INTERNET OF THINGS (IoT) UTHENTICATION

ESMA ERGUNER OZKOC

Department of Management Information Systems, Başkent University
Email: eeozkoc@baskent.edu.tr

Abstract— Internet of Things (IoT) is the self-configuring network of everyday life objects which can communicate with each other. Implementation of this kind of huge and complex networks is difficult to manage and having such a structure makes it vulnerable to attacks. Five major security issues in IoT are Authentication, Confidentiality, Integrity, Authorization and Freshness. This paper focus on Authentication issue whichis a process of verifying device credentials to join IoT network. This paper reveals that authentication schemes which are designed for IoT should meet some requirements. Zhao et.al.presented an authentication scheme based on feature extraction,secure hash algorithm and elliptic curve cryptography (ECC). This proposed scheme is evaluated according to mentioned authentication requirements.

Keywords— Authentication scheme, Internet of Things, security on IoT

I. INTRODUCTION

Development of the technology enormous in information age and Internet has become an indispensable part of our daily life. The development of the Internet can be explained by three innovations; (i) Fixed Internet (ii) Mobile Internet and (iii) Internet of Things (IoT). Fixed Internet usage in 90's was 1 billion, mobile Internet usage in 2000's was 6 billion and number of things that can connect to the Internet by 2020 is estimated as 28 billion - based on International Data Corporation (IDC) research.On the other hand according to the research made by Cisco [1], in 2020 number of devices that can connect to internet will be 50 billion. Both researches demonstrate that world will interact with billions of IoT objects. As a result of this growth, workplace productivity, personal lives, way of work and consumptions will all change.

The term "Internet of Things" is first used as a title in a presentation which was about linking the new idea of RFID in Procter&Gamble's supply chain by KevinAshton in 1999 [2]. In our lives we are surrounded with things. People or devices can connect with the things, learn about things, monitor things, search for things, manage things, control things and play with things. Things can have different type of processor, memory and battery features depend on their working areas. Devices are required to carry four features to become IoT: must have (1) a unique identity (2) ability to communicate (3) senses and (4) have access to control.

Many functions can be controlled and traced with communication between things. Popular application of the IoT's are; smart homes, wearables (smart watches, activity tracker, smart glasses), smart cities (traffic management, water distribution, waste management, urban security), smart grids, connected health, smart retail, supply chain, smart farming [3].

IoT goal is to create intelligent networks that can be connected to the internet. IoT is the self-configuring network which a new device can join automatically. Having such a structure makes it vulnerable to attacks [4]. Hence some security flaws need to be solved.

The remainder of the paper is organized as follows. The architecture of IoT given in Section II. Authentication scheme requirements are introduced and Zhao et. al's scheme is reviewed in Section III. Finally, paper concluded in Section IV.

II. IoTARCHITECTURE

IoT objects are part of the networks and responsible to gather data in the form of image, sound, video from their sensors.For this reason they should have multi-networking capabilities. Also IPv6 gives the opportunity to localize or globalize traffic with unique identity. IoTshould have multicast transport capabilities to manage resources efficiently and shouldprovide security such as authentication, encryption and access control.

The traditional IoT operates on three layer: Application layer, Transport layer and Perception layer [5-8].

Perception layer/sensor layer is the bottom layer that responsible to gather data from objects with the assistance of sensor/actuators. Gathered and processed data is sent to transport layer.

Transport layer/Network layer is responsible for data routing and transmission to other IoT devices in the network. Switching and routing devices which operates at transport layer are use recent wireless Internet technologies like Wi-Fi, LTE, Bluetooth and 3G/4G.

Application layer is the top layer where authentication, key agreement, privacy protection, data integrity and confidentiality of data are ensured.

Each layer has its own security features and requirements. IoT devices have low computational power and storage capacity. That is the reason for complex encryption algorithms and schemes are not appropriate for IoT devices. Denial of service attacks and Replay attack/Timing attackwill be the most frequent threat to the IoT network at perception layer.

Transportlayer which is the core network functions are occur, Man-in-the-middle attacks, traffic analysis, monitoring, eavesdropping, viruses, worms are exists.Also malicious information detection and key exchange mechanism should be improved to overcome these attacks.

Application layer security has the more security issues to handle because of the lack of the standardization and policies that manage the developed applications. In RFC7452 [9] and Internet society IoT white paper [10] some design issues are given but it is focused on infrastructure of IoT rather than application specification. Each application has its own authentication mechanism which is very difficult to coordinate.IoT application designers must have to consider; (i) how many different user will use the application such as user, vendor, Thing (ii) how to control gathered data and which part of the data should be public (iii) when the data will be used by whom.

III. AUTHENTICATION IN IoT

Security and privacy is the two major concerns in IoT that authentication is the key process to ensuring both.Authentication is a process ofverifying user credentials when a user wants to access resources. In the IoT case, machine authentication is referred (Machine-to-machine (M2M) or automated human-to-machine authentication). Machine authentication can be done through digital certificate (digital password verified by CA) and machine credentials (machine ID and password). The purpose of machine authentication is to enable devices to interact and communicate with each other in a secure way. Devices in IoTdifferentiate from traditional M2M devices with its heterogeneity including mobile and cloud. Therefore IoT devices have typical limitations such as memory, processing power, internet bandwidth and limited user interface. When a device want to join the IoT network it should authenticate itself to begin communication.Authentication process is performed by a device that can be a sensor, actuator, platform, terminal node or gateway.

Various M2M authentication schemes for wireless sensor networks (WSN) have been proposed[11-17]. Because of resource constrained environment of WSN, proposed lightweight authentication schemes can be adapted to IoT networks. Different cryptographic techniques are applied to schemes such as public key cryptography, private key cryptography and Elliptic Curve Cryptography (ECC). In addition to these, feature extraction mechanism for IoT authentication is used first time by *Zhao et. al.*[18].Besides this there are studies that focused on IoT authentication [18-22].

Numerous schemes have been developed for remote user authentication and features that should be in the perfect remote authentication schemeare determined [23-24]. This paper adapts these features to IoT authentication scheme which is a special case of remote user authentication.

Therefore a perfect authentication scheme which is designed for IoT, must provide the following requirements.

1. No Password or verification table is stored on gateway/platform or IoT devices.
2. The user can choose and change the password.
3. Administrator/vendor of the system cannot see the password.
4. Mutual authentication must be provided (Terminal node verify the platform and platform verify terminal node).
5. Passwords cannot be transmitted over unsecure network as plain text.
6. Authentication scheme must be easy to calculate and have low time complexity (lightweight solution).
7. Scheme must be easily detect wrong credentials entry.
8. Session key must be generated before the verification phase to ensure reliability of transmission.
9. Session key automatically re-generated at every login request.
10. Scheme stays reliable even in case of gateway/platform's secret key lost or stolen.
11. Group-based authentication must be supported because large number of IoT device accessing the network at the same time can create authentication message congestion. In other words scheme must minimize authentication overhead.
12. Terminal node anonymity must be provided.

Beside these features IoT network should resist various attacks: DoS, jamming, malware distribution, eavesdropping, traffic analysis, Spoofing, Man-in-the-middle, Replay attacks etc.

Rest of the paper will evaluate the Zhao et. al's scheme [18] according to aforementioned requirements.

Table1. Symbols through the paper

Symbols	Meaning
AN	Accountwhich is secretandonlyknownby platform and terminal.
MP	Matrix password card which is send from platform to terminal in initialization
RT	Randomnumber
ID	Identity of the terminal
SHA1	SecureHashAlgorithm- 160 bit
V	Variancewhich is calculatedbyfetaureextractionalgorithm
E	Energywhich is calculatedbyfetaureextractionalgorithm
X==X'	Whether Xequals X'

Review of Zhao et. al.'s scheme:

The scheme was first used feature extraction in identity authentication beside this it combined it with SHA1 and ECDSA (Elliptic curve digital Signature Algorithm) to improve security. The main reason of using future extraction is to reduce the amount of data which will travel over the wireless network. Thus it minimizes authentication overhead over network.

Zhao et. al.'s scheme consists of three phases: Initialization, CA verification and Mutual authentication.

Initialization phase: Initial informationis distributed between terminal node and platform such as ID, account, matrix password card, public/private key etc. All the information about terminal stored in platform.

CA verification: CA center verifies the certificates of platform and terminal node.

Mutual authentication phase: First, platform side calculate the X by using previously generated random number R_{T-1} and Account of the terminal. Platform sends it to the terminal node together with matrix password card and randomly generated number (R_T) for current login request. Terminal node calculates X' by using own information and compare with received X.Terminal node verifies platform identity if X and X' are identical. Otherwise reject the platform. If platform is authenticated; terminal updates R_{T-1} with R_T, and calculates message digest with its own information such as ID and account by using SHA1 algorithm (Y). At feature extraction process, message digest wastreated asnonobjective image. Variance and Energy is calculated as follows:

$$\text{Variance } V=\sum_{i=0}^{L-1}\left(i-\sum_{i=0}^{L-1} i\left(\frac{n_i}{N}\right)\right)^2 \frac{n_i}{N} \qquad (1)$$

$$\text{Energy } E=\sum_{i=0}^{L-1}\left(\frac{n_i}{N}\right)^2$$

L=16, n_i , number of matrices with size$i$ and N is the total number of matrices.

Then, calculated V, E and ID of the terminal are sent to platform. Platform searches received ID of the terminal from its own list of the terminals. Finds out the information of the corresponding terminal, calculates Y', Variance and Energy. Then compare calculated and received Variance and Energy values if both are the same platform legitimate the terminal node. The summary of the phase is demonstrated in Fig.1 (for detailed information see [18]).

Zhao et. al.'s scheme is evaluated according to specified authentication scheme features;

1. It is not store integrated private key but Platform holds all information about terminal node including ID, account, public/private key etc.
2. Terminal node can choose the password from given matrix password card. It is increasing the randomness of password but if matrix is leaked or stolen all possible passwords can be known by malicious. In addition the scheme does not provide any password change phase.
3. Chosen password is not seen by Administrator/vendor but terminal keeps the all possible passwords. Chosen password can be calculated by brute force attack. Success of the brute force attack depends on size of matrix password card which is not given in corresponding paper.
4. Mutual authentication is provided.
5. Matrix password card is send from platform to terminal node as a plain form over wireless network in mutual authentication phase of the scheme.
6. Authentication scheme is easy to calculate and have low time complexity (lightweight solution).
7. Scheme easily detects wrong credentials entry.
8. Session key ($K_l = K_r + K_c$) is generated before the verification phase
9. Part of the Session key $K_r$is stored in terminal node side but K_c automatically re-generated at every login request by platform side.
10. Scheme stays reliable even in case of gateway/platform's secret key lost or stolen.
11. Group-based authentication is not supported.
12. In mutual authentication phase, terminal node sends request message which contains ID of the terminal in a plain form to the platform. Means ID is openly available to the attackers who make eavesdropping. So the scheme does not provide terminal node anonymity.

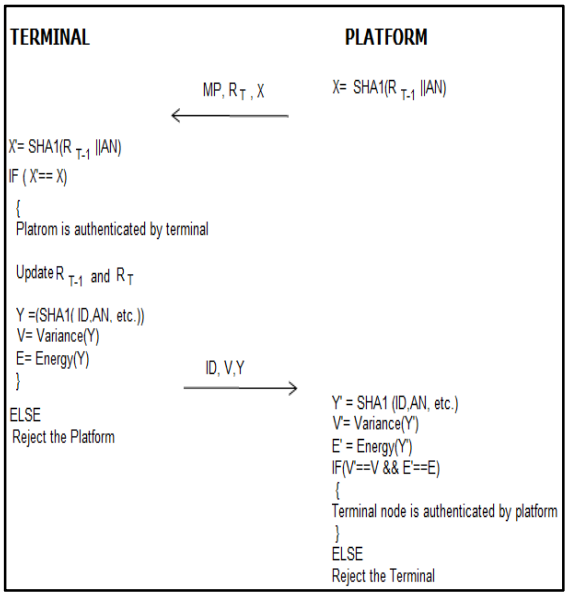


Fig.1. Mutual authentication phase of the Zhao et. al. scheme

CONCLUSION

21st century can be introduced as the Internet of Things era where digitally connected devices exist on every aspect of our lives.Rapid development of IOT has moved a step further withwidespread use of wireless networks and IPv6. Although, IoT makes our lives easier, it becomes an attractive target for hackers/cybercriminals.

The IoT network is vulnerable to various attacks at each layer therefore to avoid attacks many security

challenges and requirements are exists. In scope of this paper authentication scheme security requirements are introduced. In addition, Zhao et. al. scheme that use new technique to identity authentication in IoT is evaluated in accordance with these requirements.

REFERENCES

[1] D. Evans, "The Internet of Things how thenextevolution of the internet is changingeverything," Apr 2011, White Paper. [Online]. Available: http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

[2] http://www.rfidjournal.com/articles/view?4986(Access date: 15.05.2016)

[3] http://iot-analytics.com/10-internet-of-things-applications/ (Access date: 15.05.2016)

[4] Misra, Sudip, P. Venkata Krishna, Harshit Agarwal, AntrikshSaxena, and Mohammad S. Obaidat. "A learning automata based solution for preventing distributed denial of service in Internet of things." In *Internet of Things (iThings/CPSCom), 2011 International Conference on and 4th International Conference on Cyber, Physical and Social Computing*, pp. 114-122. IEEE, 2011.

[5] Xiaocong, Qian, and Zhang Jidong. "Study on the structure of "Internet of Things (IOT)" business operation support platform." In *Communication Technology (ICCT), 2010 12th IEEE International Conference on*, pp. 1068-1071. IEEE, 2010.

[6] Mahmoud, Rwan, TasneemYousuf, FadiAloul, and Imran Zualkernan. "Internet of things (IoT) security: Current status, challenges and prospective measures." In *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*, pp. 336-341. IEEE, 2015.

[7] Zhao, Kai, and Lina Ge. "A survey on the internet of things security." In*Computational Intelligence and Security (CIS), 2013 9th International Conference on*, pp. 663-667. IEEE, 2013.

[8] Leo, Marco, Federica Battisti, Marco Carli, and Alessandro Neri. "A federated architecture approach for Internet of Things security." In *Euro Med Telco Conference (EMTC), 2014*, pp. 1-5. IEEE, 2014.

[9] Tschofenig, H., J. Arkko, and D. McPherson. "Architectural Considerations in Smart Object Networking." *Internet Engineering Task Force, Fremont, CA, USA, Tech. Rep. RFC-7452* (2014).

[10] ISOC, "The Internet of Things (IoT): An Overview", October 2015. <http://www.internetsociety.org/sites/default/files/ISOC-IoT-Overview-20151221-en.pdf>

[11] Chang CC, Le HD, "A provably secure, efficient and flexible authentication scheme for ad hoc wireless sensor networks."IEEE Trans WirelCommun. doi:10.1109/TWC.2015.2473165, (2015)

[12] Chen, Tien-Ho, and Wei-Kuan Shih. "A robust mutual authentication protocol for wireless sensor networks." *Etri Journal* 32, no. 5 (2010): 704-712.

[13] Choi, Younsung, Donghoon Lee, Jiye Kim, Jaewook Jung, Junghyun Nam, and Dongho Won. "Security enhanced user authentication protocol for wireless sensor networks using elliptic curves cryptography." *Sensors* 14, no. 6 (2014): 10081-10106.

[14] Hsieh, Wen-Bin, and Jenq-ShiouLeu. "A Robust User Authentication Scheme Using Dynamic Identity in Wireless Sensor Networks." *Wireless personal communications* 77, no. 2 (2014): 979-989.

[15] Shi, Wenbo, and Peng Gong. "A new user authentication protocol for wireless sensor networks using elliptic curves cryptography." *International Journal of Distributed Sensor Networks* 2013 (2013).

[16] Xue, Kaiping, Changsha Ma, Peilin Hong, and Rong Ding. "A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks." *Journal of Network and Computer Applications*36, no. 1 (2013): 316-323.

[17] Yoo, Sang Guun, Keun Young Park, and Juho Kim. "A security-performance-balanced user authentication scheme for wireless sensor networks."*International journal of distributed sensor networks* 2012 (2012).

[18] Zhao, Guanglei, Xianping Si, Jingcheng Wang, Xiao Long, and Ting Hu. "A novel mutual authentication scheme for Internet of Things." In *Modelling, Identification and Control (ICMIC), Proceedings of 2011 International Conference on*, pp. 563-566. IEEE, 2011.

[19] Wu, Fan, Lili Xu, SaruKumari, and Xiong Li. "A privacy-preserving and provable user authentication scheme for wireless sensor networks based on Internet of Things security." *Journal of Ambient Intelligence and Humanized Computing* (2016): 1-16.

[20] Turkanović, Muhamed, BoštjanBrumen, and Marko Hölbl. "A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the internet of things notion." *Ad Hoc Networks* 20 (2014): 96-112.

[21] Wen, Quangang, Xinzheng Dong, and Ronggao Zhang. "Application of dynamic variable cipher security certificate in internet of things." In *Cloud Computing and Intelligent Systems (CCIS), 2012 IEEE 2nd International Conference on*, vol. 3, pp. 1062-1066. IEEE, 2012.

[22] Nguyen, Kim Thuat, Maryline Laurent, and NouhaOualha. "Survey on secure communication protocols for the Internet of Things." *Ad Hoc Networks* 32 (2015): 17-31.

[23] Liao I-En, Lee C. C., Hwang M. S. "A password authentication scheme over insecure networks". Journal of Computer and System Sciences; 2006. p. 727-740.

[24] Tsai C.S., Lee C.C., Hwang M.S. "Password Authentication Schemes: Current Status and Key issues." International Journal of Network security;.Vol.3 No.2, p.101-115. 2005.

★★★