20-22 Dec. 2007
Westin Hotel, Bali, INDONESIA

2nd International Conference on Ubiquitous Information Technologies & Applications

Organized by
Korea Information Processing Society
Korea Electronics Technology Institute

Hosted by
Sookmyung Women's University

Incorporated with
Institute of Electrical and Electronics Engineers (IEEE)

Sponsored by
MarkAny
DTV Interactive
UBIT
Easy Systems

www.icut.or.kr
Telematics System

94. Route Optimization in Nested NEMOv4 Using Chain Registration Technique (31)
Jungwook Song, Heemin Kim, Sangwook Bae, Sunyoung Han and Chan-Hyon Chang (Konkuk University) ------- 579

95. Study of Simulation for Efficient Traffic Signal and Traffic Accidents (197)
Jinsuk Back (Winston-Salem State University), You-Sik Hong (Sangji University), Cheonshik Kim (Anyang University) and Hong Jin Kim (Kyungwo University) and Jeong Gyu Lee (Korea Research Foundation) ------- 585

96. Traffic Sign Recognition Using Color Information and Error Back Propagation Algorithm (224)
Gul Won Bang (WinnerTek), Sang Won Bang (SongWon College), Soon Ja Yeom (University of Tasmania), Min Tae Lee (Chonnam National University), Kyung Woo Park (Mokpo National University), Dae Wook Kang and Byung Ki Kim (Chonnam National University) ------- 590

Application Layer Protocols

97. An OTP Ticket-Based AAA Mechanism in Ubiquitous Environment (136)
Dong-Wan Kang (Soochunhyang University), Hyun-Chang Lee (Hansei University) and Min Hong (Soochunhyang University) --------- 597

98. Efficient Oblivious Keyword Search (144)
Hyun Sook Rhee (Korea University), Hyun Jung Kim (KECE), Jong Hwan Park (Korea University) and Dong Hoon Lee (Korea University) --------- 602

99. OSI/OTS Access Control Model of RFID Network Applying RBAC in USN Environment (188)
Hae-Sang Shin, Jong-Hwa Kim, Soo Lyul Oh, Dong Soon Ahn, Kyung Woo Park, Jongmyung Choi, Seo Joon, Sung-Eui Cho, Sang Don Lee (Mokpo National University) and Sang-Won Bang (SongWon College) --------- 608

100. Interactive Lecture System Supporting Brainstorming Conference in Ubiquitous Computing Environment (193)
Myeong-Chool Ko (Konkuk University) -------------------------------------------- 613

Security

101. A Study on OTP Authentication using Automatic Generation Counter (3)
Seo-Young Kang, Sang Yeon Woo, Hong-Rae Kim and Jong-Keun Ahn (Soochunhyang University) ------- 621

102. A Media Protection Scheme Based On MPEG-4 File Format (16)
Dongkyoo Shin, Dongil Shin, Yung-Lyul Lee, Seyoung Park and Seunmi Yang (Sejong University) ------- 625

103. Forward-Secure and Chosen-Ciphertext Secure Public Key Broadcast Encryption (22)
Jong Hwan Park, Seok Koo Yoon and Dong Hoon Lee (Korea University) ------------------------------- 631

104. Ubiquitous Security via Face Recognition Using Hippocampal Neural Network (23)
Jae-Yong Lee and Dae-Seong Kang (Dong-A University) -------------------------------------------- 638

105. Information Access Control Method Using Member Authority on Discovery Services in EPCglobal Networks (59)
Gideok Han, Hong goo Moon and Hyukchul Kwon (Pusan National University) ------------------------ 644
An OTP Ticket-Based AAA Mechanism in Ubiquitous Environment

Dong-Wan Kang*, Hyun-Chang Lee**, and Min Hong*†
*Division of Computer Science and Engineering, Sookchunhyang University
**Division of Information and Technology, Hanse University
*{ipin428, mhp}@sch.ac.kr, **whlee@hansci.ac.kr

Abstract
AAA (Authentication, Authorization, Accounting) protocol is an information protection technology that systematically provides authentication, authorization and accounting functions not only in the existing wired network, but also in the rapidly developing pervasive network. Recently, standardization of the various applied services is in progress with the purpose of AAA standardization for the mobile users in the pervasive network. This proposal method uses a ticket for user authentication in the mobile device under the ubiquitous environment, and service is seamlessly provided even though the mobile device moves from the home network to the foreign network. In addition, with the ticket renewed from the foreign network, the overhead of the home authentication server can be reduced, and the anonymity ID provides a way to guarantee the anonymity of the service.

1. Introduction
With the rapid development of the Internet and the advent of the ubiquitous environment, the demands for services that are accessible by mobile devices are rapidly increasing. Although most services are provided to users on wired networks, users strongly request to use the same services on the wireless network. However, due to the characteristics of the wireless environment, providing services using the mobile device have many defects in security and the privacy of the user can be exposed to someone. In order to receive the service securely using the mobile device, AAA provides the information protection technology for the authentication, authorization, and accounting functions using various services and protocols such as WiBro, mobile IP and others as well as the conventional wired network. Currently, the IETF AAA working group has been serving on standardization of the various application services, with the goal of AAA standardization for mobile users in the wireless network. Also, various studies using AAA under the roaming service in different models and mobile IPv6 networks have been undertaken. Although several methods have been introduced using AAA to provide network service for the mobile devices, a secure and efficient method is suggested to increases the convenience of user by a ticket in this paper. Furthermore, our service guarantees the anonymity when the service uses an anonymity ID, which makes unavailable information of what service has been provided to the user. The organization of this paper is as follows. Section 2.1 describes the security requirements, section 2.2 shows an overview of ticket-based scheme and the OTP (One-Time Password) and section 3 describes the existing studies. Section 4 explains the proposed method, and section 5 illustrates the analysis of the proposed method. Finally, section 6 presents the conclusion.

2. The preliminaries
2.1. Security Requirements
The data accessing to the home authentication server from the foreign network should provide the following security matters.

- Confidentiality: The message transmitted by the user should be acknowledged only by each communication object.

† Correspondent author: Min Hong (mhp@sch.ac.kr)
• Integrity: The transmitted message should not be forged, deleted or modified. Otherwise, the user should confirm its modification.
• Authentication: The accessing user should be identified as a qualified user.
• Access Control: Disqualified user should not be able to use the service.
• Anonymity: The third party should not know the service used by the user.
• Privacy: The user's personal information should not be exposed and interfered.
• Replay Attack: The system should prevent the replay and authentication of the third party.

2.2. Overview of The Ticket-Based Scheme

A ticket is a piece of data showing that a user has authorization. The Ticket Based Model is an authentication model using the ticket and is one of the representative methods in Cross-domain Authentication between domains. The user requiring the service provides the ticket to the service provider as credential information and the service provider serves the appropriate service for the ticket after confirming the ticket. The ticket used in the AAA model is issued in mobile node after passing through the authentication and authorization setting process based on the credential information suggested by the mobile node. The user can request and achieve the service everywhere with the ticket so that the ticket based model is most appropriate model in the mobile service and the Kerberos system is the most typical ticket based authentication model[5].

2.3. Overview of One-Time Password

One form of attack on networked computing systems is eavesdropping on network connections to obtain authentication information such as the login IDs and passwords of legitimate users. Once this information is captured, it can be used at a later time to gain access to the system. One-time password systems are designed to counter this type of attack, called a "replay attack". The authentication system described in this paper uses a secret pass-phrase to generate a sequence of one-time passwords. With this system, the user's secret pass-phrase never required to cross the network at any time such as during authentication or during pass-phrase changes. Thus, it is not vulnerable to replay attacks. Added security is provided by the property that no secret information need be stored on any system, including the server being protected. The OTP system protects against external passive attacks and against the authentication subsystem. It does not prevent a network eavesdropper from gaining access to private information and does not provide protection against either "social engineering" or active attacks[3].

3. Related Works

The next step shows the typical centralized authentication method of the existing studies and the authentication method using a ticket in AAA as well as the characteristics and advantage/disadvantage of each method.

3.1. Kerberos

Kerberos uses the centralized authentication server and its encryption method uses symmetric encryption for authentication. So as the user achieves the service, the user receives the ticket-granting ticket issued from the authentication server and service-granting ticket from the ticket granting server. The user should remember a password agreed in advance for accessing each of the Kerberos members. The current Kerberos protocol has developed from version 4 to version 5 and is standardized in IETF RFC 4120[1]. In this case, the Kerberos protocol has a weakness in the password, the ticket granting server distributes the session key so that the anonymity and privacy are not secured and the message information being transported between the user and service providing server can be revealed. It also suffers from the problem of generating delay while requesting the authentication, as the Kerberos server is divided into authentication server and ticket granting server.

3.2. AAA for Real-Time Secondary Market Service

With the explosion of demand for wireless communication services, the scarcity of spectrum poses a great challenge to wireless networking. However, recent field measurements show that a significant percentage of spectrum is under-utilized. To address this problem, the research community introduced the concept of real-time secondary markets, where licensees are allowed to temporarily lease the spectrum unused by the primary users to secondary users. Also, this paper proposed the AAA system structure and a mechanism of authentication and authorization of the secondary user, synchronization between multi secondary devices and management of Secondary Market Service[6]. This method requires an identification process of ticket in all terminals by
broadcasting the ticket and using the open key and the safety of ticket relies on random number.

4. The Proposed Scheme

The conventional method generates delay and overhead when the user moves to a foreign network issuing a new ticket or requesting re-authentication and requires large amounts of computation resulting in inappropriate application in mobile environments.

![Whole Flowchart of Proposed Scheme](image)

Figure 1. Whole Flowchart of Proposed Scheme

On the contrary, the proposed method can provide service by providing a ticket to the service provider after the user utilizing the mobile device accesses the home authentication server and achieves the authentication and ticket. In addition, when using the service, it guarantees the anonymity of the user through the anonymity ID. Using such a scheme can reduce the delay in the authentication procedure and enhance the security and efficiency.

4.1. System Parameters

Next, system parameters used in this method are explained.

- \( D \) : Device, \( AAAF \) : Foreign AAA Server, \( AASH \) : Home AAA Server, \( SP \) : Service Provider
- \( PIN \) : Serial Number of Mobile Device
- \( ID \) : Identity of *
- \( PW \) : Password
- \( KS \) : Shared Key between Device and Home AAA Server
- \( SK_{D,SP} \) : Session Key between Device and Service Provider
- \( h() \) : Secure One-way Hash Function
- \( OTP \) : One-Time Password
- \( AT \) : Authentication Time
- \( E[\_] \) : Encryption with key of *
- \( Sign \) : Signature of *
- \( KU \) : Public Key of *
- \( KR \) : Private Key of *
- \( Lifetime \) : Lifetime of Ticket

4.2. The Proposed Scheme

The proposed protocol consists of 3 steps. Assume that the password and symmetric key of the user used in the communication are distributed in advance, each step is composed of the initial registration and ticket request, service request and ticket renewal in the foreign network.

4.2.1. Initial Registration and Ticket Request

**Step 1.** The device generates the serial number from the mobile device, password and \( OTP \) with XOR operation of the \( AT \). Then, the device transports the encrypted value of device ID, \( OTP \) and \( AT \) with the prior shared symmetric key to the home authentication server. \( OTP \) is based on \( AT \) so that the value is not repeatedly generated and is secure against a replay attack.

\[
OTP = PIN \oplus PW \oplus AT
\]

\[
ID_D, OTP, E_{KS}[AT]
\]

**Step 2.** Home authentication server decrypts the encrypted \( AT \), and generates \( OTP' \) by operating the mobile device stored in the device's database, password and transmitted \( AT \) with XOR operation and compares them with the transmitted \( OTP \). If the value is identical, the XOR operates \( AT \) in the device ID generating the renewal ID and ticket. The Home authentication server transports \( OTP' \), ticket, \( AT \) and session key to be used between the device and service provider by encrypting the prior to shared symmetric key.

\[
PIN \oplus PW \oplus AT = OTP'
\]

\[
OTP' \neq OTP
\]

\[
ID_{\text{new}} = ID_D \oplus AT
\]

\[
Ticket = ID_{\text{new}}, Sign_{\text{server}}[ID_{\text{new}}, \text{Lifetime}, h(OTP)]
\]

\[
OTP', E_{KS}[Ticket, AT, SK_{D,SP}]
\]

4.2.2. Service Request

**Step 1.** The device encrypts the ticket issued from the home authentication server as the transmitted session key, \( OTP' \), \( AT_{\text{new}} \) and transmits the integrity verification value to the service provider.
The service provider decrypts the transmitted message as a session key. The ticket included in the message is decrypted as a public key of home authentication server and renewal ID, the valid time and OTP applying the hash function are obtained. The system hashes the OTP inside the message transmitted from the device, generates h(OTP) and compares it with h(OTP) included in the ticket. If the compared value is right, it renews the session key by XOR operating AT_new with previous session key. After that, in order to verify the qualified service provider, it provides the operation (AT_new − 1) in transmitted AT_new and sends the renewed session key by encryption. In this step, the service provider cannot identify the information of the device although the device is authenticated. As the ticket includes the renewal ID, it provides anonymity even though the device can use any kind of service. Also, the session key is renewed with the XOR operation of AT_new and then this session key is used in communication so that the home authentication server cannot know the content, hence providing the privacy.

\[ h(OTP) \neq h(\text{OTP}) \]

\[ SK_{D-SP} = SK_{D-SP} \oplus AT_{new} \]

\[ E_{SK_{D-S}}[AT_{new} − 1] \]

4.2.3 Ticket Renewal in Foreign Network. When the device tries to renew the ticket by transporting to the foreign network from the home network, the device can renew the ticket from the foreign network, and then continuously receive service.

**Step 1.** The device sends the ticket, OTP_new and AT_{new} by encryption with the symmetric key shared in the home authentication server. This message is the ticket renewal request.

\[ E_{KS}[\text{Ticket, OTP}_{new}, TSV_{new}] \]

**Step 2.** The foreign authentication server transmitted renewal request message to the home authentication server with the value signed with the private key of the foreign authentication server.

\[ \text{Sign}_{AAF}[E_{KS}[\text{Ticket, OTP}_{new}, TSV_{new}]] \]

**Step 3.** The home authentication server decrypts the value of the public key and obtains a renewal request message from the foreign authentication server. It confirms the ticket by decrypting the ticket renewal request message with the shared symmetric key, generates OTP'_new by the XOR of the serial number and password stored in the database of the mobile device and authenticates the device by comparing the value with the transmitted OTP_{new}. After completing the authentication, the XOR operation transforms AT_{new} given by the device to the renewal ID, generates a new renewal ID and renews the ticket. The renewed ticket is encrypted by OTP_new, AT_{new} and the symmetric key are shared with the device. Then, the message is encrypted with the private key of the home authentication server, and the ticket renewal response message is transmitted.

\[ PIN \oplus PW \oplus AT_{new} = OTP_{new} \]

\[ OTP_{new} \neq OTP_{new}^* \]

\[ ID_{anong_{new}} = ID_{anong} \oplus AT_{new} \]

\[ \text{Ticket}_{new} = ID_{AAH} \cdot \text{Sign}_{AAH}([ID_{anong_{new}}, \text{Lifetime}, h(OTP_{new})], h(ID_{anong_{new}} \| \text{Lifetime} \| h(OTP_{new})) \]

\[ \text{Sign}_{AAH}[E_{KS}[\text{Ticket}_{new}, OTP_{new}, AT_{new}]] \]

Step 4. The foreign authentication server decrypts the value with its home authentication server public key and obtains the renewal response message and transports it to the device.

\[ E_{KS}[\text{Ticket}_{new}, OTP_{new}, AT_{new}] \]

Step 5. Then, the device can receive the service by using the ticket renewed in the same way as the service request step.

**5. Analysis of The Proposed Scheme**

The proposed scheme which mentioned in section 2 is analyzed, as follow Table 1.

**6. Conclusion**

With the growth of the Internet and the ubiquitous environment, there are various benefits to accessing services using mobile devices. However, the utilization of the mobile wireless network has several security issues such as exposure of privacy.

Therefore, the proposed scheme uses the OTP and ticket for device authentication under this ubiquitous environment. For roaming service from the home network to a foreign network, the ticket is used for the seamless operation of service. Furthermore, although the ticket is damaged in the foreign network or the lifetime of the ticket is expired, the ticket can be renewed without any accessing to the home.
<table>
<thead>
<tr>
<th>Table 1. Analysis of proposed scheme</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td>3.1</td>
</tr>
<tr>
<td>Confidentiality</td>
</tr>
<tr>
<td>Integrity</td>
</tr>
<tr>
<td>Authentication</td>
</tr>
<tr>
<td>Access Control</td>
</tr>
<tr>
<td>Anonymity</td>
</tr>
<tr>
<td>Privacy</td>
</tr>
<tr>
<td>Replay Attack</td>
</tr>
<tr>
<td>Efficiency</td>
</tr>
<tr>
<td>Mobile</td>
</tr>
<tr>
<td>[O: offer/security</td>
</tr>
<tr>
<td>△: partly offer</td>
</tr>
<tr>
<td>X: non-offer/security</td>
</tr>
<tr>
<td>Proposed Scheme</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>[O: offer/security</td>
</tr>
<tr>
<td>△: partly offer</td>
</tr>
<tr>
<td>X: non-offer/security</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

authentication server and can reduce the overhead of the home authentication server. Our method guarantees the anonymity of services to the devices using the anonymity ID. The ticket scheme would reduce the number of communications in the roaming network and heighten the security and efficiency. The research for a light-weight public key with ID-based ticket scheme may improve the system under the recent ubiquitous environments.

References


