IoT Security: A Survey

Maede Zolanvari (A paper written under the guidance of Prof. Raj Jain) Download 

Abstract:

The Internet of Things (IoT) is still at the top of the Gartner Hype Cycle as the most hyped technology, which means that it is the hottest topic that has gained the most attraction of the researchers currently. In recent years, there have been huge amount of research that have investigated different aspects and concerns of this field. Meanwhile, supplying privacy and security is an inseparable part of this technology. Without providing enough security, the promising benefits of this flourishing technology will be misused and worthless.

In this paper, we will first give a brief definition of IoT and then we will go through more details about the current challenges and the provided solution to provide security for IoT.

Keywords: Internet of Things, Security, Privacy, Network, Authentication, Encryption.

Table of Contents

1. Introduction

The invention of IoT by using the new version of IP address (IPv6), which goes beyond the limitations of IPv4, will change the world of Internet by providing the connectivity for an enormous number of smart connected devices near to 70 billion, or even more. Flourishing this technology has been called as the Second Economy or the Industrial Internet revolution[Chris15]. It will produce a huge market with various services, and the size of this market is estimated in the trillions of dollars. This market is a promising scheme to be successful, however only if the privacy aspects get into account before this huge process starts to be implemented widely.

The IoT's anywhere, anything, anytime nature could easily change these advantages into disadvantages, if privacy aspects would not be provided enough. For example, if any one can have access to any personal services and information, or if the information of a wide range of people can be reached by the environment automatically, the IoT would not have a reliable environment [Rodrigo11].

There is not any sufficient backbone to define control and information asymmetry policies for interaction among any different users and devices. Controlling the flow with the traditional tools will cause a huge amount of traffic that is hard to guarantee the privacy and protection for elements [Blanca14]. Also, solutions for different security requirements have direct impact on the cost and time to market. Moreover, every solution has its own business requirements which may or may not be as strict [Ajit14].

Another important issue in IoT is the quality of the user?s satisfaction. IoT should provide a better service by avoiding the rejecting certain services that may happen by current classic mechanisms used to obtain user's consent. Hence, IoT should provide different methods such as implementing consent mechanisms through the devices themselves as privacy proxies and policies for each device, which includes conditions and constraints attached to data that describe how it should be treated [Blanca14].

To provide some statistics about the popularity of IoT, we used the paper [Acquity14]. As this paper claims: *Gradually, consumers have to get adopted to this technology over the next five years. Currently, 7 percent of consumers own a wearable IoT device and 4 percent of consumers*

own an in-home IoT device. Nearly two-thirds of consumers plan to buy an in-home device in the next five years and wearable technology ownership will double by 2015, increasing from 7 percent in 2014 to 14 percent by 2015. By 2016, wearable technology is expected to double again and reach a total of 28 percent adoption rate.

2. What is IoT[Wiki]

The Internet of Things (IoT) is the network of "things" embedded with sensors, where connections through the network will enable these objects to collect and exchange data, while each thing is uniquely identifiable through its embedded computing system. The IoT allows "things" to be sensed and controlled remotely. Also, direct integration between the physical ambient and computer-based systems will be more implemented, which results in improving efficiency, accuracy and economic benefit.

"Things," in the IoT world consists of wide variety of devices, for example: heart monitoring implants, biochip transponders on farm animals, electric clams in coastal waters, automobiles with built-in sensors, or field operation devices that assist firefighters in search and rescue operations. These devices collect required information with the help of various existing technologies and then autonomously share the information between other devices. Current market examples include smart thermostat systems and washer/dryers that use Wi-Fi for remote monitoring.

Besides providing the infrastructure for the tremendous number of new devices and application areas for Internet connected automation to exchange the information, IoT is also expected to generate large amounts of data from diverse locations that is aggregated very quickly, thereby increasing the need to better index, store and process such data is an avoidable concern to flourish this technology.

2.1 Fault tolerance for IoT

Based on the fact that IoT will face billions more devices, IoT will be more vulnerable to be attacked than the Internet, and there might be some attacker that want to control some devices directly or indirectly. One way to know the level of reliability of a service is having a defined threshold for service fault tolerance. However, it should be considered that any solution for this aspect should be lightweight enough that it can be implemented on IoT. As a conclusion, we should first design all elements with secure mechanisms by improving the quality of the implementing software. Also, every element of the IoT should be able to know the real-time status of the network, to provide the feedback to other elements. Therefore, having a monitoring system would be helpful in this matter. Finally, any time that the network faces a degradation in the performance or has a failure in the performance, every element should have the ability to protect themselves. So, various privacy protocols should also be defined for these situation to instruct the elements the way they should work in unusual situations to fix the situation and be able to recover quickly. Hence, the viability of recovery services is obvious [Rodrigo11].

Also, by providing automatic services for example in M2M (Machine to Machine) communication, the need for providing safety and security will be more crucial. Some example

of these devices would be as: health monitoring sensors, car controlling, and electronic locks and environment security monitoring. To have a better understanding from the threat patterns, we should provide enough knowledge about the dangerous and loss of life resulted by abusing the IoT devices; hence, the maximum amount of the fault that is possible to be tolerated can be cleared [Ollie14].

Understanding the challenges in the way of providing privacy is the first step toward finding suitable solutions. Hence, in the next section, we will bring different challenges that are related to provide a secure basic for IoT.

3. Challenges

Providing security for this giant technology is really challenging, mainly because there is not any boundary or limitation on the way that it can go. In this section we provide the possible challenges that the IoT will face.

3.1 Context awareness for privacy

For the security methods that are based on the context awareness, it is needed that any essential part in the context would be addressed effectively. For example if an image cannot be recognized by the sensor because of the bad quality, the security enforcements can not be applied to that image. Some access features should be provided to supply the required information from context. Also, sometimes, automatic security management may work incorrectly in some context, mainly because it could not recognize the context. Providing context awareness is an essential challenge in IoT [Gianmarco14].

3.2 Digital device in a physical ambient

In recent years, in order to measure different information, coupling between physical environment and processor has been growing significantly. For instance, a car that can be driven by a computer in a center or a medicine for a patient will be used as the sensors employed on her body providing body situation. However, if there would not be any guaranteed security, all these systems can be manipulated and attacked by different hacker, and cause harmful results [Gianmarco14]. For example in the above two cases, an attacker may bring up a lethal accident by driving the car in a wrong direction, or may kill the patient by ordering wrong medicine.

Moreover, sometimes IoT devices are considered as intellectual property that they might be highly valuable; so, they need to be protected, and also, for the right of owner. However, it is an unavoidable that when a property is accessible through the physical environment, it can easily been misused by a attacker [Ollie14].

3.3 Identification in the IoT environment

In all layers of IoT, it is essential to provide identification. It is one of the biggest challenges based on the fact that IoT will face a tremendous number of applications and structures with

different unpredictable characters and patterns. This matter will be worse even in the distributed environment which is the main domain for IoT. This challenge stays valid even for bounded and closed environments. There are some hot research considering algorithms which are able to derive value from unstructured data to increase performance. There are different factors determining main criteria of an identifier, such as: governance, security and privacy. Also, lots of existing identification schemes have been created long time ago for local usage and for specific objectives. Therefore, the need to have a global reference for identification is vital.

3.4 Authenticating devices

Lots of devices that use the sensors and actuators should follow specific policy and proxy rules for authentication to authorize the sensors to public their information. Meanwhile, low cost solutions in this field has not been provided as much as needed [Gianmarco14]. Currently, if we want to provide the security for the sensors we have to use high-cost solutions which is a conflict with the main goal of IoT to provide lightweight protocols [Raza13].

3.5 Data Combination

We will have lots of different data produced by IoT. Combining these data to provide more comprehensible information can be done only by providing a large group of new general security policies, which leads us to a more complex user profile. However, these mechanisms even may put the security of users more in danger by sharing their information, that may cause even harder challenges in this matter [Gianmarco14].

3.6 Scalability in IoT

As the technology grows the number of users and devices with different type of communication and technologies grow widely. IoT needs to provide interaction for unbounded number of entities with significant differences in the interaction patterns. Therefore, IoT has to provide capabilities-based access control mechanisms, to ensure the security for this tremendous number of elements[Malisa14].

3.7 Secure Setup and Configuration

Solving the challenge of scalability of IoT has to implemented in such a way of having a secure setup and structure too. The basic design of the system can be implemented based on privacy. For example, a service can be designed in such a way that each user can manage a specific group of people being able of having access to the her information, and the list of people can be managed dynamically [Rodrigo11].Therefore, it is essential to provide a security architecture with the appropriate mechanisms. In another point of view, having symmetric or asymmetric cryptographic credentials regarding the situations provides a more secure infrastructure. The process to build this structure is challenging, especially for the large number of devices that IoT will be faced with [Gianmarco14].

3.8 CI and IoT

The impact of development of IoT on the CI (Critical Infrastructure), such as: energy, telecom and utilities, need to be cleared because IoT technology is going to be implied on the devices in CI, a clear example is the M2M (Machine to Machine) standardization activity. The new risks and new privacy issues that IoT may brings to CI is an avoidable challenge that should be considered. Moreover, providing security for IoT gets more important in this matter, because IoT in CI has to do with crucial CI's aspects, such as: providing safety to prevent industrial accidents, or supplying required services to have a constant electrical power for hospitals[Gianmarco14].

3.9 Conflicting market interest

IoT will make a very competitive market by providing correlated data from different sources. Therefore, it will help to satisfy costumers'needs more efficiently. As a result, providing different techniques to protect the personal data of people will be the main issue at combing and correlating information. This goal should be satisfied by deployment low weight privacy solutions, which is considered as a challenges[Gianmarco14].

3.10 Considering IoT in an evolving Internet

The effect of Internet evolution is undeniable on IoT. The way that the internet is used and the infrastructure of implementing Internet's elements are the two main aspects of effecting IoT. However, data security and privacy have determining roles in evolving Internet. Preparing security and privacy protection for the Internet through standardization will create challenges in this field. Hence, as the paper[Gianmarco14] asserts, this evolution will raise different questions such as: *If such an Internet environment becomes the "trusted" Internet would it be socially acceptable for IoT to remain outside? Can such an evolution indeed benefit IoT security and privacy? What are the implications for IoT governance?*

In another point of view any vendor should investigate any effect that may will have on the Internet by designing its services if the product would be successful. Hence, it should be studied carefully to ensure that the new design would not harm the Internet in all different aspects such as bandwidth usage or latency in the communication environments [Ollie14].

3.11 Human IoT Trust relationship

There should be a specific level of trust that human can have on different part of IoT. Trust on the machines along with that human beings still can have the privacy has been considered widely by researchers. Trust can be defined as the level of confidence that is possible to have on a specific service or entity. However, trust is not defined only for human beings, it can even be defined for systems or machines, for example for webpages, which shows the level of trust in the digital society. In another point of view, trust can be defined as how much we can be sure that a system is doing its job in the required way and providing true information.

Moreover, in the M2M communications in an IoT domain, each device should have the knowledge about that how much it can trust on the another machine to transfer important and sensitive information. This statement is true even for a machine that is sending crucial information to a person, in such a way that important information should not be in access of any

wrong person. As a result, trust can be defined in three ways; first, how much a user can trust on a machine; second, how much a device can trust on another device; third, how much a device can trust a user [Gianmarco14].

3.12 Data management

Other perspective can be defined as how to manage the data. Cryptographic mechanisms and protocols, usually are the best choices to protect data, but sometimes we may not be able to implement these techniques on small elements. Therefore, we should have policies regarding how to manage any type of data with various policy mechanisms. However, if this idea wants to be implemented, we should change many current mechanism[Rodrigo11].

3.13 Lifespan of every IoT's entities

The fact that any product in IoT should have a specific short lifespan, and would not survive for long years is undeniable. As an example, UDP (User Datagram Protocol) services provide a degree of amplification; which means that they respond with more data than they started to communicate with over UDP. This amplification is the result of the fact the source address can be spoofed because UDP is connectionless. Hence this amplification will result in a powerful denial of service. Thus, any device which implements such a service will face to the instability of the Internet. Also the same scenarios with GSM (Global System for Mobile Communications), WEP (Wired Equivalent Privacy) and a number of other wireless protocols have shown that this assumption is incorrect [Ollie14].

In the above section, we got familiar with the current challenges that are on the long way of flourishing IoT. It is said that IoT will come into stage at 2020 and researchers are trying to find solutions for the weakness points of IoT. In the next section, we will talk about the solutions that have been proposed and implemented to provide a safer environment for this new promising technology.

4. Solutions

28% of enterprise organizations claim that network security is much more difficult today than it was two years ago [Jon14]. The main result of getting more difficulty through providing the security is that IoT is growing quickly, and the situation will be worse even in a few years. In the following subsections, we will get noted with different proposed solutions for this matter.

4.1 Privacy-by-design principles

It is obvious that any user of the IoT systems should become aware of any information that is collected from them or about them. Hence, provider companies should have a solution to provide costumers with the notices and let them choose the boundary of using their information; however currently, lots of IoT devices do not have such a user interface. Also, the first step toward defining the privacy is to define the classification of sensitive information at the context of any IoT device. Therefore, conducting an analysis with specific method of analyzing for IoT

organizations is crucial to determine the data elements using at each IoT system. These different analysis should be provided based on collected data types to determine which are sensitive information to apply policies based on the data type.

As the paper [Brian15] asserts: *In January of 2014, the FTC (Chairman of the Federal Trade Commission) noted that IoT stakeholders have a responsibility to make security a part of their product development process, to collect the minimum amount of data necessary, and to notify consumers of unexpected use of their data and provide simplified choices regarding this use. Organizations that exploits IoT capabilities should build truly privacy controls for their systems.*

Also, it is important to have a mechanism for privacy awareness within an organization. As a result, users in the organization will have the authority to define their own desired domain for privacy by making changes to their personal IoT system.

4.2 Defining authentication framework[Brian15]

There are different scenarios for IoT authentication; for example, M2M authentication is required for the cases that IoT elements want to talk to each other. As it is clear, IoT components may communicate with different applications in cloud, mobile devices, web or even with people. The protocols for authentication may limit authorization options because many devices operate following constrained conditions. However, there are a number of diverse use cases related to the authentication of IoT components. These days there are some specific IoT authentication being exploited, such as: Pre-shared key/shared secret, Certificate-based authentication and Token-based authentication, and we choose each of these authentications based on the constraints of the device.

To use shared secrets, the scheme should be based on NIST (national institute of standards and technology) specified HMAC (Hashed Message Authentication Code) algorithm that attaches a message's content to its identity. HMACs provide data origin authentication and message integrity verification functions. An example of an HMAC scheme is HMAC-SHA-256. Certificate-based authentication can support protocols such as TLS and DTLS. IEEE defined 1609.3 certificates for use with the DSRC (Digital Short Range Communications) used in vehicle-to-vehicle communications. The use of certificates introduces the likely need for a Public Key Infrastructure that centrally manages all of the certificates provisioned to devices. This includes critical functions such as trusted registration and compromise recovery.

Token-based authentication schemes such as OATH 2 (Open Authentication 2) and OpenID Connect Federated Authentication provide useful alternatives to shared secrets and certificates, and also allow for the introduction of comprehensive policy controls applied to IoT access requirements. Certificate-based authentication in comparison with shared secret authentication is more practical with large number of devices, because the overhead about managing the secrets becomes significant for a large number of devices. Certificate-based authentication uses asymmetric algorithms and deals with the processing of certificates.

Some other authentications such as CoAP (Constrained Application Protocol) put the policies into the protocols that they support, and these kinds of authentications are the best choice for

device-to-device transactions [Kim14]. The CoAP provides four different levels of authentication: No Security, which supposes at another protocol layer, security will be implemented, PreSharedKey, which provides a single symmetric key among the users that are authorized to use the system, RawPublicKey, which is a single asymmetric key for each device implementing CoAP, and finally, Certificate, which is an authentication for devices implementing CoAP with an X.509 certificate.

PreSharedKey mode had the disadvantage of making sure that the key is safe, because it uses mainly only one key for all devices. Hence this method is only efficient for a small group of devices, otherwise for scaling the network, or in the case of revealing the key, it causes delay to provide the key among a large number of users. Meanwhile, using the rawPublicKey mode prepares a unique asymmetric keys for all users, so it copes with the problems with a single key problems. Certificate mode is similar to preSharedKey, but it only adds the additional measure of trusting segments of devices, so it is practical for employing a PKI (Public Key Infrastructure) for devices.

4.3 Identity and trust

There would be a large number of devices with different shapes and sizes, interacting together in big chaos that they need to be managed and provided by security as IoT grows. Also, the diversity in IoT device types, locations, and functions will bring more variety of policy and privacy rules. Each device should carry some information about the authentication, security and access control. In this matter, each device that wants to join the network needs to claim its identification, such as location, type of device and data, additionally, there should create trust for the network authority by approving the identification, by saving all information and details and sharing them among security IoT elements. Hence, to provide the a secure connection, it is possible that switches and routers will be implemented based on the X.509 certificates [Jon14].

4.4 IP-based security solutions [Tobias11]

While the general-purpose key exchanges are security solutions at the Internet domain, TCP/IP security protocols are one of the important parts of designing IP-based IoT security solutions. Many protocols such as IKEv2/IPsec, TLS/SSL, DTLS, HIP, PANA, and EAP are possible solutions in the 6LoWPAN and CoRE IETF working groups to provide a more secure IoT data transmission. Figure 1 shows the relationships between the discussed protocols.

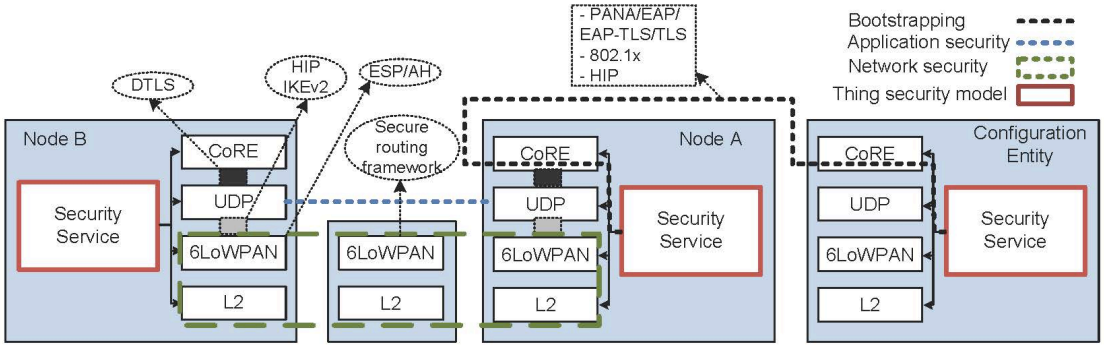

Figure 1. The relationships between IP-based security protocols[Tobias11]

The Internet Key Exchange (IKEv2)/IPsec and the Host Identity Protocol (HIP) are considered at the network layer in the OSI model. To provide a secure data delivery, both protocols use the scheme of authenticated key exchange. Also, there are there is a newer version of HIP called Diet HIP, which is being used over lossy low-power networks for the authentication and key exchanging.

Transport Layer Security (TLS) and its datagram-oriented version, DTLS, are considered at the transport layer in the OSI model. TLS provides security for TCP and provides a secure transport, while DTLS secures the datagram-oriented protocols such as UDP. Both protocols are basically similar and have the same function relatively.

The Extensible Authentication Protocol (EAP) is considered at the data link layer and as a result it does not need to the IP to be employed. This protocol supports multiple authentication methods with duplicate detection and retransmission, but fragmentation at the packets size is not allowed. The Protocol for Carrying Authentication for Network Access (PANA) is a network-layer transport for EAP for allowing to have access to the network between users. In EAP terms, PANA is a UDP-based EAP lower layer that runs between the EAP peer and the EAP authenticator.

4.5 Network segmentation

As it was mentioned before, this huge improvement in variety of type of devices will make IoT technology employ network segmentation policies. As a result, as it grows quickly, there would be thousands of dynamically configured network segments. SDN (software-defined networking) technologies will provide the required virtualization by defining the network identity and access policies for different types of traffic to apply network segments dynamically. Also, it is likely that SDN network segmentation may provide point-to-point/point-to-multi-point encryption based upon network segments and protocols [Jon14].

4.6 Automated remediation

IoT will provide the security not only inside each single network, but also, it will provide the security to be inter-networked, and as result a superior security automation intelligence, which can even predict a hazard before it happens and make required immunity before facing the problem [Jon14]. If this promising security structure for the IoT would be implemented, vast amounts of data will be generated, and consequently, it would be impossible for human beings to track the threats and alerts in real-time. Therefore, all these techniques should be supervised by automated machine intelligence to have a quick response and security control over the whole networks.

4.7 Encryption Security Solution

Encryption of information is another solution to protect the network from attack, which is widely used and popular. The most common algorithms used for encrypting are: RSA, ECC, AES, 3DES, MD5 and SHA, which are heavily computational [Arijit11]. For each possible message, a specific code is used to check the validity of the message. In addition, by using protocols such as

IPSec, the availability and authenticity will be provided for the data flow. For implying these algorithms, there should be specific dedicated processors such as Digital Signal Processors (DSP) to provide the required highly computational process. Mostly, these processors only supply one class of encryption algorithm.

Meanwhile, providing security in different layer is an important aspect which should not be forgotten. In the next section, we will have different solutions about having security in different layers.

5. Providing security on layers to defend IoT[Brian15]

The converges of IoT is an environment with millions of sensors, devices, and other smart objects. This huge convergence will cause security challenges. The first step toward designing the system, is to model all possible threats that may affect the roles or elements or data entry of the IoT system. Different scenarios of threat must be determined within different situations and then the development team should develop find security solutions by security testing. Having security through only a few layers is not enough for a completely safe implementation, as will see in the following subsections.

5.1 Network Layer

There are several methods that is used to ensure the security at network layer. For wireless networks, using Wireless Protected Access 2 (WPA2) instead of Wireless Encryption Protocol (WEP) can make the network use stronger complex wireless encryption. Also, for these networks, it is recommended to use several Service Set Identifiers (SSID), rather than just one. Hence, we can have different policies through each segment and assign each for different case of threat. As a result, if any segment gets attacked, other segments will stay safe. Also, exploiting the benefits of firewalls has other advantages. Firewalls filter the deep analytics such as Intrusion Prevention System (IPS), so the malicious traffic would stop at the port of entrance and they will be blocked. Also, using Network Access Control (NAC) to clarify the endpoint security technology such as antivirus and host intrusion prevention, will provide better safety for the network. Moreover, it is effective to index all MAC addresses for every device so that the router assigns IP addresses only to these devices and blocks any unknown devices.

On the other hand, using PPSK (Private Pre-Shared Key) for each sensor or device connected to the network. By providing different uniques keys, the access domain for each type of device can be defined easily. Also, disabling guest and default passwords in network devices such as routers and gateways should be done immediately upon unpacking a new network device. This includes strong password policies, password management and periodic change of passwords. Moreover, it is unavoidable to check the routers periodically about misconfigured NAT-PMP (NAT-Port Mapping Protocol) services. NAT-PMP is a protocol that has no any sense about the authentication mechanism and allow all hosts belonging to the router's local network to freely pass through the firewall. Misconfigured routers to NAT-PMP services are mentioned in OWASP's Top 10 Threats for Internet of Things.

5.2 Application Layer

The primary security methods that was implemented at the application will be adequate enough; therefore, the IoT does not require any specific further security implementation. Any company or vender that is selling an application should provide the security guidance for the application, for example by an efficient authorization mechanisms. For example, they should prevent from leaving any passwords in the clear in the application code; also, it is important to check for any XSS (cross-site scripting) or CSRF (Cross Site Request Forgery) vulnerabilities. Cross-site request forgery is a method of attacking a website in which the attacker conceal himself as a legitimate client, for example by changing the firewall settings. The network would not get that it has been attacked unless after the damages have been implied. OWASP (Open Web Application Security Project) recommends scanning tools such as ZAP (Zed Attack Proxy) or DAST (Dynamic Application Security Testing).

Also, it is important to check with the IoT platform vender for any vulnerabilities at the security code that might left during the platform test. This issue results from SAST (Static Application Security Testing) or DAST perspective. Using encryption for data and by using strong algorithms and adding random data to hashed data to make it harder to hack is another promising way to increase the security. However, it should be considered that based on the principles of the IoT, lightweight encryptions should be used to avoid performance degradation.

5.3 Device Layer

Sensors, gateways that aggregate data, mobile devices, cameras, RFID readers, wearables and implantable devices are examples of the devices for which we need to provide security. The device should be updated and upgraded regularly; meanwhile, it is important to check the source of the files. Also, it is important to build a strong password enforcement for the device, and change the password and default configuration regularly. Moreover, to ensure the correct functionality of the devices, they should be checked often. It is possible that by sending unauthorized radio signals, attackers would be able to reprogram the device; hence it is crucial to install and use anti-jamming device to protect our device.

5.4 Physical Layer

The basic concept of IoT is to provide connected sensors and actuators which are implemented physically in the environment. Hence, they can be available to be reached by any malicious user. For example, the sensor may be moved to another environment and produce wrong information. There would be a huge number of these sensors and actuators which is a very hard process to check them in the environment often, and see whether they are working appropriately or not[Gianmarco14].

Implementing security guidance for the physical layer has a long history even before IoT. Devices and sensors which are used in an IoT platform, need to be secured efficiently. OWASP has identified poor physical security in the top 10 IoT vulnerability. The first step is to ensure that only authorized people can have access to the data center of the secure areas, hence a physical identity and access management policy should be defined.

Some physical security tools should implemented sensitively, such as physical security controls, physical keys and monitoring cameras through the areas where the devices and sensors are implemented.

6. Summary

In this paper, first we introduced briefly the main concepts of IoT and pointed out the importance of having a secure structure for this new promising technology. we went over the current challenges associated with providing privacy which is the top essential component, because without enough security, this technology will not be useful and will just harm the human being. After that, we went through the recent solutions that have been provided, and finally, we provided the security issues at different layers of IoT. However, there is still a long way ahead to provide a complete secure structure based on the fact that IoT needs to be widespread with tremendous number of users and devices with various patterns; hence, it still needs further research to be ready before 2020.

References

[Wiki] Wikipedia
https://en.wikipedia.org/wiki/Internet_of_Things

[Chris15] Chris Folk, Dan C. Hurley, Wesley K. Kaplow, James F. X. Payne, "Security Implications of the
in AFCEA International Cyber Committee, Feb. 2015,
http://www.afcea.org/mission/intel/documents/InternetofThingsFINAL.pdf

[Gianmarco14] Gianmarco Baldini, Trevor Peirce, Maria Chiara Tallachini, "Internet of Things: IoT Governance
European Research Cluster on the Internet of Things, Jan. 2014,
http://www.internet-of-things-research.eu/pdf/IERC_Position_Paper_IoT_Governance_Privacy_

[Paul14] Paul Fremantle, Philip Scott, "A security survey of middleware for the Internet of Things"", Peer
https://peerj.com/preprints/1241v1.pdf

[Ollie14] Ollie Whitehouse, "Security of Things: An Implementers Guide to Cyber-Security for Internet of
NCC Group Publications, Apr. 2014,
https://www.nccgroup.trust/globalassets/our-research/uk/whitepapers/2014-04-09_-_security_of_
_an_implementers_guide_to_cyber_security_for_internet_of_things_devices_and_beyond-2.pdf

[Ajit14] Ajit Jha, Sunil M C., "Security considerations for Internet of Things", whitepaper, L and T Techn
http://www.lnttechservices.com/media/30090/whitepaper_security-considerations-for-internet-of

[Jon14] Jon Oltsik, "The Internet of Things: A CISO and Network Security Perspective", ESG White Pap
Systems, Oct. 2014,
https://www.cisco.com/web/strategy/docs/energy/network-security-perspective.pdf

[Rodrigo11] Rodrigo Roman, Pablo Najera, Javier Lopez, "Securing the Internet of Things", Computer Societ
58, Sep. 2011,
https://www.nics.uma.es/sites/default/files/papers/1633.pdf

[Tobias11] Tobias Heer, Oscar Garcia-Morchon, Rene Hummen, Sye Loong Keoh, Sandeep S. Kumar, Klau
in the IP-based Internet of Things", Wireless Personal Communications: An International Journa
Dec. 2011,

https://www.comsys.rwth-aachen.de/fileadmin/papers/2011/2011-heer-iot-challenges.pdf

[Arijit11] Arijit Ukil, Jaydip Sen, Sripad Koilakonda, "Embedded security for Internet of Things", Emergi Computer Science (NCETACS), 2nd National Conference on, pp. 1-6, , March 2011, http://iotsecuritylab.com/wp-content/uploads/2014/08/Embedded_Security_for_Internet_of_Thi

[Brian15] Brian Russell, Cesare Garlati, David Lingenfelter, "Security Guidance for Early Adopters of the Mobile Working Group, Apr. 2015, https://downloads.cloudsecurityalliance.org/whitepapers/Security_Guidance_for_Early_Adopter

[Acquity14] "The Internet of Things: The Future of Consumer Adoption", published in Acquity Group: Inter http://www.acquitygroup.com/docs/default-source/Whitepapers/acquitygroup-2014iotstudy.pdf

[Malisa14] Malisa Vucinic, Bernard Tourancheau, Franck Rousseau, Andrzej Duda, Laurent Damon, Rober Security Architecture for the Internet of Things", proceedings of WoWMoM, IEEE, 2014, https://cryptome.org/2014/05/oscar-iot.pdf

[Blanca14] Blanca Escribano, "Privacy and security in the Internet of Things: challenge or opportunity", Ols http://www.olswang.com/media/48315339/privacy_and_security_in_the_iot.pdf

[Raza13] Raza Shahid, "Lightweight Security Solutions for the Internet of Things", Doctoral thesis, Mlard http://soda.swedish-ict.se/5548/1/thesis.pdf

[Kim14] "Kim Rowe", 2014 http://embedded-computing.com/articles/internet-things-requirements-protocols/

Acronyms

3DES	Triple Data Encryption Algorithm
6LoWPAN	IPv6 over Low power Wireless Personal Area Networks
AES	Advanced Encryption Standard
CI	Critical Infrastructure
CSRF	Cross Site Request Forgery
CoAP	Constrained Application Protocol
CoRE	Constrained RESTful Environments
DAST	Dynamic Application Security Testing
DSP	Digital Signal Processors
DSRC	Digital Short Range Communications
DTLS	Datagram TLS
EAP	Extensible Authentication Protocol
ECC	Elliptic Curve Cryptography
FTC	Federal Trade Commission
GSM	Global System for Mobile Communications
HIP	Host Identity Protocol
HMAC	specified Hashed Message Authentication Code
IKEv2	Internet Key Exchange version 2
IPS	Intrusion Prevention System

IPsec	Internet Protocol Security
M2M	Machine to Machine
MD5	Message Digest 5
NAC	Network Access Control
NAT	Network Address Translation
NIST	National Institute of Standards and Technology
OATH	Open Authentication
OWASP	Open Web Application Security Project
PANA	Protocol for carrying Authentication for Network Access
PKI	Public Key Infrastructure
PMP	Port Mapping Protocol
PPSK	Private Pre-Shared Key
SAST	Static Application Security Testing
SDN	Software-Defined Networking
SHA	Secure Hash Algorithm
SSID	Service Set Identifiers
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
WEP	Wired Equivalent Privacy
WEP	Wireless Encryption Protocol
WPA2	Wireless Protected Access 2
XSS	Cross-Site Scripting
ZAP	Zed Attack Proxy

Last modified on November 30, 2015
This and other papers on recent advances in networking are available online at
http://www.cse.wustl.edu/~jain/cse570-15/index.html
Back to Raj Jain's Home Page