

Identity in the Internet-of-Things (IoT): New Challenges and Opportunities

Kwok-Yan Lam^{1(✉)} and Chi-Hung Chi²

¹ School of Computer Science and Engineering,
Nanyang Technological University, Singapore, Singapore

kwokyan.lam@ntu.edu.sg

² Data61, CSIRO, Geraldton, Australia

chihungchi@gmail.com

Abstract. From digitization to datafication, Internet-of-Things (IoT) plays an important role as enabler in the value creation process from big data. As is expected, security has naturally become one main concern in the IoT deployment. Due to the unique features and requirements of IoT, including limited compute resources, power, bandwidth and massive number of deployed IoT objects, and its loosely coupled networked architecture, new strategies and techniques are needed to provide feasible and practical solutions to IoT security. While substantial research efforts have been focusing on the lightweight communication protocols and cryptography/compression engines, one fundamental science question being asked is on the notion of “Identity in the Internet-of-Things” (or IDoT). In this paper, we would like to first explore the concept of IDoT and analyze why it is so unique as compared to the concept of “Identity of Users” (IDoU) in traditional networks and systems. Then we will survey on attribute-based, multi-factor authentication as an important approach to put this IDoT concept into practice. We will conclude this paper with open research issues in this direction.

1 Introduction

The Internet-of-Things (IoT) [1] has already become the most important platform to support digital intelligence for smart nations. Gartner predicts that within the next five years, there will be more than 25 billion objects deployed in every part of our daily lives and business. While this can be viewed as opportunities, it also raises a big concern about cybersecurity [2–4]. For example, hackers might use portable RFID readers to read other people’s credit cards on public transports illegally using paypass since there is no verification on the identity of the reader’s owner. Another example is that hackers can easily sniff the IoT network to get hold of the IMEI (International Mobile Equipment Identity) number of sensors and use it to pollute the IoT database through flooding it with “poisoned” data messages.

Compared to security in traditional systems, network, and data security, security in IoT is a new challenge because of its unique features and requirements. First, many IoT objects are small and have only limited CPU and battery power. As a result, strong encryption schemes are often found to be non-practical. Instead, lightweight cryptography [5–8] and protocols such as MQTT (MQ Telemetry Transport) and CoAP

(MQ Telemetry Transport) [9–11] are being investigated for IoT deployment. Second, security protection software such as those from anti-virus (AV) companies is not applicable to IOT objects because of their physical limitations. Wide variety of IoT objects from different vendors and standard groups, together with their different firmware and embedded OS further make the support of AV on every object difficult. Network security for IoT is also another challenge due to different new transport protocols of IoT objects and also the exponential increase in network traffic for cost-effective security analysis. Finally, IoT needs both encryption key management and identity management. Scalability issue comes when millions of objects are involved in the IoT network.

To address the security issues in IoT, while research efforts are still on-going in lightweight protocols, cryptography engines, and protocol stacks, researchers start to go back to the more fundamental question of what is “Identity” in the Internet-of-Things. It is hoped that this “Identity” concept can serve as the solid foundation on which cost-effective IoT security solutions can be inspired, built and put in practice.

The rest of the paper is as follows. In Sect. 2, the notion of “Identity” in the IoT is discussed. In Sect. 3, one important research topic in IoT security, attribute-based authentication, will be used to illustrate how the concept of “Identity” in the IoT can be supported. Finally, the paper will conclude in Sect. 4.

2 Concept of Identity in the Internet-of-Things (IDoT)

Under IoT, one of the root problems, in the context of cybersecurity assurance, is the lack of a rigorous notion of “Identity” in the Internet-of-Things (IDoT).

In traditional systems and networks, multi-factor authentication is often used to define and recognize the “Identity” of a user (IDoU). Typically, three categories of information are involved. They are knowledge (something they know), possession (something they have), and inherence (something they are) [12]. Good examples of these three categories are password (know), USB token or smart card (have), and finger or other biometric identifier (are) respectively. Furthermore, two or more factors might be used together to strengthen the authentication process. For Internet banking, a user is usually required to use a hardware USB token (have) and also to input his/her own password in order to verify the identity.

However, for IoT security, multi-factor authentication approach is much more complex and challenging. This is due to the new difficulties and challenges in defining and composing identity for IoT objects. In the next two sub-sections, we will first analyze different information categories that can possibly serve as identifiers to composite identity for IoT objects. Then we will discuss additional complication issues when managing these information in the IoT network.

2.1 Information Categories for Identity in the IoT

Leveraging the ideas from “Identity” of a user (IDoU) from traditional systems and network, the information stack for “Identity” in the IoT (IDoT) is shown in Fig. 1. In this information stack, there are four categories: inheritance, association, knowledge, and context.

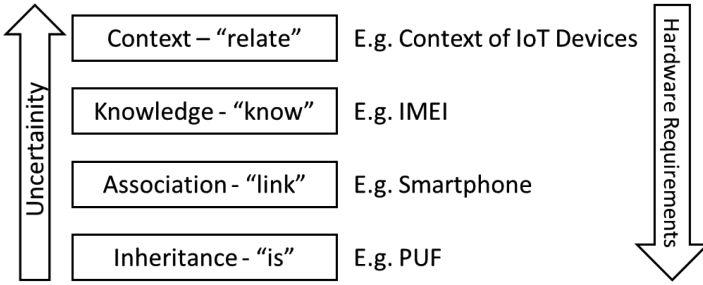


Fig. 1. Information stack for identity in the IoT (IDoT)

The first information category in the stack is the “inheritance”. Just like the biometrics identifiers (such as fingerprints and retina) of human, researchers are exploring similar type of information that are inherited from the IoT object hardware. The result is the PUF (physical unclonable function) [13], which is defined as a physical entity that is embodied in a physical structure and is easy to evaluate, but hard to predict even for an attacker with physical access, or practically impossible to duplicate even given the exact manufacturing process that produced it. Very often, it depends on the uniqueness of their physical microstructure and manufacturing process. A typical example is the Silicon PUF that is embedded into an integrated circuit [14]. When the PUF is queried with a challenge or physical stimulus, it will return an unpredictable (but repeatable) response that depends on both stimulus and the unique object-specific physical characteristics of the object containing the PUF.

This “inheritance” information categories is very attractive to aid the definition and construction of IDoT. However, as expected, it is not as flexible as other information categories because it depends on the chip/hardware manufacturers. Furthermore, since PUF can be very noisy, precautions will be needed to ensure that the expected requirements for the function can be achieved. Currently, it is only used in applications with high security requirements.

The second information category in the stack is the “association”. Unlike the “possession” information category for IDoU, it is not easy for an IoT object to process something external such as hardware token. However, under some specific situations or for some specific IoT objects such as personal wearables, it is common for the IoT objects to be associated (or linked) to a given personal gateway such as smartphone so that data will only be sent to the data cloud store through the predefined smartphone.

The third information category in the stack is the “knowledge”. Similar to the second information category, the kind and amount of information that the IoT object can know is limited when compared to the case of IDoU. One typical example of this information type is the IMEI (International Mobile Equipment Identity) of the mobile phone [15]. But changing IMEI of a mobile phone is not as trivial as changing the password, in particular when the owner of a given IoT network wants to change the IMEI of all the IoT objects that he/she deploys. Recently, one new research direction that people are investigating under this information category is to use the historical

sensed data that a given IoT object has captured to define/construct its dynamic “Identity”. However, this is still in the early stage of research.

The last information category in the stack is the “context”. Unlike in the situation of IDoU where this information category is not used so often, this category attracts a lot of attention in IoT security. Normally, IoT sensors are deployed in groups that are related to each other (e.g. all body sensors belonging to the same person being monitored). By studying the monitored behavior profile of different members within the same group and comparing it against the expected behavior profile, certain aspects of IDoT can be derived. Note that unlike the first three categories that come from the same IoT object, this information category is likely to derive from multiple inter-related IoT objects. The precision and quality of information in this category is relative lower than the other three information categories. More details of this approach will be given at the end of Sect. 3.

2.2 Complication and Challenges

From the last section, it is clear that using the proposed information stack to define IDoT is indeed a new challenge, as compared to that for IDoU. Due to the limited information availability in the middle categories (i.e. “association” and “knowledge”), together with the inflexibility of the category “inheritance” and the imprecision of the category “context”, risk based authentication [16] using multi-factors would definitely be the preferred option. And the category “context” will likely be the information target for IDoT researchers to explore. On top of the challenges to use multi-factors from the proposed information stack to define and construct IDoT, there are at least two additional issues in IoT that further complicates the management of IDoT.

The first issue is related to the ownership and user identity relationship of an IoT object. At any time t , every IoT object should have an owner, but might have one or more users. The relationship among the IoT object, owner, and users might also change with respect to time in its lifecycle. For example, a weight scale such as those from Withings can support more than one person. And the ownership of the scale might change from the manufacturer to a retirement home. Furthermore, each IoT object might capture one or more data sources (e.g. Apple iWatch has multiple sensors). All these complicate the IDoT for authentication and other subsequent processes, including authorization and governance, in particular when the upper information categories such as “context” are used to define IDoT.

The second issue is related to the management of identifies and namespace of IoT objects. On the Internet, each resource has an URI (Uniform Resource Identifier). There is also DNS (Domain Name System) that maps URI to its current resource IP address; and this DNS is managed by the organization Internet Assigned Numbers Authority (IANA) [17]. With this namespace and identifier mapping framework, the dynamics of identifiers such as IP address of an URI can be hidden and communication between URIs becomes much easier. However, in the IoT space, due to the wide variety of already existing mapping solutions from different manufacturers, defining this kind of unified identity framework will not be easy, at least not in the near future. Obviously, this will have negative impacts on IDoT when the information category “context” is used. It also affects the practicability of edge computing on IoT security [18].

3 Attribute-Based Authentication

In the last section, we see that the notion of Identity in the Internet-of-Things (IDoT) is likely to be built from multi-factors, each one of which can be considered as an attribute (or identifier) of a given IoT object. Survey on IoT security shows that there are substantial existing related work on attribute-based authentication. In this section, we would like to give an overview on what has been done on this subject. It is hoped that this overview can give inspirations on how IDoT can move forward.

In the past few years, attribute-based authentication schemes that make use of attributes of objects as part of their identifier is getting lots of attention. It is viewed as one promising way to address the identity issue in IoT because of at least three reasons. First, there are lots of semantically rich attributes associated to both the objects and the context where the objects are in. Second, the attribute values might be continuously being updated, making them to be unique as part of the identifier. Third, data owners can enforce fine-grained access policies based on the nature of data. All these make the hackers difficult to counterfeit the attribute-based digital identity.

However, designing an effective and efficient attribute-based authentication scheme is hard, given that most of current schemes are still static attribute-based, with high algorithmic complexity in communication and computation. To support IDoT, the direction should target on the design of efficient lightweight, attribute-based active authentication schemes to support the robust notion of “identity” within the Internet-of-Things with its attribute-based credential container covering not only static attributes of objects, but also dynamic behaviour attributes (e.g. those with values dependent on time) of objects and attributes of the context (e.g. location) that the object is inside.

3.1 Overview of Existing Attribute-Based Authentication Schemes

Attribute-based encryption (ABE) is defined as a type of public-key encryption in which the secret key of a user and the ciphertext are dependent upon attributes. In such a system, the decryption of a ciphertext is possible only if the set of attributes of the user key matches the attributes of the ciphertext [19]. It was firstly proposed by Sahai and Waters [20]. Later, the concept of attribute-based signature (ABS) was introduced [21], and the idea of using a credential bundle to hold the attributes of a user was proposed [22]. Most ABS adopt bilinear pairings in their schemes and this makes them complicated and less practical. In [23], Anada et al. proposed an ABS scheme without pairings in the random-oracle model. There are two main types of ABE. The first one is key-policy based [24] and the second one is ciphertext-policy based [25]. Other variants, including multi-authority ABE [26, 27] and fully decentralized ABE [28, 29], are also available.

In the design of attribute-based encryption or signature, the following properties should to be ensured:

- Zero knowledge proofs – Signer and verifier might not have prior knowledge of each other.
- Unforgeability – It should be hard to forge signatures and/or proof of possession of attributes.
- Multi-show unlinkability – Given two signatures, it is hard to know whether the signer is the same.
- Selective disclosure – Selection of attributes should only be done to those necessary for completing a transaction.
- Collusion resistance – Multiple parties cannot collude and combine all their attributes to produce a valid signature if any one party could not do it individually.
- Threshold attribute-based authentication – The verification ensures that the signer has a threshold number of at least t attributes in common with the verification attribute set.

3.2 Attribute-Based Authentication Schemes for IDoT

In the context of IoT, attribute-based authentication scheme faces both new opportunities and challenges. In addition to the intrinsic attributes of an IoT object, new types of attributes are now available to be used potentially in authentication. These include the behaviour attribute data (either as a single value or as a data sequence) of the IoT object and the attributes of the context where the object is in (e.g. location). In particular, the behaviour attribute data is interesting to be explored because under typical IoT context, both the IoT object (e.g. sensor or tracker) and the receiver (e.g. cloud store) will have access to the same sequence of monitored data, which might make DUKPT (derived unique key per transaction) management possible.

Managing both static and dynamic attributes in attribute-based authentication schemes effectively and efficiently is a real challenge. In theory, there could be more attributes than any given scheme can accommodate. Current attribute-based authentication schemes are already facing the complexity and performance challenges, in both communication and computation. With the possible expansion of the attribute set, how to select a good subset of attributes for the scheme is not trivial, given that the decision might also be influenced by the dynamic characteristics of the behaviour attribute data. Revocation of attributes is also expected to be more frequent due to the potential continuous updating of attributes. How to design an effective and efficient attribute-based authentication scheme to support both static and dynamic attributes and how to construct and maintain the attribute tree to support fast revocation are some of the open questions for research.

One important deployment scenario of IoT objects such as trackers worth mentioning here is the continuous monitoring of certain behaviour aspect of the IoT object such as location. With the continuous uploading of the monitored data stream from the device to the backend (cloud) server, both sides can access the same sequence pattern of temporal data. Thus, it might be possible to use some kind of multidimensional data stream summarization techniques to map the data stream into an important attribute to be included in the scheme. Note that the choice of the summarization technique and the

selection of attributes will be influenced by the expected dynamic pattern of its data stream. And the timestamp can be used to address the out-of-order issue of the data stream.

3.3 Context-Aware Approach to IDoT and Authentication

In the past few years, there are increasing research efforts on using situational information for IDoT authentication [30, 31]. The assumption behind this approach is that there is often expected profile on the context in which the IoT object is in [32] and on how the object should behave [33, 34]. For example, the IP address of a given IoT object should be in some predefined range; the geolocation of the object should be within a certain area; and the temperature sensor should report the body temperature of an elderly person. If the monitored behavior data profile is close to the expected norm, authentication can be granted (or at least serving as a positive assist). On the other hand, if the derivation between the monitored and the expected ones exceeds certain threshold, explicit authentication using other means might be triggered. Currently, most of these work are based on the authentication using group key agreement protocol [35].

Despite its potentials, there are a number of open research issues for this approach. Compared to the other three information categories (“inheritance”, “association”, and “knowledge”), the context information is relatively imprecise and is subject to noise. So, what will be its weight in the authentication process? Selection of attributes and setting of the threshold cut-off for the attribute norm value are also tricky because they are both application and requirements specific. More importantly, what is the science ground of making this decision? As a result, this approach serves more as an assist rather than the absolute mean to do authentication. Another piece of related work is to use neighbors to serve as notaries in the authentication scheme [36]. While this idea is able to improve the strength of the authentication scheme, the incurred cost will be an important concern for large scale IoT network.

4 Conclusion

Internet-of-Things (IoT) has generally been agreed to the foundation for digital economy; and cybersecurity is always a big concern when mission critical applications are built on top of IoT. In this paper, we argue that one root problem for IoT security is the lack of the rigorous notion of “Identity” in the Internet-of-Things (IDoT). To solve the identity problem, we propose a new information stack to describe IDoT. Different from the “Identity” of a user, this new information stack puts a strong emphasis on situational information, which is expected to be imprecise and noisy. With the expectation of using multi-factor authentication in IoT security, we survey on attribute-based authentication and analyze the pros and cons of current techniques to support IDoT. It is hoped that by granting this deep understanding, IDoT can be addressed in a more systematic and effective way.

References

1. Palattella, M.R., Accettura, N., Vilajosana, X., Watteyne, T., Grieco, L.A., Boggia, G., Dohler, M.: Standardized protocol stack for the internet of (important) things. *IEEE Commun. Surv. Tutorials* **15**(3), 1389–1406 (2013)
2. Granjal, J., Monteiro, E., Silva, J.S.: Security for the internet of things: a survey of existing protocols and open research issues. *IEEE Commun. Surv. Tutorials* **17**(3), 1294–1312 (2015)
3. Zhao, K., Ge, L.: A survey on the internet of things security. In: *Proceedings of Ninth IEEE International Conference on Computational Intelligence and Security* (2013)
4. Sathish Kumar, J., Patel, D.R.: A survey on internet of things: security and privacy issues. *Int. J. Comput. Appl.* **90**(11), 20–26 (2014)
5. McKay, K.A., Bassham, L., Turan, M.S., Mouha, N.: NISTIR 8114: Draft Report on Lightweight Cryptography. Technical Report, National Institute of Standards and Technology, U.S. Department of Commerce, August 2016
6. Bogdanov, A., Knezevic, M., Leander, G., Toz, D., Varc, K., Verbauwhede, I.: SPONGENT: the design space of lightweight cryptographic hashing. *IEEE Trans. Comput.* **62**(10), 2014–2053 (2013)
7. Eisenbarth, T., Kumar, S.: A survey of lightweight-cryptography implementations. *IEEE Des. Test Comput.* **24**(6), 522–533 (2007)
8. Mouha, N.: The design space of lightweight cryptography. *IACRA Cryptology ePrint Archive* (2015) <http://eprint.iacr.org/2015/303.pdf>
9. Jaffey, T.: MQTT and CoAP, IoT Protocols. *Eclipse Newsletter*. http://www.eclipse.org/community/eclipse_newsletter/2014/february/article2.php
10. IBM, Eurotech. MQ Telemetry Transport (MQTT) V3.1 Protocol Specification (2010). <http://public.dhe.ibm.com/software/dw/webservices/ws-mqtt/mqtt-v3r1.html>
11. Shelby, Z., Hartke, K., Bormann, C.: Constrained Application Protocol (CoAP). Draft-IETF-Core-CoAP-18, June 20 (2013)
12. Wikipedia. Multi-factor Authentication. https://en.wikipedia.org/wiki/Multi-factor_authentication
13. Maes, R., Verbauwhede, I.: Physically unclonable functions: a study on the state of the art and future research directions. In: Sadeghi, A.-R., Naccache, D. (eds.): *Towards Hardware-Intrinsic Security*, pp. 3–37. Springer, Heidelberg (2010). Wikipedia. Physical unclonable function
14. Katzenbeisser, S., Kocabaş, Ü., Rožić, V., Sadeghi, A.-R., Verbauwhede, I., Wachsmann, C.: PUFs: myth, fact or busted? a security evaluation of physically unclonable functions (PUFs) cast in silicon. In: Prouff, E., Schaumont, P. (eds.) *CHES 2012*. LNCS, vol. 7428, pp. 283–301. Springer, Heidelberg (2012). doi:10.1007/978-3-642-33027-8_17
15. Wikipedia. International Mobile Station Equipment Identity. https://en.wikipedia.org/wiki/International_Mobile_Station_Equipment_Identity
16. Williamson, G.: Enhanced authentication in online banking. *J. Econ. Crime Manage.* **4**(2), 18–19 (2006)
17. Internet Assigned Numbers Authority (IANA). <http://www.iana.org/>
18. Shi, W., Cao, J., Zhang, Q., Li, Y., Xu, L.: Edge computing: vision and challenges. *IEEE Internet of Things J.* **3**(5) (2016)
19. Wikipedia. Attribute-based Encryption. https://en.wikipedia.org/wiki/Attribute-based_encryption
20. Sahai, A., Waters, B.: Fuzzy identity-based encryption. In: Cramer, R. (ed.) *EUROCRYPT 2005*. LNCS, vol. 3494, pp. 457–473. Springer, Heidelberg (2005). doi:10.1007/11426639_27

21. Guo, S.Q., Zeng, Y.P.: Attribute-based signature scheme. In: Proceedings of IEEE International Conference on Information Security and Assurance (2008)
22. Maji, H.K., Prabhakaran, M., Rosulek, M.: Attribute-based signatures. In: Kiayias, A. (ed.) CT-RSA 2011. LNCS, vol. 6558, pp. 376–392. Springer, Heidelberg (2011). doi:[10.1007/978-3-642-19074-2_24](https://doi.org/10.1007/978-3-642-19074-2_24)
23. Anada, H., Arita, S., Sakurai, K.: Attribute-based signatures without pairings via the fiat-shamir paradigm. In: Proceedings of the 2nd ACM Workshop on ASIA Public-Key Cryptography (2014)
24. Goyal, V., Pandey, O., Sahai, A., Waters, B.: Attribute-based encryption for fine-grained access control of encrypted data. In: Proceedings of the 13th ACM Conference on Computer and Communications Security (2006)
25. Bethencourt, J., Sahai, A., Waters, B.: Ciphertext-policy attribute-based encryption. In: Proceedings of IEEE Symposium on Security and Privacy (2007)
26. Chase, M.: Multi-authority attribute based encryption. In: Vadhan, S.P. (ed.) TCC 2007. LNCS, vol. 4392, pp. 515–534. Springer, Heidelberg (2007). doi:[10.1007/978-3-540-70936-7_28](https://doi.org/10.1007/978-3-540-70936-7_28)
27. Chase, M., Chow, S.S.M.: Improving privacy and security in multi-authority attribute-based encryption. In: Proceedings of 16th ACM Conference on Computer and Communications Security (2009)
28. Lewko, A., Waters, B.: Decentralizing attribute-based encryption. In: Paterson, K.G. (ed.) EUROCRYPT 2011. LNCS, vol. 6632, pp. 568–588. Springer, Heidelberg (2011). doi:[10.1007/978-3-642-20465-4_31](https://doi.org/10.1007/978-3-642-20465-4_31)
29. Okamoto, T., Takashima, K.: Efficient attribute-based signatures for non-monotone predicates in the standard model. In: Catalano, D., Fazio, N., Gennaro, R., Nicolosi, A. (eds.) PKC 2011. LNCS, vol. 6571, pp. 35–52. Springer, Heidelberg (2011). doi:[10.1007/978-3-642-19379-8_3](https://doi.org/10.1007/978-3-642-19379-8_3)
30. Wang, H., Lymberopoulos, D., Liu, J.: Sensor-based user authentication. In: Abdelzaher, T., Pereira, N., Tovar, E. (eds.) EWSN 2015. LNCS, vol. 8965, pp. 168–185. Springer, Heidelberg (2015). doi:[10.1007/978-3-319-15582-1_11](https://doi.org/10.1007/978-3-319-15582-1_11)
31. Shrestha, B., Saxena, N., Truong, H.T.T., Asokan, N.: Drone to the rescue: relay-resilient authentication using ambient multi-sensing. In: Christin, N., Safavi-Naini, R. (eds.) FC 2014. LNCS, vol. 8437, pp. 349–364. Springer, Heidelberg (2014). doi:[10.1007/978-3-662-45472-5_23](https://doi.org/10.1007/978-3-662-45472-5_23)
32. Hayaski, E., Das, S., Amini, S., Hong, J., Oakley, I.: “Casa” Context-Aware Scalable Authentication. In: Proceedings of the 9th Symposium on usable Privacy and Security (2013)
33. Kayacik, G., Just, M., Baillie, L., Aspinall, D., Micallef, N.: Data driven authentication: on the effectiveness of user behaviour modelling with mobile device sensors. In: Proceedings of the Workshop on Mobile Security Technologies (MOST) (2014)
34. Shi, E., Niu, Y., Jakobsson, M., Chow, R.: Implicit authentication through learning user behavior. In: Proceedings of the 13th International Conference on Information Security (2011)
35. Singh, K., Muthukumarasamy, V.: Using physiological signals for authentication in a group key agreement protocol. In: Proceedings of 2011 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) (2011)
36. Gehani, A., Chandra, S.: PAST: probabilistic authentication of sensor timestamps. In: Proceedings of 22nd Annual Computer Security Applications Conference (ACSAC 2006) (2006)

Information and Communications Security
18th International Conference, ICICS 2016, Singapore,
Singapore, November 29 – December 2, 2016,
Proceedings
Lam, K.Y.; Chi, C.-H.; Qing, S. (Eds.)
2016, XII, 478 p. 83 illus., Softcover
ISBN: 978-3-319-50010-2