Authentication in the Internet of Things

Di Weng, *11621046* and Qi Song, *21521081*

Abstract—The abstract goes here.

Index Terms—internet of things, authentication.

1 Introduction

The Internet of Things (IoT) and its related technologies have been actively studied and popularized in the past few years [4]. The idea of IoT was originally formulated from the emerging advanced network infrastructures that support a large number of interconnected things or objects, such as Radio-Frequency IDentification (RFID) tags, sensors, personal accessories like smart watches and mobile phones. The objects are then given unique addresses, through which they can communicate and cooperate with each other to complete collective tasks, while the addressing scheme will also enable IoT devices to be identifiable by external services and platforms [9] [18].

However, there is a long-standing argument about the definition of Internet of Things. IoT is a generic but vague concept with several missing definitions, for example, the range of objects and addressing schemes. This leads to manifold definitions of IoT presented in prior studies. The term, *Internet of Things*, is semantically composed by two words, *Internet* and *Things*, from which two different aspects of IoT technology can be derived, namely, Internet-oriented visions and things-oriented visions, and most of the previous definitions fall into these two categories. Additionally, some other studies suggest that the third aspect, semantic-oriented visions, is also a part of the IoT framework. These three visions (Fig. 1) are discussed as follows:

Internet-oriented visions focus on the connectivity of objects inside the IoT framework. Since Internet Protocol (IP) has been widely adopted in traditional network infrastructures and is already connecting millions of devices around the world, most of the definitions in the realm of Internet-oriented vision attempt to reuse lightweight variants of the IP stack to address the connectivity issues among IoT objects. One of the definitions is canonicalized by IPSO (Internet Protocol for Smart Objects) Alliance [20], an international organization consisting of 26 companies, including several notable manufacturers of embedding processing units like ARM and Intel. IPSO Alliance proposes the usage of IP architecture on the basis of communication techniques with low power consumption like IEEE 802.15.4 and 6LoWPAN [7]. The integrated IPv6 technology provides sufficient address space for IoT objects, and low-power design enables resource-constrained IoT devices to communicate at a lower rate but consume less power. There are other similar approaches like Internet Ø, allowing "IP over anything" by reducing the complexity of the IP stack.

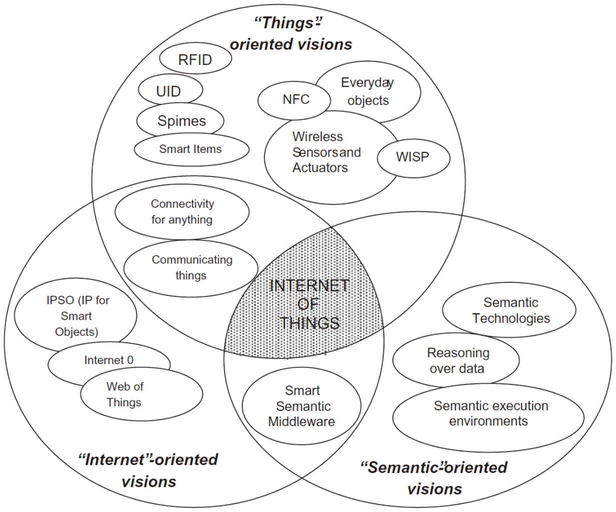
"Things"-oriented visions
RFID
UID
Spimes
Smart Items
NFC
Everyday objects
Wireless Sensors and Actuators
WISP
Connectivity for anything
Communicating things
INTERNET OF THINGS
IPSO (IP for Smart Objects)
Internet 0
Web of Things
Smart Semantic Middleware
Semantic Technologies
Reasoning over data
Semantic execution environments
"Internet"-oriented visions
"Semantic"-oriented visions

Fig. 1. Three visions of the Internet of Things paradigm by L. Atzori et al. [4], including Internet-oriented visions, Things-oriented visions, and Semantic-oriented visions. Their relations and components are described in a Venn diagram.

Things-oriented visions advocate wide-spread Radio-Frequency IDentification (RFID) tags as *things* in the IoT framework. By attaching RFID tags to everyday objects, Things-oriented visions enable users of IoT to track and identify these objects. The idea was first established by Auto-ID Labs [1], and later generalized by several studies [11] [17], which further extend identifiable tags into a Unique/Universal/Ubiquitous IDdentifier (UID) architecture. While the definition of IoT presented by these visions narrows it down to mere object identification, the maturity of RFID technologies and the popularity and enthusiasm in the business community show a promising adoption rate of such architecture. Moreover, by combining things-oriented visions with Internet-oriented visions, several unified definitions were proposed regarding both the identification and connectivity of objects, as stated by the European Commission [5]: "Things having identities and virtual personalities operating in smart spaces using intelligent interfaces to connect and communicate within social, environmental, and user contexts."

Semantic-oriented visions arise from the literature under an assumption that the number of interconnected objects exhausts the capability of direct management, where the organization of the information generated by these objects

Manuscript received June 28, 2017; revised June 28, 2017.

becomes challenging. Such issue can be addressed by integrating semantic technologies like data reasoning and semantic execution environment into the IoT framework [19].

As a promising technology, IoT was included in the list of six "Disruptive Civil Technologies" that will potentially generate huge impacts on US national power [6]. US National Intelligence Council, the author of the list, claimed that "popular demand combined with technology advances could drive widespread diffusion of an Internet of Things (IoT) that could, like the present Internet, contribute invaluably to economic development." Despite IoT's contribution to human's everyday life, it also brings severe security risks along the way due to its wide distribution and applicability. It is also stated in the aforementioned report that "to the extent that everyday objects become information security risks, the IoT could distribute those risks far more widely than the Internet has to date."

Four categories of security issues in the IoT framework are summarized by Alaba et al. [3], including application, architecture, communication, and data. With authentication and access control technologies, traditional computer networks have resolved a variety of security and privacy issues in three ways [12]: a) forbid unauthorized users to access resources; b) prohibit authorized users from accessing resources beyond their privileges; and c) grant correct resource access to authorized users. As a key issue in both categories of application and architecture, authentication technologies continues playing an important role in the security of IoT.

Two challenges arise while applying existing authentication techniques to the application and architecture of IoT devices. First, most of the IoT devices are resource-constrained, where most of the strong cryptography methods currently used cannot be computed fast enough to match the power supply of devices and the rate of information sensing. Second, the complex environment of IoT networks requires an extensible and scalable authentication scheme. The number of devices in an IoT network could scale up to millions, introducing difficulty in many aspects of traditional authentication, such as the distribution and revoking of symmetric encryption keys.

Apart from the machine authentication of IoT, which mainly consists of the authentication of application and architecture as stated above, user authentication [16] is also an essential part of IoT security paradigm. By integrating user authentication, IoT devices like mobile phones are able to identify owners with simple interactions and protect sensitive personal information from unauthorized users.

The work of this survey is divided as follows:

- **Presentation:** Qi Song presented the assigned paper [8], and Di Weng presented the survey on the authentication of the Internet of Things;
- **Writing:** Section 1, 2, and 5 were written by Di Weng, and Section 3 and 4 were written by Qi Song.

This survey is organized as follows: the machine authentication of IoT is covered in Section 2 and 3, which explain the authentication in IoT applications and architecture, respectively; then, Section 4 summarizes the user authentication in IoT framework briefly; finally, this survey is concluded in Section 5.

2 Application Authentication

Recent years have witnessed the great impacts brought by the Internet of Things technologies via a variety of applications. Applications of IoT can be categorized by: network type, scope, scale, heterogeneity, repeatability, and the involvement of users [10]. However, it remains a crucial challenge to protect the application data authentic and intact with authentication technologies while transmitting the data over IoT networks.

Studies depict that the authentication in IoT applications generally involves two validation aspects corresponding to different concerns [3]: a) peer authentication: *how does a IoT device recognize and trust its peers*; and b) data origin authentication: *how to ensure the origin of data is an authentic IoT peer*. These two validation aspects were proposed to enhance the security of machine-to-machine (M2M) communications [13] in IoT framework based on the complicated environment of IoT networks, which may comprise enormous cheap yet resource-constrained devices in contrast to traditional networks with a few hundred powerful nodes.

Several research attempts were made regarding the authentication of IoT applications. One of the earliest studies in this area was conducted by Liu et al. [12], in which they proposed an authentication and access control scheme based on Elliptic Curve Cryptography (ECC) combining both asymmetric and symmetric encryption methods. Registration Authorities (RA), a type of standalone authorization servers in IoT networks, are established to recognize the authenticity of both devices and users with predistributed certificates signed by the generated elliptic curve. Regular Elliptic Curve Diffie-Hellman (ECDH) key exchanging protocol is then performed between RA and users. This work also takes multiple domain authentication into consideration by adding a Home Registration Authority (HRA) and providing a Single Sign-On (SSO) solution for IoT users. Ndibanje et al. [14] presented a comprehensive analysis of security weaknesses in this method and proposed further improvements concerning the message exchanging performance and security assessment of the protocol.

In addition to ECC, other encryption techniques have been introduced to address the authentication issue in IoT applications as well. Attribute-Based Encryption (ABE) was adapted for the authentication of resource-constrained IoT devices by Yao et al. [21]. ABE is a cryptography method based on Identity-Based Encryption (IBE) aiming to produce encrypted texts recognizable by users with certain identities only. Extended from IBE, ABE identifies users with a set of predefined attributes. Only users with the specific combinations of attributes corresponding to the defined access policy are allowed to decrypt the cipher text, enabling broadcast encryption of the application data. However, the bilinear Diffie-Hellman scheme used by ABE is slow and computationally-intensive, which is proven unsuitable for IoT devices. Yao et al. replace bilinear Diffie-Hellman scheme of general ABE with faster elliptic curve scheme, leading to better performance and improved bit security. However, the proposed method still exhibits several inherent limitations as discussed in the paper: a) poor flexibility in revoking attributes; b) poor scalability with communication and computational overhead; and c) poor generality with multiple-authority applications.

The perception layer emerges from the evolution of IoT technologies as a substantial number of sensors are being deployed in IoT networks. Despite the significant importance of perception layers, only a few studies focus on the authentication issue of these layers. Ye et al. [22] presented an efficient authentication and access control scheme between users and the perception layer in Wireless Sensor Networks (WSN) by exploiting ECC key exchanging protocol with a mutual authentication style comprising two phases, namely, authentication and key establishment. A lightweight authentication protocol specifically designed for securing RFID tags was also proposed [2] in the literature. Nonetheless, such authentication issues, for example, how to segregate and protect sensitive application data in the heterogeneous perception layer of IoT networks, remain largely unsolved.

Neisse et al. [15] proposed SecKit, a model-based security toolkit, to address security policy management issues in IoT. By analyzing the characteristics of IoT framework comprehensively, authors designed the toolkit to support various application scenarios: a) dynamic context; b) trust management; c) digital divide; d) data flow control; e) actuator action control; and f) data anonymization. Moreover, authors formalized the security management procedure by identifying several metamodels involved in the process, including data, time, identity, role, context, structure, behavior, risk, trust, and rule. These metamodels were then implemented using the Eclipse Modeling Framework (EMF). Such formalization demonstrates the feasibility of the proposed toolkit and assists the administrators of IoT networks in creating, modifying, and enforcing security policies at a fine-grained level.

3 Architecture Authentication

4 User Authentication

5 Conclusion

The conclusion goes here.

References

[1] Auto-ID labs. https://autoidlabs.org/.

[2] F. Al-Turjman and M. Gunay. CAR approach for the Internet of Things. *Canadian Journal of Electrical and Computer Engineering*, 39(1):11–18, 2016.

[3] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi. Internet of Things security: A survey. *J. Network and Computer Applications*, 88:10–28, 2017.

[4] L. Atzori, A. Iera, and G. Morabito. The Internet of Things: A survey. *Computer Networks*, 54(15):2787–2805, 2010.

[5] A. Bassi and G. Horn. Internet of Things in 2020: A roadmap for the future. *European Commission: Information Society and Media*, 22:97–114, 2008.

[6] N. Council. Six technologies with potential impacts on us interests out to 2025. *Disruptive Civil Technologies*, 2008.

[7] D. Culler and S. Chakrabarti. 6LoWPAN: Incorporating IEEE 802.15.4 into the IP architecture. *IPSO Alliance White Paper*, 2009.

[8] M. Frank, R. Biedert, E. Ma, I. Martinovic, and D. Song. Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication. *IEEE Trans. Information Forensics and Security*, 8(1):136–148, 2013.

[9] D. Giusto, A. Iera, G. Morabito, and L. Atzori. *The Internet of Things: 20th Tyrrhenian workshop on digital communications*. Springer Science & Business Media, 2010.

[10] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami. Internet of things (iot): A vision, architectural elements, and future directions. *Future Generation Comp. Syst.*, 29(7):1645–1660, 2013.

[11] E. K. Chiew et al. Radio-frequency identity protocols class-1 generation-2 UHF RFID protocol for communications at 860 MHz–960 MHz version 1.0. 9. *On False Authentications for C1G2 Passive RFID Tags*, 65, 2004.

[12] J. Liu, Y. Xiao, and C. L. P. Chen. Authentication and access control in the Internet of Things. In *32nd International Conference on Distributed Computing Systems Workshops (ICDCS 2012 Workshops), Macau, China, June 18-21, 2012*, pages 588–592, 2012.

[13] F. Martín-Fernández, P. Caballero-Gil, and C. Caballero-Gil. Authentication based on non-interactive zero-knowledge proofs for the Internet of Things. *Sensors*, 16(1):75, 2016.

[14] B. Ndibanje, H. Lee, and S. Lee. Security analysis and improvements of authentication and access control in the Internet of Things. *Sensors*, 14(8):14786–14805, 2014.

[15] R. Neisse, G. Steri, I. N. Fovino, and G. Baldini. Seckit: A model-based security toolkit for the internet of things. *Computers & Security*, 54:60–76, 2015.

[16] L. O'Gorman. Comparing passwords, tokens, and biometrics for user authentication. *Proceedings of the IEEE*, 91(12):2021–2040, 2003.

[17] K. Sakamura. Challenges in the age of ubiquitous computing: a case study of T-Engine, an open development platform for embedded systems. In *28th International Conference on Software Engineering (ICSE)*, pages 713–720, 2006.

[18] L. Tan and N. Wang. Future internet: The Internet of Things. In *Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on*, volume 5, pages V5–376. IEEE, 2010.

[19] I. Toma, E. Simperl, and G. Hench. A joint roadmap for semantic technologies and the Internet of Things. In *Proceedings of the Third STI Roadmapping Workshop*, volume 1, 2009.

[20] J. Vasseur and A. Dunkels. IP for smart objects. *IPSO Alliance, White paper*, 1, 2008.

[21] X. Yao, Z. Chen, and Y. Tian. A lightweight attribute-based encryption scheme for the internet of things. *Future Generation Comp. Syst.*, 49:104–112, 2015.

[22] N. Ye, Y. Zhu, R.-c. Wang, and Q.-m. Lin. An efficient authentication and access control scheme for perception layer of internet of things. *Applied Mathematics & Information Sciences*, 8:1617–1624, 2014.