I. J. Computer Network and Information Security, **2019, 4, 1-8**
Published Online April 2019 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2019.04.01

IoT: Application Protocols and Security

Derek Johnson
University of Baltimore, Baltimore, MD, USA
E-mail: Derek.Johnson@ubalt.edu

Mohammed Ketel
University of Baltimore, Baltimore, MD, USA
E-mail: MKetel@ubalt.edu

Received: 14 February 2019; Accepted: 29 February 2019; Published: 08 April 2019

Abstract—The Internet of Things (IoT) commands an ever-growing population of devices across the nation and abroad. The development of privacy concerns and security goals have not kept pace with the demand for new advances in IoT. We will discuss how the IoT currently functions and why the security in this field is important as the technology grows into every device we touch. This paper will also reference current security implementations and how they expect to cover this growing consumer demand for instant data on many devices at once. With IoT devices using less power and smaller processors, there is major discussion in the computing world on what methods succeed. As standard encryption methods are simply too much for small, low power devices to handle; IoT specific security methods should be highlighted.

Index Terms—Internet of Things, Cloud Computing, Security, Privacy, Encryption, Wireless, Mobile.

I. Introduction

Never before has the world been so interconnected. An average person today could walk with a wireless network of devices on their person, each one standalone or interconnected through a personal area network to the internet. While you are out shopping, this network could access a smart refrigerator to check if you need certain foods at home before returning. While at that store, they could get a notification on any one of their devices that a person has rung their doorbell at home. That doorbell system could then stream video and audio of the visitor to you many miles away so you don't miss them. On your way back, a GPS system could interface with many other connected smart phones on the road to determine if there are any traffic blockages. At the same time, their smart devices are using sensors to collect biometric history to better serve that user in the future. Their doctor could even gain access to this biometric data on their own time to have a more accurate picture into their patients' life and health. These personal devices are part of a new wave of technology called the Internet of things (IoT). The IoT is what the community currently defines to be an internetworking of sensors, devices, vehicles, and buildings that share information with each other [3]. Global web traffic through these devices was predicted by Cisco to reach 49 Exabytes of traffic by 2021, contrast to 2018s 17 Exabytes [1]. That is not surprising considering how many services could be running on each device, each one providing a specific service or subscription the user has requested to use. The concept that even buildings are interwoven into the IoT is new to most. Sensors connected to the internet that are low-cost and low power are making great strides in how the public can see data about their world. To visualize a model of how IoT can function, see the system model in Figure 1.

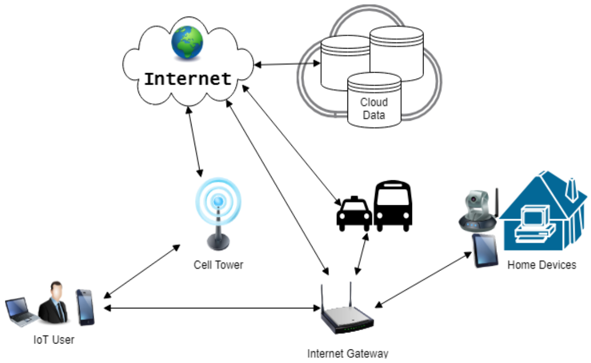


Fig.1. IoT Model

With this variety of services and devices all running in tandem, talking to each other with impunity, we are coming to a point where the current level of security is no longer adequate. In 2016, we see 325 million wearable wireless devices alone which is estimated to explode to 929 million by 2021 [1]. Wi-fi hotspots are growing as well. 2021 also sees the realization of an estimated 526.2 million hotspots that will be available to bear the weight of this device growth; Up from a paltry 96 million in 2016 [1]. This device growth includes many different manufacturers using different technologies that will have the ability to interface with each other through these vast sea of IoT devices. With that many devices, the odds appear to favor a security risk that will eventually arise. In such a large install base of devices, even one breach will be difficult to track without an in-depth investigation to analyze the issues at large. Without proper methodology and best practices in place, it only seems to be a matter of time. As existing network security protocols were not built with billions of interconnected devices in mind, IoT is a monster system to deal with for any security expert developing solutions [3].

II. Related Work

The authors of paper [5] provided a thorough overview of the concept of IoT. They presented the technical details of IoT key enabling technologies, protocols, standards, and major applications. The authors discussed the cooperative interaction between IoT and other emerging technologies such as cloud and fog computing. They also presented some application-use cases to demonstrate how these protocols function together to give the required IoT services. Finally, they highlighted possible research opportunities and future directions in this field.

IoT devices usually require lightweight security protocols. The authors in paper [2] discussed in some details lightweight cryptographic primitives and security architecture for low-resource devices in IoT environments. They also presented and analyzed several lightweight cryptographic algorithms. In paper [11], the authors proposed and analyzed a lightweight mutual authentication protocol based on a novel public key encryption scheme that is suitable for IoT devices.

Security is an important factor in IoT. In paper [3], the authors provided a survey and classification on current IoT security challenges and proposed a roadmap for future research. The authors of paper [4] presented a survey of the security issues of the main IoT frameworks. They also conducted a comparative analysis of these frameworks based on the hardware compatibility, software requirements, architecture, and security.

To guarantee packet delivery over the network without using TCP, Constrained Application Protocol (CoAP) uses Datagram Transport Layer Security (DTLS) as a building block. In paper [8], the authors presented a collaboration of DTLS and CoAP for IoT and proposed a DTLS header compression scheme to help reduce the packet size and energy consumption. The aim of paper [10] is to explain the integration the DTLS and CoAP and the use of Elliptic Curve Cryptography (ECC) optimization techniques to minimize computational overhead.

The focus of paper [15] was on the integration of cloud computing and IoT. The authors provided literature survey on the integration of these two technologies. They also identified open issues and future directions in this field. In paper [6], the authors considered the use of cloud technology for IoT. The focus of the paper was on security considerations for IoT from the perspectives of cloud providers, cloud tenants, and end-users.

III. IoT Protocols

When dealing with a new interconnected system like the IoT, a number of groups have found that they need to collaborate and help define what common points or methods the system should use. The Institute of Electrical and Electronics Engineers (IEEE), the European Telecommunications Standards Institute (ETSI), the World Wide Web Consortium (W3C), and the Internet Engineering Task Force (IETF) all have pitched in to standardize the IoT framework that is in use and still changing today [5]. With a variety of technologies at their disposal, it is important to define these standards to set a platform on which to grow.

A. Application Protocols

The main four categories are as follows: Application protocols, Service Discovery Protocols, Infrastructure Protocols, and Influential protocols [5]. This framework those groups mentioned earlier established mixes many important standard protocols. One being CoAP (Constrained Application Protocols) which, at the application layer, helps IoT devices maintain a connection over UDP. While TCP connections are important for security in their own right, UDP currently grants a connection type that meets low power requirements necessary for IoT devices [5]. To guarantee packet delivery over the network without using TCP, CoAP uses DTLS (Datagram Transport Layer Security) as a building block. DTLS is what secure CoAP is built on [3, 5, 8, 10]. Because of this, it can easily transport messages over lossy UDP connections and can still guarantee packets. With Mobile devices mainly using UDP as a source for internet, a secure resource saving protocol like CoAP is necessary. REST (Representational State Transfer) protocol is a similar model but runs on TCP which does not favor IoT device needs for low power communication types. REST and CoAP are similar enough however to where proxy communication between the two would work [5]. CoAP is just one of seven currently defined protocols that are used today. These protocols provide different ways to accomplish similar goals based on the devices used. Having a broad set of protocols to accommodate potentially billions of devices is a safe bet for the future.

Another popular protocol in use is MQTT (Message Queue Telemetry Transport). This is used primarily to send notifications out to interested parties that subscribe to a particular message broadcast [5]. It is considered an M2M (machine to machine) protocol which means connections don’t need a human to intervene and can synchronize with devices on its own as programmed. You may be familiar with how Facebook has notification alerts for you whenever there is activity that warrants your attention. MQTT is the protocol that makes it possible [5]. With MQTT, there is a Publisher, Broker and Subscriber base that is common with message update protocols. Publishers send notice to the broker, which makes deliveries to subscribers automatically. As the message needs to be available to many different device types, it contains a basic message header type in its frame data that is available for many devices to use [5]. This efficient method of broadcasting is important for IoT devices as they are small, battery powered devices in most cases [2, 3, 4, 6]. The many "Things" tend to require efficient transmission of relevant data to accomplish tasks with their limitations. Given that this protocol thrives in low bandwidth, low memory and low power environments, it more than serves a purpose in the field of IoT [5].

Moving from quick notification subscription broadcasts with MQTT, we move on to XMPP (Extensible Messaging and Presence Protocol). XMPP is primarily used in instant messaging services [5]. As an open source protocol, it has become popularized by online community efforts to make it available on any operating system [5]. XMPP is highly customizable; being able to deploy end-to-end encryption services between different services [5]. Unfortunately, being that it uses XML (Extensible Markup Language), it is not friendly to devices that have issues supporting a large network load without compression [5]. AMQP (Advanced Message Queuing Protocol) is very similar protocol to XMPP in that it is a popular messaging middleware protocol. It does require TCP to guarantee messages however. AMQP also follows the MQTT style of subscribe and publish [5].

DDS (Data Distribution Service) is similar to the previous protocols MQTT and AMQP. This protocol also happens to excel at M2M connections using multicast to reach devices with its messages [5]. Each message DDS sends can be customized to fit policy guidelines required by company developers implementing IoT applications with Quality of Service policy built in [5]. Anything they would need such as Security level, urgency of messages, or priority can be customized with DDS before broadcast. All of this can be accomplished without the Broker MQTT must use [5].

B. *Service Discovery*

For an IoT device to be useful on the net, it will need to be able to find clear names for resources. This method must be dynamic and adaptable to the many devices it supports. Popular IoT mainstay protocols that handle requests of this nature include mDNS and DNS-SD (Multicast Domain Name Service and Service Discovery respectively). Multicast DNS is handy for locally stored networks of things as all information does not need to be hunted for. The information it needs is already available and will run without requiring major system resources to back it up [5]. mDNS acquires the names it needs from a simple multicast message it sends out to the network [5].

When using DNS-SD, a more standard flavor of DNS similar to how a normal computer requests information is used. It will utilize mDNS to send the message but it will forward that request to UDP [5]. DNS-SD is also used to find specific services running on a network that require updates like a print server for example [5]. Both DNS-SD and mDNS require a cache to store resolved name information as it relates to known IPs. This is detrimental to devices with very low storage ability. Issues regarding those devices can be resolved by carefully timing storage use so it must be monitored occasionally [5].

C. *Infrastructure Protocols*

Routing for the IoT can be a herculean task. We have standard routing of packets with hops across physical networks however, in the IoT we must traverse multiple devices and device states while maintaining the integrity of the original request. RPL (Routing Protocol Low-power Lossy Networks) is a standard specifically created to accommodate devices lacking in resources to support normal routing. The IoT is full of devices in varying states of existence. Some have smaller power at hand, some have all they need, and some are mobile and only accessible over wireless connections. With that in mind, we need to have a way to keep all of the information about the network updated. By using a DODAG (Destination Oriented Directed Acyclic Graph) there will be a virtual diagram of node information in each information message [5]. To maintain this graph, a series of messages are relayed to each node. These messages consist of an information message which gathers node rankings, an advertisement message that goes out to each node. A Solicitation message which requests the information from any reachable node that is close, and a simple acknowledgement message which responds to node advertisement messages [5]. These messages can distribute themselves all over low power networks until a proper path is formed. A preferred parent node is how the system can become reliably useful in a lossy network environment. By transmitting upward and downward through the routes, a system can get around any problem areas and still deliver a payload.

6LowPAN (Low Power Wireless Personal Area Network) was a protocol developed in response from a need to reduce packet data over IPv6 [5]. 6LowPAN specifically selects required packet header data to maintain an IPv6 connection. For all intents and purposes, it is a method of compression that allows a tiny device to be able to use IPv6 through packet header reduction [2, 11]. By reducing overhead on the network accessibility of a device, they save power and become more efficient with every connection through the network layer.

The standard of the Physical layer in Figure 2 is IEEE 802.15.4 [5]. This specification was enacted as a Physical MAC (Medium Access Control) for LR-WPAN networks (Low Rate - Wireless Personal Area Network) [5]. For IoT, this is a premier protocol that almost does it all. While using a low power network device, it can help guarantee secure connections with encryption and provide authentication for M2M and regular users. 802.15.4 can transfer data at multiple rates depending on the devices need. 250kbps at 2.4GHz, 40Kbps at 915Mhz, or as low as 20Kbps at 868MHz [5]. The higher the frequency, the more powerful the connection. The lower the signal is, the higher range you can cover at loss of device throughput. When used in its Full Function mode, the standard supports storing a full routing table for enhanced access to devices on the network. A Full Function device can act as the main node that joins devices into a PAN as a Coordinator. In the Reduced Function mode, the protocol only supports star topology networking and will require a coordinator to function properly [5].

Moving onto a different kind of network, EPCglobal (Electronic Product Code) supports a different kind of IoT device. Specifically, RFID (Radio Frequency Identification). EPC's system keeps track of identifiers in the network from the identifiers in the tags. The scalability is enormous, supporting up to 68 billion serials for a product class [5]. By simply having tags and tag readers, a single warehouse can keep track of inventory in an instant from anywhere. The tags are cheap and lend a hand in device management, tracking a unique device out of millions wherever in the world that device is tasked to go. By using an Object Naming Service, a company could instantly know the location, date and time of manufacture. If devices are faulty, it would assist in investigating the exact cause of any issues. Just like serial numbers, companies need to track unique objects. RFID simply enables a company to have that number available over the air to work with other IoT devices in that field.

D. *Influential Protocols*

Current internet-based technologies, especially for security needs, are geared for a desktop style device that has the power and capacity for higher scale processing versus smaller IoT devices. For IPv6, the standard is IPsec [5]. In combination with 6LowPAN, security can be attained with IPsec but it doesn't usually meet the strict power guidelines [3]. Lightweight models like ECC (Elliptic Curve Cryptography) can be used by 6LowPAN to meet energy requirements [2]. IoT requires many networking specifications to enable a space for interoperability. IEEE 1905.1 was created to help define that space IoT needs to properly converge technologies [5]. By combining technology across the layers, you can have a mix of wi-fi, Ethernet, and even RF bands that can coexist without needing to alter any underlying structure.

IV. IoT Layer Model

For all of these protocols to work in concert, there is a structure to how they flow with each other. Just like with the OSI seven-layer model for standard networking, Smart devices for IoT follow a similar principal. Some in the field even use a 6 Layer model [7]. While there is no completely finalized structure, most agree upon a basic three-layer model for IoT [4]. These consist of Application, Perception and Network layers [4]. The categories of protocols we discussed earlier plug into these layers. Service Discovery and Infrastructure protocols run in the Network Layer, Sensors or devices themselves are categorized in the Perception Layer, and Application Protocols run in the Application layer of course [4, 5].

A. *IoT Open Source*

Manufacturers today have a lot to be thankful for. With the broad availability of free and open software, companies and even regular people from all over the world can test and build new devices far faster than ever before. Through free software packages using Apache or operating systems like Linux, one can simply purchase a mini computer system and get started developing immediately. Computers that can meet this goal include for example, a BeagleBone Black device or Raspberry Pi. The industry recognizes that in order for IoT to become a game changing technology, it must uniformly adopt open standards for all electronic devices in the future [9]. By creating a uniform space for devices, you therefore create a means for the technology to speak to another device becoming platform agnostic.

This leads us to what choice companies have when creating new "Things". Developing prototype systems from scratch is an expensive proposition if open-source technology didn't exist. That prohibitive barrier to innovation could be the reason we are seeing the flood gates drop today with devices like Raspberry Pi, as that barrier has dropped significantly in price. As those devices run on a Linux base, a person with a budget of $100 could purchase a few devices easily to begin researching if their models are valid before continuing [9]. Having open source protocols and hardware in the field available to anyone who wants to participate in the internetworking of devices around the world will not have a hard time getting materials to do so. The only limit is time.

V. Security

As of this moment, we are seeing new devices accessing the internet and creeping their way into every aspect of your life. Every time a person checks the thermostat in their home or makes a purchase using their Cell Phone NFC virtual wallet, they are using IoT without realizing it. These devices have unique sensor technology that collects various types of data every minute of the day. Biometric walking data is one example or average heart rate status through your smart watch. These aggregate the data straight to health apps on your phone or tablet device. Some of it is related to the concept of having a smart home. When you come home, you could tell a hardware assistance device like Google home or Amazon Alexa devices to turn on certain lights, raise the home temperature, or to reorder groceries you have saved in a "must rebuy" list you created online. You could issue those commands on the go through your phone or in person when you arrive. All of these devices are listening and generating a profile on your wants and needs to better assist you while you are home. This data is valuable as it uniquely identifies your habits, what you are likely to eat, what times you usually arrive home or when you have scheduled times away. If a threat was able to get a hold of this data, they could track your movements and plan a home invasion when you are away or even steal your identity by acting as you in your place.

Generally, systems are secure. It is the people who have access to those systems that are not. Using phishing emails or confidence tricks, a hacker could bait an unwitting person into giving them access. Once acquired, all they would need to do is access your Google Mail account while you aren't paying attention. As that system is tied to personal Google services, theoretically that person now has access to every service Google provides using your name. As most password reset emails from services go straight to your email account, someone could again easily gain access to other accounts. It’s like a domino effect. When one security wall crumbles, it will likely spread and cause chaos in a very short amount of time. Doubly so if a dedicated team of threats are working against you. IoT is a unique piece of this security puzzle as all of these personal devices could be synced to your internet accounts online in the cloud. All of your online data would be accessible. With all of the new users flooding into the open device space, you are seeing a flurry of new attacks like this against owners of IoT devices. Education is important for new users and will be even more so in the future. You can engineer the best lock in the world but it will be useless if someone has all of the keys. While not nearly as important as safe practices by the public, having open standards that everyone understands will help security researchers find and patch holes in software. Instead of one person making all of the improvements, the community at large makes the effort in open source projects so that, together, risks to devices can be mitigated.

B. *Lightweight Cryptography*

One of the major uses for the internet is its ability to be a marketplace for the world. It is trivial to have items imported to locations anywhere by using a credit card and a click of your mouse. You can access these shopping websites on most internet connected devices, including IoT equipment. When someone puts in their personally identifying information along with payment information, how is that data kept secure? Encryption is the primary method. With IoT, we need encryption methodology to protect data primarily in transit across different systems.

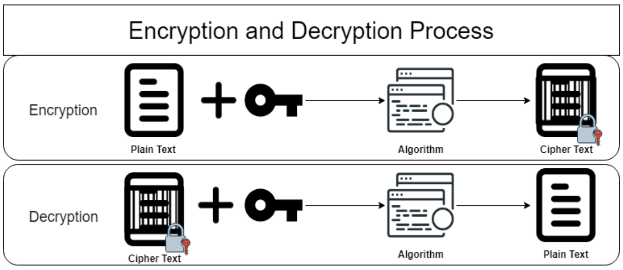


Fig.2. Standard Encryption Summary

In Figure 2, a general explanation for encrypting and decrypting is shown. You take data and apply a key with an algorithm to create unreadable ciphertext. To decrypt, all you would need is the key which solves the algorithm leaving the original message intact and readable. For IoT, existing encryption solutions are either too demanding or bulky and cannot be processed on most low power IoT devices [2]. To respond to that need, Lightweight algorithms are being developed and tested for these devices. These ciphers must have specific things to be considered useful. They should have a small key size, small block size, simpler rounds, and simpler key schedules [2]. The reasoning for this is to increase efficiency with End to End communications between devices and to have greater adoptability [2].

There are two main types of algorithms: Symmetric and Asymmetric [2]. Symmetric algorithms use one key for decryption while Asymmetric keys need two (a Public and Private Key). Symmetric algorithms are faster by far as they only need to account for one key. Asymmetric keys are slower and require greater processing time than most IoT devices can handle, but are more secure [2]. To determine what type of algorithm would apply to a device, Saurabh Singh et al proposes a Hybrid lightweight model that would determine which algorithm to use automatically. Based on live data flowing to and from IoT devices, this model deploys a type of sorting that organizes data to be encrypted [2]. Using metrics like data size, battery power, memory space and computational ability, the HLA can efficiently use IoT resources based on their actual ability while preserving security [2]. An example of ciphers that could theoretically be deployed with this, include a Symmetric HIGHT (High Security and Lightweight) Cipher and an ECC Asymmetric Cipher [2]. 6LowPAN devices already employ an ECC algorithm in their nodes, which can be used for their security [2].

C. *IoT Cloud Security*

The Cloud is a place where interconnected devices all gather to join in their demand for data. For IoT, this is an invaluable, irreplaceable resource that demand for is growing daily [15].

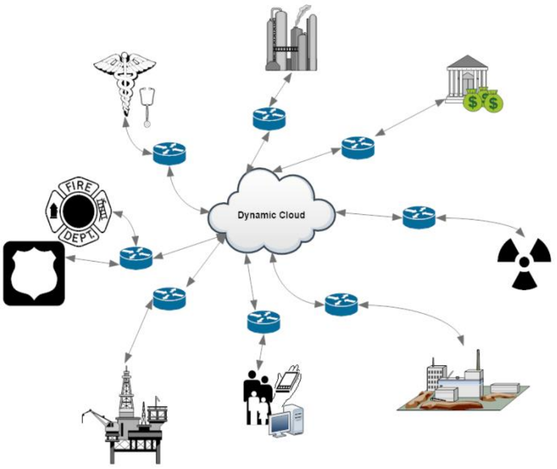


Fig.3 Cloud Interconnection

In Figure 3, there is a unique gathering of devices, automated M2M sensors, power grid systems, weather monitoring data aggregation, entertainment, and emergency services are all accessing the cloud. Being a data gathering space for a seemingly infinite number of devices, one could only imagine how 24/7 access to this data is important. As a compliment for all IoT, the cloud is a true meeting point for systems, services, and devices of all shapes and size [6, 12, 15]. Furthermore, the cloud is not just a place to store data to offload full devices. Cloud services can number crunch big data for large databanks of information [6]. For firms that cannot afford warehouse sized supercomputers, the cloud allows businesses of all sizes to run services or software directly on cloud space. These services can be rented for far cheaper than doing it all in-house.

Generally, there are three main services the Cloud offers today. SaaS (Software as a Service), IaaS (Infrastructure as a Service), and PaaS (Platform as a Service) [6]. With IaaS, the Network and Hypervisor is maintained and run directly from the cloud provider. Moving to PaaS; the platform service does all of the things IaaS can do but adds application management with operating system support. Finally, with SaaS you see total management of everything done by the cloud [6, 12].

Since the cloud acts as a unique, separate entity, it has a natural barrier in place. Being external from an agency or business gives the cloud natural risk mitigating features that help guarantee safety. The cloud acts as a gate that devices must authenticate and pass through [6]. For each thing to talk to another thing it will need to go through this wall of policy before it can even authenticate with another similar device [6]. Proper validation of data passing through reduces the risk of malicious devices attempting to gain access [6]. Validation also prevents bad or rogue data corrupting a cloud database. For security, data validation is a basic but important step that cannot be ignored.

Certification of a cloud vendor's security ability is increasingly coming up in conversation. For emergency health and certain government functions, a vendor must certify that they are in fact secure and must demonstrate so to auditors [6]. Health law in the United States for example is governed by a specific policy called HIPAA. HIPAA (Health Insurance Portability and Accountability Act of 1996) requires a high level of security in regards to patient data. Certification is not a cheap process either as any change or upgrade could require recertification or evaluation of a vendor's process [6]. Balancing security with development of new features is going to be a challenge for businesses of the future to get right.

VI. Challenges And Threats

IoT devices are comprised of many things. "Things" is intentionally vague as part of its original definition [4]. As they can be many different shapes and sizes, they must first be able to handle the computational task of being an internet connected device. IoT devices, as discussed earlier, are currently plagued by certain design limitations. 1) Devices typically run on battery power and must be able to run in low-power environments. 2) Devices, due to their size, have limited memory. 3) Devices may have a lower ability to process information due to the small size of IoT sensors [2, 3, 4, 6, 13]. On top of that, these devices need to be secured in an environment where they may communicate with threats executed from a distance using Cellular LTE, via PAN WiFi, or even Bluetooth [3]. With the size of the network growing at a staggering rate, there remains the issue of how millions of devices continue to secure themselves for the future and protect others from harmful interference in an always online world.

One of the largest challenges cloud and internet providers face is a DDoS attack (Distributed Denial of Service) [3, 14]. A DDoS occurs when an exponential amount of internet traffic overwhelms a specific network target. When you have a large cache of infected IoT devices online, Hackers can exploit that to cause immediate disruption to whatever system they wish. Targeted botnets like this can be instigated when code is mass injected into devices that have not had updates or are poorly secured with default passwords.

Threats to harm actual people are a factor as well. With medical devices entering the IoT field, you have to wonder what would happen if bad data could be injected? Would this trigger an IoT system to inject medicine too early or too much [3]? What if your car's IoT sensors detected an accident and suddenly deployed the brakes? These are the threats that come out of having always online - wirelessly accessible devices.

A. Future Solutions

In order for security to be effective, the community should focus on three ideals. 1) Security by design, 2) Machine Learning, and 3) Polymorphic Security [3]. With Secure-by-Design principals in place, a proper set of rules are enforced from the very beginning. The main one being that security should be aggressively tested in the unit until all hardware and software security holes are patched, long before the product even makes it to consumers. Security needs to be deeply set into every facet of development [3]. This is proactive as developers can resolve entire categories of risks instead of just one at a time as they are encountered [3]. As threats can be extremely unpredictable, it's also important to be knowledgeable about attacks before they happen through regular user training after a final release.

For Machine Learning, there needs to be a solution where applications can inherently know when malicious activity is being performed on a device just through monitored action [3]. The entire cycle of machine learning is a long process. A cycle of steps must be repeated and exposed to the machine in question so they can inherently know and understand patterns through training [3]. By listening for a series of specific keystrokes or specific frequency of network traffic, a machine can identify and report any suspect actions without human backup. Polymorphic types of security see threats just like those machines that were trained. These types however focus on counterattack [3]. These systems are specifically designed to mitigate damage that can be caused by an attacker gallivanting across your network. By quickly identifying a threats signature it was exposed to, the system will adapt its hardware and software sets to do so [3].

In Figure 4 there is a diagram that shows what a future secure framework may look like. By having a detection module validating all interaction with the device, machine learned polymorphic security can check for bad input or output that may be a security risk [3]. It can then mitigate those flaws dynamically.

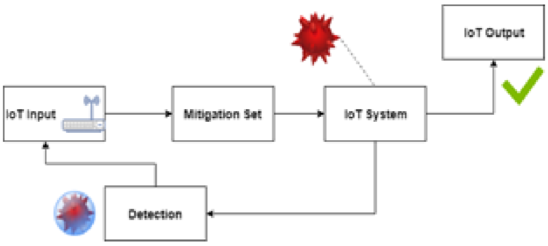


Fig.4. IoT Polymorphic Security Model

VII. Conclusions

In conclusion, the IoT is a broad network with billions of possible technology combinations. This is a field that is currently under a period of explosive growth and is not scheduled to slow down any time soon. Scaling security to meet the needs of the future IoT is going to be a great challenge as certain network layers haven't even been set in stone yet. Hackers are constantly finding new ways to upset the balance between efficiency and security in this field using open technologies to do so. This creates a cycle of break-ins by hackers and patches offered by the community in response. Polymorphic systems in the future will be able to relieve the pressure off of users here. These will break the cycle of one-at-a-time patches and actively mitigate disaster from occurring. Leveraging currently existing technology like AES or IPv6 to gain insight to the needs of low power devices is helping to create a solid basis for new devices to thrive efficiently. With this paper we hope to have imparted a sense of understanding about how different and homogenous the system actually is and will be going forward.

References

[1] Cisco Systems, "Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2016-2021," https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html, 2017.

[2] Saurabh Singh, Pradip Kumar Sharma, Seo Yeon Moon, and Jong Hyuk Park, "Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions," Journal of Ambient Intelligence and Humanized Computing, Springer, 1-18, May 2017.

[3] Francesco Restuccia, Salvatore D'Oro, and Tommaso Melodia, "Securing the Internet of Things: New Perspectives and Research Challenges," IEEE Internet of Things Journal. Vol. 1, No 1. January 2018.

[4] Ammar Mahmoud, Russello Giovanni, Crispo, Bruno,"Internet of Things: A survey on the security of IoT frameworks," Journal of Information Security and Applications, Elsevier, 38, 8-27, 2018.

[5] Ala Al-Fuqaha, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari, Moussa Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols and Applications," IEEE Communications Surveys & Tutorials, 2015.

[6] Jatinder Singh, Thomas Pasquier, Jean Bacon, Hajoon Ko, and David Eyers, "Twenty Security Considerations for Cloud-Supported Internet of Things," IEEE Internet of Things Journal. 269 - 284. 2016.

[7] Stephen Morrow and Colin Bull, "The Internet of Things and Getting Security Right," https://www.sqs.com/_resources/whitepaper-the-internet-of-things-and-getting-security-right.pdf, 2016.

[8] Ajit A. Chavan and Mininath K. Nighot, "Secure CoAP Using Enhanced DTLS for Internet of Things," International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 12, December 2014.

[9] Amit Pundeer, "Open Source IoT Ecosystem," White Paper, HCL Engineering and R&D Services. https://www.hcltech.com/white-papers/engineering-and-rd-services/open-source-internet-things-iot-platforms, 2015.

[10] Angelo Capossele, Valerio Cervo, Gianluca De Cicco, and Chiara Petrioli, "Security as a CoAP resource: an optimized DTLS implementation for the IoT," IEEE International Conference on Communications (ICC), 2015.

[11] Nan Li, Dongxi Liu, and Surya Nepal, "Lightweight Mutual Authentication for IoT and Its Applications," IEEE Transactions on Sustainable Computing, 2017.

[12] Martin Henze, Lars Hermerschmidt, Daniel Kerpen, Roger Häußling, BernhardRumpe, and KlausWehrle, "A comprehensive approach to privacy in the cloud-based Internet of Things," Future Generation Computer Systems, Elsevier, Volume 56, 701-718, March 2016.

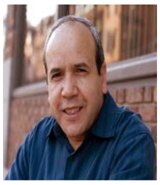
[13] Elisa Bertino, Kim Kwang Raymond Choo, Dimitrios Georgakopolous, and Surya Nepal "Internet of Things (IoT): Smart and Secure Service Delivery," ACM Transactions on Internet Technology (TOIT) - Special Issue on Internet of Things (IoT): Smart and Secure Service Delivery: Volume 16 Issue 4, December 2016.

[14] Gaurav Somani, Manoj Singh Gaur, Dheeraj Sanghi, Mauro Conti, and Rajkumar Buyya, "DDoS attacks in cloud computing: issues, taxonomy, and future directions," Computer Communications, 2017.

[15] Alessio Botta, Walter De Donato, Valerio Persico, and Antonio Pescapé, "Integration of Cloud computing and Internet of Things," Future Generation Computer Systems, 684 – 700, 2016.

Authors' Profiles

Derek Johnson received his B.Sc. degree in Applied Information Technology from the Yale Gordon College of Arts and Sciences at the University of Baltimore. Currently, Derek holds multiple active CompTia certifications and has been active in IT education and work since 2007. Presently, he is employed in the Government sector working with Databases, Security, and Networking.



Mohammed Ketel received his Ph.D. degree in Electrical and Computer Engineering from New York University, Tandon School of Engineering (then Polytechnic University). He is currently an Associate Professor in Applied Information Technology at the University of Baltimore. His research interests include cloud/fog computing, secure communications and networking, and Internet of Things. He is a member of ACM and IEEE.

How to cite this paper: Derek Johnson, Mohammed Ketel,"IoT: Application Protocols and Security", International Journal of Computer Network and Information Security(IJCNIS), Vol.11, No.4, pp.1-8, 2019.DOI: 10.5815/ijcnis.2019.04.01