Security of Things

Mohit Dodhia [1], Anudeep [2], Aditya Jain [3], Varchas Shishir [4]
[1, 2, 3, 4] Computer Science and Engineering Department, SRM Institute of Science and Technology, Chennai, Tamil Nadu, India

Abstract – IoT Security is the area of endeavor concerned with safeguarding connected devices and networks in the Internet of things (IoT). The Internet of Things involves the increasing prevalence of objects and entities – known, in this context as things -- provided with unique identifiers and the ability to automatically transfer data over a network. Much of the increase in IoT communication comes from computing devices and embedded sensor systems used in industrial machine-to-machine (M2M) communication, smart energy grids, home and building automation, vehicle to vehicle communication and wearable computing devices. The main problem is that because the idea of networking appliances and other objects is relatively new, security has not always been considered in product design. IoT products are often sold with old and unpatched embedded operating systems and software. We aim to design a product that directly deals with these problems. The tool would be able to monitor, log and analyze the data of the network while distributing administrator level controls to the user. The tool would also be able to distribute software level support for the network such as Encryption, PKI, etc.

Index Terms – Security, IoT, Authentication, PKI, Analytics.

1. INTRODUCTION

Internet of Things (IoT), as we all understand, is an amalgamation of physical devices, electronic devices, sensory devices and other embedded systems encapsulated by The Internet which allows these devices to form a network and communicate among themselves. These devices or objects can be remotely controlled via The Internet, and because they form a deep, integrated network which contains a lot of data, IoT falls under Cyber-Physical Systems. IoT has various applications in our day-to-day life and we are seeing a huge growth in IoT Development as well. Tech Giants like Google and Apple have developed their own IoT devices to encourage the application of Smart Homes.

While IoT hordes a lot of features that can make a consumer's life easy, it also has a huge set of issues and exploits that can raise an alarm. As mentioned before, IoT is a cluster of devices which are inter-connected together, and because of this the number of exploits and shortcomings of different devices increase exponentially. Handling different vulnerabilities can become a herculean task, owing to the vastness of an IoT network, so different layers and protocols of the network need to be worked on in order to secure it from threats.

The aim of this paper is to make the reader understand the different kind of threats an IoT system can be under and what tools, terminologies or protocols should be followed to secure the network as a whole. Various tools, Open Source protocols and APIs will also be referenced for the reader to study them properly, if desired. Certain mathematical models will be mentioned as well if the need absolutely arises; in such a case, the reader is advised to properly understand these models to better understand the nature and importance of the model and the aid it provides in solving our problem.

2. LITERATURE SURVEY

As described above, IoT has a lot of vulnerabilities which need to be addressed immediately. We are going to discuss these vulnerabilities in brief before moving on to finding appropriate solution(s) for them so as to give the reader a better understanding of what is happening and how the solutions are designed to help us.

IoT can broadly be classified into four major layers [5]:

- Physical Layer
- Medium-Access Communication (MAC) Layer
- Networking Layer
- Application Layer

Each of these layers have their own set of vulnerabilities. For instance, the biggest vulnerability of MAC Layer has been Authentication and Authorization. IoT devices (a. k. a. "Things") are compact in size, which makes it very difficult to monitor; unauthorized access to an IoT network can cause massive data theft and/or duplication. Ipso facto, the attacker might turn your own device against you. The infamous Stuxnet malware stands testimony to how adverse an attack on an IoT network can be.

To put things into perspective here are some common vulnerabilities that can compromise an IoT network:0

- Administrative credentials of Things are hard-coded into the hardware itself. OEMs manufacture these hardware in huge quantities and coming across those credentials can be very easy. These credentials are also sold on the Dark Web where anybody can gain access to these credentials and use them against you.
- Encryption is the next challenge that IoT networks face. Encrypting an entire chunk of data before

transmitting it to multiple Things is a very tedious task, which is why ciphers with less computational requirements are opted for. Weak ciphers are very easy to crack and it could comprise the integrity of your data.

- Authentication is another hurdle that needs to be addressed as it is the most important criteria for accessing information on the network. An unauthorized access to the network is very horrifying even though it may not sound like it.
- Periodic analysis of the your IoT devices is also important but is not very commonly approached. A deep analysis can reflect a lot of things about your network. Essentially, an analysis is a tangible process which can show you what is going on with your network.

To give the reader a wider scope of this domain, we have referred to three different papers which address the same problem. Before we go forward with our understanding of those papers, we would like to let you know that our opinions might not be the same as those of the authors who have written these papers. We shall not be diving into these trivialities and we utterly respect the opinions of these authors.

The paper [6] "SECURITY AND PRIVACY IN THE INTERNET OF THINGS: CURRENT STATUS AND OPEN ISSUES" by Mohamed Abomhara and Geir M. Køien of University of Agder, Norway describes the basic idea of IoT which includes its vision, architecture, application domains, supporting technologies, security threats and challenges. The paper also includes describes the current state of IoT, along with the security and privacy threats and challenges. The vision of IoT as discussed in the paper is the interconnectivity between people and things at any given instance via any network or service. Development of numerous applications related to IoT has been made possible. Security confrontations related to security services such as authentication, privacy, trustworthiness & end-to-end security have been discussed in this paper. This paper also elucidates upon the future research directions, some of which are being followed by us.

The paper [12] "INTERNET OF THINGS SECURITY" by Yassine Chahid, Mohamed Benabdellah and Abdelmalek Azizi of Mohammed First University, Morocco gives the essentials on the security aspect of an IoT network. The paper contains a survey of the past of the security measures of an IoT based network and how it has changed over time and what could be improved further along in the future. The various layers of an IoT network has been discussed in great detail along with the faults and security problems located in each layer. Further along, the security measures that must be taken for ensuring the safety of each layer on an IoT based network has been discussed in detail as well. This includes security measures of the perception layers, network protocol attacks and network layer security measures. Several brief solutions for the issues of the Internet of Things has been discussed.

The paper[4] "SECURITY FOR THE INTERNET OF THINGS: A SURVEY OF EXISTING PROTOCOLS AND OPEN RESEARCH ISSUES" by Jorge Granjal, Edmundo Monteiro and Jorge Sa Silva focuses entirely on the various layers of IoT, which have been described above. Nevertheless, this paper sheds light on the networking aspect of each layer and how certain modifications and ramifications might help in securing the network as a whole. We do not support this approach. We believe that in order to secure the whole network, all layers should be removed of their vulnerabilities or patched at the very least. However, this paper sheds enough light on the networking aspect of Things to ignore it. It is with most certainty that following these networking protocols would yield immediate results.

Thus, Internet of Things, while helpful, can also come with a lot of security issues. IoT hardware is generally compact in size which makes it more difficult to manage it in terms of security. Monitoring the whole of an IoT network also becomes a herculean task, considering the number of devices and layers involved in the network.

3. MODULE DESCRIPTION

In our proposed model, there are six key modules, each working around the same principle but in a different way.

The six modules are:

- Network Scanning
- User-check Authorization
- Router-Router Authentication
- Sensor-Router Authentication
- Router-Device Authentication
- Device-Device Authentication

3.1. Network Scanning

It is important to keep a track of all devices and peripherals connected to each other which comprises the IoT network. This is done by tabulating a list of all devices connected to the network in real-time and monitoring when the device(s) disconnect and reconnect to the network.

This tabulated data is sent over the analytics team to better monitor each device and look for any malicious activity.

3.2. User-check Authorization

Once we have information of all the devices connected to the network, we can segregate them based on the amount of access they have across the network. Segregating them gives the

administrator more flexibility to check these devices and what they are accessing.

If any device is trying to overstep the access that's been allotted to it, the system will prompt the admin to take action against the device by cutting Internet access, followed by other networking features.

3.3. Router-Router Authentication

Routers make up for a crucial component in the IoT framework by helping in connecting devices and peripherals to the network. A router becomes a gateway through which multiple devices connect themselves to the Internet. This can also be a cause of worry because if an unauthorized router is deployed in the network, it can potentially take control of the flow of devices and compromise the integrity of the IoT network.

To overcome this shortcoming, router authentication should be made mandatory if it is to be deployed in a network. To verify the authenticity of a router, digital certificates known as PKI Certificates [9] are put to use. PKI Certificates are digitally signed certificates issued by trusted and verified certification authorities to indicate that a particular certificate is clean and can be put to use without having to worry about its integrity in terms of security. Now, providing certificates to large devices is fairly easy for a Certification Authority (CA), but to provide and govern the certificates for devices such as routers can be a tough task for CAs. However, it is possible for a CA to issue certificates for small devices, which in our case, is advantageous to our cause.

PKI certificates can be used to authenticate routers on the network, thereby allowing complete transparency in the network. Deployment of any unauthorized router in the network will easily be detected before the deployment is completed and the router can be taken down immediately before the network gets compromised in any way.

3.4. Sensor-Router Authentication

While authenticating routers seem easy enough for the small device, it is not exactly the same for sensors. Sensors are compact devices with low computational resources, which cannot process the authenticating measures that are required by PKI certificates.

So, in order to implement authentication for sensors and routers, Entity Authentication is employed. Entity Authentication [3] is a security property that is informally defined as the ability to verify identities. It involves two aspects: Identification and verification. It requires an Identity (MAC address, IP address, user name, etc.). Verification is achieved bye executing a protocol which uses a trusted third-party service. During the process, the identity is used to verify its authenticity by sharing information which is only the identity is privy to.

3.5. Router-Device Authentication

Apart from small-scale devices that govern the flow of an IoT Network, another set of Things also form a major composition of the IoT Network.

For devices and router to authenticate among themselves, we will be making use of OAuth 2.0 or SAML.

OAuth 2.0[11] uses a token-based authentication system to verify the authenticity, while SAML uses Single Sign-On to do the same.

Either one or both can be used to implement authentication among the devices as these protocols are more than enough for the task at hand.

3.6. Device-Device Authentication

Device-Device Authentication is of utmost important in an IoT Network. This is because devices are an ever-changing variable in the network; this is to say that devices constantly change in the network. Devices are added and removed constantly because they are easy to carry around and are generally very user-friendly.

To ensure no unauthorized device enter the network, multiple protocols are implemented together to ensure complete authenticity of the devices. These protocols combined together will be referred to as Hybrid Protocol from hereon.

Hybrid Protocol [10] makes use of OAuth 2.0, OpenID Connect [7], and SAML [8] to perform authentication. Essentially speaking, these are some of the most efficient protocols for authentication, and using them together only goes to show how efficient this can be. Hybrid Protocol is used in various forms by many tech giants like Google and Facebook for their products. It is incredibly light-weight and fast, and also yields very accurate results.

4. DIAGRAMS

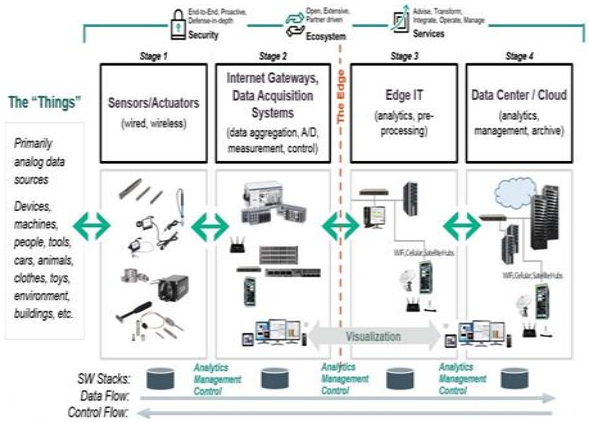

Figure 1. System Architecture

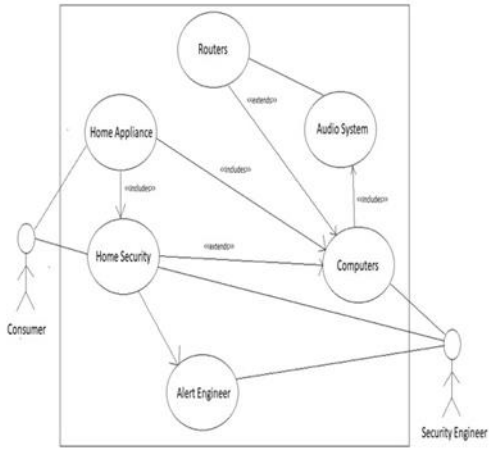

Figure 2. Use Case Diagram

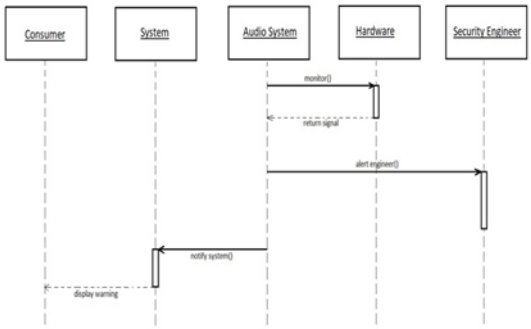

Figure 3. Sequence Diagram

5. IMPLEMENTATION

Now that we have discussed about the models, it's time to talk about how can the above-mentioned technologies be implemented to solve the problem at hand.

For the sake of simplicity, let's divide the above-mentioned modules into two groups:

- Technical Feasibility
- Physical Feasibility

Technical Feasibility comprises all the computational resources required to secure and safeguard the IoT Network. So according to our description, four of our six modules fall under this category.

- Router-Router Authentication
- Sensor-Router Authentication
- Router-Device Authentication
- Device-Device Authentication

Contrary to Technical Feasibility, Physical Feasibility requires human resources along with computational resources to do complete the task at hand. The remaining two modules that fall under this category are:

- Network Scanning
- User-check Authorization

To better understand each component, we will describe how each of the following modules can be implemented.

5.1 Network Scanning

Network Scanning, as the name suggests, is the process of scanning a network to check how many devices are connected. This can be done with the help of built-in tools in an operating system or using a third-party service for accomplishing the same task.

The built-in tools for scanning a network are available in every modern operating system and are fairly easy to use as well.

Third-party services, like Network Inventory Advisor and Wireless Network Watcher, can provide an arsenal of options for controlling the network, provided the it has been granted administrator privileges.

5.2. User-check Authorization

The entire purpose of this module is to make sure no device is trespassing the boundary of access that is granted to it. This can be easily monitored by the network administrators with or without using any tools. If any device is trespassing, the administrators can revoke their Internet access immediately and flag the device for malicious activity. As can be judged by the process, it is a labour intensive task and requires professionals. This task may seem trivial but it is actually of great importance. If any devices permeate the network without being authorized, it could effectively compromise the entire network.

5.3. Router-Router Authentication

As we have stated above, for a router-to-router authentication to work effectively, we need to employ the usage of PKI [9]. Using PKI not only strengthens the security of the authentication process but it also does the authentication process for you.

PKI Certificates are issued and distributed by a Certification Authority (CA). This CA requires a lot of data to verify the authenticity of the product. So, in order to generate a PKI certificate for a router, we need to provide every information about the router to CAs so as to receive the PKI Certificate for our implementation.

Some of the best CAs in the current market are:

- Comodo
- Symantec
- GoDaddy
- GlobalSign
- DigiCert
- IdenTrust

Applying to these CAs will definitely yield a sturdy PKI Certificate which can be implemented directly.

5.4. Sensor-Router Authentication

To implement sensor-to-router authentication, we will use Entity Authentication [3]. Entity Authentication has a broad array of entities that can be used for checking authenticity of the device, like IP Address, MAC Address, etc.

By registering these entities in the network database, we can check the authenticity between a router and a sensor. We simply have to check if the entities of the sensor match with that in the database. The same procedure can be followed by a sensor for checking the authenticity of a router.

5.5. Router-Device Authentication

To authenticate between router and device, we will make use of two popular authentication protocols:

- OAuth 2.0
- Security Assertion Markup Language (SAML)

OAuth 2[11] is an open standard authentication delegation that is used to access information without providing passwords. OAuth 2 is widely used across various platforms and is fairly easy to implement as well. Some commonly used implementations are Jersey, Apache Oltu and Spring Security OAuth.

Security Assertion Markup Language [8] (SAML) is an XML-based, open-standard data format for exchanging authentication and authorization data. SAML uses Single Sign-On (SSO) to address the problem of re-authentication. As the name suggests, SSO uses a single user access to grant access to all other features of the network. Just like OAuth 2, it is very easy to implement.

5.6. Device-Device Authentication

Device-to-device authentication is the simplest of all authentications we have seen so far. By Device, we mean products that are powerful and are used in day-to-day life, e.g. smartphones, computers, etc. These devices have enough computational power to support protocols that require more than average resources.

We will implement what is known as "Hybrid Protocol" [10] as it is a mixture of many protocols. In our definition of Hybrid Protocol, we will make use of OAuth 2, OpenID Connect [7] and SAML to tightly secure the authentication of users connecting to the network. With the advantages of these three protocols combined, the security of authentication on these devices increase tremendously.

6. CONCLUSION AND FUTURE ENHANCEMENTS

By implementing the above-mentioned protocols and and terminologies, it can be said with certainty that IoT devices will be secured. However, keeping the firmware of Things up-to-date should be the customer's role. Firmware updates and patches by OEMs also help in keeping the product safe.

Apart from implementing protocols, a thorough periodic analysis of the network also helps in keeping the network and devices in check. A dedicated SIEM tool or a Data Analytics tool can provide in-depth knowledge of the IoT ecosystem in place and can help govern the network in case of a threat.

API Management [1] is also another field in IoT Security that is worth looking into. APIs make Things functional and it is important to keep them functional. Any corruption in the API can render the device useless and, in certain cases, can compromise the entire system [2].

REFERENCES

[1] Ashish Patro, Suman Banerjee, Outsourcing coordination and management of home wireless access points through an open API, May 2015
[2] Bojan Suzic, User-centered security management of API-based data integration workflows, April 2016
[3] D.A. Melnikov, Y.N. Lavrukhin, A.P. Durakovsky, V.S. Gorbatov, V.R. Petrov, Access Control Mechanism Based on Entity Authentication, Aug. 2015
[4] Jorge Granjal, Edmundo Monteiro, and Jorge Sá Silva, Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues, January 2015
[5] Michael Schukat, Pablo Cortijo, Public key infrastructures and digital certificates for the Internet of things, June 2015
[6] Mohamed Abomhara, Geir M. Køien, Security and privacy in the Internet of Things: Current status and open issues, December 2014
[7] Nitin Naik, Paul Jenkins, Securing digital identities in the cloud by selecting an apposite Federated Identity Management from SAML, OAuth and OpenID Connect, May 2017
[8] Payal Sharma, Vikas Kumar Sihag, Hybrid Single Sign-On Protocol for Lightweight Devices, Feb. 2016
[9] Ray Hunt, PKI and Digital Certification Infrastructure, August 2002
[10] Tsung-Han Hsieh, Kuei-Ying Lin, Pi-Chung Wang, A hybrid MAC protocol for wireless sensor networks, June 2015
[11] Victor Sucasas, Georgios Mantas, Ayman Radwan, Jonathan Rodriguez, An OAuth2-based protocol with strong user privacy preservation for smart city mobile e-Health apps, May 2016
[12] Yassine Chahid, Mohamed Benabdellah, Abdelmalek Azizi, Internet of Things Security, April 2017