The Internet of Things: Architecture, Security Threats, and Risk Mitigation Techniques

Eric Samuel Brown *eric.brown@ubalt.edu*
Applied Information Technology
University of Baltimore
Baltimore, Maryland, USA

Mohammed Ketel *mketel@ubalt.edu*
Applied Information Technology
University of Baltimore
Baltimore, Maryland, USA

Abstract

Devices in the consumer, commercial, healthcare and industrial sectors are becoming increasingly more connected to the Internet. These interconnected devices range from smart devices in the home and wearable health monitoring devices to sensors and actuators within critical infrastructure environments. The framework of connected devices that share data is referred as the Internet of Things (IoT). There is an increasing security concern regarding this framework and devices that are considered part of IoT. As the number of devices that are able to send sensitive information over networks increases, so does the threat of this data being compromised. To mitigate and minimize this threat, research has been performed to develop a number of potential approaches to increase security levels for these IoT devices. This paper will present a few of those security risks and mitigations, as well as best practices to implement by administrators of IoT networks.

Keywords: Internet of Things, Architecture, Security, Mitigation, Best Practices.

1. INTRODUCTION

Since these initial developments of terminology and device connectivity, the number of connected IoT devices has grown exponentially with numbers into the billions worldwide. These devices, primarily hardware, range from smart home devices that provide home security or monitor and adjust heating and lighting [1, 2], commercial devices that manage inventory and share analytical data [1], wearable healthcare devices that monitor glucose or blood pressure levels [2, 3], and industrial devices such as smart meters (also known as AMI, advanced metering infrastructure) that provide energy consumption data to electrical generation and distribution companies [1, 2].

The primary functionality of these devices is the ability to exchange time-critical, analytical data and remotely control objects. Data within IoT can be shared over locally wired connections or Wi-Fi, and often times over wide-ranging areas simultaneously utilizing WAN infrastructure and cloud platforms [4].

Similarly, to other computing hardware and software with externally facing connections, the connectedness of IoT devices presents cyber-security risks that can affect the availability of critical devices. Additionally, developmental flaws, lack of security standards, and high complexity of proprietary technology within IoT promote vulnerabilities that can be exploited by attackers [4].

Due to the heterogeneity and the exponential growth of IoT devices it is not possible to use a single architecture. Also, due to the diversity of IoT applications and the different communication technologies involved in them, it is not feasible to use a common architecture.

Using diverse devices, technologies, and network protocols in an IoT solution presents one of the biggest architectural challenges for IoT. Security, automation, and orchestration must be maintained across all of the layers of the IoT architecture. A cohesive approach is also needed for the proper integration of these different technologies [5].

As technology continues to evolve, wireless technology enabled by Zigbee, Bluetooth, etc. is becoming more prevalent in IoT systems. Smartphones have also known as a huge success in the evolution of IoT since they are the first mobile devices with universal internet connection. Cloud computing has been evolving and continues to improve the process of storing, processing, and accessing information of IoT applications. For the future many things are moving toward being self-sufficient. Since the cost of wireless communications are decreasing it's been predicted that pretty soon everything will eventually be interconnected. As more people use smart things and smart phones, more data will be collected. This will cause them to be more prone to become vulnerable to security threats and access of private data [6].

An organization or company may need to determine how to manage and mitigate security and privacy risk for the sheer number of IoT devices. The security and privacy risk management and mitigation practices should apply to the device type and also to the device usage [4]. Best practices are also required for securing IoT.

2. RELATED WORK

In paper [1], the authors discussed major application domains impacted by IoT. These applications were classified based on network availability, scale, user involvement, etc. They reviewed key enabling technologies and presented a Cloud centric vision implementation of IoT. Paper [2] provided an overview of the integration of Cloud and IoT. The benefits, implementation challenges, architecture, and applications scenarios of this integration were also discussed. In addition, open research issues and future research directions were highlighted.

The characteristics of IoT devices include heterogeneity, massive scale, low cost design, resource scarcity, etc. These characteristics can cause limitations to security design and privacy. It is also easier to hack or compromise IoT devices than traditional information technology (IT) devices such as computers, laptops, etc. The purpose of [4] is to help organizations government agencies, and businesses understand, incorporate and manage cybersecurity and privacy into these IoT devices throughout their lifecycles. Risk mitigation recommendations and strategies that are important for organizations are also provided by [4]. In reference [16], ENISA provided a collection of good practices to ensure security of IoT in both Industry 4.0 and Smart Manufacturing domains.

As IoT continues to become increasingly popular there are still many challenges that come with it. One of the latest concerns with IoT is privacy. In paper [6], the authors proposed a few ideas that will alleviate privacy concerns. They came up with a privacy awareness model for IoT. They also provided a detailed analysis of the IoT evolution in regards to the features and technologies involved. And finally, they analyzed privacy threats and challenges in regards to the privacy awareness model. The paper also mentioned the privacy legislation and its impact on IoT. In [22], the authors reviewed and studied the privacy of IoT through the privacy laws principles and the representative privacy enhancing technologies (PETs). They also compared, analyzed, and evaluated the privacy requirements of these PETs at different IoT architecture layers.

Paper [7] provided an in-depth overview of IoT by introducing its different elements, architectures, enabling technologies, protocols and standards, and application domains. The paper also addressed IoT open issues in the context of security, privacy, performance, and management. As argued in [8], a complete understanding of IoT features and meaning was not provided by the three-layer architecture. Consequently, they established new five-layer architecture in the belief that this new architecture is more helpful to understand the basis of IoT and its development.

Paper [9] discussed the challenges pertaining to IoT focusing on issues within the conceptual layers. Each layer is vulnerable to threats and attacks. The authors think that for the future we need to have better protocols, guidelines, identity management, and more session layers to keep up with users' demands. The authors also believe that we are focusing too much on certain parts of the IoT protocol while we should be incorporating newer protocols in order to minimize security threats.

Many technologies have been developed to support wireless networking including Bluetooth, Wi-Fi, RFID, etc. Paper [10] reviewed the popular wireless connectivity technologies operating in the license free industrial, scientific and medical (ISM) band. They discussed their important technical concepts and provided guidelines for choosing the appropriate wireless technology for different IoT applications. Paper [11] explored the key characteristics of the IEEE 802.11ah standard and showed the importance of this standard of in supporting different IoT applications.

In paper [12], the authors presented the limitations of IoT devices and discussed possible solutions to these problems. They also studied IoT security attacks and countermeasures. Then, they analyzed the security issues at various layers of the IoT architecture. Paper [13] provided a comprehensive list of vulnerabilities and possible countermeasures across the different layers of the IoT architecture.

3. IOT ARCHITECTURE COMPONENTS

The basic architecture of an IoT system consists of three tiers: IoT end devices, gateway/communication network, and the cloud [2, 5]. Figure 1 illustrates the three-tiers architecture.

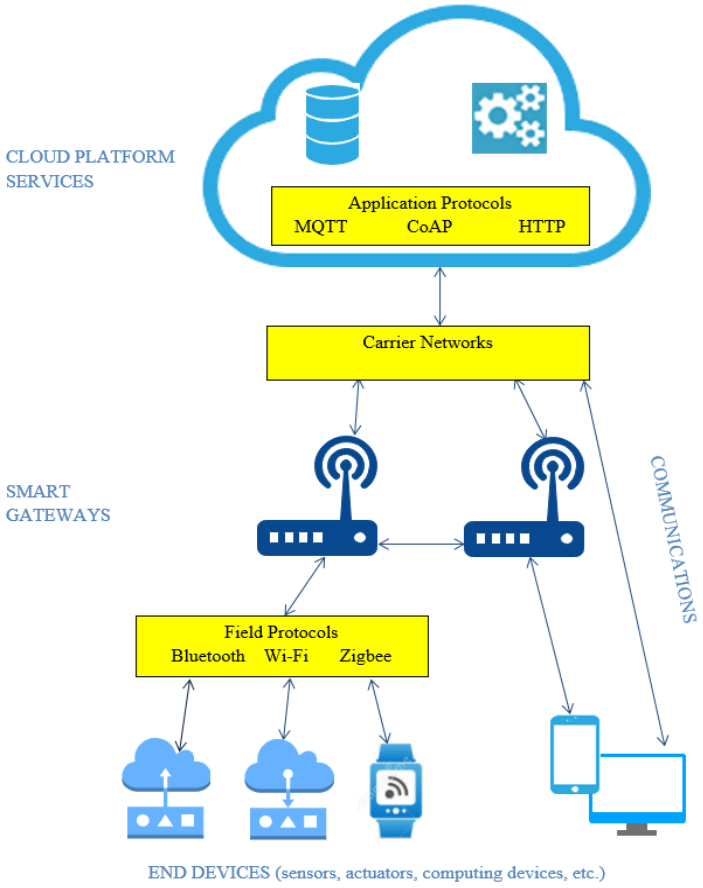

FIGURE 1: IoT Architecture Components.

3.1 Devices

IoT end (edge) devices are highly diverse and have different computing, communication, and storage capabilities. These devices are equipped with sensors and actuators that enable them to interact and act upon a real- world environment. Sensors are responsible for sensing, observing, measuring changes, or detecting events in a physical environment and converting these into information [1, 2, 5]. Changes to the environment are performed by the actuators in response to the instructions and feedback coming from the upper layers of the IoT system. Information is typically transmitted from these devices over wireless network technologies such as Bluetooth 5, Zigbee, Wi-Fi, Cellular, etc. For limited resource devices, it is common to pass that information through an IoT gateway that has relatively more processing power [5].

3.2 Gateway

Some resource limited edge devices cannot connect directly to the cloud and an IoT gateway is required in such situations. The gateway acts as a protocol translator and manages the data transmission between different wireless network technologies that are part of an IoT system. Gateways also provide functionality, such as data pre-processing, real-time processing, and secure connectivity to the cloud [2, 5].

3.3 Cloud

Devices and applications in an IoT system generate massive data. The Cloud computing platform is an important entity in IoT and offers off-site high-speed processing and vast storage capacity at a low cost to this huge amount of data [1, 4]. The cloud is also responsible for data analytics to derive useful insights. Data analytics provide industries and end users applications useful business information and help companies make critical decisions when necessary [1, 2, 5].

4. IOT: LAYERD ARCHITECTURES

The architecture describes the structure of the physical, communication, services, and storage aspects of an IoT solution. To ease the management of complex IoT systems, modular approaches are used to divide the architecture into multiple tiers and focus on each tier independently [2, 5]. The details and guidelines provided by the architecture are usually specific to an IoT application domain, such as industrial, energy, smart city, healthcare, etc.

Researchers have proposed various IoT architectures and over time. Enhancements and security concerns have challenged IoT researchers to implement extra and improved layers over time.

4.1 Three-Layer Architecture

The earliest and most basic is the three-layer architecture made up of the perception, network, and application layer, Figure 2.

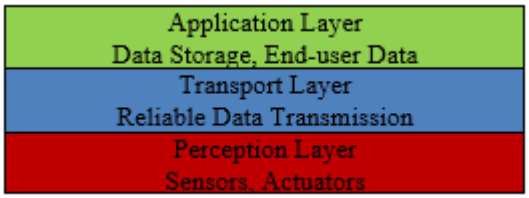

FIGURE 2: Three-Layer IoT Architecture.

- Perception Layer

The perception layer is also known as the sensor layer or the recognition layer [5, 7, 8]. This layer contains the physical sensors and actuators, the devices that perform “sensing”. These devices produce the data from environments such as pressure changes, temperature changes, vibration,

video surveillance, motion, etc. The devices in the perception layer pass data onto the network layer via wired or wireless transmission mediums.

- Network layer

Also known as the transmission layer, this layer is responsible for the reliable transmission of collected data from devices in the perception layer up to the application layer.

- Application Layer

The application layer, or often called the service layer, is where data is stored, processed, and delivered as IoT applications or services to end-users. Applications such as health monitoring, smart home devices, logistics trackers, or energy management systems belong to this layer [7, 8].

4.2 Four-Layer Architecture

As argued in [8], the three-layer architecture does not provide a complete understanding of IoT features and meaning. Another potential hole is security. Because most of the IoT devices are small and not running on low power systems, there is not a lot of room for encryption and security. These devices are vulnerable for many different types of attacks which leave personal data on the front line to be hacked.

Due to development in IoT and the advancement of security threats, researchers developed an added layer to the architecture. The support layer was added between the network and application layer to implement user authentication for security, Quality of Service (QoS) management, and pre-processing of data, Figure 3 [7].

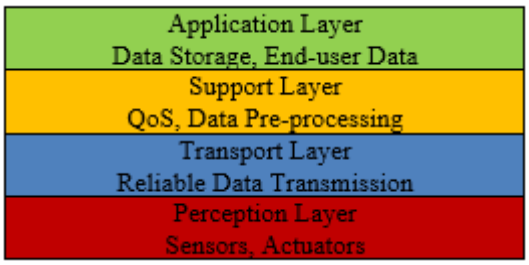

FIGURE 3: Four-Layer IoT Architecture.

4.3 Five-Layer Architecture

Due to challenges with security and storage, a five-layer architecture was developed to improve previous models, Figure 3. This architecture renames the network layer to the transport layer. Additionally, the transport layer has been renamed to the processing layer and an additional layer has been added above the application layer, the business layer [7, 8].

- Transport Layer

Similar to the network layer, the transport layer processes data from the perception or processing layers by use of wired LAN interfaces or wireless interfaces like Wi-Fi, ZigBee, or Bluetooth.

- Processing Layer

The processing layer is also known as the middleware layer. This layer provides in-depth processing and storage for data coming from the transport layer before passing it to the application layer.

- Business Layer

The business layer resides above the application layer and provides IoT device management, user privacy and, data analysis. Data pushed up the IoT architecture can be utilized in this layer for analytical purposes such as business models [8]. Figure 4 illustrates the five-layer IoT architecture.

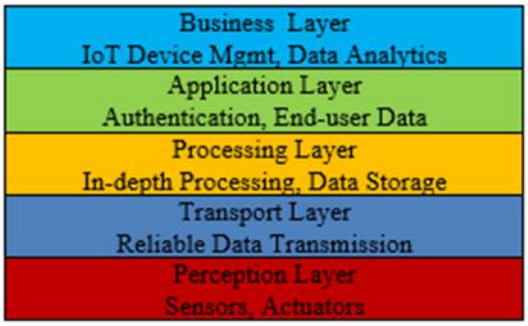

FIGURE 4: Five-Layer IoT Architecture.

Because different companies make different devices for IoT, there is no such architecture that all these companies utilize, but there is a basis of one from which these companies can use.

Each layer is vulnerable to threats and attacks [9]. Some threats in the perception layer consist of wireless signal strengths, which can be compromised by disturbing waves. Another threat is physical attacks since IoT nodes are located in the environment they can be tampered with. Traffic analysis and the diversity of network components/protocols have been security concerns within the network layer. The diversity of components allows devices to become vulnerable to DoS attacks and it also allows for manipulation of the devices. The application layer lacks policies and standards regarding the interaction and development of applications [9].

5. IOT PROTOCOLS AND COMMUNICATION TECHNOLOGIES

The different and diverse network technologies enable IoT devices to communicate with applications, cloud services, and other devices. These technologies rely on standardized protocols to ensure a reliable and secure communication between diverse devices. Numerous new and competing networking technologies from different vendors are being incorporated into the IoT system.

There are two types of IoT devices. The first type connects directly to the Internet through the complex IP suite that requires a large amount of memory and power from the device. The second type can use non-IP protocols designed for low power consumption and connect to the Internet via a smart gateway [10].

IoT network technologies are typically structured into three basic layers [5]; the Application, the Internet, and the Physical/Access Layers, as shown in Figure 5.

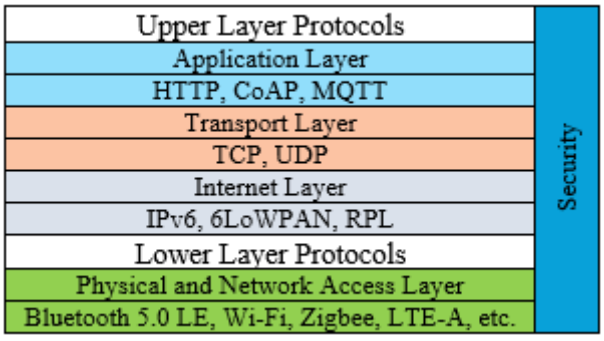

FIGURE 5: IoT Network Technologies.

5.1 IoT Network Technologies: Application Layer

Existing protocols, such as HTTP/HTTPS, are pervasive over internet applications and are important for many devices. However, the overhead of HTTP/HTTPS and some other traditional Internet protocols can be a problem for small IoT devices in terms of memory size and power requirements. Other small, simple and binary protocols are needed to meet these requirements. There are multiple application-layer protocols optimized for IoT use. The most well-known potential protocols include Message Queue Telemetry Transport (MQTT) and the Constrained Application Protocol (CoAP).

- MQTT

The MQTT protocol follows an asynchronous publish-subscribe and uses the TCP protocol for reliable packet transmissions. It is a many-to-many communication protocol that involves many constraints clients and a central broker that manages and controls the exchange of packets between clients [7]. With MQTT, it is easy to use TLS and use modern authentication protocols to authenticate clients. For mission-critical communications MQTT can guarantee message delivery and ensure quality of service. One disadvantage of MQTT is packet retransmissions in poor network environment that can cause network congestions [7].

- CoAP

CoAP is an application protocol based on the REST model and runs over the UDP transport protocol. It is tailored for IoT devices where power, memory, and computing resources are limited. It is also designed for low-power networks that exhibit high/variable data loss, low data rates, and lossy communication links. CoAP is designed to easily interoperate with HTTP through a proxy and shares the GET, PUT, POST, and DELETE methods similar to HTTP. For CoAP, the Datagram Transport Layer Security (DTLS) that supports AES and RSA is used to provide the assurance and security for data transfer over UDP [7].

5.2 IoT Network Technologies: Internet Layer

Internet layer technologies provide the identification and routing of the data packets. The commonly used IoT technologies at this layer include IPv6, RPL, and 6LoWPAN.

- RPL

RPL is designed to provide IPv6 connectivity to resource-scarce devices lacking the support of normal routing. It is designed as a distance vector routing protocol and supports simple and complex traffic models [7]. RPL offers flexibility and proactive construction of a topology that is organized as one or more Destination Oriented Direct Acyclic Graph (DODAG). This graph is maintained by a series of information messages that gather advertisements and node rankings that goes out to each node [7]. The security measures provided by RPL include data integrity/ confidentiality and self-healing methods to guarantee appropriate network operations.

- 6LoWPAN

6LoWPAN is a simple low-cost network protocol suitable for many IoT applications. It supports the application of IPv6 to resource-scarce devices characterized by low power, , low memory usage, low bit rate, short range, and limited computational power. 6LoWPAN uses compression techniques to reduce IP overhead and thus enable efficient flow of IPv6 datagrams over constrained communication links. Lightweight model like AES-128 link layer security can be used to provide encryption and authentication [7].

5.3 IoT Network Technologies: Physical and Network Access Layer

There are numerous communication technologies at the physical and the network access layer available for IoT applications. The more frequently used technologies for IoT utilization are summarized below:

- Zigbee

Zigbee is a commonly used wireless IoT communication protocol developed by ZigBee Alliance. Zigbee supports reliable, medium-range communications for use in smart homes, hospitals,

HVAC, and security. ZigBee is particularly useful for low memory and low processing applications. Zigbee provides security capability using 128-bit keys for symmetric encryption. Symmetric-Key Key Establishment (SKKE) protocol is utilized for this key exchange [10, 11].

- Bluetooth 5.0 LE

Bluetooth is another short-range wireless standard for IoT applications. The most recent version of the Low Energy (LE) version of Bluetooth is 5.0, released in 2018. Bluetooth 5.0 LE uses connectionless data transfer which it optimal for low-power devices (i.e. battery-powered) that transfer small amounts of data. The most recent version, 5.0, increases the speed of communication between IoT devices to a data-rate of 2 Mbps.

Additionally, 5.0 offers a “long-range mode” that utilizes Forward Error Correction (FEC) to recover data due to transfer errors. This long-range mode can extend ranges as far as 800 meters, line-of-site. One trade-off in the extended range is reduced data transfer speeds and higher power consumption [10, 11].

- RF Links

Radio frequency (RF) links are a method of allowing IoT communication via radio waves. Depending on the type of RF equipment used for transmission, a range of possible communication is between 100m and 1km.

IoT uses Radio frequency identification system (RFID) to identify and track IoT objects consisting of RFID tags and readers. The tags contain data about the device or process that are queried by readers, or transceivers, through an RF interface, which is then passed onto an IoT application [11].

RFID technology supports the use of symmetric key encryption, using standards ciphers such as AES and DES. AES is a better suited encryption implementation as it is a faster and less taxing on some RFID applications. However, there exists a lightweight version of DES, DESL (DES light).

- Wireless Fidelity (Wi-Fi)

Wi-Fi, or IEEE 802.11x standards, are commonly used for IoT devices communication. The original IEEE 802.11 standards, however, are not optimal for IoT applications due to higher power consumption, coverage range, and number of supported devices supported. IEEE 802.11ah standard (also referred to as Wi-Di HaLow) allows for coverage range up to 1.5 km, as opposed to a few hundred meters, and can support up to 8000 associated stations per access point (AP) versus 2007 in legacy IEEE 802.11 versions [10, 11].

In addition to the increased performance IEEE 802.11ah provides Wi-Fi IoT devices, 802.11ah supports the newest Wi-Fi Protected Access (WPA), or IEEE 802.11i, WPA3. WPA3 uses equivalent 192-bit cryptographic encryption AES-GCM-256 for enterprise mode and AES-CCM-128 for personal mode.

- LTE-A

Long-term Evolution (LTE) is the standard for high-speed wireless communication for mobile phones and data terminals. This cellular communication provides a solution for long-range data transfers and low latency. More recent versions of LTE (i.e. Cat 0, Cat 1, Cat M1, Cat NB1) can provide lower power, low throughput cellular communications for IoT devices used in smart metering, asset tracking, and health monitoring.

- WirelessHART

Wireless Highway Addressable Remote Transducer (HART) protocol is defined in IEE 802.15.4, a standard for Personal Area Networks (PAN), similar to Zigbee. Wireless HART is designed for industrial environments with high-level electromagnetic interference such as process automation spaces and is intended for low-frequency information updates over a range of tens of meters [10].

One of the major challenges with IoT is to make sure that communication networks are secure. IoT communication channels are vulnerable to several attacks and threats such as routing attacks, where a malicious node tries to redirect the routing path during data transit; DDoS attacks aimed to flood the target servers with a large number of unwanted requests; access attack: in which an unauthorized adversary gains access to the IoT network with the purpose to steal information or data rather than to cause damage to the network. So proper security measures are required to combat or mitigate such attacks and threats.

6. IOT SECURITY RISKS

IoT devices are generally insecure due to a myriad of challenges from development to implementation [12, 13]. While there are numerous proposed IoT architectures, there is currently no overarching standard in place for the IoT framework and comparatively to standards such as the OSI model for networking or Purdue Reference Model for developing Operational Technology (OT) architecture and therefore there is a lack of security requirements and best practices fulfilled during development of devices. A standard IoT security model would allow for increased homogenization of devices, simultaneously implementing secure frameworks and protocols into the design and promoting interoperability between devices that are often built with competing and proprietary software [14].

IoT hardware often contains vulnerable components and due to the complexity of the IoT hardware supply chain, it is challenging to track the source or level of product security built in.

IoT devices are also constrained by their hardware capabilities due to their generally small form-factor, the need to conserve power, and to minimize the cost of components. These hardware constraints also limit the ability to handle taxing processing that occurs with traditional secure web protocols and encryption [15].

Due to IoT devices often being remotely located from the enterprise environment, applying security updates can be challenging for an organization. IoT devices are also often wireless and require updates sent over-the-air which makes them vulnerable to Man-in-the-Middle attacks. Additionally, IoT devices that are required for high-availability environments may not receive updates for long periods of time and are only updated during scheduled downtime or maintenance, therefore vulnerabilities remain for an indefinite timeframe [16]. Organizations may also choose not to update IoT software or firmware due to the lack of expected behavior after the updates have been applied. There is uncertainty if an update will be compatible with current device setup and configuration.

7. SECURITY MITIGATIONS

There is no “silver bullet”, or single solution that when used, will completely protect IoT networks and their devices. A common technique in both IT and OT environments is to use defense-in-depth strategy. This strategy implements multiple security mechanisms that minimize the impact of an attack since a breach or exploit of one still requires an attacker to bypass other measures in place [17]. The following sections will discuss some of those measures that can create a strong defense-in-depth strategy in IoT environments.

7.1 Network Segmentation

Proper network segmentation is critical to prevent attackers from easily maneuvering through IoT networks by using lateral movement techniques through a flat network. Network segmentation can also prevent commodity or focused malware attacks from propagating easily from the corporate/enterprise environment down into the perception layer onto critical IoT devices.

A common way of implementing segmentation is logically separating devices using VLANs based on functionality or how critical devices are to business operations [18].

Using a Demilitarized Zone (DMZ) can re-duce the risk of so-called “wormable” malware from impact IoT devices. The DMZ sits between the Enterprise network and the IoT devices with firewalls between zones, Figure 6. Firewall rules should be put in place that minimizes unfettered traffic between zones.

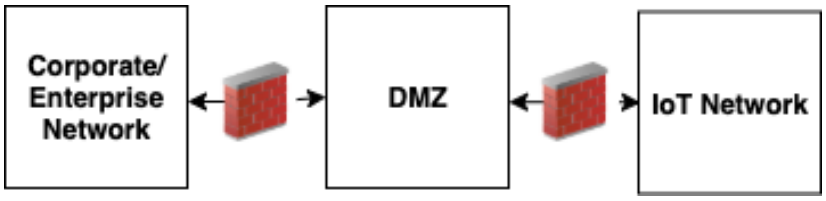

FIGURE 6: IoT Demilitarized Zone.

7.2 Patching

As security vulnerabilities are found in device software or firmware, vendors will release patches to mitigate the known security issues. It is important that the vendors collaborate with asset owners in order to properly implement patching solutions. Since the uptime of many IoT devices is critical, patches must be tested to determine if they are compatible with current configurations and won’t interfere with current processes and functionalities [19].

Another approach to test updates is to gradually deploy patches to small group of IoT devices whether inside a lab environment or is a non-critical section of the IoT network. Once any patches have passed testing requirements, then patches should be pushed to devices at a larger scale.

Patching updates for software and firm-ware must also be authenticated to ensure that they are downloaded from a known and trusted source [20] using block cipher such as Advanced Encryption Standard (AES) [12]. The Public Key Infrastructure can be utilized with asymmetric encryption algorithms for Rivest-Shamir-Adelman (RSA) for key transport or Diffie-Hellman (DH) for key agreement. Additionally, MD5, SHA1, or SHA256 hash algorithms can be used to ensure that updates maintained their integrity during transit [12, 13].

7.3 Access Control

Implementing physical and networked access control across IoT devices also will decrease the potential attack surface of an IoT infrastructure. Where possible, IoT endpoints such as sensors & actuators, IoT controllers such as Real-time Automation Controllers (RTACs) & programmable logic controllers (PLCs), and IoT networking devices like switches and routers should have physical security measures in place to prevent tampering. Devices can be put in cabinets with locks to deter unauthorized access. IoT controllers often have physical keys that prevent any change to their CPU state (i.e. Run, Stop, Prog). Any open and unused RJ-45 or USB ports in networking devices should be disabled via BIOS or have port blockers to deter tampering and indicate if they have been tampered with. Any physical access should to these devices should also be logged and monitored.

Networking access control should also be put in place to prevent any unauthorized access from external entities and to limit the access from users in the internal enterprise. Access Control Lists (ACLs) should be implemented to ensure users are able to access only the endpoints and services that are necessary for their role. This strategy is also known as the Principle of Least Privilege; only providing users the authority to access the minimal amount of resources required such as limiting what endpoints or subnets that a user can access or preventing write privileges to all or particular files.

Administrators should also perform whitelisting in their IoT network. Whitelisting is the practice of identifying which applications, protocols, users, etc. are approved and expected in their IoT network communication. Insecure proto-cols (i.e. HTTP, Telnet, SMBv1, SNMPv1) that currently

exist in communication need to be vetted to ensure if they are absolutely necessary, and if not, should be restricted within ACLs in gateways or firewalls [13].

7.4 Authentication Mechanisms

Authentication mechanisms will also assist in hardening the security posture of an enterprise IoT infrastructure. One of the low-hanging fruit that administrators can use to increase security on IoT devices is to change the default credentials on any management hardware or software during provisioning. Other mechanisms include the use of Multi-factor Authentication (MFA), session timeouts, and lockout functions.

MFA, often referred to as two-factor authentication (2FA), is a method of authentication that uses more than one credential to identify a user. This is typically a one more of the following: something the user has (card or fob), something the user knows (password or PIN), and something the user is (biometrics) [21]. For example, a user must have a password to login to and IoT device management interface then validate with a PIN sent to their smartphone. This is useful in mitigating security risk by requiring an attacker to obtain more than just username and password to gain access.

Session timeouts and lockout functions can also limit the attack surface in IoT environments. Enterprise employee or vendor access using VPNs or otherwise should be limited by sessions. This can be implemented in time window intervals or timeout due to inactivity, which will prevent an attacker from hijacking a session for unfettered access. Lockout procedures should also be put in place after a certain number of incorrect logins.

8. IOT BEST PRACTICES

While eliminating all cybersecurity risk in IoT devices with technological safeguards is not reasonably attainable, implementing security mitigations with IoT best practices reinforces a defense-in-depth strategy to even further reduce an organization's attack surface.

8.1 Security-by-Design

IoT ware (hardware, software, and middleware) should be developed with a "Security by Design" mindset. IoT cybersecurity should be implemented into the device design using a "smart manufacturing system development lifecycle [16]." A system development lifecycle with a security focus offers valuable safeguards for organizations implementing IoT & smart devices into their environments:

1. Security vulnerabilities are identified early and are more easily mitigated and at lower costs than if discovered after implementation.
2. A broad understanding of the challenges and financial and human resources required to implement security controls.
3. Effective and failed techniques for implementing security controls are realized throughout each SDLC, reducing cost and improving the efficiency of later cycles.
4. System interoperability is improved by considering security controls at multiple stages in the development cycle.

In addition to using a Security SDLC internally, organizations should consider risk and security analysis be performed by third-party companies during development and design stages [16].

8.2 Data Privacy

Organizations that use IoT devices should be thoughtful of how they implement data privacy with the IoT devices in their environment. Firstly, the organization should define what data is processed by these devices during the design phase of any project that introduces new networked hardware in their business. There should be decisions made to define what data is sensitive to the client, the organization, or the process running on the devices. Data encryption should be considered and an evaluation on where it can be used and the effects that would occur

on latency to any critical processes. Sensitive data send between these de-vices should be stored at and encrypted at-rest externally to these devices, as possible. Addition-ally, any data that contains Personally Identifiable Information (PII) should be stored separately from other data [22].

8.3 Asset Management

Asset management is also integral into maintaining a secure IoT environment. Performing periodic asset inventory at regular intervals can also prove advantageous for an organization. Since IoT devices are often remotely located from the enterprise environment, it is suggested that organizations use a tool to dynamically discover, identify, and enumerate IoT assets in their environment. Secure management of IoT devices should also be considered, using VPN for access from only authorized users [16].

8.4 Device Security Settings

To secure IoT devices, their Confidentiality, Integrity, and Availability must be protected (typical CIA security requirements). In other words, their information should only be accessible to those with authorization, it should be consistent and accurate, and it should be accessible whenever it is needed [9]. Security needs to come embedded in devices and not be an add-on. Security must also be user-friendly, so device owners can configure privacy and security settings. Users should be made aware of the risks and be provided with the tools necessary to protect their devices. For instance, one type of common attack is possible because users fail to change the default identification. Hackers can then scan for open ports and run default authentication combinations until they are able to access the device [7, 9].

9. CONCLUSION

As the number of connected devices continues to grow and technologies created to facilitate these devices are introduced, researchers and practitioners will continually face the challenge of securing these devices and their sensitive data flows. This paper presented a few of those security risks and mitigations, as well as best practices to implement by administrators of IoT networks. Although there exists a rapid increase and popularity of IoT devices and technology, many of the same defensive strategies from traditional enterprise networks apply.

10. REFERENCES

[1] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of Things (IoT): A vision, architectural elements, and future directions,” Elsevier, Future Generation Computer Systems Volume 29, Issue 7, pp. 1645-1660, 2013.

[2] J H. Atlam, A. Alenezi, A. Alharthi, R. Walters, and G. Wills, “Integration of Cloud Computing with Internet of Things: Challenges and Open Issues,” 2017 IEEE International Conference on Internet of Things (iThings), pp. 670 – 675, 2017.

[3] S. Baker, W. Xiang, and I. Atkinso, “Internet of Things for Smart Healthcare: Technologies, Challenges, and Opportunities,” IEEE Access, Volume 5, pp. 26521 – 26544, 2017.

[4] K. Boeckl, et al, “Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks” National Institute of Standards and Technology (NIST), Internal Report NISTIR 8228, June 2019.

[5] A. Gerber, and S. Kansal “Simplify the development of your IoT solutions with IoT architectures,” https://developer.ibm.com/articles/iot-lp201-iot-architectures [Accessed March 30, 2020].

[6] J. Ziegeldorf, O. Morchon, and K. Wehrle , “Privacy in the Internet of Things: threats and challenges,” Security and Communication Networks, John Wiley & Sons, pp. 2728–2742, 2014.

[7] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, “Internet of Things: A Survey on Enabling Technologies, Protocols and Applications,” IEEE Communications Surveys & Tutorials, pp. 2347 - 2376, 2015.

[8] M. Wu, TJ. Lu, FY. Ling, J. Sun, and HY. Du, “Research on the architecture of Internet of Things,” IEEE 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), 2010.

[9] T. Yousuf, R. Mahmoud, F. Aloul, and I. Zualkernan, “Internet of Things (IoT) Security: Current Status, Challenges and Countermeasures,” International Journal for Information Security Research (IJISR), Volume 5, Issue 4, pp. 608- 616, 2015.

[10] N. Lethaby, “Wireless connectivity for the Internet of Things: One size does not fit all,” Texas Instruments (TI), pp. 6 – 12, 2017.

[11] V. Baños-Gonzalez, MS Afaqui, E. Lopez-Aguilera, and E. Garcia-Villegas, “IEEE 802.11ah: A Technology to Face the IoT Challenge,” MDPI, Sensors, pp. 1 -21, 2016.

[12] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, “A Survey on Security and Privacy Issues in Internet-of-Things,” IEEE Internet of Things Journal, Volume 4, Issue 5, pp. 1250 – 1258, 2017.

[13] AM. Nia, and NK. Jha, “A Comprehensive Study of Security of Internet-of-Things,” IEEE Transactions on Emerging Topics in Computing 5 (4), 1-19, 2016.

[14] A. Banafa, “Three Major Challenges Facing IoT,” IEEE IoT Newsletter, https://iot.ieee.org/newsletter/march-2017/three-major-challenges-facing-iot [Accessed November 5, 2019].

[15] S. Singh, PK. Sharma, SY. Moon and JH. Park, “Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions,” Springer, Journal of Ambient Intelligence and Humanized Computing, 2017.

[16] ENISA, “Good Practices for Security of Internet of Things in the context of Smart Manufacturing” November 2018.

[17] S. Wang, R. Shumba, and W. Kelly, “Security by Design: Defense-in-Depth IoT Architecture”, Journal of The Colloquium for Information System Security Education (CISSE), Edition 4, Issue 2, pp. 2 - 9, 2017.

[18] E. Fernandez, N. Yoshioka, and H. Washizaki, “Abstract and IoT security patterns for network segmentation”, 2019. Procs. Asian PLoP'19, 2019.

[19] OTA, “IoT Security Upgradeability and Patching”, (OTA) Online Trust Alliance, U.S. Department of Commerce and National Telecommunications & Information Administration, 2016.

[20] L. Shade, “Implementing Secure Remote Firmware Updates”, Embedded Systems Conference Silicon Valley 2011, pp. 1 – 18, 2011.

[21] NIST, Back to basics: Multi-factor authentication (MFA) https://www.nist.gov/itl/applied-cybersecurity/tig/back-basics-multi-factor-authentication. [Accessed December 18, 2019].

[22] C. Li and B. Palanisamy, “Privacy in Internet of Things: from Principles to Technology”, IEEE Internet of Things Journal, pp. 1-15, 2019.