Assessing Vulnerabilities in Bluetooth Low Energy (BLE) Wireless Network based IoT Systems

Salwa Javeed Parkar[1], Ninad Avinash Patil[2]

[1,2] Final year Student, Dept. of M.C.A, V.E.S. Institute of Technology, India.

Abstract - *With the advent of the internet of things (IoT), big data analytic and cloud computing services had also got tremendous breadth in the evaluation of more secure computing environments, such as better resource management and vulnerability analysis. Since its inception in 2013, Bluetooth Low Energy (BLE) has become the standard for short-distance wireless communication in many consumer devices, as well as special-purpose devices. Bluetooth Low Energy (BLE) has become a remarkable success. Due to its unique properties of low power requirements and its ubiquitous availability in practically every smartphone, it outnumbered classic Bluetooth BR/EDR in most areas. To accurately assess the vulnerability of Bluetooth low energy (BLE) wireless network enabled IoT systems, we proposed a novel approach to extend the calculation formula for Authentication, which is one of the variables used in the conventional base score equations of the National Infrastructure Advisory Council's Common Vulnerability Scoring System (CVSS) v2. We demonstrated the weakness of the current CVSS v2 base score equations and how to overcome the weakness using an example BLE wireless network-based shopping cart IoT system.*

Key Words: Bluetooth, Bluetooth low energy, Internet of things, Vulnerability analysis, Wireless Network.

1. INTRODUCTION

The Internet of Things (IoT) refers to the inter-connectivity of devices and is enabled by the technologies such as RFID, Bluetooth, NFC, Wi-Fi, and Mobile Network. It is a Modern paradigm, rapidly growing around wireless communications. The capacity offered by the IoT make possible of developing large number of IOT applications such as Smart home, Smart city, smart health etc. The communication technology used in IoT differs from application to application. The Internet of Things (IoT) and big data analytics are merging to generate the next wave of the technological revolution [1]. IoT systems will create a new spectrum of data on the internet and influence the whole world of big data by connecting many devices equipped with various types of sensors to the internet via a wireless network. Bluetooth is a set of short-range wireless protocols operating in the 2.4 GHz industrial, scientific and medical (ISM) band. The Bluetooth specification is split into two major parts. One part is called Bluetooth BR/EDR, also known as Bluetooth classic, the other one is called Bluetooth Low Energy (BLE) which was added in version 4.0. Both are nearly completely independent protocols. As its name suggests, BLE is intended for low power devices, or to put in another way, devices with limited power supply (e.g., battery powered) as well as limited computational and memory capabilities. Since these devices should last as long as possible without replacing the battery, special communication protocols, like BLE are necessary. Bluetooth low energy (BLE) [2] wireless network technology is quickly becoming the low-power wireless solution of choice in a wide range of IoT applications [3, 4]. As an example, consider a real-world IoT system based on a spontaneous wireless hyper-connected network [5] as represented by the BLE equipped shopping cart application in Fig. 1. A customer's path through the store, as well as how consumer data is gathered and handled are shown in Fig. 2. Retailers aim to detect the pathways of shopping carts throughout stores and the things customers wish to buy by collecting and analysing consumer behaviour in real time. Many retail chain operators are testing Bluetooth beacons in their department shops to track the movements of shopping trolleys. This Bluetooth Low Energy wireless network technology is intended and expected to allow for the anonymous tracking of customers as they move about businesses by recognizing the shopping carts that customers are using. Customers will also be able to pay for their products via the BLE wireless network rather than going to the cashier counters. However, without proper network security in place to ensure that each customer has limited access to very specific information in his/her own shopping information account, such a system may become a vulnerable entry point from which attackers can access the store's entire information management system.

Fig 1: Example of BLE wireless network enabled shopping cart.

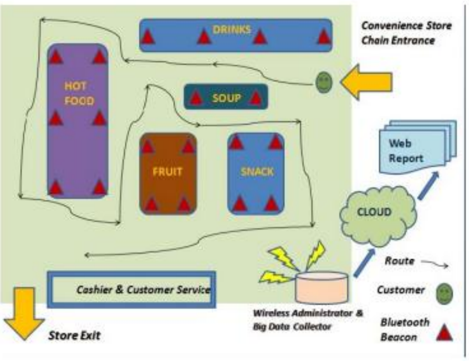

DRINKS
Convenience Store Chain Entrance
HOT FOOD
SOUP
FRUIT
SNACK
Web Report
CLOUD
Route
Customer
Bluetooth Beacon
Cashier & Customer Service
Wireless Administrator & Big Data Collector
Store Exit

Fig 2: Example of route movement and customer behaviour capturing by using BLE wireless network enabled shopping cart.

Being wireless, a BLE interface is particularly exposed to potential attacks. An attacker does not need physical access to the device and has a low risk of being caught in action. This makes security of BLE interfaces a major concern. Potential attack goals include sniffing, denial-of-service (DoS), spoofing, injection of messages, partial or full takeover of a connection, tracking, and localization.

BLE wireless networks, have inherited vulnerabilities [6] that are common to all wireless network technologies. Threats to BLE wireless networks include:

A) Blueprinting: Attackers utilize the foot printing process to collect information such as IP addresses, network protocols, domain names, Access Control Lists, and so on.

B) Blue sniffing: Attackers take unauthorized data like SMS messages, calendar info, images, phone book contacts, and chats from the Bluetooth-enabled device through a Bluetooth connection.

C) Bluebugging: Attackers use an application like Bloover, a proof-of-concept bugging tool, to seize control of the target's phone.

D) Bluejacking: Attackers send text messages requesting contact list insertion, such as business cards; the process permits attackers to continue sending more messages.

E) Bluesmack: Denial of Service attacks are launched against Bluetooth devices by attackers. According to several recent polls [24], due to the vulnerabilities of wireless networks utilized in IoT, the security framework and implementation in IoT will need to alter.

Customer authentication is a vital component of a security architecture. BLE wireless networks often employ a five-parameter authentication system, which employs the five parameters listed below:

A) hwndParent: A window that serves as the Authentication wizard's parent.

B) hRadio: A valid local radio handle used for authentication on all local radios, with the function call succeeding if any radio succeeds.

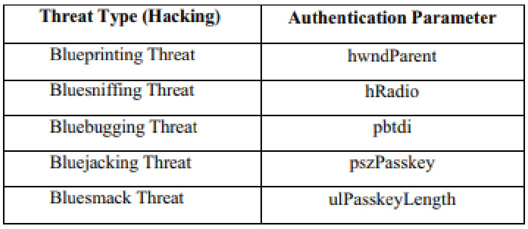
C) pbtdi: A BLUETOOTH DEVICE INFO structure containing the record of the Bluetooth device to be authenticated.

D) pszPasskey: A personal identification number used to authenticate devices.

E) ulPasskeyLength: The length of pszPasskey in characters.

In conclusion, numerous considerations must be addressed while creating a security architecture for a BLE wireless network-based IoT system.

Table 1 includes all the criteria addressed previously.



Threat Type (Hacking)	Authentication Parameter
Blueprinting Threat	hwndParent
Bluesniffing Threat	hRadio
Bluebugging Threat	pbtdi
Bluejacking Threat	pszPasskey
Bluesmack Threat	ulPasskeyLength

Table 1: Security Factors associated with BLE wireless networks

One of the most significant jobs in creating a BLE wireless network-based IoT system is assessing the system's vulnerabilities. The most well-known technique in this regard is to use the National Infrastructure Advisory Council's (NIAC) suggested Common Vulnerability Scoring System (CVSS) [31-33]. CVSS has several versions. CVSS v2 takes the method of assigning a base score (BS) for each vulnerability based on two sets of only six base metrics. All of these fundamental measures remain stable over time and across diverse user contexts. To represent more precise time and place characteristics, BS can be changed using temporal and environmental ratings. Temporal and environmental ratings are not connected in vulnerability databases; hence fidelity is lost. These six-base metrics – Access Complexity, Authentication, Access Vector, Confidentiality Impact, Integrity Impact, and Availability Impact – will be transferred to fixed numerical values and employed in the base score calculations to determine BS.

2. BLUETOOTH LOW ENERGY PROTOCOL AND SECURITY

A. Bluetooth Low Energy Protocol Stack Architecture

The BLE protocol stack architecture is composed of three blocks (as shown in Figure 3 a):

A) Application block: The application block implements software based on the manufacturer's need, which may vary from device to device.

B) Host block: This block is responsible for the protocols and profiles implemented in BLE devices and defines the packet semantics.

C) Controller block: This block features much of the device's hardware, including the radio interface and its physical characteristics. This block is responsible for data broadcasts over the wireless media.

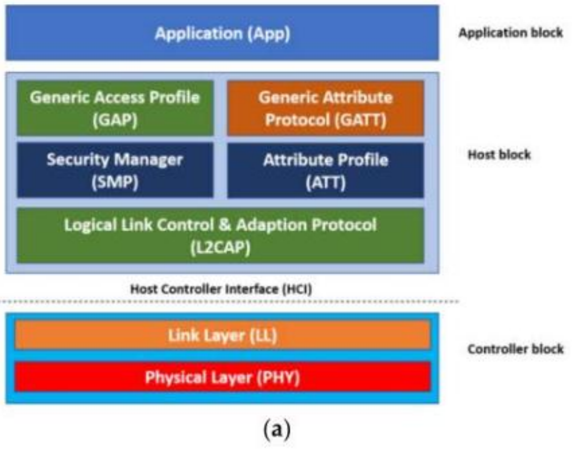


Fig 3 (a): Bluetooth Low Energy (BLE) protocol stack

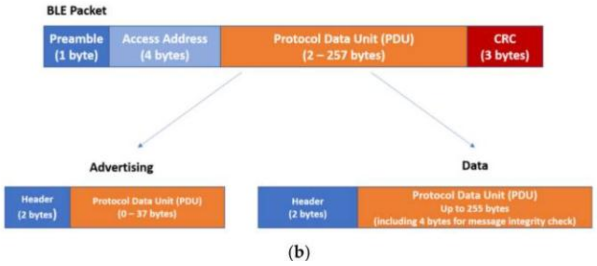

BLE Packet
Preamble (1 byte)
Access Address (4 bytes)
Protocol Data Unit (PDU) (2 – 257 bytes)
CRC (3 bytes)
Advertising
Data
Header (2 bytes)
Protocol Data Unit (PDU) (0 – 37 bytes)
Header (2 bytes)
Protocol Data Unit (PDU) Up to 255 bytes (including 4 bytes for message integrity check)
(b)

Fig 3 (b): Bluetooth Low Energy (BLE) protocol packet format

The BLE specification defines one type of packet with two different payloads to be transmitted by BLE devices. These payloads are advertising packets and data packets (Figure 1b). Advertising packets are used when a device is either in discovery mode or is broadcasting. On the other hand, data packets are only used when a device has established a connection with another device. Both packets can potentially be used to transmit application data. However, data packets are allotted more payload space than advertising packets and, as a result, are used when more data needs to be transmitted between devices.

Bluetooth LE utilizes two methods to transmit data: broadcasting and connections. Broadcasting is used when a device chooses not to establish or is incapable of establishing a connection to another device. During broadcasting, a BLE device will intermittently send out advertising packets containing the required data about how to connect with the device. The data transmitted in these advertising packets are not encrypted, thus any kind of application data can be viewed by any device, making privacy non-existent. Contrarily, connections are used when two or more devices need to exchange data. Connections begin with advertising packets to identify which device to connect. Once the devices have identified each other, they begin exchanging data packets.

Connections serve the needs of private communications as they can implement BLE security features.

B. Bluetooth Low Energy Security

While security options are part of the BLE standard, the Bluetooth Special Interest Group (SIG) recommends but does not require security options to be implemented to allow flexibility for manufacturers. The manufacturer then decides whether security measures should be implemented or not. Within the host block, BLE devices can implement many security features, including association models, key generation, encryption, and random addressing. All these features can be used to ensure the security of the data transmitted during a connection to avoid threats, such as passive eavesdropping and MAC address fingerprinting.

Pairing is the most important security procedure in Bluetooth. Pairing is when authentication and key establishment take place between the two devices that connect. BLE defines two main pairing modes: Legacy Pairing and Secure Connections. BLE Legacy Pairing uses Secure Simple Pairing (SSP) of Bluetooth 2.1 (BR/EDR) but without the FIPS-approved Elliptic Curve Diffie-Hellman (ECDH) key exchange and HMAC-SHA-256 algorithms for pairing and message integrity [6]. Secure Connections (SC), introduced in Bluetooth 4.2, upgrades BLE Legacy Pairing to use ECDH with longer keys and provides data integrity. In this study, we focus on LE Legacy Pairing, which is the mode specified for Bluetooth versions 4.0 and 4.1.

LE Legacy Pairing uses a custom key exchange protocol, where the devices exchange a Temporary Key (TK) and use it to create a Short-Term Key (STK) to be used as the encryption key for the communication.

3. PROBLEM STATEMENT AND HYPOTHESIS

A. Problem Statement

Due to CVSS v2's inability to add extra parameters relevant to the unique authentication mechanism of such a system in the computation of the base scores, traditional CVSS v2 base score formulae cannot effectively assess the vulnerability of a BLE wireless network-based IoT system.

B. Hypothesis

We will be able to apply CVSS v2 to accurately assess the vulnerability of a BLE wireless network based IoT system if we can find a way to extend the base score equations of CVSS v2 so that calculation of base scores include extra factors relevant to the specific authentication mechanism of a BLE wireless network based IoT system.

4. METHODOLOGY

A. Identify a compatible extension

Let's look at one of the CVSS v2 basic equations that focuses on vulnerability exploitability to see if we can include details of BLE wireless networks into it:

$$Exploitability=20(AccessVector)(AccessComplexity)(Authentication)$$

Where Access Vector is a variable indicating how a vulnerability might be exploited. It is frequently given to 0.646 for a Bluetooth network because "the attacker must have access to the susceptible system's broadcast or collision domain [38]." Access Complexity is a variable that defines the ease or difficulty with which the detected vulnerability may be exploited. Because of the open nature of a Bluetooth network, it is generally easy to gain access to the vulnerability, hence the Access Complexity score is frequently more than 0.7 [38]. Authentication is a variable that describes how many times an attacker needs authenticate to a target in order to exploit it. Authentication, according to earlier work [38], "does not involve (for example) authentication to a network in order to acquire access." This value should only be set to Single or Multiple for locally exploitable vulnerabilities if additional authentication is necessary after first access." Authentication typically receives a score of 0.45 for numerous necessary authentications, 0.56 for a single required authentication, and 0.704 for no authentication. This can also be expressed as:

$$Authentication = f(n) = \begin{cases} 0.45, & n \geq 2 \\ 0.56, & n = 1 \\ 0.704, & n = 0 \end{cases} \qquad (1)$$

Where n is an integer.

Obviously, authentication becomes an ideal target for us to make some adjustments so that the characteristics of BLE wireless networks are represented in the computation of the vulnerability's base score using the CVSS v2 base equations.

Authentication will be considered as a function of the number of authentications necessary, denoted as an integer n, and authentication risk factor, denoted as r and defined as the likelihood that an authentication technique employed by a BLE wireless network fails due to assault, where 0 r 1. That is to say:

$Authentication = f(n, r)$, and

$$f(n,r) = \begin{cases} \frac{r}{n} + f(n), & if\ n \geq 1, 1 \geq r \geq 0 \\ f(n), & if\ n = 0, 1 \geq r \geq 0 \end{cases} \qquad (2)$$

Where n is an integer and f(n) is defined by (1).

It is obvious that f(n, r) defined in (2) has the convergence property, which means that when r = 0, f(n, 0) converges back to f(n) defined in (1). (1). That is to say:

$$Authentication = f(n, 0) = f(n) \qquad (3)$$

That is, we may assert that we have discovered a natural extension of Authentication that is consistent with its original meaning.

B. Application of the extension

To show (2)'s ability to incorporate the peculiarities of a BLE wireless network into the base equation of CVSS v2, we will utilize the Bayesian Theorem on an example involving two types of events mentioned in Table 1. The first event will be defined as F1 when the BLE wireless network is attacked by at least one of the thread types mentioned in the first column of Table 1. We also define the second event as F2, which occurs when one of the five authentication parameters is compromised. If we suppose that P(F1) is 0.2 and P(F2) is 0.3, then P(F2|F1) is 0.15. (Which denotes the probability that during the attack, at least one of five authentication parameters is hacked). Now we will define r = P(F1|F2), which represents the probability of the BLE wireless network being attacked when one of the five authentication parameters is compromised. Based on the Bayesian Rule, we can simply determine:

$$r = P(F1|F2) = [P(F2|F1)P(F1)]/P(F2) = 0.15x0.2/0.3 = 1 \quad (4)$$

That is, the risk rate in this situation is extremely high.

Now, plugging the result of (4) into (2), we get:

$$f(n,1) = \begin{cases} \frac{1}{n} + f(n), & if\ n \geq 1, 1 \geq r \geq 0 \\ f(n), & if\ n = 0, 1 \geq r \geq 0 \end{cases} \qquad (5)$$

Let's assume n can only be 1, 2, and 3. Then we have

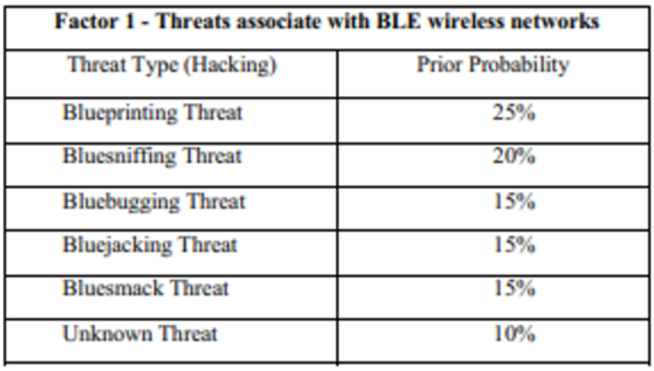
$$Authentication = f(n) = \begin{cases} 0.78, & n = 3 \\ 0.95, & n = 2 \\ 1.56, & n = 1 \end{cases} \qquad (6)$$

According to (6), the score value for the Authentication variable drops as the number of additional authentications necessary after first access grows. This corresponds to real-world semantics: the more authentications necessary, the less susceptible the system.

5. MODEL EXPERIMENT AND RESULT

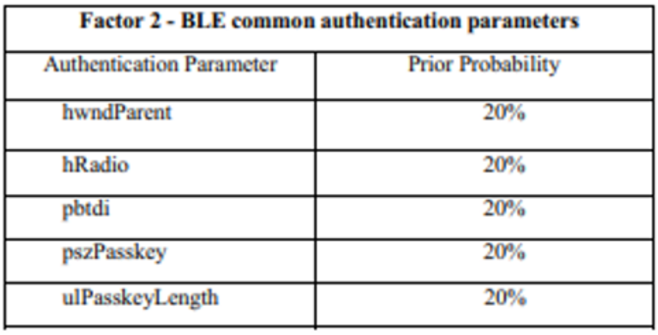
We utilize the BLE wireless network equipped shopping cart in Fig. 1 to demonstrate a vulnerability in which all of the variables used in the CVSS v2 base equations have been substituted with particular data values used in real-world scenarios. The authentication of the BLE wireless network requires that any of the five parameters have the right data value. In summary, a potential hacker with a proper data value for only one of five criteria has a good chance of being authorized. This is an extremely ineffective authentication technique. In order to accurately assess the vulnerability of a BLE enabled shopping cart system, the influence of these unique authentication features must be included in the CVSS v2 base score formulae. As a result, we will use our modification in this example to demonstrate the shortcomings of the standard CVSS v2 base score equations with respect to such a system, as well as how those shortcomings may be addressed and compensated for by our addition. We developed the trials in the context of a BLE-enabled shopping cart application. We modelled attacker behavior by employing popular tactics used by attackers to carry out various sorts of Bluetooth assaults.

A BLE wireless network contains two customers' wireless nodes (one customer's BLE equipped shopping cart and one BLE beacon in the retail store) and one hacker's probable unlawful entry node via which the hacker is attempting to access the wireless network. Based on this sample BLE wireless network, we then analyse two elements. In this example, Factor 1 is about threat categories. Blueprinting, Blue sniffing, Bluebugging, Bluejacking, and blue smack are all known threats linked with the BLE wireless network. In addition, we have included an unknown danger in this example. Based on existing facts, we have given a prior probability to each sort of threat. In this situation, Factor 2 refers to the existing standard BLE five authentication parameters-based authentication approach. Again, we provide a weight of 20% to each of the five separate authentication parameters as the prior probability. We created two tables, Tables 2 and 3, containing the prior probability values in both components, which will be utilized in the base score computation when we assess the Authentication variable in CVSS v2 base score equations using the addition we suggested. We've assumed that an IoT service is running on the Bluetooth Low Energy wireless network. There are no firewalls involved in this typical situation. We can assume that the BLE wireless network includes a vulnerability that allows remote attackers to circumvent authentication and get access. We next utilize the traditional CVSS v2 base score formulae to assign the data values indicated in Table 4 to various variables in the CVSS v2 equations, and the resultant base score is 2.48.



Factor 1 - Threats associate with BLE wireless networks	
Threat Type (Hacking)	Prior Probability
Blueprinting Threat	25%
Bluesniffing Threat	20%
Bluebugging Threat	15%
Bluejacking Threat	15%
Bluesmack Threat	15%
Unknown Threat	10%

Table 2: BLE common threat types and the attacking probabilities



Factor 2 - BLE common authentication parameters	
Authentication Parameter	Prior Probability
hwndParent	20%
hRadio	20%
pbtdi	20%
pszPasskey	20%
ulPasskeyLength	20%

Table 3: BLE authentication parameters and the hacking probabilities

Bluetooth Beacon
Hackers
A Wireless Bluetooth BLE Network At Risk

Fig 4: A BLE wireless network exposed to a hacking scenario

CVSS v2 Metric	Variables and Value	Assumption

Exploitability	AccessVector = 1.0
	AccessComplexity =0.75
	Authentication = 0.56
		Wireless Network, Access Complexity is High, and Single Authentication is required

Impact	ConfidentialityImpact =0.66
	IntergrityImpact =0.66
	Availabilit Impact =0.66
		Complete
		Complete
		Complete

Table 4: Calculate using CVSS Base Metrics for BLE vulnerabilities

The detailed calculation steps are provided below:

$$BS \text{ (Base Score)} = round\ to\ 1\ decimal((0.6\ Impact + 0.4\ Exploitability - 1.5)\ f(Impact)) \tag{7}$$

$$Impact = 10.41\ (1 - (1 - [ConfImpact{=}0.660])\ (1 - [IntegImpact{=}0.660])\ (1 - [AvailImpact{=}0.660])) = 10.41\ (1 - (1 - 0.660)\ (1 - 0.660)\ (1 - 0.660)\ ) = 0.409 \tag{8}$$

$$Exploitability = 20\ ([AccessVector = 1.0])\ \ ([AccessComplexity = 0.75])\ \ ([Authentication = 0.56]) = 8.4 \tag{9}$$

$$Impact \text{ is not 0 so } f(Impact) = 1.176 \tag{10}$$

$$\text{So, } BS \text{ (Base Score)} = round\ to\ 1\ decimal(\ (0.6\ \ [Impact = 1.176] + 0.4\ \ [Exploitability{=}2.45] - 1.5)\ [f(Impact) = 1.176]\ ) = (\ (0.6 \text{ x } 0.409) + (0.4 \text{ x } 8.4) - 1.5\ ) \text{x}1.176 = (0.2454 + 4.5 - 1.5) \text{ x}1.176 = 2.48 \tag{11}$$

Because the base score is merely 2.48, it is possible to conclude that this sample BLE wireless network has very little vulnerability. However, as we shall see in the subsequent further examination of the sample BLE wireless network, this may be a false outcome.

Let's have a look at how the expanded Authentication formula given in (2) is used in this example BLE wireless network.

We shall assume the following two events:

- **Event H:** Any of the threats mentioned in the first column of Table 2 attacks the BLE wireless network.
- **Event D:** One of the five authentication parameters listed in Table 3 is compromised.

In this case, we will additionally apply the prior probabilities shown in Tables 2 and 3.

We will assess one conceivable scenario: the danger of a BLE wireless network being attacked if one of the five authentication parameters is successfully hijacked.

That is, we must determine the risk rate r = P(H|D). We have developed a model based on the Bayesian Theorem.

$$P(H|D) = [P(D|H)P(H)]/[P(D)] \tag{12}$$

In this example, we define P(H) as the prior probability for H, and we get

P(H) = (0.25 + 0.20 + 0.15 + 0.15 + 0.15 + 0.10) / 6 = 0.1667

by taking the average of the potential outcomes in Table 2.

P(D) is also defined as the prior probability for D; by averaging the alternative outcomes in Table 3, we get, P(D) = (0.2 + 0.2+0.2+0.2+0,2)/5 = 0.2. Finally, we define P(D|H) as the probability that a prediction for D provided by "H was Succeed" is achievable, and we assume that P(D|H) = 0.95.

Therefore, we have,

$$r{=}P(H|D) = 0.95\text{x}0.1667\ /\ 0.2 = 0.792 \tag{13}$$

By using (2), we have

$$f(n, 0.792) = \begin{cases} \dfrac{0.792}{n} + f(n), & if\ n\ \geq 1, 1 \geq r\ \geq 0 \\ f(n), & if\ n = 0, 1 \geq r\ \geq 0 \end{cases} \tag{14}$$

Because we assumed that just one authentication is necessary, n = 1, and f(n) is defined by (1), we will obtain

$$\text{Authentication} = f(1, 0.792) = 0.792 + 0.56 = 1.352 \tag{15}$$

If we use result of (15) to recalculate (9), we will have

$$Exploitability = 20\ ([AccessVector = 1.0])\ \ ([AccessComplexity = 0.75])\ \ ([Authentication = 1.352]) = 20.28 \tag{16}$$

Using the result of (16) to recalculate (11), we will have,

$$BS \text{ (Base Score)} = round\ to\ 1\ decimal(\ (0.6\ \ [Impact = 1.176] + 0.4\ \ [Exploitability{=}2.45] - 1.5)\ [f(Impact) = 1.176]\ ) = (\ (0.6 \text{ x } 0.409) + (0.4 \text{ x } 20.28) - 1.5\ ) \text{x}1.176 = (0.2454 + 8.112 - 1.5) \text{ x}1.176 = 8.064 \tag{17}$$

By comparing the base scores in (11) and (17), we can observe a significant difference in whether or not the characteristics of the BLE wireless network have been incorporated in the CVSS v2 base score formulae. The higher the score in (17), the more important it is to consider the practical situation of the BLE wireless network, because it is a wireless network with high vulnerability due to its specific five parameters-based authentication mechanism in an open-air physical environment, and a hacker can attack five targets at the same time to achieve the same goal – compromising the authentication of the targeted BLE wireless network. We may evaluate the success of any security enhancement methods by expanding the CVSS v2 base score formulae. For example, in the above case, increasing the needed number of authentications from 1 to 2 reduces the basic score from 8.064 to 4.493. Similarly, if we suppose n= 3, the base score falls even more to 3.562. In addition, when n=4, the basic score becomes 3.096. This trend suggests that requiring two or three authentications for a BLE wireless network will significantly reduce overall system vulnerability. However, it also implies that there is a tipping point beyond which just raising the total number of needed authentications on a BLE wireless network would not be particularly useful in further decreasing the overall system's susceptibility. We must consider additional system characteristics in order to achieve more success in improving the system's susceptibility. That is, with our addition, we can turn CVSS v2 into a useful tool for helping us build a more secure BLE wireless network-based IoT system.

6. CONCLUSION

We offered a logical expansion to one of the variables utilized in CVSS v2 base score calculations in this study. We also highlighted the shortcomings of the present CVSS v2 base score calculations, as well as the advantages of this addition, using an example BLE wireless network-based shopping cart IoT system. That is to say, our hypothesis has been approved. Future work will concentrate on two areas: identifying opportunities to expand more factors in CVSS v2 and adding new temporal and environmental scores. In addition, we will undertake further tests with more realistic real-time circumstances.

REFERENCES

[1] Holler, J., Tsiatsis, V., Mulligan, C., Avesand, S., Karnouskos, S., & Boyle, D. (2014). From Machine-to-machine to the Internet of Things: Introduction to a New Age of Intelligence. Academic Press.

[2] Granjal, J., Monteiro, E., & Silva, J. S. (2015). Security in the integration of low-power Wireless Sensor Networks with the Internet: A survey. Ad Hoc Networks, 24, 264-287.

[3] Gomez, C., Oller, J., & Paradells, J. (2012). Overview and evaluation of bluetooth low energy: An emerging low-power wireless technology. Sensors, 12(9), 11734-11753.

[4] Nishide, R., Yamamoto, S., & Takada, H. (2015). Position Estimation for People Waiting in Line Using Bluetooth Communication. MOBILITY 2015, 16.

[5] Choi, A. J. (2014, November). Internet of Things: Evolution towards a hyper-connected society. In Solid-State Circuits Conference (A-SSCC), 2014 IEEE Asian (pp. 5-8). IEEE.

[6] Sandhya, S., & Devi, K. S. (2012, February). Analysis of Bluetooth threats and v4. 0 security features. In Computing, Communication and Applications (ICCCA), 2012 International Conference on (pp. 1-4). IEEE.

[7] Lee, I., & Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. Business Horizons.

[8] Hou, J. L., & Yeh, K. H. (2015). Novel Authentication Schemes for IoT Based Healthcare Systems. International Journal of Distributed Sensor Networks, 501, 183659.

[9] Wan, J., Chen, M., & Leung, V. C. (2014). M2M CoMMuniCations in the Cyber--PhysiCal World. Machine-to-Machine Communications: Architectures, Technology, Standards, and Applications, 1.

[10] Rawat, P., Singh, K. D., Chaouchi, H., & Bonnin, J. M. (2014). Wireless sensor networks: a survey on recent developments and potential synergies. The Journal of Supercomputing, 68(1), 1-48.

[11] Sadeghi, A. R., Wachsmann, C., & Waidner, M. (2015, June). Security and privacy challenges in industrial internet of things. In Proceedings of the 52nd Annual Design Automation Conference (p. 54). ACM.

[12] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: a survey on enabling technologies, protocols and applications.

[13] Suresh, P., Daniel, J. V., Parthasarathy, V., & Aswathy, R. H. (2014, November). A state of the art review on the Internet of Things (IoT) history, technology and fields of deployment. In Science Engineering and Management Research (ICSEMR), 2014 International Conference on (pp. 1-8). IEEE. [14] Petersen, H., Baccelli, E., Wählisch, M., Schmidt, T. C., & Schiller, J. (2014). The Role of the Internet of Things in Network Resilience. arXiv preprint arXiv:1406.6614.

[14] Vermesan, O., & Friess, P. (Eds.). (2014). Internet of Things-From Research and Innovation to Market Deployment (pp. 74-75). River Publishers.

[15] Petrov, V., Edelev, S., Komar, M., & Koucheryavy, Y. (2014, March). Towards the era of wireless keys: How the IoT can change authentication paradigm. In Internet of Things (WF-IoT), 2014 IEEE World Forum on (pp. 51-56). IEEE.

[16] Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. Computer Networks, 76, 146-164.

[17] Chan, P., Cohen, M., & Qu, Y. (2014, April). Effective Method to Detect and Encapsulate Run Time Vulnerabilities on Cellular Networks. National Security Innovation Competition (NSIC).

[18] Bevec, A., Bothner, P., Chan, P., Chike, I. N., Masciulli, M., Markowski, M., & Still, G. W. (2012, October). Modeling mobile network connectivity in the presence of jamming. In MILITARY COMMUNICATIONS CONFERENCE, 2012-MILCOM 2012 (pp. 1-4). IEEE.

[19] Chan, P., Nowicki, D., Man, H., & Mansouri, M. (2012). System Engineering Approach in Tactical Wireless RF Network Analysis. INTECH Open Access Publisher.