Journal of Telecommunication, Electronic and Computer Engineering
ISSN: 2180 – 1843 e-ISSN: 2289-8131 Vol. 15 No. 2
jtec.utem.edu.my

A Survey Study of Common Security Failures and Mitigations for the Internet of Things (IoT)

M. Scott
Northern Arizona University, Flagstaff, Arizona USA
mjs672@nau.edu

Article Info

Article history:
Received Dec 30th, 2022
Revised Mar 5th, 2023
Accepted Apr 12th, 2023

Index Terms:
Internet of Things
IoT Architecture
Security Failures
Security Mitigations

Abstract

The Internet of Things (IoT) is transforming the world on almost a daily basis. There are tens of billions of things interconnected and that number is growing daily. Everywhere the IOT is present security is critical, especially in healthcare applications. Reported frequently are exploitations of security failings within the IoT. The exploitation of IoT security failures can result in dramatic consequences including loss of human life. This makes it essential to create a culture of awareness of the potential security failures within the IoT and their available mitigations. This article begins the engendering of that awareness. Presented is a simplified three-tier architecture of the IoT to serve as a lens to view the commonalities in the diverse IoT ecosystem. While there are multiple security weaknesses in the IoT ecosystem and numerous individual malicious attacks potentially exploiting them the viewpoint presented provides for the distillation of those into a common group that indicates a finite set of mitigation techniques. When applied these mitigations make the entire IoT ecosystem secure against the currently known exploitations.

I. INTRODUCTION

Just prior to the 2013 occurrence of the annual Black Hat convention in Las Vegas, a well-known ethical hacker named Barnaby Jack suddenly died of a drug overdose. Jack died before he could deliver another swath of research, he had become known for over the past several years. Jack had been researching Internet of Things (IoT) application security flaws. Previously he had identified security flaws that placed insulin pumps in jeopardy of malicious hacking. His new research that went unrepresented was another critical IoT application with severe security failures. Jack had made it known that he found an exploitable failure in the security of pacemakers interconnected via the IoT ecosystem. He indicated that exploitation of this failure could result in the death of patients [1].

The IoT has exploded onto the technology scene. With almost ten (10) billion things connected and that number expected to more than double within the next two (2) years there are few areas of daily life where the IoT is not present. In many places where the IoT is already present such as the healthcare example [1], smart cities and buildings, smart power grids and industrial control systems (ICS) security is critical [2]. These varied applications use the IoT while bringing improvements to business, industry, and the lives of individuals around the globe by necessity both communicating and processing sensitive and critical data as well as requiring users to contribute personal and confidential information. Already as reported in the media, there have been exploitations of the IoT. As the IoT charges ahead at a rapid pace it is essential to engender a culture-wide awareness of potential security failures throughout the industry [3].

This research takes steps to begin the engendering of security failure awareness for the IoT. The IoT consists of a three-layer architecture. All the potential security failures map directly to one or more of those layers.

This survey study will first provide a common background for the diverse IoT ecosystem. Next, the author will present a common IoT security architecture for the IoT as a lens for viewing the commonality in the IoT ecosystem. There will be a survey of the literature and the IoT security failures and exploiting malicious attacks supported by the literature. The discussion will focus on how the survey of the literature supports reducing the security failings in the IoT ecosystem's six (6) distinct common weaknesses. The discussion will focus on commonalities and relationships found through the literature survey examining how just four (4) common types of malicious attacks exploit the six (6) weaknesses. Finally, the author will present via the literature survey that just four (4) common categories of techniques will mitigate the six (6) common IoT weaknesses and prevent the four (4) common types of attacks. The author will provide and discuss examples of these techniques. The conclusion will address future research opportunities demanded by the inherent characteristics of the IoT ecosystem.

II. BACKGROUND

Currently, the IoT ecosystem comprises billions of devices and will grow in this decade to over fifty billion interconnected things [4]. The IoT and its interconnected things can be commonly found throughout everyday life. Everywhere there is connectivity to the Internet and localized communication networks there are IoT devices and applications. The IoT is found in manufacturing facilities, transportation systems, office buildings, hospitals, homes and

even embedded in human beings [4], [5]. The rapid development of communication technologies such as Wi-Fi and cellular telephony coupled with the ease of developing bespoke electronic devices has made the IoT one of the fastest expanding and most diffuse technology disrupters of our age [6].

The speed at which the IoT is expanding, and the diversity of applications brings ever expanding security vulnerabilities [4], [6], [7]. The potential harm resulting from an exploited IoT vulnerability including to human life begs the deployment of security mitigations [7]. Given the vastness of the IoT ecosystem and the bespoke nature of IoT applications product developers and security practitioners cannot simply take an ad hoc approach. Therefore, equipping practitioners and developers with a standard reference model for identification of common security failures and the associated mitigations is warranted.

III. A COMMON IOT SECURITY ARCHITECTURE

As the IOT moves rapidly and new applications arise frequently, there is no widely accepted global standard architectural reference model [8], [9]. Therefore, for the purposes of security failure analysis it is best to view the IoT architecturally as a simplified three-layer stack. Those three (3) layers are the device layer, the network layer, and the software layer [10] as depicted below in Figure 1. Some in the field break the network layer into two (2) parts; network and transport layers [9], [11]–[13]. While still others break the software layer down into two (2) separate layers. Those are the middle-ware and application software layer [7], [8], [14] . For the purposes of security failure analysis both are simply network and software. The device layer contains the physical things that monitor and control an environment. The network layer is a transmission layer that routes data and information between things in the device layer and applications in the software layer [10]. The software layer performs functions such as data analytics and provides a means of interface for users [15].

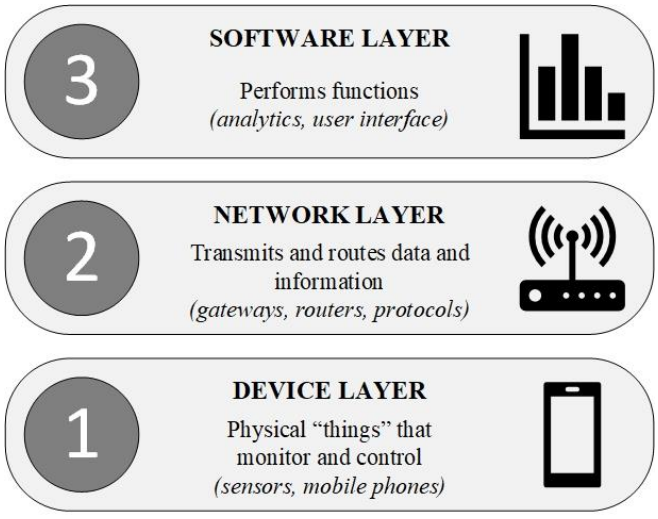

Figure 1. IoT Simplified Three-Layer Architecture

A. Device Layer

The device layer sometimes referred to as the perception layer contains components and assemblies used to monitor, measure and control; the "things" of the IoT (labeled number 1 in Figure 1 above). Typically, these devices include sensors collecting various data such as temperature, humidity, force, pH, acceleration, and strain [7], [8]. Additional devices comprise Arduino or Raspberry assemblies employing communication technology of one type or another (e.g., ethernet) to interconnect sensors and devices via the Internet with peer devices and the network layer of the IoT. Identification of devices and service discovery also occur in the device layer [7].

The IoT ecosystem integrates directly into the process and activities it monitors. This means that IoT devices must meet a variety of unique requirements. These requirements include compact and lightweight physical form factor, protection against environment, tamper resistance and low energy consumption. The result is often a constraint of resources available for security functions [14].

B. Network Layer

The network layer performs the crucial functions of routing and transporting data between the device layer and the software layer [lee]. This occurs without any alteration of the data [8]. The routing of data between layers is conducted by physical network components such as routers, switches, and gateways. The transport of the data from devices to software is accomplished via a variety of protocols including MQTT, constrained application protocol (COAP), transmission control protocol (TCP) and the user datagram protocol (UDP) [7], [11], [13].

Currently there is no standard protocol for IoT deployments. The network layer may employ a single common protocol or a variety of different protocols dependent upon devices and software serviced. Security in the network layer is highly dependent upon the protocols employed. Securing the network layer has the added challenge of the propagation of threats across multiple IoT layers [lee].

C. Software Layer

The software layer pre-processes, stores and processes data acquired from the device layer then provides for interface by the end user. The pre-processing of data is done by software layer components referred to as middleware. This software provides data handling services and controls the ingestion of data into storage for use in analytics and application interfaces. Bespoke applications fulfilling user requirements form the high functioning elements of the software layer. These components comprise analytics and interfaces unique to each IoT deployment such as monitoring and reporting energy usage, forecasting increases in medication dosage through trending of bodily functions and vital signs [7], [8].

The software layer is where the IoT processes data into readable and understandable formats. When this data is personal or sensitive security becomes paramount. There is also the added security challenge through the introduction of human users into the interaction with applications and data. These include issues of trust and privacy [7], [8].

IV. IOT LAYER SECURITY FAILURES

Applying a functional technology perspective to the IoT finds that architecturally it comprises three (3) layers. These layers as previously identified are the device layer, network layer and software layer. Each layer performs a specific function [15] as previously outlined and depicted in Figure 1. Despite the wide variety of specific functions and

applications within the IoT ecosystem, there are common security failures within the architectural layers and the gateways that interconnect the layers [2]. Figure 2 below portrays common security failures within each IoT layer as identified from the survey of the literature, the specific attacks on these failures and the resulting effects upon the IoT ecosystem.

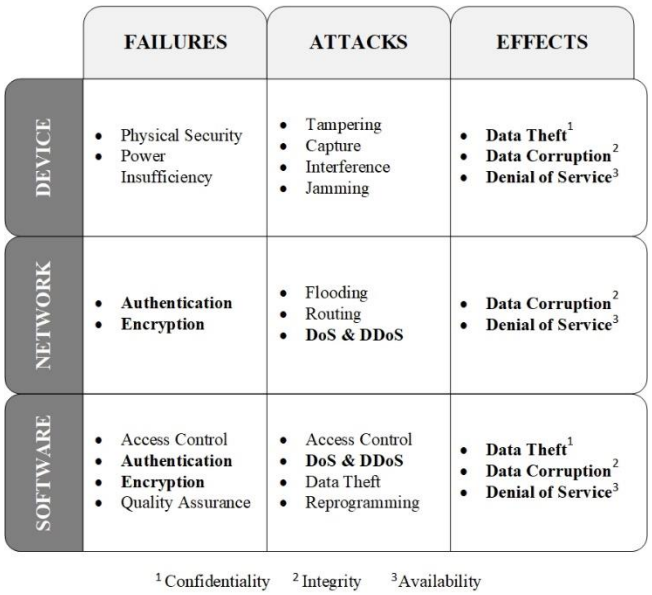

Figure 2. IOT Architectural Security Failures, Attacks & Effects

A. Device Layer Potential Failures

The potential security failures within the device layer include physical security deficiencies and insufficiency of power. These security failures affect the confidentiality, integrity and availability of a system and its components [9], [15]. When these failures occur, they are often subject of exploitation through tampering or capture attacks or interference and jamming [2], [16], [17].

1) Tampering

One of the most significant common attack surfaces in the device layer particularly in the healthcare IoT ecosystem are the physical devices themselves [9], [18]. Tampering of devices may occur through physically damaging of the device or altering communications assemblies and their function [9], [19].

Device tampering includes physical disconnection from the network, increasing/decreasing the frequency of communications, altering the readings of sensors and draw down of device power supplies [9], [19], [20]. Tampering may be targeted against a single device, groups of devices or the gateways interconnecting the device layer with the other IoT architectural layers [17]. This can lead to denial of service through depletion of power supplies or data theft and corruption. [15].

2) Capture Attacks

Captured devices while occurring within the device layer pose the greatest threat to the network layer [9]. When a device is captured, it may stop transmitting altogether or data theft [18]. More commonly the captured device is used to conduct denial of service (DoS) type attacks on the network layer [21].

3) Interference

The IoT ecosystem commonly employs wireless radiofrequency (RF) communications at the device layer. The integrity of device communications can be disrupted through radio interference. High powered sources of RF on the same or adjoining frequencies can deprive devices and sensor from the ability to consistently send and receive communications leading to denial of service [21].

4) Jamming

Like interference device layer sensor communications may be denied through a jamming attack. A high-power RF source on the same frequency as the device prevents the intended signals from being sent or received. For the entire time the jamming signal is present there can be a denial of service [21]–[23].

B. Network Layer Potential Failures

Potential failures of security in the network layer include authentication inadequacies, lack of proper encryption and leaving ports open unnecessarily. These failures of security effect the confidentiality, integrity and availability of data, information and entire IoT sub-systems [4]. The occurrence of security failures such as these allow for an IoT sub-system to be successfully attacked using flooding, routing attacks, denial of service (DoS) and distributed denial of service (DDoS) attacks [2], [16].

1) Flooding

Network flooding attacks are amongst the confounding and most perturbing of network layer threats [9]. During this type of flooding attack captured devices will broadcast signals such as HELLO to every other reachable device. Devices that receive the signal add the attacking devices to their scan list [9], [17], [19], [24]. These messages propagate across the entire network and repeat. The result is a denial of service and complete loss of availability of the network due to the high volume of repeated malicious messages [21].

2) Routing Attacks

Well established routing attacks [smith] on the network layer have become common due to the fact the routing configurations of network gateways and switches are unencrypted [9]. Malicious attackers may alter these configurations [9], [25] creating looping communications [9]. Routing attacks break the connection between the device layer and other layers within the IoT architecture. The result of routing attacks range from data corruption between devices and software applications to complete denial of service in the network layer [9], [12].

3) Denial of Service (DoS, DDoS)

Due to the dependence upon wireless technologies the IoT ecosystem as a whole and the network layer is particularly susceptible to denial of service (DoS) attacks [9]. The DoS among the most common attacks against the network layer insert high volumes of useless data packets into the network. Attacker compromised nodes may also refuse connection requests from other devices and nodes on the network [26]. When DoS attacks are conducted en masse involving thousands of attacking nodes that produce erroneous data packets of generous size they become distributed denial of service (DDoS) attacks [21], [27]. These large-scale attacks completely overcome the ability for the network to respond to genuine requests and consume memory. The result is a complete loss of both device and network availability [21].

One of the most common DDoS attacks stems from a now well-known malware identified as Mirai. First identified in 2016 this malware has generated DDoS attacks injecting 1.1 Tbps of erroneous messages into IoT applications. Despite approaching a decade in age Mirai continues to evolve with

new versions appearing daily including high-volume versions that can be rented online [28].

C. Software Layer Potential Failures

Within the software layer, there are several potential security failures. These include access control insufficiencies, lack of authentication and permissions management, missing encryption, and lack of overall software quality assurance. These failures of security effect the confidentiality, integrity and availability of data and information necessary for IoT functionality [15]. When these security failures occur, they allow for exploitation of an IoT sub-system through a wide variety of attacks including access control attacks, path-based denial of service (DoS, DDoS), data theft and reprogramming attacks [2], [16].

1) Access Control Attacks

Proper access control is a serious and common challenge in the IoT ecosystem [29]. When unauthorized users gain access to devices or software applications the software layer is placed in jeopardy. Malicious users can use unencrypted access channels such as inter-node communications without authentication [2]. Once a node or device is successfully attacked malicious users can access data and control communications under the guise of an authorized user [2], [30]. When unauthorized users can conduct malicious activities without authentication in the software layer there may be data corruption, theft, or denial of service [2].

2) Denial of Service (DoS, DDoS)

The vast amount of IoT applications deployed in the software layer coupled with the necessity for them to be continuously connected to the Internet makes the software layer susceptible to DoS attacks such as Mirai [28]. This susceptibility arises from the difficulty in establishing common authentication and permission controls across the wide variety of applications and elements within the software layer [22]. These attacks typically beginning with an infection of unprotected elements within the device layer. The infection moves across the network layer to attack servers and applications in the software layer [28]. Once the software layer is infected the resources there are used to propagate further DoS attacks [28] across point-to-point communication pathways developing into DDoS attacks [22], [23].

3) Data Theft

The IoT ecosystem includes many applications that utilize confidential and sensitive data. This is especially prevalent in healthcare related IoT applications. Data both at rest and significantly in transit are vulnerable to data theft [1}. The lack of authentication and encryption place data at risk of theft and exposure [31].

4) Reprogramming Attacks

The rapid pace of expansion of the IoT ecosystem and demand for new applications has led to many software applications releasing without adequate quality assurance [32]. This lack of software quality leading to the absence of encryption and authentication controls makes IoT applications susceptible to reprogramming attacks [33]. These attacks target the quality gaps in software to gain access to application source code, reprograms it to propagate denial of service and facilitate data corruption and theft [2], [23].

V. DISCUSSION

The survey of the literature in alignment with the simplified three-tier IoT architecture exposes several commonalities amongst the three architectural layers. These commonalities (depicted as the highlighted elements in Figure 2) appear in security failures, malicious attacks, and the resulting effects upon the IoT ecosystem. Additionally, the literature survey exhibits an enabling relationship between attacks on the device layer and exploitations in the network and software layers.

A. Commonality of IoT Security Failures

The survey of the literature finds a total of eight (8) security failures across the three-layered simplified IoT architecture that can be reduced through commonality. At the device layer there are two (2) failures, the lack of physical security and power insufficiency as identified by Neshenko et. al., [15] and Varga et.al., [9]. These are exploited by tampering, capture, interference and jamming attacks [2], [16], [17]. Within the network layer there are also two (2) security failures, inadequate authentication, and lack of encryption [15]. Both are exploited by DoS/DDoS type attacks [22], [23], [28]. The software layer contains a total of four (4) security failures. Two (2) being lack of proper access control and software quality assurance as noted by Neshenko et. al., [15] and Hassija et. al., [2]. Both being exploited by access control, DoS/DDoS and reprograming attacks [2], [22], [23], [28]. While another two (2) software layer failures are inadequate authentication and lack of encryption as found by Neshenko et. al., [15] in the network layer [15]. These are exploited through both DoS/DDoS [22], [23], [28] type attacks and data theft [31]. Owing to the duplication of security failures found in the network and software layers by Neshenko et. al., [15] the literature survey supports a reduction from eight (8) individual to six (6) distinct common IoT security failures:

- Lack of Physical Security
- Power Insufficiency
- Inadequate Authentication
- Lack of Encryption
- Lack of Access Control
- Lack of Software Quality Assurance

B. Commonality of Malicious Attacks

Through the literature survey we find that the six (6) common IoT security flaws are exploited by a total of eleven (11) malicious attacks throughout the three-layered simplified IoT architecture. These also are reduced. The reduction is both by commonality and through a series of enabling relationships.

The four (4) malicious attacks that occur in the device layer all provide enabling vectors for flooding, routing, and DoS/DDoS attacks [9], [15], [19]–[23]. Tampering and capture attacks occurring in the device layer enable data theft attacks in the software layer [15], [17], [18]. Flooding and routing attacks that occur in the network layer in turn result in DoS/DDoS type attacks. Owing to the identification of common DoS/DDoS type attacks in both the network [21], [26], [27] and software layers [22], [23], [28] the literature survey supports a reduction from eleven (11) individual to four (4) distinct common malicious attacks on the six (6) common security failures in the IoT ecosystem:

- Dos/DDoS attacks
- Data Theft Attacks
- Access Control Attacks
- Reprogramming Attacks

This distillation of malicious attacks compares with research by Bahaa et.al., [34] that found a similar distribution with 35% of all identifiable attacks on the IoT ecosystem being DoS/DDoS attacks, 17% being access control attacks and 12% being data theft attacks and finally 10% being reprogramming type attacks (e.g., SQL injection, shell code). Figure 3 below graphically depicts this statistical breakdown of malicious attacks.

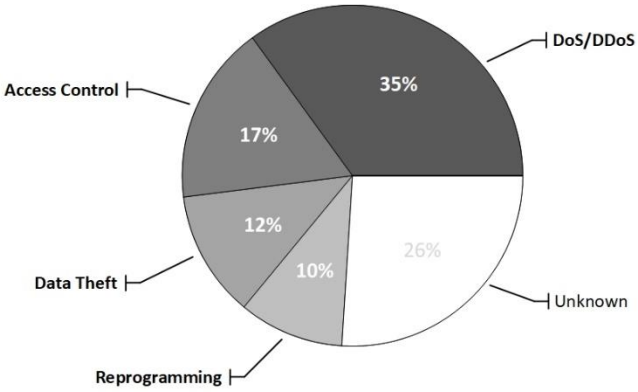

Figure 3. Common IoT Malicious Attacks

C. IoT Security Failure Mitigations

As previously noted, the survey of the literature exposes six (6) common distinct IoT security failures exploitable by four (4) common distinct types of malicious attacks. Further survey of literature focused on mitigation techniques reveals a similar reduction to four (4) distinct techniques that mitigate the six (6) common failures thereby preventing all the four (4) common types of malicious attacks:

- Device Hardening
- Secure Network Topology
- Security Protocols
- Quality Assurance in the SDLC

Table 1
Mitigations for Common IoT Security Failures & Attacks

Failures	Layer	Mitigation	Attacks
Physical Security Power Insufficiency	Device	Device Hardening	DoS/DDoS Data Theft
Authentication Encryption	Network Software	Network Topology Security Protocols	DoS/DDoS
Access Control Quality Assurance	Software	Security Protocols SDLC	DoS/DDoS Data Theft Access Control Reprogramming

Table 1 summarizes the security failures, IoT layer location and prevented malicious attacks for each of the four (4) mitigations resulting from the survey of the literature. The ensuing discussion provides specific examples of currently available mitigations.

1) Device Hardening

Hardening of IoT devices comprises two categories of techniques. The first being focused on the physical form factors of devices and their deployed state. As IoT devices often conduct critical functions such as those related to human health and well-being, the highest quality of components (RF circuits, chipsets) [8] are necessary to prevent exploits. Shielding of devices from electromagnetic interference (EMI) and precise antenna designs will mitigate jamming and interference [8]. Inclusion of non-volatile memory for data storage and configuration parameters will prevent exploitation and data loss on interruption of device power [16]. Devices must be rated for the environmental conditions in which they will operate with the ability to withstand temperature, humidity, vibration, shock, and other conditions [2]. Finally, once IoT devices are placed into operation they must be regularly inspected for degradation, damage, or tampering [16]. Even the highest quality devices will degrade over time and those built to withstand physical abuse can sustain damage from failed attempts at physical tampering.

The second category of device hardening techniques focuses on the system configuration parameters of devices and gateways withing the IoT device layer. The rapid pace of IoT development drives manufacturers to shorten the time to market of products. This can lead to security gaps or vulnerabilities that are mitigated by the release of updated firmware or software. IoT devices must be updated to the most recent versions of these software and firmware before deployment [35]. IoT devices are manufactured for a variety of applications. Therefore, they are equipped with many distinct functions and features that specific IoT applications and uses may not require. Any unused or outdated services, features, ports, or functions should be disabled. Default BIOS and other passwords must be updated to unique settings. Boot functions must be set to prevent unauthorized execution from alternative sources [35]. Devices must utilize error checking [8] and event logging of events must be enabled. A simple checksum or parity bit function enabled will prevent tampering [8] and logged events will provide notification of attempts at tampering enabling immediate investigation and intervention [35].

2) Network Topology

Much of the value derived from the IoT ecosystem stems from the ability to interconnect multiple sensors and devices. The greatest value is often derived from the ability to form networks of mobile devices deployed in vehicles and even individual human beings. The technologies available enable the IoT network layer to be extremely flexible. However, with that flexibility comes security failures exploitable by the common malicious attacks.

Proper deployment of a secure network topology enabling access and authentication controls prevents security failures in the network layer and those that propagate from the device layer [36]. One such topology is proposed by Qabulio et al., [36]. Qabulio et al., [36] places a base station server in the network layer. This base station (BS) contains a network control unit (NCU) with sub-units capable of identifying tampered and malfunctioning nodes, jamming, and eavesdropping. Every message or data transmission with the physical layer routes via the BS where there is verification against the sub-units of the NCU. The result is only

authenticated messages are accepted in the network layer to receive access to the software layer [36]. This topology completely prevents the DoS/DDoS that results from tampering, jamming, interference, flooding, and routing attacks.

3) Security Protocols

Security protocols are difficult within the IoT. The limited computing power, intermittent data loss and energy resources require lightweight encryption. Therefore, alternatives to typical transport protocols such as TCP or UDP and other protocols such as Hypertext Transfer Protocol (HTTP) are required [37].

The Constrained Application Protocol (COAP) developed in 2014 uses less bandwidth than HTTP and provides a more stable transport for IoT applications than UDP and is optimized for the IoT ecosystem. However, COAP requires a security protocol to protect the data transmissions [37]. A certificate-based protocol such as Transport Layer Security (TLS) used to secure HTTP is required [38].

Kothmayr et al., [39], employs a thirteen (13) byte long header for all messages from the device layer. This datagram transport layer security protocol (DTLS) allows for detection of message alteration. This handshaking provides a two-way authentication of all messages between the device layer and the software layer [39]. DTLS while deployed primarily in conjunction with COAP is also able to operate with the unstable UDP transport protocol providing a means of securing legacy IOT applications [38].

Shafagh et al., [40] developed Talos a data framework utilizing Partial Homomorphic Encryption. This approach shows promise in initial testing where data transmission security improved with only moderate consumption of power [40].

Zhang et al., [41] is pursuing an encryption approach with the intent to be low energy dependent so as not to exacerbate the power insufficiency already inherent in IOT devices. This Coverage Inference Protocol (CIP) employs Boundary Node Detection (BOND) and Location Based Symmetric Key (LBSK) elements. This combination enables the approach to prevent compromises of data transmissions from both external actors and overtaken nodes on the trusted network. Small scale testing shows promise. However, this approach remains unproven at scale for the larger IoT [41].

4) Software Development Lifecycle (SDLC)

The rapid pace of the expanding IoT ecosystem leads to the release of IoT products with the proper inclusion and validation of quality to ensure security [32]. Software assurance whether of embedded binary or source code firmware is essential to avoid introduction of security failures into an IoT sub-system. Integrating quality assurance including security reviews into the SDLC is an effective means of mitigating software security failures. Costin et. al., [42] and Temkar & Bhaskar [32] both provide mechanisms for embedding software quality assurance within the SDLC.

Costin et al., [42] deploys a firmware-testing program identifying security failures within embedded firmware prior to deployment on the IoT sub-system. When this program becomes part of the software development lifecycle (SDLC) there is the elimination of security failures prior to operation service. The program from Costin et al., [42] consists of a three-part process. The first step is use of a static analysis tool against the firmware root. Next, the firmware runs on an emulator. When the firmware successfully executes within the emulator it undergoes a dynamic analysis. Finally, the emulator analysis results are reviewed, and a final manual evaluation identifies security failures for remediation [42].

Temkar & Bhaskar [32] employ an analytic hierarchy process (AHP) comprising a multiple parameter determination method. This method integrated into the SDLC provides for evaluating the quality of software against a series of criteria. Through a four-stepped process consisting of design, quality burden, consistency, and feature testing [32]. Throughout this process criteria such as security, maintainability, compatibility, and efficiency are evaluated. During each stage of the process the software under development is given a rating and upon completion an overall consistency rating is calculated. This rating indicates the compliance of the software with the quality criteria [32].

VI. CONCLUSION & FUTURE WORK

In conclusion, the IoT has quickly become ubiquitous in critical applications. That ubiquity and criticality demands security. This survey study determined that when viewed through the lens of a simplified three-tier architecture the security failings in the IoT ecosystem may be reduced to just six (6) distinct common weaknesses. The survey found that in turn these six (6) weaknesses are exploited by four (4) common types of malicious attacks. Finally, the survey determined that four (4) common categories of techniques will mitigate the six (6) common IoT weaknesses and prevent the four (4) common types of attacks. Examples of these techniques were discussed.

The concepts presented are well supported by the surveyed literature. However, the rapid pace of development of the IoT ecosystem will most assuredly result in new yet unknown malicious attacks. These attacks will reveal new security failures in the IoT. As time advances new research is necessary to confirm the findings of this survey and identify new IoT security failures, malicious attacks, and mitigation techniques. Undoubtably the distilled set of failures, attacks and mitigations will expand.

ACKNOWLEDGMENT

The author wants to thank the faculty of Northern Arizona University including Professors Linda Hamons D.CS. and Dr. Rick Keeling for their guidance and support.

REFERENCES

[1] M. Ashton, "Debugging The Real World: Robust Criminal Prosecution In The Internet Of Things," *Ariz. Law Rev.*, vol. 59, no. 805, pp. 805–835, 2017, [Online]. Available: https://www.rt.com/usa/hacker-pacemaker-.

[2] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures," *IEEE Access*, vol. 7. Institute of Electrical and Electronics Engineers Inc., pp. 82721–82743, 2019, doi: 10.1109/ACCESS.2019.2924045.

[3] F. Meneghello, M. Calore, D. Zucchetto, M. Polese, and A. Zanella, "IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8182–8201, 2019, doi: 10.1109/JIOT.2019.2935189.

[4] M. O'Neill, "Insecurity by Design: Today's IoT Device Security Problem," *Engineering*, vol. 2, no. 1, pp. 48–49, Mar. 2016, doi: 10.1016/J.ENG.2016.01.014.

[5] A. N. Ozalp, Z. Albayrak, M. Cakmak, and E. Ozdogan, "Layer-based examination of cyber-attacks in IoT," 2022, doi: 10.1109/HORA55278.2022.9800047.

[6] M. Abomhara and G. M. Køien, "Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks," *J. Cyber Secur. Mobil.*, vol. 4, no. 1, pp. 65–88, Jan. 2015, doi: 10.13052/jcsm2245-

1439.414.

[7] M. R. Islam and K. M. Aktheruzzaman, "An Analysis of Cybersecurity Attacks against Internet of Things and Security Solutions," *J. Comput. Commun.*, vol. 08, no. 04, pp. 11–25, 2020, doi: 10.4236/jcc.2020.84002.

[8] T. Aziz and E. Haq, "Security Challenges Facing IoT Layers and its Protective Measures," *Int. J. Comput. Appl.*, vol. 179, no. 27, pp. 31–35, Mar. 2018, doi: 10.5120/ijca2018916607.

[9] P. Varga, S. Plosz, G. Soos, and C. Hegedus, "Security threats and issues in automation IoT," Jul. 2017, doi: 10.1109/WFCS.2017.7991968.

[10] I. Makhdoom, M. Abolhasan, J. Lipman, R. P. Liu, and W. Ni, "Anatomy of Threats to the Internet of Things," *IEEE Commun. Surv. Tutorials*, vol. 21, no. 2, pp. 1636–1675, 2019, doi: 10.1109/COMST.2018.2874978.

[11] W. Abbass, Z. Bakraouy, A. Baina, and M. Bellafkih, "Assessing the internet of things security risks," *J. Commun.*, vol. 14, no. 10, pp. 958–964, Oct. 2019, doi: 10.12720/jcm.14.10.958-964.

[12] S. A. Kumar, T. Vealey, and H. Srivastava, "Security in internet of things: Challenges, solutions and future directions," in *Proceedings of the Annual Hawaii International Conference on System Sciences*, 2016, vol. 2016-March, pp. 5772–5781, doi: 10.1109/HICSS.2016.714.

[13] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A Survey on Security and Privacy Issues in Internet-of-Things," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1250–1258, 2017, doi: 10.1109/JIOT.2017.2694844.

[14] I. Lee, "Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management," *Futur. Internet*, vol. 12, no. 9, p. 157, Sep. 2020, doi: 10.3390/FI12090157.

[15] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, "Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations," *IEEE Commun. Surv. Tutorials*, vol. 21, no. 3, pp. 2702–2733, 2019, doi: 10.1109/COMST.2019.2910750.

[16] I. Butun, P. Osterberg, and H. Song, "Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures," *IEEE Commun. Surv. Tutorials*, vol. 22, no. 1, pp. 616–644, 2020, doi: 10.1109/COMST.2019.2953364.

[17] N. M. Lobanchykova, I. A. Pilkevych, and O. Korchenko, "Analysis of attacks on components of IoT systems and cybersecurity technologies," in *CEUR Workshop Proceedings 2021*, 2021, pp. 83–96, [Online]. Available: http://www.kinf.ath.bielsko.pl/pl/oleksandr-korchenko.

[18] A. K. Pathak, S. Saguna, K. Mitra, and C. Ahlund, "Anomaly Detection using Machine Learning to Discover Sensor Tampering in IoT Systems," in *IEEE International Conference on Communications*, Jun. 2021, pp. 1–6, doi: 10.1109/ICC42927.2021.9500825.

[19] L. Damghani, H. Damghani, H. Hosseinisan, and R. Sharifi, "Classification of Attacks on IOT," in *4th International Conference on Combinatorics, Cryptography, Computer Science and Computing*, Nov. 2019, pp. 245–255, doi: 10.1142/9789812837042_0003.

[20] R. Smith, D. Palin, P. P. Ioulianou, V. G. Vassilakis, and S. F. Shahandashti, "Battery draining attacks against edge computing nodes in IoT networks," *Cyber-Physical Syst.*, vol. 6, no. 2, pp. 96–116, Apr. 2020, doi: 10.1080/23335777.2020.1716268.

[21] F. Hu, *Security and Privacy in Internet of Things (IoTs) Models, Algorithms, and Implementations*. CRC Press, 2016.

[22] R. Khader and D. Eleyan, "Survey of DoS/DDoS attacks in IoT," *Sustain. Eng. Innov.*, vol. 3, no. 1, pp. 23–28, Jan. 2021, doi: 10.37868/sei.v3i1.124.

[23] K. Sonar and H. Upadhyay, "A Survey: DDOS Attack on Internet of Things," 2014. [Online]. Available: www.ijerd.com.

[24] T. Sherasiya and H. Upadhyay, "Intrusion Detection System for Internet of Things," *Int. J. Comput. Sci. Eng.*, vol. 5, no. 2, pp. 91–98, 2016, [Online]. Available: www.ijariie.com2244.

[25] A. Tabassum and W. Lebda, "Security Framework for IOT Devices Against Cyber- Attacks," *arXiv*, vol. 1912, no. 01712, 2019.

[26] S. Gautam, A. Malik, N. Singh, and S. Kumar, "Recent Advances and Countermeasures against Various Attacks in IoT Environment," in *2nd International Conference on Signal Processing and Communication, ICSPC 2019 - Proceedings*, Mar. 2019, pp. 315–319, doi: 10.1109/ICSPC46172.2019.8976527.

[27] H. Tyagi and R. Kumar, "Cloud computing for IoT," in *Internet of Things (IoT): Concepts and Applications*, Springer International Publishing, 2020, p. 121.

[28] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and other botnets," *Computer (Long. Beach. Calif).*, vol. 50, no. 7, pp. 80–84, Jul. 2017, doi: 10.1109/MC.2017.201.

[29] H. Mrabet, S. Belguith, A. Alhomoud, and A. Jemai, "A survey of IoT security based on a layered architecture of sensing and data analysis," *Sensors (Switzerland)*, vol. 20, no. 13. MDPI AG, pp. 1–20, Jul. 01, 2020, doi: 10.3390/s20133625.

[30] A. K. Das, S. Zeadally, and D. He, "Taxonomy and analysis of security protocols for Internet of Things," *Futur. Gener. Comput. Syst.*, vol. 89, pp. 110–125, Dec. 2018, doi: 10.1016/j.future.2018.06.027.

[31] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, "Internet of Things: Security Vulnerabilities and Challenges," in *2015 IEEE symposium on computers and communication (ISCC)*, 2015, pp. 180–187.

[32] R. Temkar and A. Bhaskar, "Quality Assurance of IoT based Systems using Analytic Hierarchy Process," *Turkish J. Comput. Math. Educ.*, vol. 12, no. 10, pp. 6759–6767, 2021.

[33] M. Sirshar, M. Khan, K. Naeem, and T. Akbar, "Software Quality Assurance testing methodologies in IoT," no. December 2019, 2019, [Online]. Available: www.preprints.org.

[34] A. Bahaa, A. Abdelaziz, A. Sayed, L. Elfangary, and H. Fahmy, "Monitoring real time security attacks for IoT systems using devsecops: A systematic literature review," *Inf.*, vol. 12, no. 4, 2021, doi: 10.3390/info12040154.

[35] S. K. Choi, C. H. Yang, and J. Kwak, "System hardening and security monitoring for IoT devices to mitigate IoT security vulnerabilities and threats," *KSII Trans. Internet Inf. Syst.*, vol. 12, no. 2, pp. 906–918, Feb. 2018, doi: 10.3837/tiis.2018.02.022.

[36] M. Qabulio, Y. A. Malkani, and A. Keerio, "A framework for securing mobile wireless sensor networks against physical attacks," Oct. 2017, doi: 10.1109/ICET.2016.7813265.

[37] J. Cynthia, H. Parveen Sultana, M. N. Saroja, and J. Senthil, "Security Protocols for IoT," in *Ubiquitous computing and computing security of IOT*, vol. 47, Springer Science and Business Media Deutschland GmbH, 2019, pp. 1–28.

[38] K. T. Nguyen, M. Laurent, and N. Oualha, "Survey on secure communication protocols for the Internet of Things," *Ad Hoc Networks*, vol. 32, pp. 17–31, Sep. 2015, doi: 10.1016/j.adhoc.2015.01.006.

[39] T. Kothmayr, C. Schmitt, W. Hu, M. Brünig, and G. Carle, "DTLS based security and two-way authentication for the Internet of Things," *Ad Hoc Networks*, vol. 11, no. 8, pp. 2710–2723, Nov. 2013, doi: 10.1016/j.adhoc.2013.05.003.

[40] H. Shafagh, A. Hithnawi, A. Dröscher, S. Duquennoy, and W. Hu, "Talos: Encrypted query processing for the Internet of Things," in *SenSys 2015 - Proceedings of the 13th ACM Conference on Embedded Networked Sensor Systems*, 2015, pp. 197–210, doi: 10.1145/2809695.2809723.

[41] C. Zhang, Y. Zhang, and Y. Fang, "A Coverage Inference Protocol for Wireless Sensor Networks," *IEEE Trans. Mob. Comput.*, vol. 9, no. 6, pp. 850–864, 2010, doi: 10.1109/TMC.2010.29.

[42] A. Costin, A. Zarras, and A. Francillon, "Automated dynamic firmware analysis at scale: A case study on embedded web interfaces," in *ASIA CCS 2016 - Proceedings of the 11th ACM Asia Conference on Computer and Communications Security*, 2016, pp. 437–448, doi: 10.1145/2897845.2897900.