International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 19 (2017) pp. 8270-8272
© Research India Publications. http://www.ripublication.com

A Roadmap to Security in IoT

Raman Dugyala
Professor, Computer Science and Engineering Department, Vardhaman College of Engineering,

N Hanuman Reddy
Associate Professor, Computer Science and Engineering Department, Vardhaman College of Engineering

N. Chandra Sekhar Reddy
Professor, Department of Computer Science and Engineering, MLR Institute of Technology

J. Phani Prasad
Assistant Professor, Computer Science and Engineering Department, Vardhaman College of Engineering

Abstract

It is a known fact that IoT is the most talked about future technology these days. It is nothing but connecting the physical world to the cyber world through internet. Our daily physical devices can be connected by incorporating software programmes, sensors and embedded electronic circuits to feel their presence in the Web and also helping the humans to control/ operate the devices through internet connectivity / connected devices viz., Smart Phone, Tablets, PCs. But same as any upcoming technologies, IoT too has many hurdles in its implementation, security being the most important.

After the huge WikiLeaks expose during Mar-17 that CIA can spy on people using any device connected to Internet such as your Smart TV, or a Camera or even your Microwave Owen, the idea of security in IoT rang very serious bells among industry experts. And the recent ransomware attacks rubbed some more salt in to the wounds. Both the incidents sent tremors throughout the security world and gave birth to yet another discussion on how secure is the future technology that the world is moving towards, i.e., IoT. Here in this paper, I try to shed some light on the basic security concerns and most happening security technologies of IoT.

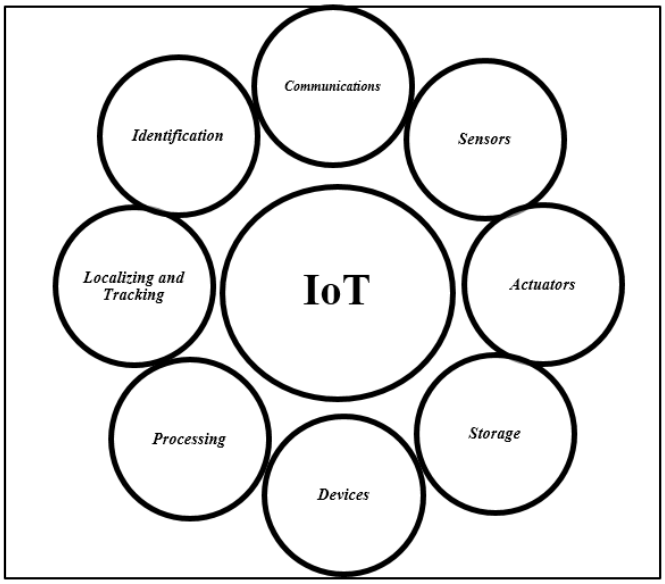
INTRODUCTION

With the emerging wireless communications, electronics, micro-electro mechanical systems (MEMS), and mobile computing, IoT is developing rapidly, and being applied both in the industrial and academic research and also in day to day life [3], viz., smart grid [4], e-health [5], environment monitoring [6], e-home, smart cities and so on. By way of connecting sensors, smart devices and intelligent daily things with the Internet, the data can be captured or re-distributed automatically and virtual world of information can be incorporated seamlessly with the real world [7]. IoT based Applications not only help people live smartly and easily, but also bring various challenges. For one instance, according to the unique architecture proposed by H. Ning and H. Liu [8], pervasive data gathering is vital in the perception layer. Moreover, the application layer will be accountable for data processing, which will require allocation of the composed data among its users. The other issue being, with more sensors existing and able to be connected to the user for assembling data, individuals need to regulate their personal data and secure the data and preserve the privacy. These two contradicting aspects create the data collection, dispersal and application bring more complex security challenges in IoT applications. For example, in a unique IoT application as smart city, information is normally gathered from many sources owned by several administrative domains (e.g., Public/Private transport providers and smart phones). The information collection can be done without the knowledge of user and data transmission could be in plaintext. As the huge data collected is shared among various sectors, that may be accessible to unauthorized users which may cause serious security issues or can even be made use of to harm the privacy of owners of the information if there are no security restrictions on it. Another example is, consider the case of medical monitoring wherein, the data collected through the body sensors on a patient should always be transmitted to the central medical server of the clinic and should be accessible to only the specified doctors, as the body data is sensitive data. The privacy can be exploited if it is sent in plaintext or without any proper access control restrictions on it. Also, the

multi-hop wireless broadcast mode in IoT is vulnerable to eavesdropping.

FRAMEWORK

Before working on the security of IoT one should have a closer look at the framework of the IoT.



The first level of devices can be seen in the above figure viz., Sensors, Actuators, smart devices e.t.c. Hence the primary objective of any IoT security analyst will be defending the path between the devices and the Internet as the data must flow between these devices to any other controlling devices through this path.

A. *Network Security in IoT:* Securing the path between the application devices and the network will be a difficult task compared to other securing mechanisms since it involves various protocols used by various devices. The problem becomes more complex if different standards, potentials of the devices.

B. *Encryption in IoT:* The data flowing between the devices has to be encrypted which seems quite typical but once the motion of the devices is considered there will be challenges in deciding the protocols that are to be used while static and also while in motion. As said earlier the boundless variety of devices adds complexity to the problem.

C. *IoT Validation:* Any IoT system would require to provide its users the ability to validate / authenticate IoT device. This may also include allowing users in manifold to validate the devices as in case of a connected Home.

D. *Installing digital certificates:* The IoT devices need to be loaded with digital certificates either before commercial use or even after installing them at the user premises. This challenge include giving X.509 digital certification, providing framework for Public / Private key creation, administration, renouncing the keys created, and also governing the keys.

E. *Securing data Analytics:* Since IoT is an amalgam of devices communicating among them, there needs to be a centralized monitoring system that analyses the flow of data between the devices to check if there is any deviation from the predetermined path specifics. This involves anticipatory modelling of the data and also exception detection. Research is in progress to use AI, Big Data and Machine learning to attain aforesaid objectives.

F. *Application Security:* As discussed above, the data flow between various devices and back end network can be validated and authenticated using APIs. Automatically, the security of the APIs used has to be ensured to maintain overall security of the IoT system.

G. *Updates:* Another important aspect of maintaining an IoT system will be facing the challenge of providing continuous updates to the devices in IoT. There comes the problem of sending the updates securely using the protocols for OTA updates.

CONCLUSION AND FUTURE WORK

Various aspects of security challenges faced in developing and maintaining an IoT system were discussed in brief. This can be viewed as a roadmap for budding researchers looking to work on the security platform of IoT. However, there can be more unforeseen issues while fully rolling out the IoT systems which require situation specific solutions to the issues. I intend to dig deeper and bring more issues in the same line to continue this work further.

REFERENCES

[1] https://www.forbes.com/sites/gilpress/2017/03/20/6-hot-internet-of-things-iot-security-technologies/#3a8f99181b49

[2] https://www.forrester.com/report/TechRadar+Internet+Of+Things+Security+Q1+2017/-/E-RES117394

[3] J. Gubbia, R. Buyyab, S. Marusic, M. Palaniswami, Internet of Things (IoT): a vision, architectural elements, and future directions, Future Gener. Comput. Syst. 29 (2013) 1645–1660.

[4] M. Yun, B. Yuxin, Research on the architecture and key technology of Internet of Things (IoT) applied on smart grid, in: Advances in Energy Engineering, ICAEE, 2010, pp. 69–72.

[5] S.T. Ali, V. Sivaraman, D. Ostry, Authentication of lossy data in body-sensor networks for cloud-based

healthcare monitoring, Future Gener. Comput. Syst. 35 (2014) 80–90.

[6] N. Dlodlo, Adopting the Internet of Things technologies in environmental management in South Africa.2012, in: Proc. International Conference on Environment Science and Engineering, Singapore, vol. 3, 2012, pp. 45–55.

[7] D. Bandyopadhyay, J. Sen, Internet of Things: applications and challenges in technology and standardization, Wirel. Pers. Commun. 58 (1) (2011) 49–69.

[8] H. Ning, H. Liu, Cyberentity security in the Internet of Things computer, IEEE Comput. Soc. 46 (4) (2013) 46–53.

[9] R. Roman, P. Najera, J. Lpoez, Secure the Internet of Thing, IEEE Comput. 44 (9) (2011) 51–58.

[10] H. Ning, H. Liu, L.T. Yang, Aggregated-proof based hierarchical authentication scheme for the Internet of Things, IEEE Trans. Parallel Distrib. Syst. (99) (2014) 1–11.

[11] A. Sahai, B. Waters, Fuzzy identity-based encryption, in: Advances in Cryptology-EUROCRYPT 2005, in: LNCS, vol. 3494, Springer-Verlag, Aarhus, Denmark, Berlin, 2005, pp. 457–473.

[12] A. Fiat, M. Naor, Broadcast encryption, in: Advances in Cryptology-Crypto93,in: Lecture Notes in Computer Science, vol. 773, 1994, pp. 480–491.

[13] V. Goyal, O. Pandey, A. Sahai, B. Waters, Attribute-based encryption for finegrained access control of encrypted data, in: Proceedings of the 13th ACM Conference on Computer and Communications Security, CCS'06, ACM, NewYork, NY, USA, 2006, pp. 89–98.

[14] J. Bethencourt, A. Sahai, B. Waters, Ciphertext-policy attribute-based encryption,in: Proceedings of the 2007 IEEE Symposium on Security and Privacy, SP'07, IEEE Computer Society, Washington, DC, USA, 2007, pp. 321–334.

[15] R. Ostrovsky, A. Sahai, B. Waters, Attribute-based encryption with nonmonotonic access structures, in: Proceedings of the 14th ACM Conference on Computer and Communications Security, ACM, 2007, pp. 195–203.

[16] B. Waters, Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization, in: D. Catalano, N. Fazio, R. Gennaro, A. Nicolosi (Eds.), PKC 2011, in: LNCS, vol. 6571, Springer, Heidelberg, 2011, pp. 53–70.

[17] N. Attrapadung, B. Liber, E. de Panafieu, Expressive key-policy attribute-based encryption with constant-size ciphertexts, in: PKC 2011, in: LNCS, vol. 6571, 2011, pp. 90–108.

[18] C. Wang, J. Luo, A key-policy attribute-based encryption scheme with constant size ciphertext. in: 2012 Eighth International Conference on Computational Intelligence and Security, pp. 447–451.

[19] C. Chen, Z. Zhang, D. Feng, Efficient ciphertext policy attribute-based encryption with constant-size ciphertext and constant computation-cost, in: X. Boyen, X. Chen (Eds.), ProvSec 2011, in: LNCS, vol. 6980, Springer-Verlag, Berlin, Heidelberg, 2011, pp. 84–101.

[20] P. Junod, A. Karlov, An efficient public-key attribute-based broadcast encryption scheme allowing arbitrary access policies, in: DRM'10, Chicago, Illinois, USA, October 4, 2010.

[21] D. Lubicz, T. Sirvent, Attribute-based broadcast encryption scheme made efficient, in: Progress in Cryptology-AFRICACRYPT 2008, in: LNCS, vol. 5023, Springer-Verlag, Berlin, 2008, pp. 325–342.

[22] S. Hohenberger, B. Waters, Attribute-based encryption with fast decryption, in: Public-Key Cryptography—PKC 2013, in: Lecture Notes in Computer Science, vol. 7778, 2013, pp. 162–179.

[23] M. Chase, Multi-authority attribute based encryption, in: Theory of Cryptography, Springer, 2007, pp. 515–534.

[24] D. McGrew, K. Igoe, M. Salter, Fundamental elliptic curve cryptography algorithms, Internet Engineering Task Force (IETF), Request for Comments: 6090, February 2011. http://tools.ietf.org/html/draft-mcgrew-fundamentalecc-04.

[25] V.G. Martínez, L.H. Encinas, C.S. Ávila, A survey of the elliptic curve integrated encryption scheme, J. Comput. Sci. Eng. 2 (2) (2010) 7–13.

[26] A. Lewko, T. Okamoto, A. Sahai, K. Takashima, B. Waters, Fully secure functional encryption: attribute-based encryption and (hierarchical) inner product encryption, in: Advances in Cryptology-EUROCRYPT 2010, in: LNCS, vol. 6110, Springer-Verlag, Berlin, Heidelberg, 2010, pp. 62–91.