M/AR:M/MAV:A/MAC:L/MPR:N/MUI:N/MS:U/MC:H/ MI:H/MA:L
Bluetooth Device Address Spoofing		
BLEScanner	8.0	AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:F/RL:W/RC:C/CR :M/IR:M/AR:M/MAV:A/MAC:H/MPR:N/MUI:N/MS:C/MC:H /MI:H/MA:H
HCItool > HCIconfig > Spooftooph	0	
Information Disclosure		
Gatttool/Bluetoothctl	8.4	AV:A/AC:H/PR:H/UI:R/S:C/C:H/I:H/A:H/E:F/RL:O/RC:C/CR :M/IR:M/AR:M/MAV:A/MAC:L/MPR:L/MUI:N/MS:C/MC:H/ MI:H/MA:H
Command Injection		
Gatttool/Bluetoothctl	8.4	AV:A/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H/E:F/RL:O/RC:C/CR :H/IR:H/AR:L/MAV:A/MAC:L/MPR:L/MUI:N/MS:C/MC:H/ MI:H/MA:L

V CONCLUSION

The experimental results suggested that the F-test was statistically significant and rejected the null hypothesis; the applied NIST security controls and best practices did not mitigate well-known Bluetooth attacks for IoT sensors using the BLE. The research question and the data suggested that the application of NIST, recommended security controls, and best practices did not mitigate successful, well-known attacks for IoT sensors using BLE. Furthermore, this study showed the rationalization of future research in securing personal wearable and experimentation in scanning technologies for IoT BLE devices.

REFRENCES

[1] Rose, K., Eldridge, S., & Chapin, L. (2015). The internet of things: An overview. The Internet Society (ISOC). Retrieved from https://www.internetsociety.org/wp- content/uploads/2017/08/ISOC-IoT-Overview-20151221-en.pdfAlgorithm_Based_on_Aes_RSA_and_Twofish_for_Bluetooth_Encryption

[2] Hogan, M., & Piccarreta, B. (2018). Interagency report on status of international cybersecurity standardization for the Internet of Things (IoT) (No. NIST Internal or Interagency Report (NISTIR) 8200 (Draft)). National Institute of Standards and Technology. Retrieved from https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8200.pdf

[3] Lonzetta, A., Cope, P., Campbell, J., Mohd, B., & Hayajneh, T. (2018). Security vulnerabilities in bluetooth technology as used in iot. Journal of Sensor and Actuator Networks, 7(3), 28. doi:10.3390/jsan7030028

[4] Fernandes, E. (2017). Securing Personal IoT Platforms through Systematic Analysis and Design. (Doctoral Thesis). Retrieved from ProQuest Database. (Accession No.10612074) Retrieved from https://deepblue.lib.umich.edu/handle/2027.42/137083

[5] Freemantle, P., & Scott, P. (2017). A survey of secure middleware for the Internet of Things. PeerJ Computer Science, 3, e114. doi:10.7717/peerj-cs.114
[6] Batool, K., & Niazi, M. A. (2017). Modeling the internet of things: A hybrid modeling approach using complex networks and agent-based models. Complex Adaptive Systems Modeling, 5(1), 4. doi:10.1186/s40294-017-0043-1
[7] Creswell, J. W. (2002). Educational research: Planning, conducting, and evaluating quantitative and qualitative research. Upper Saddle River, NJ: Prentice-Hall.
[8] Padgette, J., Scarfone, K., & Chen, L. (2017). NIST Special Publication 800-121 Revision 2, Guide to Bluetooth Security. doi:10.6028/nist.sp.800-121r2
[9] Franklin, J. M., Howell, G., Boeckl, K., Lefkovitz, N., Nadeau, E., Shariati, D., ... & Peck, M. (2019). Mobile device security corporate-owned personally-enabled (COPE).
[10] Tzezana, R. (2017). High-probabi.(Barcena & Wueest, 2015). ty and wild-card scenarios for future crimes and terror attacks using the Internet of Things. foresight, 19(1), 1-14. doi:10.1108/FS-11- 2016-0056
[11] Grammatikis U.K. Department for Digital Culture, Media & Sport. (2018). Secure by Design: Improving the cyber security of consumer Internet of Things Report. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/686089/Secure_by_Design_Report_.pdf
[12] Díaz López, D., Blanco Uribe, M., Santiago Cely, C., Vega Torres, A., Moreno Guataquira, N., Morón Castro, S., … Gómez Mármol, F. (2018). Shielding iot against cyber-attacks: An event-based approach using siem. Wireless Communications and Mobile Computing, 2018, 1-18. doi:10.1155/2018/3029638
[13] Stanislav, M., & Beardsley, T. (2015). Hacking iot: A case study on baby monitor exposures and vulnerabilities. Retrieved from Rapid7 website https://www.rapid7.com/globalassets/external/docs/Hacking-IoT-A-Case-Study-on-Baby-Monitor-Exposures-and-ulnerabilities.pdf
[14] Ometov, A., Solomitckii, D., Olsson, T., Bezzateev, S., Shchesniak, A., Andreev, S., & Koucheryavy, Y. (2017). Secure and connected wearable intelligence for content delivery at a mass event: a case study. Journal of Sensor and Actuator Networks, 6(2), 5. doi:10.3390/jsan6020005
[15] Askov, E. N. (1985). Single-subject, multiple-baseline designs in evaluating adult literacy programs (ED264441). ERIC. https://eric.ed.gov/?id=ED264441
[16] Mwathi, D. G., Okelo-Odongo, W., & Opiyo, E. (2017). Vulnerability analysis of 802.11 authentications and encryption protocols: cvss based approach. International Research Journal of Computer Science, IV(VI),
[17] Elia, I. A., Antunes, N., Laranjeiro, N., & Vieira, M. (2017, September). An analysis of openstack vulnerabilities. In 2017 13th European Dependable Computing Conference (EDCC) (pp. 129-134). doi:10.1109/EDCC.2017.29