User Authentication Method with Mobile Phone as Secure Token

Ryu Watanabe and Yutaka Miyake
KDDI R&D Laboratories, Inc.
Ohara 2-1-15 Fujimino Saitama, Japan
Email: ryu@kddilabs.jp and miyake@kddilabs.jp

***Abstract*—In this paper, we propose a user authentication method with mobile phone. In our proposal, a mobile phone with a Subscriber Identity Module (SIM) card is used as security token for user authentication on WEB services. This authentication method named SIM-based authentication provides a secure authentication because of robustness of the SIM card. However, currently, the use of SIM-based authentication is limited to mobile phone. The terminals without a SIM card cannot use this style. In addition, only the mobile operator can use this method because the shared key hidden in the card is not open to service providers. In order to overcome this limitation, we realize pairing between mobile phone and terminals, which do not have SIM cards and the SIM-based authentication method can be applied to the terminals. In addition, the single sign on (SSO) technique is also applied in order to provide SIM-based authentication for service providers.**

Keywords*—*authentication; SIM; identity management.

I. Introduction

Recently, Internet services have become more attractive and many users frequently use the services. The services are varied, and online shopping or auction sites are common. User authentication function is important for services that require payments. Many Internet sites still use ID/password (PW) pairs for this purpose. However, malicious attack techniques have recently improved [1][2][11][12], and thus the number of incidents has increased. In order to cope with this problem, some sites apply multifactor authentication methods [3], such as biometrics or One Time Password (OTP). The use of Public Key Infrastructure (PKI) also provides secure authentication. Some Internet banking sites require the random number table for executing money transfer. These methods are practical for malicious attacks. However, such methods usually require dedicated devices or items, for instance, sensors for fingerprints, a one time password generator or random number table. Therefore, more convenient user authentication method is required for Internet service use. On the other hand, in the case of a mobile phone, another authentication method exists. So, a mobile phone uses a subscriber identity module (SIM) for the connection to the base station. (The Universal Integrated Circuit Card (UICC) is the different name of the SIM card. In this paper, we use the word SIM for the card.) The SIM card is removal and can be transferred between different mobile phones. By using SIM cards, mobile carriers can identify users. Using SIM card for user authentication has some good features. The SIM card is one of the tamper resistant modules and it is difficult to duplicate. In addition, users do not have to memorize some secret information such as password. However, currently, use of this authentication method is limited to the connection to the base station for mobile phones or device authentication on Wi-Fi communication. Moreover, only the mobile carrier can apply this authentication method because the secret information inside SIM cards is not open to service providers. Therefore, when the SIM-based authentication method can be used for user authentication of WEB service use, a more secure user authentication method is brought to both users and service providers. In addition, as described previously, this method requires a SIM card. Other terminals, such as a tablet or notebook PC, do not have SIM cards. In this case, if the mobile phone with a SIM card cooperates with mobile terminals without SIM cards, then secure authentication can be utilized on all mobile terminals. In order to cope with these two problems, the authors we proposed the SIM-based authentication method for mobile terminals without SIM cards. We also implemented a proto-system based on the proposal. The authorswe confirmed the functions in an Internet environment. In order to provide the SIM-based authentication for Internet service providers, the single sign on (SSO) technique is used. In addition, for secure usage, pairing between mobile phone with mobile terminal without SIM is confirmed at application level. After this section, we denote related work in section II. In section III, IV and V, we explain our proposal, the implementation based on our proposal, and discussion, respectively. In section VI, the conclusion is drawn.

II. Related work

A. Authentication method

User authentication methods for Web services are categorized into three basic factors: the knowledge base factor, ownership factor, and inherence factor. The first factor uses something the user knows (e.g., password or Personal Identification Number (PIN)). The second factor uses something the user has (e.g., secure token, software toke, cell phone) [5]. The third factor uses something the user is or does (e.g., fingerprint, deoxyribonucleic acid (DNA) sequence, face) [4]. Because of security problems, the authentication methods that use the last two factors or combination of multiple factors have gradually become widespread.

1) SIM-based authentication: The SIM-based authentication method is one of the authentication methods with the ownership factor. Firstly, this method is used for only the connection between a base station and mobile phone. Then, the method is extended to identify user terminal on Wi-Fi connection as EAP-SIM or EAP-AKA. EAP means extensible authentication protocol and AKA means authentication and key agreement [6], which are standardized in 3GPP [7] and IETF. EAP protocols are used on user device authentication on Wi-Fi connection establishment. In SIM-based authentication, by checking the response managed with the secret key, the mobile carrier authenticates the user terminal. So, the secret is shared with the authentication server of the mobile carrier.

Currently, the theses authentication methods are limited and not used for user authentication for Web services. For this purpose, another SIM-based authentication method was proposed, which is called Generic Bootstrapping Architecture (GBA). Basic idea is same. It also uses a dedicated shared secret key installed inside the SIM card. The design is based on the AKA. In the GBA method, the user, who wants to use a Web service (called the Network Application Function (NAF)), is authenticated by the Bootstrapping Server Function (BSF), then the BSF issues a dedicated temporary identifier and key pair for the services, and then authentication is executed between the user terminal and the service. The lifetime of the key is limited. Therefore, when it is expired, the user has to restart the sequence. The GBA is standardized; however, it does not use current Internet services because the browser function for the GBA method from the Web browser is not prepared. In addition, not all SIM cards can use the GBA function. Some function is also required for the SIM cards. The Application programmable interface (API) for this purpose is under standardization.

Therefore, in our proposed scheme, we customized the mobile phone and test type card to use the SIM-based authentication function based on the EAP-AKA' authentication protocol, which is derivation of EAP-AKA.

B. Identity Management Technique

The identity management (IdM) technique is used for control of user information. Originally, it was invented for control of user account management on an intranet. Then, the target area of the IdM technique expanded to the Internet. One of the main functions of the IdM technique is SSO, which realizes centralized authentication. A user account control server named identity provider (IDP) authenticates the user then transmits the result to the service server named service provider (SP). The SP provides the user a service depending on the results. Figure II-B shows the concept of SSO. In order to prevent linking, which is a privacy problem, pseudonyms are used for user identification between servers. Therefore, if service servers conspire with each other, the user identifier on both servers cannot be known. For realizing the IdM technique, some specifications and implementations are released from standardization organization. OpenID [9] and SAML [8] are representative of them.

1) OpenID: The OpenID mechanism is a decentralized authentication scheme for the SSO mechanism. OpenID users identify themselves with a URI and XRI. In the OpenID scheme, the identity provider and service provider are referred to as the OpenID provider (OP) and relying party (RP), respectively. The latest version of OpenID is OpenID connect. The OpenID technique is also used on the Internet service site. The combination of SIM-based authentication method and OpenID has been proposed [10]. In this identity management system, users and service provider are provided secure and convenient authentication.

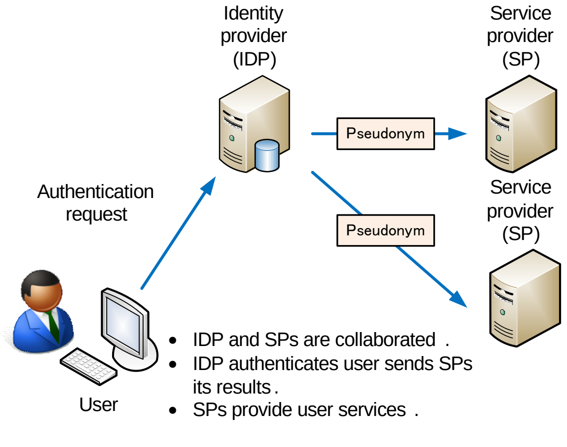
Identity provider (IDP)
Service provider (SP)
Pseudonym
Authentication request
Pseudonym
Service provider (SP)
User
• IDP and SPs are collaborated .
• IDP authenticates user sends SPs its results .
• SPs provide user services .

Figure 1. Concept of SSO

2) SAML: SAML (Security Assertion Markup Language) is an XML-based open standard data format produced by OASIS for exchanging authentication and authorization data between an identity provider and a service provider. Based on the SAML, some Web Brower single sign on profiles are defined such as liberty identity web services framework.

III. Our Proposal

A. Requirement

The concept of our proposal is described. A user wants to use some Web service on a mobile terminal, such as tablet or note PC, which do not hold a SIM card inside. It is supposed that such terminals have a wireless local area network (LAN) connection to the Internet. Usually, the service provider authenticates the user by using ID/PW pair. Instead of using the ID/PW pair, in our proposal, mobile phone is used as key device for user authentication. So, the system requires a mobile phone by the user. Under this concept, the SIM-based authentication can be used for any kind of terminals.

However, there are some problems. First, the mobile terminal and mobile phone have to contact each other by some method. Second, service providers cannot use SIM-based authentication directly. In addition, some security mechanism is required between the paired terminal and phone in order to avoid malicious use from another user.

The requirement for the system is summarized below.

1) Connection between mobile terminal and mobile phone
2) Delegated authentication scheme
3) Safety mechanism for avoiding malicious use

B. System Concept

Based on the requirements described above, we designed the prototype. For the first requirement, some connection methods can be used. In order to communicate with each other, a bidirectional connection is required and a unidirectional one is not appropriate. Therefore, we decided to use Wi-Fi and Bluetooth connections. In addition, we assume this connection is already established. So, the establishment of the communication method between the mobile terminal and mobile phone is out of the scope of this paper.

For the second requirement, we applied the identity management mechanism. So, the SSO mechanism is used. The mobile carrier, who knows the shared secret, behaves as the IDP. And the service providers unite with the mobile carrier and delegate user authentication to it. So, using tThe identity management technique is used better for security reasons to avoid privacy problems such as linkability.

For the third requirement, we applied mutual authentication on the applications for a SIM based-authentication. Currently, the browser API is not prepared for mobile phones. In addition, for our proposal, the mobile terminals without SIM cards and mobile phones have to communicate on the application level. Therefore, we implemented mobile applications for both terminals and phones. These applications also have to associate with each other before executing the SIM-based authentication.

C. Malicious attacks

Here, we denote malicious attacks, which we suppose. The aim of the malicious users is spoofing. They want to be authenticated as legitimate user. However, they do not have legitimate SIM or cannot duplicate the SIM because of the SIM resiliency. In addition, the SIM-based authentication method has a protection against eavesdropping. It uses a challenge and response (CHAP) type authentication and manages its lifetime. Therefore, if a response is eavesdropping, it cannot be used different session. In addition, the SIM-based authentication applies mutual authentication in the message exchange. So, user can notice that the server is faked, even though the attacker prepares a fake server and induce to it by phishing mail.

However, if the attacker can replace the application for our proposal, they can achieve man-in-the-middle type attack because the attacker can put modified messages both user terminal and server via the contaminated application. In order to cope with this problem, in our proposal, the applications share the secrete information. By using this information, the applications both mobile phone and mobile terminal confirm their legitimacy. Therefore, it is required that the secret is pre-shared among all the application and implemented securely. For this purpose, obfuscated codes can be used. However, in current version, this countermeasure against reverse-engineering is not supported and we will apply the feature in next version.

The totalwhole concept of the proposal is shown in Figures 2 and 3. Figure 2 shows the preparation before our proposed scheme and Figure 3 shows the communication among servers, user terminal and user mobile phone, respectively. So, in our proposal, the SIM-based authentication scheme and SSO technique are utilized.

IV. Implementation

A. System Specification

Based on the proposal, we implemented the proto-system. The system specification is summarized on Table I.

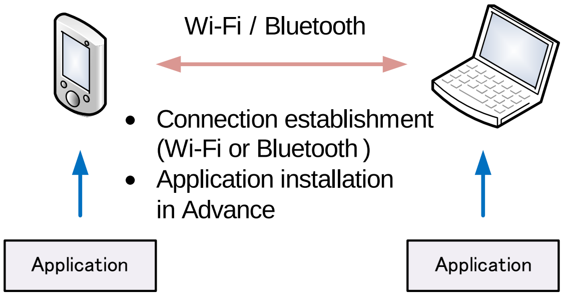
Wi-Fi / Bluetooth
• Connection establishment (Wi-Fi or Bluetooth)
• Application installation in Advance
Application
Application

Figure 2. System preparation for our proposal

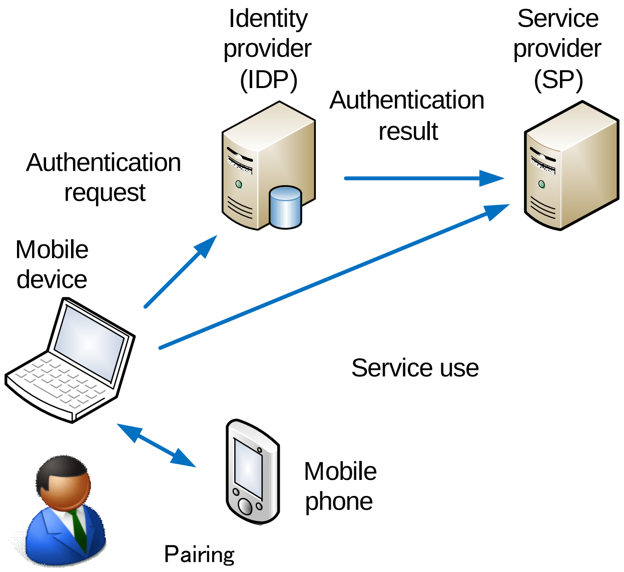

Figure 3. Concept of our proposal

As a mobile phone, we used the Android OS smartphone Nexus One because the kernel of the phone is open and can be modified. For the OpenID platform (IDP and SP servers), the Linux base OS (CentOS) and open module (php OpenID) are used. In addition, Windows OS tablet is used for the user mobile terminal. In our proposal, the EAP-AKA' method is used as SIM based authentication method. As mentioned previously, not all the SIM card is hold the GBA function, so, in our implementation, we selected EAP-AKA based authentication method. Usually, the mobile phone OSs including Android OS do not provide access to SIM card. Therefore, we modified the OS for this purpose. So, the use of the proto-type is limited currently.

In order to limit restrict the mobile terminals, which can contact to the mobile terminal, before the executing SIM-based authentication, named EAP-AKA', the pairing between applications on user mobile terminal and user mobile phone has to be confirmed. The steps for the pairing are summarized below. Before this step, the installation of dedicated applications for both user terminal and phone in advance.

1) At first, user operates the application on mobile phone

Table I. SYSTEM SPECIFICATIONS

Mobile Phone	
Terminal	Nexus One
OS	Android (Customized)
Mobile terminal without SIM	
Windows tablet	Toshiba WT301
OS	Windows 7
OpenID platform	
Server OS	CentOS
OpenID module	php-openid
Application	
Module	java

and change the mode to active in order to accept the request from user terminal. Only the active mode, the application listens to the request from mobile phone. (At this time, the wireless connection between mobile phone and mobile terminal is supposed to be constructed.)

2) Then user sends request from the mobile terminal to the mobile phone.
3) The mobile phone, which catches the request, executes mutual authentication using the secret hidden in the application.
4) If the application on the mutual authentication is successfully achieved on them, then the mobile phone shows accept code (four-six digit number) on the display.
5) User inputs the number to the application on mobile terminal. Then the pairing process is finished.

This process is similar to the paring method of Bluetooth. The purpose is same. Once the pairing is constructed, the user terminal can send authentication request to the mobile phone.

The flow sequence of our proposed scheme is described below. Before this authentication flow, ID association between an IDP and SP has been completed successfully in advance. The figure 4 shows the whole sequence.

1) A user accesses an SP from the browser on the mobile terminal without a SIM card or UIM.
2) The SP redirects the request to IDP.
3) The IDP generates the session ID for the user authentication and sends it to the browser on the user's mobile terminal.
4) The browser launches the application on the mobile terminal and passes the session ID to the application.
5) The application on the mobile terminal searches the mobile phone, which is on standby near the mobile terminals.
6) Connection is confirmed between applications.
7) The application sends an authentication request to the authentication application on the mobile phone, which is found in the previous step.
8) The SIM-based authentication method (EAP-AKA') is executed between the mobile phone and the IDP.
9) The IDP redirects the user authentication result to the SP.
10) The SP generates the session ID for service provisioning.
11) The SP provides the Web service to the user.

The time for the authentication was measured on the prototype. The process time on authetication server is less than 1 second without network delay in ten times average.

V. DISCUSSION

For the pairing between applications on both mobile phone and mobile terminals, the secrete parameter number, which is decided by user is required. If the number parameter is securely protected by user, no one can know it except the legitimate user. Therefore, malicious user cannot execute pairing behind legitimate user's back. In addition, the applications mutually authenticate each other before pairing by using securely embedded secret parameter . When an application cannot validate the other application, the request is denied. So even though a malicious user remakes the application, the modification is detected.

Whole communication between the terminals and the mobile phone IDP and SP are protected by using Secure Socket Layer (SSL) connection, therefore, secrets that is exchanged between them cannot be eavesdropped. Even though, the parameters are stolen by some method parameters included the response has life time and managed with the communication session. So it cannot be reused.

Our proposed system applies the SSO technique for user authentication on SP. Therefore, unwanted information about user is not sent to SP. The important parameter such as telephone number i is not revealed to service providers.So, the IMSI that is one of the important parameter is also kept inside IDP.

VI. CONCLUSION

In this paper, we proposed a SIM-based authentication method for mobile terminals. By using a mobile phone with SIM card as an authentication token, the secure user authentication is realized on mobile terminals without SIM card for WEB service use. The authorswe believe that by using our proposal, more flexible and useful user authentication is brought to both users and service providers.

REFERENCES

[1] A. Vorobiev and J. Han, "Security Attack Ontology for Web Services," Semantics, Knowledge and Grid, 2006. SKG '06. Second International Conference on, 2006, pp. 42-47.

[2] T. S. Chen; F. G. Jeng, and Y. C. Liu, "Hacking Tricks Toward Security on Network Environments," Parallel and Distributed Computing, Applications and Technologies, 2006. PDCAT '06. Seventh International Conference on, 2006, pp. 442-447.

[3] S. R. Basavala, M. Kumar, and, A. Agarrwal, "Authentication: An overview, its types and integration with web and mobile applications," Parallel Distributed and Grid Computing (PDGC), 2012 2nd IEEE International Conference on, 2012 pp. 398-401.

[4] S. Asha and C. Chellappan, "Authentication of e-learners using multimodal biometric technology," Biometrics and Security Technologies, 2008. ISBAST 2008. International Symposium on, 2008, pp. 1-6.

[5] H.K. Lu and A. Ali, "Communication Security between a Computer and a Hardware Token," Systems, 2008. ICONS 08. Third International Conference on 2008, pp. 220-225.

[6] J. Arkko, H. Haverinen, "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)," RFC 4187, IETF.

[7] 3GPP,
⟨http://www.3gpp.org/⟩ 07.07.2013

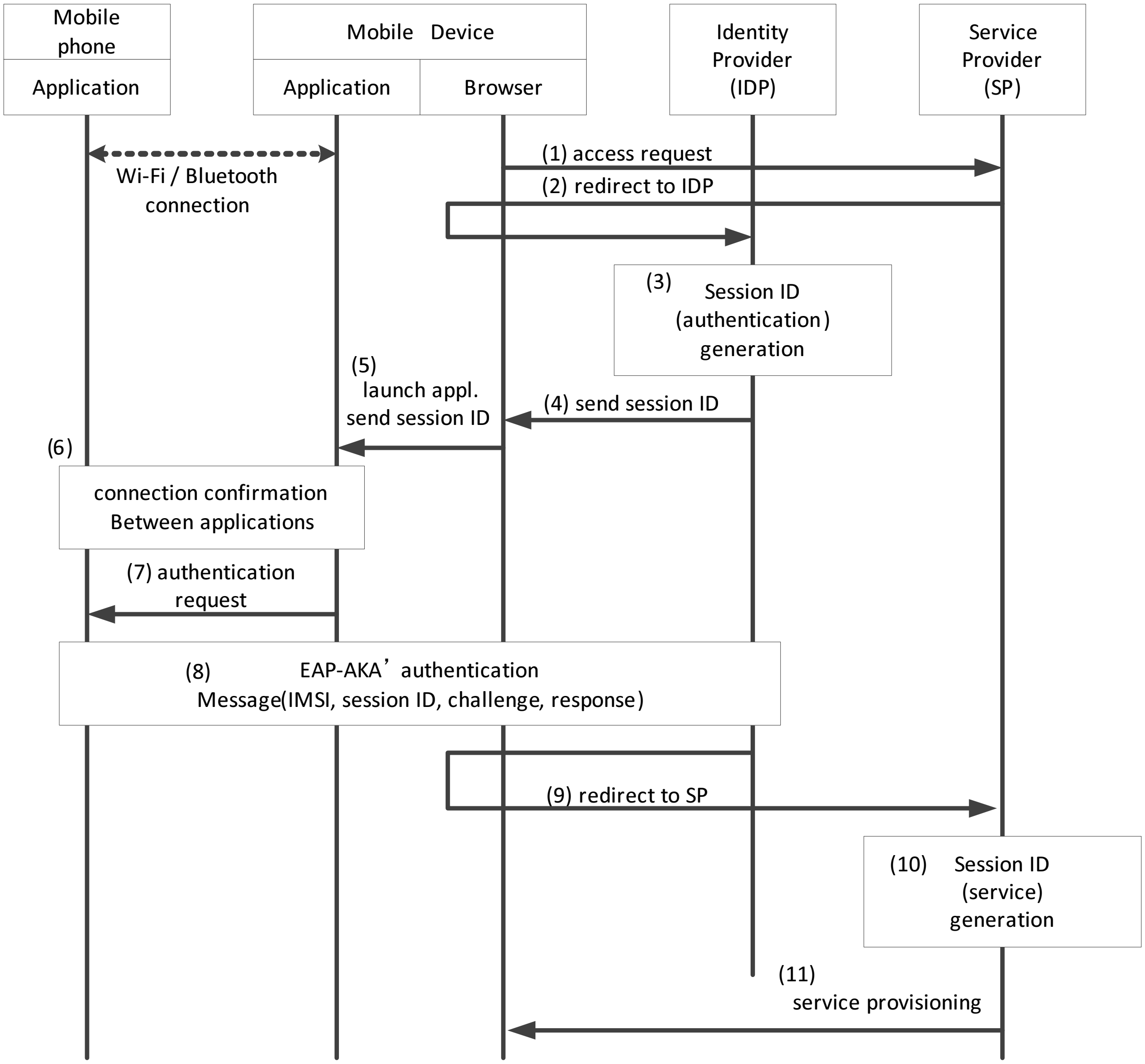
Mobile phone
Application
Mobile Device
Application
Browser
Identity Provider (IDP)
Service Provider (SP)
Wi-Fi / Bluetooth connection
(1) access request
(2) redirect to IDP
(3) Session ID (authentication) generation
(4) send session ID
(5) launch appl. send session ID
(6)
connection confirmation Between applications
(7) authentication request
(8) EAP-AKA' authentication Message(IMSI, session ID, challenge, response)
(9) redirect to SP
(10) Session ID (service) generation
(11) service provisioning

Figure 4. Sequence of our proposed method

[8] OASIS SAML V2.0, ⟨http://www.oasis-open.org/specs/index.php#samlv2.0⟩ 07.07.2013.

[9] OpenID, ⟨http://openid.net/⟩ 07.07.2013

[10] A. S. Ahmed and P. Laud, "Formal Security Analysis of OpenID with GBA Protocol," MobiSec, volume 94 of Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Springer, 2011, pp. 113-124.

[11] H. M. Sun, Y. H. Chen, and Y. H. Lin, "oPass: A User Authentication Protocol Resistant to Password Stealing and Password Reuse Attacks", Information Forensics and Security, IEEE Transactions on, Vol. 7, 2012, pp. 651-663.

[12] C. Xu and Y. Yang, "Password guessing attack on a key exchange protocol based on ECDLP", Progress in Informatics and Computing (PIC), IEEE International Conference on, Vol. 1, 2010, pp. 449-452.