Advanced Science and Technology Letters
Vol.136 (ITCS 2016), pp.59-63
http://dx.doi.org/10.14257/astl.2016.136.15

A Study of User Authentication Protocol Based on the ECC and OpenID Techniques in the Internet of Things

Jong J. Lee[1], Youn-Sik Hong[2], and Ki Young Lee[3*]

[1,3] Dept. Of Infomation and Telecommunication Enginering, Incheon National University,
[2] Dept. Of Computer Science and Engineering, Incheon National University,
Incheon, 22012, Korea
{ljj21089, yshong, kylee} @inu.ac.kr

Abstract. Authentication is a communication protocol processing procedure. In the Internet of Things, secure communication should be constructed between one "thing" and another by such a procedure. The identity that the second "thing" or object claims should be consistent with what the first one claims. Claimed identity information becomes a single message. Based on this message, we verify the identity of the "things". The purpose for both communication partners to implement authentication protocol is to have solid communication in the high layer (e.g., application layer). In order to do that, usually the authentication protocol has several sub-tasks such as identification key establishment, or key switching and consultation. In an authentication process, identity of the claimer can be acquired through message identification. In authenticated key establishment protocol, key establishment materials are also important protocol messages, which is part of entity authentication. In this paper, we focus on simple and efficient secure key establishment based on ECC (Elliptic Curve Cryptosystem). And we proposed ECC and OpenID based user authentication scheme. Our analysis shows that our approach can prevent attacks like eavesdropping, the man-in-the middle, key control attack, and replay attacks.

Keywords: Internet of Things, User Authentication, ECC, OpenID

1 Introduction

Nowadays, through the communication between various smart devices including a smart phone, it may be provided to the user after be generated a secondary data. Because a series of information can be gathered, processed, handled and controlled. In these environments, it may be exposed to the attack by sending the information to users which was not justified. Therefore, execution process of authentication for the user is required. However, due to constrained environment such as a low-power, ultra-small objects in the Internet of Things, there are omitted case for necessary authentication phases and process. Accordingly, security damage incidents and accidents are increasing, due to the exposure of the transmitted information to device

*Corresponding Author

ISSN: 2287-1233 ASTL

that it does not authentication and authorization though secure authentication phases. At this time, man-in-the-middle attacks such as an information gathering, imitation, blocking and an invasion of privacy can occur.

In order to solve these security vulnerabilities and problems, various user authentication methods are proposed in earlier studies. In earlier user authentication and identification technologies, there are divided such as ID-based, certification-based and SIM-based methods. And first, ID-based as a traditional authentication method can be lightweight and fast operation, however, there are problems for a relatively low safety and key management [1]. The certification-based method has the problem of the certification management, because it is how to authenticate using by issued certification. Finally, the SIM-based method is a how to perform the authentication by storing and managing authentication information in file system of a SIM card, thus, it is physically strong. However, it is necessary such as a separate software, a how to manage. Likewise, there is still problem on the aspect of safety and efficiency. In this paper, we analyze the problems and limitations on applying earlier user authentication methods in Internet of Things. And we also propose the method and architecture for user authentication in the Internet of Things. We also propose the hybrid authentication method to apply using both OpenID-based scheme and public key based algorithms.

2 Proposed Scheme

2.1 Architecture

Based on what we have learned from current literatures of Internet of Things, we may reasonably draw an abstract architecture for it (as shown in Fig. 5). “Things” or objects become end nodes in the Internet environment. They have unique global addresses (e.g., IPv6 address) and are capable of communicating with each other over the Internet. In order to organize and manage massive resources, every object will pre-register on a nearby trustworthy access point or gateway (denoted as Registration Authority, or RA). This assumption has another advantage that the RA can expend computing and storage capacity of the “things” or objects for authentication purpose. Meanwhile, RA is also able to maintain a history record of all access requests for auditing purpose.

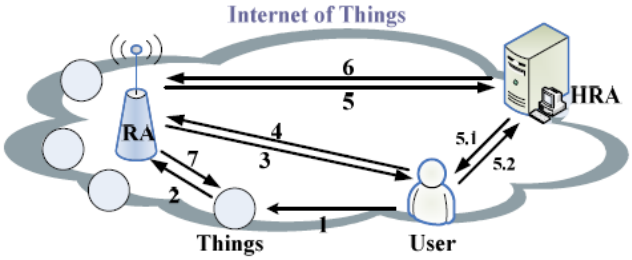

Fig. 1. The architecture of the proposed scheme

2.2 Authentication Protocol

As shown in Fig.1, a complete request procedure for accessing a "Thing" involves seven steps.

- Step 1: User request to access a "Thing";
- Step 2: "Thing" sends an authentication request to its RA for verification purpose;
- Step 3: RA request User ID;
- Step 4: User response with HRA information;
- Step 5: RA verifies the user HRA information and sends ID verification request to the HRA;
- Step 5.1: HRA challenge the user with a question;
- Step 5.2: User response the challenge with an answer;
- Step 6: HRA response ID OK or not;
- Step 7: RA response the "Thing" about the user ID and issue a session key with the user as we described.

To better describe our protocol, we first introduce some relevant terms here.

Table 1. Notations used in the proposed scheme

Symbol	Description
F_p	a finite field
E	an elliptic curve defined on F_p with a large order
P	a point on E
G	the group of elliptic curve points on E
h()	One-way hash function
s	the RA's private key
ID_u	the identity of the user
ID_t	the identity of the "thing"

To establish a session key for two entities, taking a user and an object as an example, only three steps are required as follows.

- Firstly, the RA who is responsible for the object will produce a random P∈G and compute P_s= sP in F_p. Note that, the s is a secret key that is assumed to be assigned before the RA has joined the IoT. For each user with ID_u, RA will generate P_u = h(ID_u) and the private key of the thing S_u = s P_u
- Secondly, the user generate an ephemeral private key *a* and compute Q_u = *a* S_u and $Q_u{}'$ = *a*P. Then the user will send an authentication message {ID_u, Q_u, h($ID_u||ID_t||Q_u||Q_u{}'$)} to the RA. Once receive the message, RA will compute $Q_u{}''$ = $s^{-1}Q_u$ and check whether h($ID_u||ID_t||Q_u||Q_u{}''$) equal to h($ID_u||ID_t||Q_u||Q_u{}'$) or not. If not, authentication fails. Otherwise go to step 3.
- The third step is session key establishment. Similarly, the RA will choose a random ephemeral key b and compute Qt = *b*P for the desired "thing". The session key will be h(*ab*P) based on ECC algorithm.

3 Analysis of Proposed Scheme

The online version of the volume will be available in LNCS Online. Members of institutes subscribing to the Lecture Notes in Computer Science series have access to all the pdfs of all the online publications. Non-subscribers can only read as far as the abstracts. If they try to go beyond this point, they are automatically asked, whether they would like to order the pdf, and are given instructions as to how to do so.

Please note that, if your email address is given in your paper, it will also be included in the meta data of the online version.

3.1 Eavesdropping Attack

Each run produces a different session key, and knowledge of past session keys does not allow deduction of future session keys. In our scheme, the session key is calculated by one way hash and session secrets. Know that only the user and RA know the abP, which is computed from the random ephemeral key. That is, even if the previous session secrets are revealed, the other secrets will remain unknown to the adversary.

3.2 Man-in-the-middle Attack

Compromising of a long term secret key, such as SA' at some point in the future, does not lead to compromise of communications in the past. Note that in our scheme, even if the adversary compromises the RA's secret key, it cannot compromise the previous session key because the adversary cannot know the ephemeral key a or b such that it cannot compute the session key. Also, our protocols satisfy both partial forward

secrecy and perfect forward secrecy since it is hard to compute the session key without knowing the ephemeral key a or b .

References

1. Truong, T.-T., Tran, M.-T., Duong, A.-D.: “Robust mobile device integration of a fingerprint biometric remote authentication scheme,” Advanced Information Networking and Applications (AINA), pp.678-685, 2012.
2. Weis, S., Sarma, S., Rivest, R.: “Security and privacy aspects of low-cost radio frequency identification systems”, International Conference on Security in Pervasive Computing, Berlin: Springer, pp.454-469, 2003.

