ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 5, Issue 2, pp: (143-149), Month: April - June 2017, Available at: www.researchpublish.com

Security of Internet of Things

JYOTI GUPTA

M.Tech in Software Engineering

Abstract: **IOT is playing more important role in our life day by day. We use many devices which are based on IOT at home, office, etc. IOT-Internet of Things provides many facilities to us to make life easier. With the great potential of IOT, it comes with many challenges also. As IOT is based on internet, security problem is also there. IOT works on three layers: - 1. Perception Layer, 2. Transportation Layer, 3. Application Layer. This paper will analyze the security problem of these three layer and also try to find the solutions of these problem.**

Keywords: **Internet of Things (IoT), Layers:- Perception Layer, Transport Layer, Application Layer, M2M, Bandwidth.**

I. INTRODUCTION

Today's everyone is based on technology, this technologies are also based on Internet. So there is different variety of IOT applications which uses in our daily life. They cover more equipment which makes our life better, but there are also many challenges with IOT. If we are talking about scalability, then IOT applications require large number of devices but they are more difficult to implement because of time, memory, flexibility, processing.

Nowadays, IOT is widely used in every sector. There are many IOT applications such as smart home, smart phone, access card etc. we all know todays everyone is based on smart phones. They can do all the work by using their smart phones which allow people to do many things. Some of the examples camera, wrist watches and calculator are most useful things in our life on daily basis but people have done almost all these things by using their smart phones. People are doing all the things by using smart phones which they used to do on personal computer.

These IOT applications provides better convenience way to people, but if it cannot give the proper security of personal privacy then any private information can be leaked to anyone. So the security of IOT is must if we are talking about Internet of things. We cannot be ignored the security of IOT. If IoT cannot provide solutions for security issues, nobody will not use the IOT devices. Thus from all the problems with IOT, security issue is very important.

II. MAJOR FINDINGS

With the analyses conducted in this project, it is shown that the causes for not securing devices sufficiently in many cases is oversight on the developers side more than purposefully ignoring security. Many manufactures developing devices for the home market will assume that their devices will only be used in a private setting, rely on the users network security, and that anyone connected to the same network should have the same rights to the device as the owner. This is especially the case with audio-visual systems, which often include no security on connections, firmware updates or privacy. This case was proven in a real worlds encounter at a popular venue, where the audio system of a well known manufacturer was connected to the public Wi-Fi, making it possible to control the audio in the venue, as well as manipulating the associated account for the streaming music service. Good security mechanisms can be vulnerable through flawed implementations. An analysis is made of a popular WiFi conncedted storage device that uses off the shelf security mechanisms that are part of the 802.11 specification. While the developers of this device used relatively secure mechanisms in their product for authentication, authorization and encryption.

III. DEFINING CHALLENGES AND SYSTEM CATEGORIES IN IOT

It was possible to take control of the whole system by acquiring a single packet of any type. A device is not more secure than its weakest point, and introducing Internet communication to outdated protocols and marketing them as the future of IoT does nothing but damage the future of security in IoT.

A lot can be shown from the data logged by IoT devices, but the level where this becomes a privacy issue is a matter of opinion. The question of user privacy is tackled throughout and presented in the analyses of devices, as well as in an analysis on data from a specific user, gathered from a smart-grid meter. The user's daily routine become quickly apparent, as well as when the user has been on holiday, takes a day off work, etc. We show why this is a challenge and possible solutions to the problem where it can be solved, but the overall problem with privacy is defining where exactly something becomes a privacy issue.

1. Challenges and System Categories in IoT:

Throughout the thesis, three distinct constraints are used to separate devices in IoT from traditional desktop computing, and lays the foundation for the presented challenges, namely the **power** requirement, **bandwidth** requirement and **processing** requirement. These constraints will always be present in IoT, so how one works around them, and to what degree the device is constrained by the different constraints, will define how a device and its security mechanisms are designed and implemented.

The amount of available power will strongly dictate the challenges and possible solutions available. Using the power-constraint as the main differentiator of IoT systems, the IoT space is separated into tree distinct categories:

Constrained, **Unconstrained**, and **Mixed Systems**. If a device is severely constrained by power, processing capabilities and availability will likely be low as it will not listen continuously to conserve power. One can forget LCD displays, as the common user interfaces in these devices are buttons, LEDs, microphones, or other sensors. Unconstrained devices will less often be constrained by bandwidth, but also less mobile, than any of the other categories. Mixed systems will usually include multiple types of wireless communication, and need more processing capabilities on the unconstrained nodes to process requests from the constrained devices. What approach is taken to secure a device will be decided from what category the product falls under.

A. Biggest Challenges Surfaced:

Some challenges quickly appear as the most severe, and so fundamental that they will affect all other challenges in the space. One of the hardest challenges within IoT is affected by all three of these constraints, namely the initial paring process. **Key distribution** on a device with little processing power in itself is a challenge, adding low availability and a lack of user interface makes it even harder.

In the most capable devices, the concept of Public Key Infrastructure (PKI) can be introduced to control authorization, but protocols like Secure Sockets Layer (SSL), Transport Layer Security (TLS) or Datagram Transport Layer Security (DTLS) will often require too much of an IoT device, resulting in extensive use of Pre-Shared Key (PSK) in the least capable IoT devices today. Many protocols designed for less capable devices will use a direct pairing process, usually requiring user interaction to initiate the pairing. Some solutions require push of a button, and close proximity, which is often a bad solution if the nodes are mounted in out of reach places, while others require the user to input or simply accept a pairing key. Different out of band solutions are presented such as using external ports to connect to a computer or media device, using another wireless radio such as Radio-frequency identification (RFID)/Near Field Communication (NFC), using a photo resistor (light sensor), or simply audio through a microphone.

a. Post-production management is a hard and potentially severe problem for IoT. When a product is shipped, and security vulnerability is discovered, the need to update devices will be urgent. If not, one would have to recall several batches of devices, causing a huge economic loss. We present the problems related to post-production updates, showing the possible alternatives existing today and the lack of security focus in the existing protocols. Several future solutions are presented depending on the capabilities and physical connections on the devices, both in-band, and out-of-band methods.

Emphasis is put on exactly how devastating a flawed or altered update can be, and thus urging developers to make use of authentication and authorization to ensure that the update comes from the manufacturer, and that the update has not been tampered with by a third party

b. M2M:

The early years of Internet of Things (IoT) started with Machine to Machine to machine (M2M) communication. While M2M is still an ambiguous term, it is more specific than the IoT term. Machine to Machine communication indicates two machines communicating with each other, usually without human involvement. The communication platform is not defined, and can be both wireless and wired communication.

The term M2M stems from telephony systems. In these systems, different endpoints needed to exchange information between each other, such as the identity of the caller. This information was sent between the endpoints without a human being needed to initiate the transmission. The M2M term is still very much in use, especially in the industrial market, and is commonly regarded as a subset of IoT.

In later years, the M2M acronym has been given alternate meanings such as Machine to Mobile, Machine to Man, Mobile to Mobile, Mobile to Man etc. [JS10], but these are not in wide use.

IV. CHALLENGES IN INTERNET OF THINGS

The Internet of Things is facing security challenges that differ vastly from regular desktop computing, due to the unique constraints. In this chapter we show the main constraints, what challenges they cause, and challenges that will surface in the future.

The challenges that are presented includes some of the typical challenges within IT security such as authentication, authorization, availability and confidentiality, and also challenges such as privacy, usability, DoS and physical security which are not **as** prominent challenges in the more classical computer systems. While other factors such as psychological, economical, environmental and political will impact the future of IoT, and possibly present other challenges, this is considered to be beyond the scope of the thesis.

a. Constraints:

There are many limiting factors associated with security in the Internet of things, the three most prominent being:

a) Processing capability

b) Power requirements

c) Bandwidth requirements

When faced with these constraints, one will quickly understand that we cannot simply use the same security features as are used in desktop computers without considering how it will impact our devices.

a) Processing capability is becoming less of an issue as time passes, as increasingly faster chips are developed every year. How much of an impact processing performance has on a device will be dependent on the type of device. If it is not important that the device is ready to receive data or act on events all the time, processing speed will not be an issue in that regard. Such devices will typically be temperature sensors that transmit on set intervals. If the chip knows that it will need to transmit sensor values every *X* minutes, it will be able to encrypt the payload in between each measurement. But it the device needs to act on certain events such as motion and need to report this data in real time, it cannot be preoccupied with encryption over a long time.

b) Power requirements are a big problem with the current Internet of Things. The device's power usage will have an impact on processing speed, bandwidth, and temperature and/or battery life. As many of the devices are operating with a battery as the only energy source, it is desirable to have the longest operating time possible and thus low power usage. But whatever way we look at it, securing data will require increased power usage compared to no security, as some form of computation is required and all computation will consume power.

But even though we include security mechanisms in the devices, there are many differences between what solutions we implement. There are clear differences in between different encryption algorithms, key generation algorithms, digital signature algorithms and hashing algorithms with regards to power efficiency [RPHJ11]. In addition, different chips will also have an impact on how these algorithms perform.

c) Bandwidth is often a scarce resource in the Internet of things. To conserve energy and keep heat waste low, one needs to power the radio for as short amount of time as possible. This means that one would like to use as high frequency as possible, and have as small payload as possible to transmit data quickly. But with higher frequency, the range of the wireless radio decreases, and we need to increase transmission power to transmit data over longer distances. At the same time we do not want to waste power by having the signal reach further than necessary. One thus needs to find the best intersection between the desired speed and range for the specific application depending on payload and available power.

Encrypted data will always cause some bandwidth overhead, but the impact on the actual packet size has not been prohibitive until now, as packet sizes have been relatively large in traditional network systems. With protocols specifically tailored for the Internet of Things, on the other hand, the percentage increase in packet size is becoming prohibitive as the packet size is compressed to the bare minimum.

Balancing these three factors is crucial for any device in the Internet of Things. Currently, when designing new devices, one need to make trade-offs, and decide which to make for each specific case:

To preserve computational power one can offload processing to central servers, but this will require transmitting more data or more often, resulting in energy usage by the wireless radio rather than the processor. If we instead process the data locally before transmission, we reduce energy cost in the radio, but increase processing and storage cost in the device. To reduce power cost in the radio, one can use adaptive power control for the radio, but this will require slightly more processing, and can increase retransmissions as a result of increased packet loss if the distance or interference is highly variable.

Another solution often used in IoT is the concept of a central hub, handling communication between two different networks, with different constraints. This concept is implemented in wireless sensor networks, and home automation systems amongst others. The hub is often not constrained by power, but is not placed where there is a need for the service, and thus constrained by the environment. These hubs are usually a link between network connections with long range requiring large amounts of power, like cell-networks, parabola-connections or Wi-Fi-connections, and network connections with shorter range, but low power requirements such as

ZigBee, Z-Wave or Bluetooth Low Energy. In wireless sensor networks, devices will report their data to the hub directly, often using a form of mesh networking, and the hub will then forward either processed or unprocessed data to central storage.

b. Current Challenges:

The current Internet of Things is considered quite simple compared to what is theoretically possible. Many devices will connect to a phone acting as a hub to a central server, connect to a stationary home hub, or connect directly to a central server. Some devices will use a mesh network connected to a hub to communicate with a central server.

During this section, the different current and future challenges in IoT are presented.

Authorization:

Authorization is the act of granting access to different parts of the system only to devices that should have access. Authorizing a device within IoT have some challenges that does not exist in desktop computing, where the concept of a user with different user-names and passwords will be entered into the service a user wishes to use. In IoT, the user is not actively using the device through an advanced user interface. As devices are physical, they can be lost or sold to other users, and thus the principle of "a single device equals a single user" will not be viable. The concept within IoT can better be explained as a user using both a service and a device, with these three.

V. SOLUTION TO CHANGES IN INTERNET of THINGS

a. Authorization:

Many simpler back-end systems in the Internet of Things will typically use a unique client key in the header of a request to authorize a device to communicate with the back-end. This will require an adversary to get a hold of the key to access the device, and if an encrypted connection is required to communicate, will be a viable solution. If this solution is to be

utilized, the key is required to be transferred to the device, either after the encrypted connection is set up, or during production.

Products that can handle a standard HTTP TLS connection will usually use this to communicate with the back-end and transfer the key. Though if the product is capable of communicating in this way, we are closer to a basic networked computer, and might as well use regular account login to the back-end using a mobile application, and receiving a device-specific access token related to the user account.

Authorization should ideally be on device-level, and related to a user as a separate value, as we should be able to exclude lost devices without excluding the user account, and grant different permissions to different devices that the same user owns. As the unique value specifically defines a device, it does not need to be changed during the life of a product, and can be added during production. But as it needs to be related to the user in some way, a system for association still needs to be implemented, and will usually be a part of the key distribution process.

b. Authentication:

Using authenticated encryption as explained in Sect. 2.3, any changes made by an adversary in transit would be detected as the MAC would not match. For an adversary to be able to manipulate data, they would need to have the correct key used to generate the MAC.

An ongoing competition called Competition for Authenticated Encryption: Security, Applicability, and Robustness (CAESAR) is currently running to provide new authenticated encryption algorithms.

c. Reduce Bandwidth Overhead:

To reduce the bandwidth needed, one wants to transmit data only when needed and keep the packet small, while still keeping the need for retransmissions to the minimum. Several protocols are designed specifically with this goal in mind, but their use is often limited to a specific use case, and no **one** general solution exists

VI. CONCLUSION

While the concept of combining computers, sensors, and networks to monitor and control devices has been around for decades, the recent confluence of key technologies and market trends is ushering in a new reality for the "Internet of Things''. IoT promises to usher in a revolutionary, fully interconnected "smart" world, with relationships between objects and their environment and objects and people becoming more tightly intertwined. The prospect of the Internet of Things as a ubiquitous array of devices bound to the Internet might fundamentally change how people think about what it means to be "online".

The Internet of Things is happening now, and there is a need to address its challenges and maximize its benefits while reducing its risks. The Internet Society cares about IoT because it represents a growing aspect of how people and institutions are likely to interact with and incorporate the Internet and network connectivity into their personal, social, and economic lives. Solutions to maximizing the benefits of IoT while minimizing the risks will not be found by engaging in a polarized debate that pits the promises of IoT against its possible perils. Rather, it will take informed engagement, dialogue, and collaboration across a range of stakeholders to plot the most effective ways forward.

REFERENCES

[1] Allgemeiner Deutscher Automobil-Club (ADAC). Sicherheitslücken bei bmw connected drive. January 2015. Available at http://www.adac.de/sicherheitsluecken.

[2] P. Karlton A. Freier and P. Kocher. The secure sockets layer (ssl) protocol version 3.0. RFC6101, 2011.

[3] National Security Agency. The case for elliptic curve cryptography. January 2009. Available at https://www. nsa.gov/business/programs/elliptic_curve.shtml.

[4] Amazon. Dash button. August 2015. Available at https://www.amazon.com/oc/dash-button.

[5] Carna Botnet (anonymous). Internet census 2012. October 2012. Available at http://internetcensus 2012.bitbucket. org/paper.html.

[6] Kevin Ashton. That 'internet of things' thing. June 2009. Available at http: //www.rfidjournal.com/ articles/pdf? 4986.

[7] August. Smart lock. Available at http://august.com.

[8] Daniela Miao Michael Specter Britt Cyr, Webb Horn. Security analysis of wearable fitness devices (fitbit). September 2014. Available at https://courses.csail.mit. edu/6.857/2014/files/17-cyrbritt-webbhorn-specter-dmiao-hacking-fitbit.pdf.

[9] Paul Brody and Veena Pureswaran (IBM). Device democracy. September 2014. Available at http://www-935.ibm.com/services/us/gbs/thoughtleadership/internetofthings/.

[10] Xiangqian Chen, Kia Makki, Kang Yen, and Niki Pissinou. Sensor network security: a survey. Communications Surveys & Tutorials, IEEE, 11(2):52–73, 2009.

[11] Summit Data Communications. Ble overview. February 2013. Available at http://www.summitdata.com/blog/ble-overview/.

[12] US Federal Trade Commission. Internet of things – privacy & security in a connected world January 2015. Available at http://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things privacy/150127iotrpt.pdf.

[13] cr.yp.to. Caesar: Competition for authenticated encryption: Security, applicability, and robustness. May 2015. Available at http://competitions.cr.yp.to/caesar.html.

[14] T. Dierks and C. Allen. The tls protocol version 1.0. RFC2246, 1999.

[15] Josh Datko. Crypto for makers - projects for the beaglebone, pi and avrs. July 2014. Available at https://jbdatko.files.wordpress.com/2014/07/cryptomakers_nopause.pdf.

[16] Tim Dierks. Security standards and name changes in the browser wars. May 2014. Available at http://tim.dierks.org/2014/05/security-standards-and-name-changes-in.html.

[17] Tanja Lange Daniel J. Bernstein. Security dangers of the nist curves. May 2013. Available at http://www.hyperelliptic.org/tanja/vortraege/20130531.pdf.

[18] Adam Dunkels, Luca Mottola, Nicolas Tsiftes, Fredrik Österlind, Joakim Eriksson, and Niclas Finne. The announcement layer: Beacon coordination for the sensornet stack. In Wireless sensor networks, pages 211–226. Springer, 2011.

[19] J. Loughney E. Jankiewicz and T. Narten. Ipv6 node requirements. RFC6434, 2011.

[20] IPSO ETSI and OMA. Coap#3 and oma lwm2m plugtests. 2013. Available at https://portal.etsi.org/CTI/Downloads/TestReports/CoAP3_LWM2M_ Plugtest_TestReport_v1.0.pdf.

[21] FitBit. Integrate with ios 8 health app. October 2014. Available at https://community.fitbit.com/t5/Feature-Requests/Integrate-with-iOS-8-Health-App/idi-p/319432.

[22] Fortinet. Internet of things: Connected home - survey results. June 2014. Available at http://www.fortinet.com/press_ releases/2014/internet-of-things.html.

[23] Broadband Forum. Tr-069 gears up for ten more years as device management evolves to services management. June 2014. Available at http://www.broadbandforum.org/news/download/pressreleeases/2014/BBF_Q2meeting_TR-069_FINAL_25June2014.pdf.

[24] Carles Gomez, Joaquim Oller, and Josep Paradells. Overview and evaluation of bluetooth low energy: An emerging low-power wireless technology. Sensors,12(9):11734–11753, 2012.

[25] Bluetooth Special Interest Group. Bluetooth core specifications. December 2014. Available at https://www.bluetooth. org/en-us/specification/adopted-specifications.

[26] Bluetooth Special Interest Group. Bluetooth le security developer documentation. December 2014. Available at https://developer.bluetooth.org/TechnologyOverview/Pages/LE Security.aspx.

[27] Portal Guard. Quantifying the costs of hacking. May 2012. Available at http: //www.portalguard.com/costs_ of_hacking.html.

[28] K Hartke and O Bergmann. Datagram transport layer security in constrained environments, 2012. Available at http://www.ietf.org/proceedings/83/slides/slides-83-lwig-2.pdf.

[29] Hewlett-Packard. Internet of things research study. July 2014. Available at http://h30499.www3.hp.com/ hpeb/attachments/hpeb/application-security-fortify-on-demand/189/1/HP_IoT_Research_Study.pdf.

[30] Anil Jain, Lin Hong, and Sharath Pankanti. Biometric identification. Communications of the ACM, 43(2):90–98, 2000.

[31] Philipp Jovanovic and Samuel Neves. Dumb crypto in smart grids: Practical cryptanalysis of the open smart grid protocol. Cryptology ePrint Archive, Report 2015/428, 2015.

[32] Du Jiang and Chao ShiWei. A study of information security for m2m of iot. In Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on, volume 3, pages V3–576. IEEE, 2010.