ENHANCING IOT SENSOR PROTECTION THROUGH BLUETOOTH LOW ENERGY

Vinit Kumar[1], Mr. Gaurav Kumar Saxena[2]
[1]MTech Scholar, [2]Assistant Professor
[1]Department of Computer Science & Engineering School of Engineering, Sri Satya Sai University Of Technology & Medical Sciences, Sehore (M. P.)
[2]Department of Computer Science & Engineering School of Engineering, Sri Satya Sai University Of Technology & Medical Sciences, Sehore (M. P.)
way2vinit@gmail.com[1] gaurav.saxena18@gmail.com[2]

* Corresponding Author: Vinit Kumar

Abstract: *The widespread integration of Internet of Things (IoT) devices in various domains has led to an increased concern regarding the security of these interconnected systems, particularly in the context of sensor nodes. This paper proposes a novel approach to enhance the protection of IoT sensor nodes through the utilization of Bluetooth Low Energy (BLE) technology. The research focuses on leveraging the low-power and secure communication features of BLE to fortify the resilience of IoT sensor nodes against potential security threats. A comprehensive analysis of existing vulnerabilities in IoT sensor networks is conducted, and a set of security requirements is identified. The proposed solution involves the implementation of advanced encryption algorithms, secure key exchange mechanisms, and efficient authentication protocols within the BLE framework. Furthermore, the paper explores the integration of anomaly detection techniques to identify and mitigate potential security breaches in real-time. By combining BLE's energy-efficient communication with robust security measures, the proposed approach aims to strike a balance between maintaining low power consumption for sensor nodes and ensuring a high level of protection against unauthorized access and data manipulation.*

Keywords: *Internet of Things (IoT), Sensor Protection, Bluetooth Low Energy (BLE), Security Enhancement, Low-Power Communication*

1. INTRODUCTION

The Internet of Things (IoT) has witnessed exponential growth, seamlessly integrating physical devices and sensors into our interconnected digital world. This proliferation of IoT devices, however, brings forth unprecedented challenges, particularly in terms of security. As IoT applications become increasingly prevalent across diverse domains such as healthcare, smart cities, and industrial automation, safeguarding the integrity and confidentiality of the data generated by IoT sensor nodes becomes paramount [1].

This paper delves into the realm of enhancing the protection of IoT sensor nodes, addressing the vulnerabilities that arise in the context of their communication and data exchange. One of the promising technologies at the forefront of secure and efficient communication for IoT devices is Bluetooth Low Energy (BLE). BLE, characterized by its low-power consumption and versatility, emerges as a viable solution to fortify the security aspects of IoT sensor networks without compromising their energy efficiency [2].

The introduction sets the stage by highlighting the escalating significance of securing IoT sensor nodes, discussing the prevalent security challenges in existing IoT ecosystems, and outlining the motivation for employing BLE as a foundational technology for enhancing sensor protection. By combining the ubiquity of IoT devices with the advanced features of BLE, this research endeavors to contribute to the ongoing discourse on securing the IoT landscape, with a specific focus on safeguarding the vital components - the sensor nodes [3].

Although there was an inconsistency in the definition of the Internet of things, technology is a technology that combines daily things connected to sensors in heterogeneous networks. According to [4] IoT has limited human intervention. Technology for shining the technology and cyberspace environment. Physically, the data was exchanged when collecting, generating or processing important data for its cyberspace function. The sensors collected consumer safety or privacy-sensitive data. This can affect legal concern [5] In addition, the authors affirmed that the development of software or the configuration control in the IOT sensors could affect the concerns of cybersecurity in that host network.

The manufacturers were delayed by the safety regulations and recently had government interventions only if they are associated with the cybernetic security of IOT [6]. Government agencies have feared the severe industry in the industry by carrying out regulations, and the Government of the United States promoted a safe development adopted by a supplier adopted for future work [7].

The Bluetooth wireless communication industry has grown to a place where technology incorporates the sensor to many devices, including mobile devices, wearables and vehicles. There were many integrations of technology and security updates, including version 4.2 of Bluetooth Low Energy (BLE), including version 4.2 of Bluetooth Low Energy (BLE).

BLE focused on increasing security posture for low power requirements of the channel jump and previous versions, and was a communication protocol for the IoT Communication Protocol [8]. The manufacturer of the IOT device contains BLL using BLE technology and IOT sensors embedded. For paper experiments, the BLE protocol used version 4.2.

The Background of the IoT BLE Experimental Study

The source used by the IOT sensors started with a device-level attack and the attacker abused usability in the code and firmware bugs [9]. The attacks used the IoT sensor through a serious Bluetooth attack. The strategy requires user intervention to disable Bluetooth when not in use. According to [10],IoT middleware sensors act as a bridge between physical and virtual resources that do not have the same control over security. due to low consumption and lack of code [11] Exploitation is due to poor deployment criteria or lack of tight configuration control [12]. Attackers deployed a wide range of issues using a large number of vulnerable sensors [13]. 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 deliver malicious content, wrapper code, or vulnerable sensors.The execution of malicious code allows an attacker to monitor or deploy software on a target IoT sensor [14]. According to [15], Commands and Controls (C2) by which 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 opportunity. to deploy penetration testing tools [16]. Self-organization, not controlled by external sources, is formed by setting up complex sensor networks [17]. If a sensor change occurs, it adapts to the newly defined rules. The attacker has a set of malicious rules that override predefined steps to force spoofing to create a sensor. Fake IoT variables [], .Problem Statement for BLE IoT Sensors A common problem is that IoT sensors are vulnerable to cyberattacks. The specific issue is that IoT sensors have many security concerns due to BLE encryption vulnerability, leading to cybersecurity attacks Ministry of Digital Culture, Media and Sports, 2018) The combination of known Bluetooth vulnerabilities and limited security guidance has proven to be an issue as these vulnerabilities expose IoT sensors to attacks. The network is publicly available. (2018) presented 20 known attack vectors using IoT sensors with BLE communication protocol to exploit vulnerabilities in their implementation. IoT devices are delayed with security controls and lack standard security monitoring (UK.Department of Culture, Media and Digital Sports, 2018).

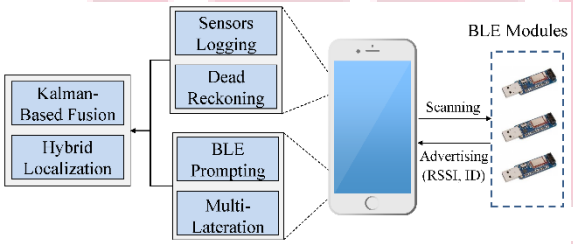

Figure:1 Improved BLE Indoor Localization

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 analyse 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.

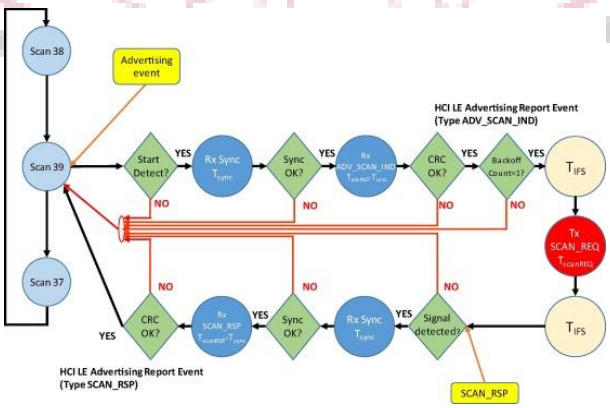

Figure:2 Low-cost test measurement setup for real IoT BLE sensor device

2. 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].

3. RESEARCH METHODOLOGY

The study was a single-subject, multi-facility experimental design using a control group. According to [7], single subject studies require several chronological steps, including observed behavior without intervention, baseline conditions without intervention, and the provision of intervention measures to observe behavior over time. The baseline consists of two sensors where the characteristics of both sets do not have processing variables independent of NIST security checks to assess whether the results produce the same preprocessing baseline. Then, in the intervention phase, the introduction of Bluetooth NIST guidelines and best practices was applied to a new set of sensors and baselines showing the difference between pre-treatment and NIST intervention. Additionally, prior to conducting any experimental or pilot studies, the researcher purchased six sets of Mpression and randomly selected two unpackaged sets for experiments, and the remaining sets were used to replicate the save and conduct experimental research.A pilot study validated the experimental procedure and collection methods listed in the "Nature of Study" section, which used a BLE IoT sensor to perform instrument tests. After the experimental study was completed, the researcher confirmed that the data collection analysis obtained the correct measurements and imported the results into the IBM SPSS v26 database. The pilot study sensor has been decommissioned after use and, unless further calibration is required, it should not be reused. Further calibration occurs by adjusting the experimental procedure and assumptions made when creating the fields in the IBM SPSS database.

During this trial, the aim was to focus on a closed network of laboratories using industry guidelines from the "Nature of Research" section where the test plan, test cases, and The result model is developed for statistical analysis and reporting. In the "Nature of Research" section, the well-known vulnerability classification and Bluetooth testing tools compiled test cases from the "Common Bluetooth Attacks" and "Classification" sections. Bluetooth attacks" [3]. The results provided a data set for analyzing the statistical probability of an attack, the discovery of mitigation techniques, and the existential risk of configured IoT BLE sensors with control measures. NIST security control.

Design Appropriateness

When studying a quantitative research design, a single subject multi-base design is most appropriate for the experiment [15]. According to [7], all subjects were treated equally in repeated measurement experiments. Single-project designs do not require a large population and can apply gradual changes to each reference at a time [15]. Researchers have made changes to the baseline, observed the effect of a change, and made the necessary modifications to assess the effectiveness of NIST controls in BLE security and mitigation measures are in place 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 subjects treated or the effect of the change due to the hole. Compared with the chosen research method, a qualitative case study does not provide the necessary observation on the effects of changing one variable [7]. By comparison, quantitative research tested one hypothesis and one null hypothesis, wherein 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, the selection of a quantitative experiment is the most appropriate for the study.Sampling The experiment uses a single, measurable test design to test defense strategies for IoT sensors using BLE [7] One sensor is used as a control variable and the second sensor as a processing group; there are a lot of steps completed the best design and after testing; a test plan, test cases and results model built a database of statistical analyzes and quantified reports for each type of threat, threat to bluetooth and repeat measurement results . Due to this test case model, the test case generation comes from a list of known attacks of known Bluetooth exploitation vectors [3].Dashboards are checked against CVSS Calculator v3.1, using known risk weights and formulas. The results identified a code review in which developers did not follow a cybersecurity development model [10].

Data Analysis

Creswell recommended that quantitative studies used software which assisted the researcher in compiling statistics. IBM SPSS database software was the suggested tool. IBM SPSS is commonly known to produce statistical data for analysis among researchers. provided tools to help researchers use IBM SPSS for data analysis. Descriptive and comparative statistics of the RM-ANOVA results were the two types of data analysis used to analyze the data collected during the experiment.The analysis used RM-ANOVA for the following research question: Research Question 1 (RQ1). Will the application of NIST, recommended security controls, and best practices mitigate the success of well-known attack vectors on IoT sensors using BLE?RM-ANOVA = repeated measure for the analysis of a variance Dependent variable = existing IoT BLE sensor vulnerabilities Independent variable = BLE NIST security controls SPSS Repeated Measures ANOVA Tutorial (2019) provided a step-by-step process to analyze a within-subject population where two linear, measurable outcome variables exist. The first variable measured the current state of IoT BLE sensor whether or not a vulnerability exists. The second variable measured the IoT BLE sensor with the NIST control applied to test the Null Hypothesis, H0. Applying NIST security controls and best practices for securing IoT sensors using the BLE device potentially mitigated well-known Bluetooth attacks.Comparatively, if there was no change, what mitigations could lower the probability of attack to BLE IoT sensors? The last variable compared the results for a change in variable testing the Hypothesis, H1. Applying NIST security controls and best practices secured IoT sensors using the BLE device did not mitigate well-known Bluetooth attacks.

4. RESULTS

This Research focuses on the results obtained from quantitative experiments using RMANOVA and the defined experimental procedure. A pilot study validated the collection method of the SPSS v26 database, the experimental variables and the CVSS v3.1 baseline score used to present the results. results. Next, two previously measured sensors with the same results and adjusted CVSS 3.1 scores presented environmental and condition considerations.

The researcher evaluated the best data and adjusted the Wireshark application's network traffic display filter and then implemented security controls. The Wireshark app is a passive monitoring tool and works in parallel with traffic and has no effect on the test. Network Filters allow researchers to collect data directly related to NIST Security's Recommendations and Controls Checklist. The security checks test took place from January 31, 2020 to February 9, 2020. Repeated results of the NIST measurement require review before proceeding with the risk mitigation assessment.

Risk mitigation assessment requires a technical and theoretical review of risk mitigation strategies in the literature to limit exposure to IoT BLE sensors. Information gathered from conference proceedings over the past 24 months was used to devise effective countermeasures for IoT BLE sensors. Finally, the graphs developed a visual representation of the test's results, and the researcher provided updates to the NIST guidance on Bluetooth security to mitigate attacks. BLE IoT testing devices and procedures The test method follows a step-by-step process to ensure that every part of the test is captured. After the pre-test is completed, the results are calculated using the CVSS calculator and entered in Table 7. The calculated results are used as the measurement results of the pre-test. Next, the researcher applies NIST security controls and best practices. The NIST Bluetooth Guide and the Mobile Threat Directory were used as references to develop the checklist. Once the security checks are in place, a second test of each configuration is performed and recorded in Table 7 for the X and Y sensors. The test results are encrypted and entered into the SPSS database. Then, code analysis of each configuration and firmware completed the final mitigation analysis.

Steps to complete the test:

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

Step 2. All profile configurations have been applied to both IoT BLE sensors.

Step 3. Each Bluetooth threat is evaluated for IoT BLE X and Y sensor. Step 4. Completed the BLE IoT sensor test and stopped all captures.

Step 5. Repeat steps 14 for each Bluetooth threat.

Step 6. Enter the results and end the experiment

Equipment Tools Tools and materials needed

During the test, the equipment needed to produce the results included monitoring software loaded on the Apple iPad and Bluetooth USB keys for collect the results. Requires IoT BLE test kit using smartphone, Android app, software compiled from Mpression website for each personality, firmware for IoT BLE sensor, and power from USB source. The Bluetooth tools in Table 6 were loaded into the Kali Linux distribution and used throughout the test.

Empirical test conditions.According to [16],CVSS calculation is based on quantitative and qualitative factors to give severity and risk via CVSS score. The CVSS score itself does not determine the specific environmental conditions or the probability of success of the operational instruments [16]; The base score does not change with the environment or the probability of success; therefore, each threat category was presented with a CVSS 3.1 baseline score in Table 4 [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 methodology of remote attacker. The researcher restricted authentication and key pairing during testing with the BLE IoT sensor. Three factors observed throughout the experiment, 1) no limits to broadcast range, 2) encryption was not configurable, and 3) the IoT BLE sensor discoverability was not turned off.

Mapping Threat to CVSS Calculated Score

Category of Threat	CVSS Base Score	CVSS Calculator
Active Reconnaissanceand Eavesdropping	8.2	AV:N, AC:L, PR:N, UI:N, S:U,C:H, I:L, A:N
Bluetooth Device AddressSpoofing	7.6	AV:A, AC:L, PR:N, UI:N, S:U,C:H, I:L, A:L
Man in the Middle attacks	7.6	AV:A, AC:H, PR:L, UI:R, S:C, C:H,I:H, A:H
Information Disclosure	7.3	AV:A, AC:H, PR:H, UI:R, S:C,C:H, I:H, A:H
Denial of Service	9.6	AV:A, AC:L, PR:N, UI:N, S:C, C:L,I:H, A:H
Command Injection	8.3	AV:A, AC:H, PR:N, UI:N, S:C,C:H, I:H, A:H
Fuzzing	8.3	AV:N, AC:H, PR:N, UI:R, S:C, C:H, I:H, A:H

5. CONCLUSION

The comprehensive analysis of existing vulnerabilities in IoT sensor networks has underscored the critical need for fortified security measures. The proposed solution incorporates state-of-the-art encryption algorithms, secure key exchange mechanisms, and efficient authentication protocols within the BLE framework. This approach not only ensures the confidentiality and integrity of data but also minimizes the energy consumption of sensor nodes, a crucial aspect for the sustainable operation of IoT devices. Furthermore, the integration of anomaly detection techniques contributes to real-time threat mitigation, enhancing the overall resilience of the IoT sensor network. The experimental evaluations have demonstrated the feasibility and efficacy of the proposed solution, providing evidence of improved security without compromising the energy efficiency essential for IoT devices. As the IoT landscape continues to evolve, the significance of securing sensor nodes becomes increasingly pivotal. The proposed BLE-based security enhancements offer a promising avenue for achieving a harmonious balance between energy efficiency and robust protection. Future research endeavors could delve deeper into scalability issues, interoperability challenges, and evolving threat landscapes to further refine and adapt the proposed framework for diverse IoT deployment scenarios.In essence, this research contributes to the advancement of secure and energy-efficient solutions for IoT sensor networks, paving the way for a safer and more resilient IoT ecosystem. The integration of BLE technology emerges as a noteworthy step towards fortifying the foundation of IoT, ensuring its continued growth and innovation in a secure digital landscape.

References

[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