2016 IEEE 2nd International Conference on Big Data Security on Cloud, IEEE International Conference on High Performance and Smart Computing, IEEE International Conference on Intelligent Data and Security

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

Yanzhen Qu
Colorado Technical University
Colorado Springs, CO 80907, USA
yqu@coloradotech.edu

Philip Chan
Colorado Technical University
Colorado Springs, CO 80907, USA
Philip.chan@faculty.umuc.edu

Abstract— With the materialization of the internet of things (IoT), big data analytic and cloud computing services give rise to extra breadth in the assessment of more secure computing environments, better resource management and vulnerability analysis. In order to accurately assess the vulnerability of Bluetooth low energy (BLE) wireless network enabled IoT systems, we have proposed a novel approach to extend the calculation formula for Authentication which is one of variables used in the conventional base score equations of the Common Vulnerability Scoring System (CVSS) v2 proposed by the National Infrastructure Advisory Council. Through an example BLE wireless network based shopping cart IoT system we have demonstrated the weakness of the current CVSS v2 base score equations and how to overcome the weakness through our extension.

Keywords— internet of things, big data analytics, Bluetooth low energy wireless network, vulnerability analysis

I. INTRODUCTION

The Internet of Things (IoT) and big data analytics are coming together [1] to form the next wave of the technological revolution. By connecting many devices that have been equipped with various types of sensors to the internet through a wireless network, IoT systems will produce a new spectrum of data on the internet and impact the entire world of big data. Bluetooth low energy (BLE) [2] wireless network technology is now emerging as the low-power wireless technology of choice in many IoT applications [3, 4]. As a specific example, let's look into a possible real world IoT system using a spontaneous wireless hyper-connected network [5] as illustrated by the BLE enabled shopping cart application shown in Fig. 1. The route trace of a customer in the store and how the customer data is collected and processed are shown in Fig. 2.

Retailers want to identify the routes of shopping carts around stores and the products customers are interested in purchasing by providing real time data collection and analysis of consumer behavior. Many retail chain operators are testing Bluetooth beacons to track the movements of shopping carts in their department stores. This BLE wireless network technology is designed and anticipated to permit the anonymous tracking of customers as they move around stores by identifying the shopping carts that customers are using. Additionally, customers will be allowed to pay for their purchases through the BLE wireless network without having to go to the cashier counters. However, without proper network security in place to ensure that every customer can only have restricted 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 a BLE wireless network enabled shopping cart

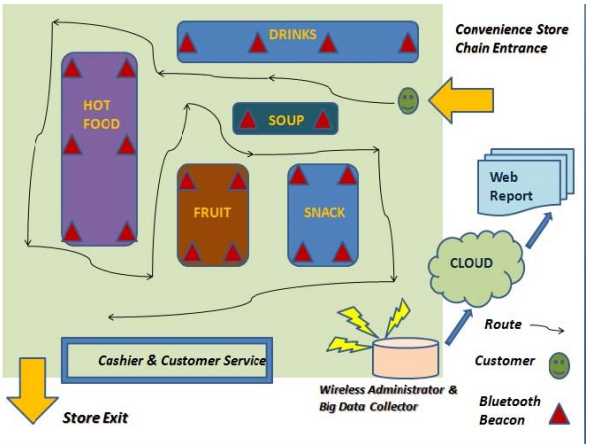

Fig. 2. Example of route movement and customer behaviour capturing by using BLE wireless network enabled shopping cart

However, BLE wireless networks have inherited vulnerabilities [6] common to all wireless network technologies. Possible threats to BLE wireless networks are: (1) Blueprinting:

978-1-5090-2403-2/16 $31.00 © 2016 IEEE
DOI 10.1109/BigDataSecurity-HPSC-IDS.2016.63

Attackers use the foot printing process to collect information such as IP addresses, network protocols, domain names, Access Control Lists, etc. which can be used to prepare attacks; (2) Bluesniffing: Attackers take unauthorized data like SMS messages, calendar info, images, phone book contacts, and chats from the Bluetooth-enabled device through a Bluetooth connection; (3) Bluebugging: Attackers take control of the target's phone using a program like Bloover, which is a proof-of-concept tool for bugging; (4) Bluejacking: Attackers send text messages such as business cards request for contact list insertion; Process allows attackers to keep sending extra messages; and (5) Bluesmack: Attackers initiate Denial of Service attacks against Bluetooth devices. Some recent surveys [24] suggest that due to the vulnerabilities of wireless networks used in IoT, security framework and implementation in IoT will require changes.

One critical component of a security framework is customer authentication. BLE wireless networks commonly apply a five parameter authentication mechanism which uses the following five parameters: (1) hwndParent - A window that serves as the parent of the Authentication wizard; (2) hRadio - A valid local radio handle used for authentication on all local radios, where if any radio succeeds, the function call succeeds; (3) pbtdi - A structure of type BLUETOOTH_DEVICE_INFO that contains the record of the Bluetooth device to be authenticated; (4) pszPasskey - A personal identification number to be used for device authentication; and (5) ulPasskeyLength - The size, in characters, of pszPasskey.

In summary, there are many factors that need to be considered when designing a security framework for a BLE wireless network based IoT system. We have included all the factors discussed above in Table 1.

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

When designing a BLE wireless network based IoT system, one of the most important tasks is to assess the vulnerabilities of such a system. In this aspect, the most well-known approach is to apply the Common Vulnerability Scoring System (CVSS) proposed by the National Infrastructure Advisory Council (NIAC) [31-33]. CVSS has multiple versions. In this research we will use CVSS v2. The approach of CVSS v2 is that for each vulnerability a base score (BS) based on two groups of only six base metrics will be assigned. All these base metrics stay constant over time and also across different user environments. BS can be adjusted by using temporal and environmental scores to reflect more accurate time and space factors. Temporal and environmental scores are not linked in vulnerability databases and thus are lost in fidelity. These six base metrics – Access Complexity, Authentication, Access Vector, Confidentiality Impact, Integrity Impact and Availability Impact – will be mapped to fixed numerical values and used to determine BS with the base score equations. For example, Access Complexity really describes the degree of easiness or difficulty to exploit the discovered vulnerability, while Authentication describes how many times an attacker will be authenticated to a target device or system after the hacker has gained access to the network. "For locally exploitable vulnerabilities, this value should only be set to Single or Multiple if further authentication is required after initial access" [38]. Below is an example of the base score equations of CVSS v2.

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

$Impact = 10.41\ (1 - (1 - ConfImpact)\ (1 - IntegImpact)\ (1 - AvailImpact))$

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

$f(Impact)$ "A function of Impact", we have $f(Impact)$ =0 if Impact=0; otherwise Impact = 1.176

From this example, we clearly see that there is no place in the equations to include other relevant factors such as those defined in the Table 1. That is, if we apply the current CVSS v2 base score equations to evaluate the vulnerability of a BLE wireless network based IoT system, we may not get an accurate result because these equations lack the ability to consider the impact of many specifics of BLE wireless networks.

To overcome this weakness, in this paper we will present a novel approach based on Bayesian probability to extend the base score equations of CVSS v2 such that all the relevant factors defined in the Table 1 will be included in the calculation for base scores. The next section will review the current related literature. The third section will present the problem statement and hypothesis. The forth section will present the methodology. The fifth section will cover the experiment and that will be followed by the conclusion and future work.

II. RELATED WORK

A. Prior Research Efforts on Internet of Things

The need for ultimately integrating the Cloud and the internet of things (IoT) has given rise to many challenges derived from such integration [26]. IoT security technologies are essential in the deployment of successful IoT-based products and services [7]. Popular deployment of IoT-enabled devices can bring great benefits like network resilience [14], leveraging spontaneous wireless networking capabilities and enabling communication services when conventional communication infrastructure is out. Physical connectivity challenges and traffic prioritization schemes with security implementation are top priorities. IoT based applications in healthcare are using a sensor-tags based communication architecture [8] that uses a secure single sign-on based authentication scheme. Recent surveys [10, 12, 13] on IoT and wireless sensor networks provide possible paths in development and security standards. Other research works on industrial IoT systems with security

and privacy challenges can offer answers to a more holistic security framework [11]. Machine-to-Machine secure communications [9] in a cyber-physical world is a significant research challenge. Techniques suitable for BLE wireless network enabled devices are of smart grid applications [25] with security concerns and network vulnerabilities. The IoT spectrum, from BLE devices at the edge, to cloud on the backend, and everything in between, needs to establish better security links, interoperability standards and architectures [15]. Some recent surveys [27, 29] on evolution, detection and analysis of malware for smart devices like BLE provide some recent progress in vulnerability detection techniques. Other researchers [28, 30, 39, 40] recommend the use of wireless sensor network with high sensing fidelity and industrial radio vulnerabilities as vectors for simple and complex attacks on control systems, to help in critical infrastructure recommendations for securing wireless networks used.

B. Prior Research Efforts on Security Vulnerability

Among all the prior research, the most important work is the CVSS base score equations proposed by the NIAC [31-33]. Evaluating targeted systems through base scores has been generally accepted as the standard method to assess security vulnerabilities of a given system. Some pre-defined factors are required to set up the system vulnerabilities and the exploit difficulties. The impacts of successful attacks by hackers relate to a combined sum of confidentiality, integrity and availability factors. A formula or algorithm is used with a set of input information to build a base score value between 0.0 and 10.0. When a base score of 10.0 is reached, it means the highest degree of severity in terms of vulnerability to being assaulted by potential adversaries. A set of risk matrices are then ordered using the score value according to the severity of the vulnerability scale to speedily identify the most critical troubles within a given system. The most popular version of CVSS is v2. However, the CVSS v2 is relatively weak with regard to attempts to assign only low dimensional severity scores to common system security issues. Therefore due to its limited capabilities, the current CVSS v2 cannot be used for evaluating the ever expending IoT assets like BLE wireless network based IoT systems without some extension.

Prior research on security metrics and recent work [32] on ranking states using attack graphs are all based on probabilities of attackers reaching these states with randomized models [34]. When we rank attack graphs with intrusion detection techniques, the amount of effort spent along the paths of action may be used as a metric. Some attack scenarios can even replace attack graphs using attack trees with advanced attack graphs [35]. Others propose a framework for building better network security metrics, like assault resistance-based metric and Bayesian network-based metrics [36]. All of these are probabilistic approaches with quantitative techniques [22, 23] for better network protections in wireless networks [20, 21]. There exist possible methods to protect run time vulnerabilities on wireless networks [18] through modeling of mobile network connectivity [19]. Most authors address several significant issues to calculate better metrics with dependencies for dissimilar attack stages using common attack graph and recurring structures. These findings correspond to our research in Bayesian probabilistic security metrics in the context of IoT wireless communication. Other IoT publications [16] suggest BLE enabled device authentication using wireless key implementations with a flexible infrastructure [17] that is able to deal with security threats in a dynamic IoT environment. Some empirical studies are published on the number of zero day vulnerabilities for a single day based upon existing known vulnerabilities [37].

III. Problem Statement and Hypothesis

A. Problem Statement

The conventional CVSS v2 base score equations cannot accurately assess vulnerability of a BLE wireless network based IoT system due to CVSS v2's inability to include extra factors relevant to the specific authentication mechanism of such system in the calculation of the base scores.

B. Hypothesis

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

IV. METHODOLOGY

A. Identify A Compatible Extention

To find a way to incorporate specifics of BLE wireless networks into the base equations of CVSS v2, let's look at one of the base equations which focuses on the exploitability of a vulnerability:

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

Where AccessVector is a variable that shows how a vulnerability may be exploited. For a Bluetooth network, it is often assigned to 0.646 because "the attacker must have access to the broadcast or collision domain of the vulnerable system [38]." AccessComplexity is a variable that describes the degree of easiness or difficulty to exploit the discovered vulnerability. For a Bluetooth network, due to the open air it is relatively easy to access to the vulnerability so that the score assigned to AccessComplexity is often >0.7 [38]. Authentication is a variable to describe the number of times that an attacker must authenticate to a target to exploit it. According to previous work [38], Authentication actually "does not include (for example) authentication to a network in order to gain access. For locally exploitable vulnerabilities, this value should only be set to Single or Multiple if further authentication is required after initial access." The typical scores assigned to Authentication are 0.45 for multiple required authentications, 0.56 for single required authentication, and 0.704 for No authentication. This can also be defined as

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

Where *n* is an integer.

Obviously, Authentication becomes a perfect target for us to make some changes so that the specifics of BLE wireless networks will be reflected in the calculation of the base score of the vulnerability through the base equations of CVSS v2.

We will consider Authentication as a function of the number of authentications required, which is denoted as an integer *n*, and authentication risk factor, which is denoted as *r* and defined as the probability of an authentication method used by a BLE wireless network fails due to attack, where $0 \leq r \leq 1$. That is:

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

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

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

It is evident that *f(n, r)* defined in (2) exhibits the convergence property such that when $r = 0$, then *f(n, 0)* converges back to *f(n)* defined in (1). That is:

$$\text{Authentication} = f(n, 0) = f(n) \quad (3)$$

That is, we can claim that we have identified a natural extension for the Authentication which is compatible with the original semantics of Authentication.

B. Application of the Extention

To demonstrate the ability of (2) to integrate the specifics of BLE wireless network into the base equation of CVSS v2, we will apply the Bayesian Theorem to an example in which two types of events listed in the Table 1 will be used. We will define the first event as the BLE wireless network is attacked by at least one type of thread listed in the first column of Table 1, and we denote this event as *F1*. We also define the second event as one of the five authentication parameters is hacked, and we denote this event as *F2*. Then if we assume 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 indicates the risk rate of the BLE wireless network being attacked when one of five authentication parameters has been hacked. Based on the Bayesian Rule we can easily know that

$$r = P(F1|F2) = [P(F2|F1)P(F1)]/P(F2) = 0.15\text{x}0.2/0.3 = 1 \quad (4)$$

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

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

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

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

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

From (6) we can see that as the number of further required authentications after initial access increases, the score value for Authentication variable decreases. This is consistent with the real world semantics: the more authentications required, the less vulnerable the system will be.

V. MODEL EXPERIMENT AND RESULT

We use the BLE wireless network enabled shopping cart shown in Fig. 1 to show a vulnerability example in which all the variables used in the CVSS v2 base equations have been replaced with specific data values used in real situations. The BLE wireless network's authentication requires any of the five parameters to have the correct data value. In short, a potential hacker with a correct data value for only one of five parameters will have certain probability to get authenticated. This is a very weak authentication mechanism. The impact of this specific authentication characteristics must be reflected in the CVSS v2 base score equations in order to have an accurate assessment on the vulnerability of BLE enabled shopping cart system. Therefore we will apply our extension in this example to show what is the weaknesses of the conventional CVSS v2 base score equations with regard to such system, and we will also show how that weakness can been addressed and compensated by our extension. We have used the BLE enabled shopping cart application as the context to develop the experiments. We have modelled attacker behavior by applying the common approaches an attacker may use to conduct various types of Bluetooth attacks.

Fig. 3 illustrates a scenario in which a BLE wireless network has two customers' wireless nodes (one customer's BLE enabled shopping cart and one BLE beacon in the retail store) and one hacker's possible illegal entry node through which the hacker is trying to penetrate into the wireless network. Next, we consider two factors based on this example BLE wireless network. Factor 1 in this case is about threat types. We will include all known threats associated with the BLE wireless network such as Blueprinting, Bluesniffing, Bluebugging, Bluejacking, and Bluesmack. Additionally we have also added another unknown threat into this case. We have pre-assigned prior probability for each type of threat based on known facts. Factor 2 in this case is about existing common BLE five authentication parameters based authentication mechanism. Again we give equal importance of 20% weight as the prior probability to each of the five different authentication parameters. We have built two tables Table 2 and Table 3 with the prior probability values in both factors, which will be used in the calculation for base score when we evaluate the Authentication variable in CVSS v2 base score equations by using the extension proposed by us. We have assumed that an IoT service is running on the BLE wireless network. In this typical case, no firewalls are involved. We can presume the BLE wireless network contains a vulnerability which may provide opportunities for remote attackers to bypass authentication and gain access. We then use the conventional CVSS v2 base score equations, and assign the data values defined in Table 4 to various variables in the CVSS v2 equations, and have calculated out the final base score to be 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

Fig. 3. A BLE wireless network explosed 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 (Base Score) = $round\ to\ 1\ decimal((0.6\ Impact + 0.4\ Exploitability - 1.5)\ f(Impact))$ (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 (8)

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

$Impact$ is not 0 so $f(Impact)$ = 1.176 (10)

So, BS (Base Score) = $round\ to\ 1\ decimal$((0.6 [$Impact$ = 1.176] + 0.4 [$Exploitability$=2.45] − 1.5) [$f(Impact)$ = 1.176]) = ((0.6 x 0.409) + (0.4 x 8.4) − 1.5) x1.176 = (0.2454 + 4.5 − 1.5) x1.176 = 2.48 (11)

As the base score is only 2.48, it may lead to the conclusion that this example BLE wireless network has very low vulnerability. However, that may be a misleading result as we will soon demonstrate in the following continued evaluation to the example BLE wireless network.

Now let's see how the extended Authentication formula as defined in (2) is applied in this example BLE wireless network.

We will assume two events as following:

- Event H: the BLE wireless network is attacked by any type of the threats listed in the first column of Table 2
- Event D: one of five authentication parameters as defined in Table 3 is hacked

We also will use the prior probabilities presented in Table 2 and Table 3 in this example.

We will evaluate one possible situations: the risk rate of a BLE wireless network being attacked given that one of five authentication parameters is hacked successfully.

That is we need to find out the risk rate $r = P(H|D)$. Based on the Bayesian Theorem, we have

$$P(H|D) = [P(D|H)P(H)]/[P(D)] \quad (12)$$

In this example, we define P(H) as the prior probability for H, by taking the average of the possible outcomes in Table 2, we get P(H) = (0.25 + 0.20 + 0.15 + 0.15 + 0.15 + 0.10) / 6 = 0.1667. We also define P(D) as the prior probability for D, by taking the average of the possible 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 of a prediction for D is possible given by "H was Succeed", and we assume that P(D|H) = 0.95.

Therefore we have

$$r=P(H|D) = 0.95x0.1667 / 0.2 = 0.792 \quad (13)$$

By using (2), we have

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

Because we have assume that only single authentication is required, that is $n = 1$, and $f(n)$ is defined by (1), therefore we will have

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

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

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

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

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

By comparing the base scores in (11) and (17), we can see the big difference between whether or not the specifics of BLE wireless network have been included in the base score equations of CVSS v2. The higher score in (17) implies the importance of considering the practical situation of the BLE wireless network as it is a wireless network with high vulnerability due to its specific five parameters based authentication mechanism under 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. By extending the base score equations of CVSS v2, we can also evaluate the effectiveness of any security enhancement measures. For example, if we simply increase the required number of times of authentications from 1 to 2 in the previous example, we will see the base score decreases from 8.064 to 4.493. Similarly, if we assume n= 3, we will see the base score further decreases to 3.562. Furthermore, when n=4, the base score will become 3.096. This trend implies that having 2 or 3 times required authentications for a BLE wireless network will greatly reduce system vulnerability as a whole. However it also suggests that there is a balance point on which only through increasing total number of times of required authentications on a BLE wireless network will not be very effective to further reducing the vulnerability of the entire system. We have to evaluate other factors of the system in order to achieve more success on improving the vulnerability of the system. That is with our extension, we can make CVSS v2 become an effective tool to assist us to design a more secure BLE wireless network based IoT system.

VI. Conclusion

In this paper, we have presented a natural extension to one of the variables used in CVSS v2 base score equations. We have also demonstrated the weakness of the current CVSS v2 base score equations and the benefit of this extension through an example BLE wireless network based shopping cart IoT system. That is we have successfully approved our hypothesis. Future work will focus on two aspects: identifying an opportunity to extend other variables in CVSS v2, and adding more temporal and environmental scores. Additionally we will also conduct more experiments that incorporate more realistic real-time scenarios.

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.

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

[16] 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.

[17] 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.

[18] 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).

[19] 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.

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

[21] Chan, P., Nowicki, D., Man, H., & Mansouri, M. (2011). Managing Vulnerabilities of Tactical Wireless RF Network Systems: A Case Study. International Journal of Engineering Business Management, 3(4), 22-33.

[22] Chan, P., Mansouri, M., & Man, H. (2010, July). Applying systems engineering in tactical wireless network analysis with Bayesian networks. In Computational Intelligence, Communication Systems and Networks (CICSyN), 2010 Second International Conference on (pp. 208-215). IEEE.

[23] Chan, P., Mansouri, M., & Hong, M. (2010). System Engineering Approach Tactical Wireless RF Network Analysis with Vulnerability Assessment using Bayesian Networks. International Journal of Simulation Systems, Science & Technology, 11(6), 67-75.

[24] Chen, M., Wan, J., González, S., Liao, X., & Leung, V. (2014). A survey of recent developments in home M2M networks. Communications Surveys & Tutorials, IEEE, 16(1), 98-114.

[25] Mahmood, A., Javaid, N., & Razzaq, S. (2015). A review of wireless communications for smart grid. Renewable and Sustainable Energy Reviews, 41, 248-260.

[26] Botta, A., de Donato, W., Persico, V., & Pescapé, A. (2014, August). On the Integration of Cloud Computing and Internet of Things. In Future Internet of Things and Cloud (FiCloud), 2014 International Conference on (pp. 23-30). IEEE.

[27] Suarez-Tangil, G., Tapiador, J. E., Peris-Lopez, P., & Ribagorda, A. (2014). Evolution, detection and analysis of malware for smart devices. Communications Surveys & Tutorials, IEEE, 16(2), 961-987.

[28] Singhal, S., Gankotiya, A. K., Agarwal, S., & Verma, T. (2012, January). An investigation of wireless sensor network: a distributed approach in smart environment. In Advanced Computing & Communication Technologies (ACCT), 2012 Second International Conference on (pp. 522-529). IEEE.

[29] Shuai, C., Reny, S., & Shuifeng, Z. (2014). Wireless sensor network positioning based on the unilateral side of two reference nodes. Computers & Electrical Engineering, 40(2), 367-373.

[30] Reaves, B., & Morris, T. (2012). Analysis and mitigation of vulnerabilities in short-range wireless communications for industrial control systems. International Journal of Critical Infrastructure Protection, 5(3), 154-174.

[31] Scarfone, K., & Mell, P. (2009, October). An analysis of CVSS version 2 vulnerability scoring. In Proceedings of the 2009 3rd International Symposium on Empirical Software Engineering and Measurement (pp. 516-525). IEEE Computer Society.

[32] Cheng, P., Wang, L., Jajodia, S., & Singhal, A. (2012, October). Aggregating CVSS base scores for semantics-rich network security metrics. In Reliable Distributed Systems (SRDS), 2012 IEEE 31st Symposium on (pp. 31-40). IEEE.

[33] Schiffman, M., & Cisco, C. I. A. G. (2005, June). A complete guide to the common vulnerability scoring system (cvss). In Forum Incident Response and Security Teams (http://www. first. org/).

[34] V. Mehta, C. Bartzis, H. Zhu, E. Clarke, and J. Wing. 2006. Ranking attack graphs. In Recent Advances in Intrusion Detection 2006.

[35] J. Pamula, S. Jajodia, P. Ammann, and V. Swarup. A weakest adversary security metric for network configuration security analysis. In Proceedings of the ACM QoP, pages 31–38, 2006.

[36] M. Frigault, L. Wang, A. Singhal, and S. Jajodia. Measuring network security using dynamic bayesian network. In Proceedings of 4th ACM QoP, 2008.

[37] M. McQueen, T. McQueen, W. Boyer, and M. Chaffin. Empirical estimates and observations of 0day vulnerabilities. Hawaii International Conference on System Sciences, 0:1–12, 2009.

[38] Mell, P., Scarfone, K., & Romanosky, S. (2007, June). A complete guide to the common vulnerability scoring system version 2.0. In Published by FIRST-Forum of Incident Response and Security Teams (pp. 1-23).

[39] Guo, P., Wang, J., Li, B., and Lee, S. A Variable Threshold-value Authentication Architecture for Wireless Mesh Networks. Journal of Internet Technology,15(6): 929-936, 2014.

[40] Xie, S., Wang, Y. Construction of Tree Network with Limited Delivery Latency in Homogeneous Wireless Sensor Networks. Wireless Personal Communications, 78(1): 231-246, 2014.