Internet of Things: Security Challenges for Next Generation Networks

KrishnaKanth Gupta
Amity School of Engineering and Technology
Amity University UttarPradesh
Noida, India
Krishnaknth143@gmail.com

Sapna Shukla
Amity School of Engineering and Technology
Amity University UttarPradesh
Noida, India
sshukla@amity.edu

Abstract – Internet of Things(IoT) is the next big boom in the networking field. The vision of IoT is to connect daily used objects (which have the ability of sensing and actuation) to the Internet. This may or may or may not involve human. IoT field is still maturing and has many open issues. We build up on the security issues. As the devices have low computational power and low memory the existing security mechanisms (which are a necessity) should also be optimized accordingly or a clean slate approach needs to be followed. This is a survey paper to focus on the security aspects of IoT. We further also discuss the open challenges in this field.

Keywords –Internet of things, security challenges, Next generation networks

I. INTRODUCTION

Internet of things (IoT) is more than machine to machine communication. "IoT is a network of dedicated physical objects (things) that contain embedded technology to sense or interact with their internal state or external environment. The IoT comprises an ecosystem that includes things, communication, applications and data analysis.[1][16]". Massive objects are to be connected to internet. The objects will communicate with other objects by pervasive computing but there is heterogeneity in the architectures. On top of this security is another big challenge in IoT implementation. Main challenge of IoT is to reduce power consumption and minimize the utilization of resources.

IoT finds application in many fields like medicine(e.g. monitoring pulse rate of patient and keeping track of the data and with raw data it will specify or send the information to doctor about it), Home automation (e.g. controlling room temperature), Industrial plants (e.g. Quality control), Fitness equipment (e.g. calories to be burnt) , Smart cities (e.g. bus on way signal to daily commuters) etc. Wireless sensor networks which are connotations of IoT can show us some solutions. Wireless sensor networks is used to sense the object and transmit the information, for sensing it doesn't need much computation power but transmitting the sensed data needs some communication path which may lead to security issue.

In this paper we discuss the design considerations in form of challenges in section II, section III discusses the need for rethinking on security with the IoT dimension. Section IV discusses the ongoing research in the security field of IoT and section V concludes the paper.

II. CHALLENGES IN IOT

Various challenges that have to be considered while designing any protocol or architecture for the IoT are described below.

*Massive scaling***:** The smart devices being deployed in the network are large in number so, we need to give authentication, maintaining, protecting, use, and support of such large things are major problem. Many of things in network will require their own energy source will energy scavenging and enormously low power circuits eliminate the need for batteries? Collection of data and its storing and usage of it may concern in massive scaling.

*Architecture and dependencies***:**
[21-23]As many things are connected to internet it is necessary to have an adequate architecture that permits easy connectivity, control, communications, and useful applications. Coming to dependencies how will these objects interact in and across applications? Many things or set of things must be disjoint and protected from other devices. At other times it makes sense to share devices and information. One possible approach is to borrow ideas from smart phone world.

*Big Data being generated***:**
[20]In IoT there will exist a vast amount of raw data being continuously collected. It will be necessary to develop techniques to convert raw data into usable knowledge. For example this can be more helpful in medical stream by monitoring the person heart rate, pulse, blood pressure and that raw data should be converted into usable knowledge by giving precautions to person or doctor like medical streams it can be implemented in many fields like industrial, home appliances.

*Robustness***:**
[20]IoT applications works on the basics of sensing, automation and computation platform. In this deployments it is common for devices to know their locations, have synchronized clocks, know their neighbour devices when cooperating and have coherent set of parameter settings such as consistency, sleep, awake schedules, appropriate power levels for communication.

Security & Privacy :

978-1-5090-2084-3/16/$/31.00©2016 IEEE

[21]Privacy is the most concern in IOT , the data which storing in cloud using big data should not be seen by any other person. To solve these problems privacy policies for each system should be specified. Once specified either the individual IOT applications or the IOT infrastructure must enforce privacy.

The fundamental problem that is pervasive computing in the internet today that must be solved is dealing with security attacks. Security attacks are problematic for the IOT because of the minimal capacity of things be used, the physical accessibility sensors, actuators and objects, and the openness of the system, including the fact that most devices will communicate wirelessly. Backdoor is the most concern in IOT security which can caused by vendors while at updates of things happen. Identifying and naming of the object is also an important thing in IOT. And use of wireless sensor networks plays a crusial role in IOT which may leads to security issues.

III. Need for Security in IoT Network

By 2020 Gartner has predicted that 25 billion IoT will be used. Table 1 shows the various categories of industries that will be using IoT.

Table 1
Internet of Things Units Installed Base by Category[16]

Category	2013	2014	2015	2020
Automotive	96.0	189.6	372.3	3,511.1
Consumer	1,842.1	2,244.5	2.874.9	13,172.5
Generic Business	395.2	479.4	623.9	5,158.6
Vertical Business	698.7	836.5	1,009.4	3,164.4
Grand Total	3,032.0	3,750.0	4,880.6	25,006.6

Institute of Electrical and Electronics Engineers(IEEE) and Internet Engineering Task Force(IETF) is also working towards the design of communication and security issues of IoT. New distributed applications would be developed for communication between IoT (which are constrained devices) and the Internet.

IV. Ongoing Research and Challenges in IoT Security

Any security mechanism should be designed to provide confidentiality, integrity, authentication and non-repudiation.

A. *Identifying and locating object in IoT*

[1][2]Identifying an object in any network is the first issue, proper and scalable identification method is the foundation of IoT. Identification methodology not only defines the object's uniqueness but also gives the network location of the object which is also important. Domain name system (DNS) is a good method of identifying a host. Host's property is reflected through fully qualified domain name (FQDN) naming policy, and provides address mapping through DNS resolution. Based on the success of DNS, object name service (ONS) is published. Locating an object is done by IP addressing like IPv4/IPv6.Named Data Networking (NDN).

Challenges in this are object identification to ensure the integrity of records used in naming architecture. Although Domain Name Systems provide name translation but still it is insecure naming system. Attacks like man in the middle attack, DNS cache poisoning attack is possible. So a new naming service suitable for IoT architecture is required.

B. *Authentication and authorization in IoT*

Authentication of object is an important issue. Authentication can be achieved by many methods like ID/password, pre-shared secrets, public key crypto systems. Authorization can be achieved by database-based or crypto-based access control. But due to heterogeneity and complexity of the objects and networks in IoT, traditional authentication and authorization methods may not be applicable. Rapidly growing no of objects will make key management a difficult task. A scalable solution is a must. Some research [3][4] has attempted to resolve this problem but no common agreements are made and still it's a challenging area.

C. *Privacy in IoT*

Information about user behaviour is collected to enrich the user experience in the Internet. The same applies to IoT and so preserving the privacy of the collected data is an issue to be addressed so that personal information cannot be misused. Challenges in this section are divided into two categories, one is data collection policy which describes the policy during data collection where it enforces the type of collectable data and access control of a thing to data. Second challenge is data cleansing to ensure data anonymity. Both cryptographic protection and concealment of data relations are desirable.

D. *Lightweight Cryptosystems and security protocols*

In IoT there are various resource-constrained devices such as sensor nodes, pervasive computing devices which have commonly limited computing power, this may not be suitable for constrained devices.

Symmetric-key cryptosystems, public-key cryptosystems provides more security features but require high computational power. Public-key cryptosystems are often desirable when data integrity and authentication are needed. Therefore cryptosystems and security protocols which require less computational power remains a challenge for IoT security. Some research work [5][6] are targeted towards this problem.

E. *Software vulnerability in IOT*

[10][11][12][13]Software vulnerability plays an important role in current research domain. During the development stage of a piece of software, programming bugs are produced by developers and are unavoidable. This leads to software vulnerability. Software vulnerabilities lead to number of backdoor security breaches. First attackers exercise malicious intents without any artifact in a victim's system. A backdoor can be planted in a vulnerable device by attackers to control

device. Due to resource constraints security mechanisms can't be applied in IoT. Another type of back door is easy to deploy by product distributors or maker's for management or testing purpose. This kind of examination has been done with system updates and security patches which cause backdoor security breaches which can be easily deployed but are hard to examine.

E. Operating system platforms

Adapting to operating system of mobile devices platform's may create security issues. For example the IoT developers are attracted towards Anrdoid platform which is popular operating system for many pervasive devices because of it's open and embedded system oriented design. Many of its features are adopted in IoT devices like power saving, near field communication, voice control, multi sensors. Besides platform's like IOS, windows, Mozilla OS, Anroid is supported by a large development community and hence bootstrapping IoT towards many possible directions.

If heterogeneous devices connect to android system forming personal area network (PAN), the security issues specifically for android will be brought up. Google announced bouncer for protecting apps, the price of being penetrated rises and the attack will be amplified. Deeper analysis into such possibilities is desirable [7]. Insiders attacks are most challenging issue to deal with, and this issue is not well addressed although some researchers made attempts to address policy enforcement in [8][9].

F. By wireless sensor networks

Wireless sensor network plays an important role in IoT, the issue causing in wireless sensor networks are false node, node modification, DDOs attacks, node malfunction, message corruption, traffic analysis, spoofed attacks, skin hole attacks, Sybil attacks, worm hole attacks in wireless sensor networks. Authentication, cryptographic algorithms can't be implemented on wireless networks because of constrained resources, low computational power. There are many security approaches which are providing security for wireless sensor networks[14][15].

V. CONCLUSION

So by this paper we discuss the present IoT challenges and issues on IoT security. We also discuss the design guidelines to be considered while designing any solution for the IoT.

REFERENCES

[1] GS1, *Object Name Service (ONS) Standard* [Online]. http://www.gs1.org/gsmp/kc/epcglobal/ons/, accessed on October 8, 2014

[2] L. Zhang, A. Afanasyev, J. Burke, claffy, L. Wang, V. Jacobson, P. Crowley, C. Papadopoulos, B. Zhang, "Named Data Networking," in *ACM SIGCOMM Computer Communication Review*, July 2014

[3] W. Shang, Q. Ding, A. Marianantoni, J. Burke, and L. Zhang,"Securing building management systems using named data networking," IEEE Network Special Issue on Information-Centric Networking, April 2014.

[4] J. Liu, Y. Xiao, and C. L. P. Chen. "Authentication and Access Control in the Internet of Things," In *IEEE 32nd International Conference on Distributed Computing Systems Workshops*, June 2012.

[5] Cole, Peter H., and Damith C. Ranasinghe. "*Networked RFID systems and lightweight cryptography*," London, UK: Springer. doi 10 (2008): 978-3. 233

[6] S. Raza, H. Shafagh, K. Hewage, R. Hummen, and T. Voigt, "Lithe: Lightweight Secure CoAP for the Internet of Things," in *IEEE Sensors Journal*, Vol. 13(10), 2013.

[7] Z. Yang, M. Yang, Y. Zhang, G. Gu, P. Ning, and X. S. Wang, "Appintent: Analyzing sensitive data transmission in android for privacy leakage detection," in *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, 2013, pp.1043–1054.

[8] M. Conti, V. T. N. Nguyen, and B. Crispo, "Crepe: context-related policy enforcement for android," in *Information Security*, Springer,2011, pp. 331–345.

[9] K. Z. Chen, N. M. Johnson, V. D'Silva, S. Dai, K. MacNamara, T. R.Magrino, E. X. Wu, M. Rinard, and D. X.Song, "Contextual Policy Enforcement in Android Applications with Permission EventGraphs," in *NDSS*, 2013.pg.234

[10] A. Cui and S. J. Stolfo, "Reflections on the engineering and operation of a large-scale embedded device vulnerability scanner," In *BADGERS. ACM*, Apr. 2011.

[11] A. Costin, J. Zaddach, A. Francillon, and D. Balzarotti. "A Large Scale Analysis of the Security of Embedded Firmwares," In *USENIX Security Symposium*, August 2014.

[12] D.Davidson, B.Moench, S.Jha, and T.Ristenpart. "FIE on Firmware: Finding Vulnerabilities in Embedded Systems Using Symbolic Execution," In *USENIX Security Symposium*, August 2013.

[13] J. Zaddach, L. Bruno, A. Francillon, and D. Balzarotti. "Avatar: A Framework to Support Dynamic Security Analysis of Embedded Systems' Firmwares," In *Network and Distributed System Security Symposium*, February 2014

[14] "Security in Wireless Sensor Networks: Issues and Challenges"Al-Sakib Khan pathan, Hyung-Woo Lee,Choong Seon Hong ,Kyung Hee Advanced Communication Technology, 2006. ICACT 2006. The 8th International Conference

[15] "Security Issues in Wireless Sensor Networks", Tanveer Zia and Albert Zomaya, Systems and Networks Communications, 2006. ICSNC '06. International Conference onDate of Conference:Oct. 2006.

[16] www.gartner.com

[17] Research Directions for the Internet of Things, John A. Stankovic, *Life Fellow, IEEE*

[18]IEEE Standard for Local and Metropolitan Area Networks—Part 15.4:Low-Rate Wireless Personal Area Networks (LR-WPANs), IEEE Std.802.15.4-2011 (Revision of IEEE Std. 802.15.4-2006), (2011) 1-314, 2011.

[19]*IEEE Standard for Local and Metropolitan Area Networks—Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment 1: MAC Sublayer*, IEEE Std. 802.15.4e-2012 (Amendment to IEEE Std. 802.15.4-2011), (2011) 1-225, 2012.

[20]N. Kushalnagar, G. Montenegro, and C. Schumacher, IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, Goals, RFC 4919, 2007.

[21] J. Hui and P. Thubert, Compression Format for IPv6 Datagrams Over IEEE 802.15.4-Based Networks, RFC 6282, 2011.

[22] P. Thubert *et al.*, RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks, RFC 6550, 2012.

[23] C. Bormann, A. Castellani, and Z. Shelby, "CoAP: An application protocol for billions of tiny Internet nodes," *IEEE Internet Comput.*, vol. 1, no. 2, pp. 62–67, Mar./Apr. 2012.