Cross-domain Authentication Mechanism Design and Research Based on the Mobile Internet

Xiao-hui CHENG¹, Ming-yue LI²,a and Li-yun ZHANG³

¹,²,³College of Information Science and Engineering, Guilin University of Technology, Guilin, China

Keywords: The mobile Internet, Cross-domain authentication, Single sign-on, SAML.

Abstract. With the development of mobile communication, users put forward a higher security requirement in the process of intelligent mobile terminal to access different applications. A cross-domain authentication mechanism in the mobile Internet environment has been designed in this paper, which is B/S pattern. Firstly, the trust relationship between the Single Sign-on servers has been established by using SAML, then the design frame is Single Sign-on, as well as using HTTPS and ECC to encrypt data and the data transmissions. The user only needs to authenticate identity successfully in one trusted domain, then he can visit other trusted domains easily and does not need to authenticate identity again under the context that without exit. It is shown that a cross-domain authentication mechanism in the mobile Internet environment has been designed which raises the reliability of mobile terminal. This article uses identity-based encryption to calculate the public key and private key. Finally the paper verifies the proposed mechanism. Experiments show that this mechanism is convenient for the user's authentication, meanwhile it ensures the security and scalability of the system. It is proved that the cross-domain authentication mechanism has some reference meanings in the future research in this field.

Introduction

Authentication is a common method in obtaining trust in computer, by which the user has been authenticated and impostor has been prevented. The cross-domain authentication is a computer certification process between two different domains. The network is developing in the direction of distribution, and users usually need to log on the system which is composed of multiple heterogeneous and autonomous trusted domains. Cross-domain authentication is an efficient measure to solve the problem that the user should input credentials such as ID and password each time when using a particular service.

The study on cross-domain authentication so far mainly focuses on cross-domain authentication model or certification scheme and rarely thinks about the cross-domain authentication mechanism in Internet environment. Literature 1-2 put forward two kinds of cross-domain authentication model, and they are the cross-heterogeneous authentication model based on the public key infrastructure technology[1] and the cross-domain authentication protocol model based on the hypercube[2]. The paper respectively expounds the different certification process when users access resources in heterogeneous domains, and simplifies the work of distribution and management between authentication servers that share common key, as well as introduces a new trust mechanism to better manage and control the list of trusted root certificates.

To improve the safety and reliability of mobile terminal in the mobile Internet environment, the author aims to solve the relevant problems of multi-domain authentication in the mobile Internet environment, and starts from the authentication framework of single sign-on, proposing a new efficient ID-based encryption scheme in the mobile Internet environment, by which to achieve the goal that when user authenticated successfully in a trusted domain, so there is no need to exit and authenticate again when accessing to other trusted domains.
Cross-domain Authentication Module Design

Single Sign-on and Single Sign-on Model

Single sign-on (SSO) is a sort of uniform identity authentication and authorization mechanism, which allows the user to have an active identity authentication in network, then he can access all the authorized network resources and application systems without having to log in again, that is “Once logged in, many certification”.

SSO solutions provide a unified framework for security and authentication, easing much of the burden on users, administrators, and developers. Meanwhile, it also helps to eliminate the islands of information and improve the fusion of information.

There are more than two SSO servers called the authentication system in the whole system of cross-domain authentication, which even can be different products. Through the standard communication protocol SAML, SSO servers can exchange authentication information so that SSO across different servers and environments is achieved. SSO model in this article is shown in Fig. 1.

![SSO model](image)

Figure 1. SSO model.

When the user wants to access application system 1, he needs to pass the authentication of SSO server 1, then he will obtain a randomly send ticket from SSO server 1. It can be identified that the ticket is generated by SSO server 1 when the user visits SSO server 2. For the two SSO servers have exchanged authenticated information through the SAML before, the client can still complete the function of SSO.

The Establishment of Trust between the Single Sign-on Servers

In the mobile Internet environment, service consumers and providers are strangers, and they do not trust each other in advance. The trust relationship is needed to establish between different domains, which it is a bridge between the domain and domain. In order to establish a cross-domain authentication, all of the domain involved need to build trust between security domains. To ensure the authenticity and legitimacy of the identity of the two domains is the premise of follow-up communications[3].

It is shown in Fig. 1 that the key of cross-domain access is how to establish trust between single sign-on servers of different domains. The author applied the communication protocol SAML to achieve the authorization access control of different SSO servers, so the client just needs to authenticate the identity in his own security domain then he can access other trusted domain’s resources, and finally the cross-systems granted transparent access between two inter-domains is accomplished. Fig. 2 shows the process of the establishment of the trust relationship between SSO servers.
Figure 2. Multi-SSO servers’ trust relationship establishment.

The Fig. 2 shows two SSO servers. Each SSO server is equivalent to a security domain, and each security domain has its own user provisioning repository. These security domains can represent different business units or different companies. Users send their identity through the SAML token, and point out their identity to the target security domain. The user in the token is in the external security domain instead of the local, making the SSO server needn’t to manage other security domain’s account or identity authentication data.

The Identity-Based Cryptosystems

In order to simplify the CA management of the user certificate in traditional public PKI key cryptosystems, Shamir first proposed Identity-based Cryptology (IBC) in 1984[4]. Until the year 2001, by ways of the bilinear pairing of elliptic curve and the method of quadratic residue and strict formal proof Boneh etc and Cocks accomplished the Identity Based Encryption system (Identity-based Encryption,IBE). The basic idea of IBE is to bind the user's identity and his public key, namely the public key is derived from user's mobile phone number, name, Email address and the IP address so there is no need to distribute. On the basis of the user's identity information Private Key Generator (Private Key Generator, PKG) generated private key and sent it to the corresponding user through security channel. A private key tends to lag behind the generation of public key since it is generated by PKG according to the public key selected by user so that it is often sent by online distribution.

When new user A login system for the first time, the private key generator is responsible for verifying the identity information of user A, at that time user B can get the public key of user A. After that the IBE software encrypts a message and uses three parameters of the system to generate the public key for the information: starting value, existing weeks and the recipient's identity information (usually in the form of Email address), and then transmits it to user A in the form of cipher text in the security network. At the same time different IBE servers require a security channel to transmit the private key to user A. Since user A acquires the private key from generator, it can decrypt the message. Another case is that if the user receives the IBE encrypted E-mail messages but didn't use IBE encryption before, then he can use the encrypted E-mail address as a public key to request a private key for authentication to the private key generator, so that he is qualified to decrypt the contents of all encrypted E-mail.

The Accomplishment of Cross-domain Authentication under the Mobile Internet

The Design of Cross-Domain Authentication

The process of cross-domain authentication in detail is shown in Fig. 3. It is supposed that domain A and domain B have established trust relationship by SAML. Firstly mobile client B login SSO server in its own domain to get the access token. Then client B requests to access domain A’s SSO server and sends the token at the same time. After SSO server A receives the token, the token will be sent to SSO server B for verification; and then SSO server B verifies this token by querying database B. If consistent, application server A will provide service for mobile client B; if not, deny it. Thus it can achieve the goal that user login only once, so he can cross domain access all the application servers in
domain A.

Figure 3. The detailed process of cross-domain authentication.

The Detailed Design of Module

The module design of the system mainly consists of SSO server module, application server module, database module, and mobile client module, which are shown in Fig. 4.

Figure 4. The general module of system.

In the module design of the system, the SSO server provides authentication and authorization service. Database provides users and ticket information list. The application server's authentication and authorization business agent is responsible for the implementation of server side authentication and authorization. Mobile client authentication and authorization interface is in charge of providing external related service invocation for clients. Mobile client authentication and authorization agent is responsible for implementing certification and authorization of terminal device.

The Analysis of System Safety

Compared with the traditional PC client, the security issue mobile client faced is rooted in the three typical characteristics such as personal, the Internet, open and so on. What’s more, the Google company regards opening as the core development direction on the Android system, so that the security issue is becoming particularly serious which is often met by application developers. To guarantee the security of data transmission from two aspects in this paper: the first one is that the transmitting data itself is encrypted. This process uses HTTPS to encrypt the information. When the
user requests to access the web, the data request will be encrypted by the web page. The third party is unable to get the data after it has already been encrypted and authenticated. Thus the problem of data being hijacked and tampered can easily be solved. The second is that the data is transmitted through the information encryption channel between the client and the server. After the server receives the information it will return a receipt to the client, but the security of this method is very unstable, so we need to add a specific authentication information. ECC is used to encrypt ticket in this step, which is one of the public key encryption algorithms, because ECC has the advantage of less time-consuming in digital signature, higher security performance and shorter key length, which makes it a better performance in the safety of mobile terminal.

The Experimental Test and the Result Analysis

The Experimental Test

This paper uses UC browser of the android telephone to test. Fig. 5 shows that the user inputs the URL in the mobile client browser and then enters user name and password. Fig. 6 shows that the user login the SSO server and chooses the APP to access. Fig. 7 shows that the SSO server authorizes the user to cross domain access the APP. Fig. 8 is referred to that the user log out and deletes ticket from domain A and domain B. Fig. 9 shows the cancellation of success. The address bar displays the domain name, and the real IP address is https://192.168.1.1:8080, then the jsp’s name follows behind.

![Figure 5. User log in.](image)

![Figure 6. Application choose.](image)

App1 App2

Figure 6. Application choose.

![Figure 7. The transmission of ticket’s clear text.](image)

![Figure 8. Delete ticket from domain A and B.](image)
The Analysis of Result

Experiments prove that it is feasible to simulate the cross-domain authentication in mobile client, which can be put into use in reality.

Acknowledgement

As the research of the thesis is sponsored by National Natural Science Foundation of China (No: 61262075) and major scientific research project of Guangxi higher education (No: 201201ZD012), we would like to extend our sincere gratitude to them.

References

[1] Zheng Li, Chen Ze-Mao, Qin Yan-Lin, Zhu Ting-ting. Cross-domain Authentication Scheme Based on Zero Knowledge Proof [J]. Computer and Digital Engineering, 2014, 42(3): 446-449. (In Chinese)

[2] Yao Yao, Wang Xing-wei. A New Protocol of Hypercube-Based Cross-Domain Authentication [J]. Journal of Northeastern University (Natural Science), 2010, 31(7): 925-937. (In Chinese)

[3] Tang Li-juan. Research of SAML & SSO and Entrepreneurial SSO Framework Design [D]. Shandong University, 2011. (In Chinese)

[4] Li Xi. Research on Identity-based Cryptography and its Application in Wireless Mobile Payment [D]. Huazhong University of Science and Technology, 2009. (In Chinese)