A Unified Authentication and Management Platform Based on OTP

Shiliang Wu[1]*, Junwei Zou[1], Chunxiao Fan[1], and Xiaoying Zhang[1]

[1]Post Code.Beijing Key Laboratory of Work Safety Intelligent Monitoring,School of Electronic Engineering, Beijing University of Posts and Telecommunications,
Beijing, P.R.China, 100876.
e-mail: W._1101@163.com; Buptzjw@gmail.com; Fcx100@gmail.com;
Zhangxy1264@163.com

Abstract. With the rapid development of global information technology, the application systems of the enterprises are becoming more and more complicated. On the other hand, the security will be faced with double security challenges: how to ensure that only legitimate users are able to access the corresponding application resources; secondly, how not to increase the burden of the users when the systems implement safety protection measures. So application system must be transformed to correct the imperfections. This paper proposes a unified authentication and management platform which employs intelligent mobile phone as the carrier, challenge code as the uncertain factor of dynamic password generation mode, and single sign-on in the broker mode based on Cookie technology. Based on the experimental results, the platform demonstrates a much better enterprise information security and a more convenient user management system.

Keywords one-time password • smart phone • single sign-on• authentication

1 Introduction

With the advancement of informationization process, the system in corporate departments or government presents a trend of diversification and complex. Most of these systems have separated identity authentication and access control method may also be different. They use the traditional account with static password mode to log in. So the system may exist the following problems: when access to the different system, the user will be required multiple authentication; duplicate account password to log in gives the user a burden; each system has its own identity authentication mechanism, which is undoubtedly a repeated construction; in traditional way of authentication, the user's account and password can be easily stolen by others which may cause huge losses.

This paper proposes a kind of unified authentication management platform design which employs intelligent mobile phone as a carrier to generate dynamic password. This platform uses dynamic password to improve security and completes single sign-on technology. User data is centrally stored in authorized platform. Unified authorization data is centrally stored in distributed subsystem.

1.1 Problems

Single sign-on protocol is used in a multiple application system for the user’s unified authentication and management. However, the implementation of these methods in the legacy systems requires the changes in the system and we need to build the new infrastructure to implement the different single sign-on methods provided by the different vendors. This creates a burden for the organization to implement the single sign-on. Old system must reconsider how to manage user data and upgrade itself [1].

In traditional authentication, due to the authentication information passing through the network and that password is unencrypted, the attacker wiretaps net data and easily extracts the username and password from the authentication data. In the complex network environment using the traditional static password authentication mode has already can't satisfy the need of security. On the other hand, there are many kinds of dynamic password. The traditional dynamic password almost uses hardware password token. Hardware token is not convenient to carry and need a certain cost.

1.2 Related Technologies Research

The One-Time-Password (OTP) will add uncertain factors to original data to generate dynamic password [2]. Each time you login, the authentication information is not the same. The illegal user can not be verified, even if the illegal user intercepted the correct password and submitted it to the authentication server again .So don't worry about the password intercepted by third party in transmission during authentication[3].

In a broker-based single sign-on model, it has a centralized authentication and user account management server [4]. The use of central authentication server and a central database reduces the management cost, avoids duplication and provides a public and independent certification third party, like a broker. The model consists of three parts: client, unified authentication management server and application server while supports certification services. This paper compares those methods ’perform, merits and faults, easy or difficult degrees, maneuverability, exc. Finally, get an optimal solution to solve those problems.

2 The Overall Architecture of Unified Authentication and Management platform

The unified authentication and management platform can be divided into two parts: the dynamic password authentication module and single sign-on authorization management module, as figure2.1. The dynamic password module consists of a client and authentication server. The client in this system is a smart phone which is installed OTP software. The OTP software can use local data to generate OTP for authentication. The authentication server's function includes OTP opening, OTP authentication and OTP updating. Single sign-on, authorization management module consists of subsystem, user data management server and authentication module. Subsystem does not need to authenticate the user's validity, but redirect the user to authentication module. User data management server manages all subsystem's user data. Authentication module provides authentication credentials and set authentication rules of communication between subsystem and platform.

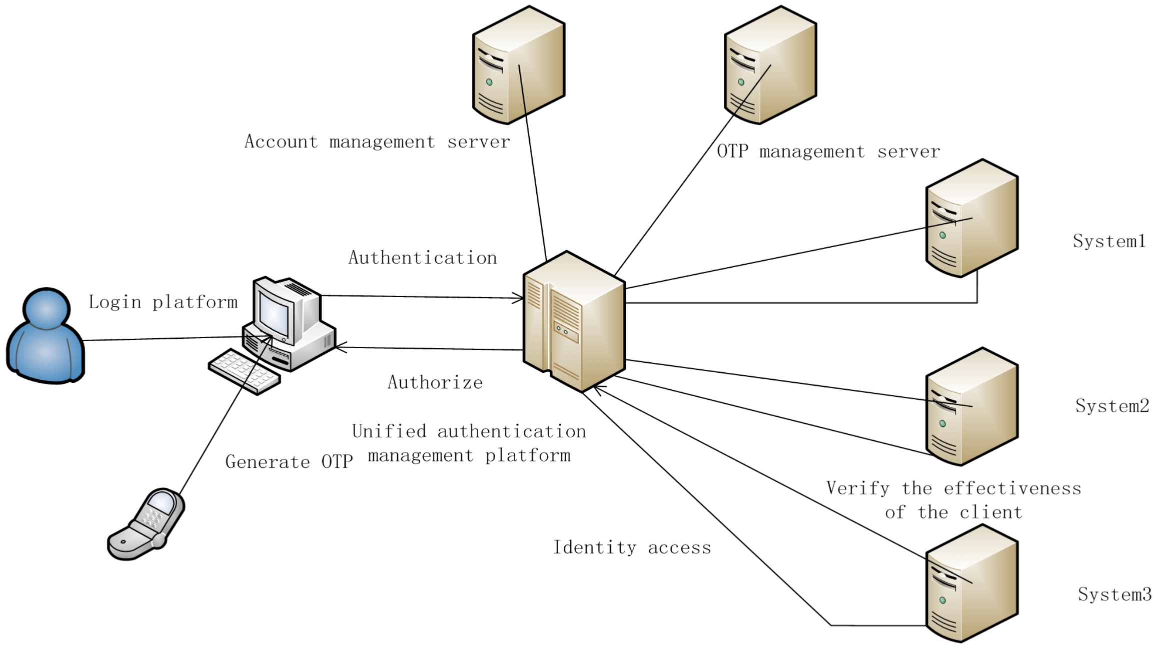

Fig. 2.1 the architecture of platform

3 The Design of Unified Authentication and Management platform

The platform's authentication uses user account with dynamic password. This design of dynamic password generation uses seed data in the client and dynamic factors (challenge code) as the basic data and SHA1-3DES algorithm to generate dynamic password. The functions of dynamic password platform include dynamic password business opening, certification, and maintenance [5].

3.1 The Design of Authentication Scheme Based on Dynamic Password

3.1.1 Dynamic Password Opening

First, the user must download the OTP software from the platform and install it in the phone. Opening OTP business is a process that client generate seed data and send it with other data which are needed, such as phone number. Meanwhile the client stores it in its database. Figure3.1 show the flow of the dynamic password opening.

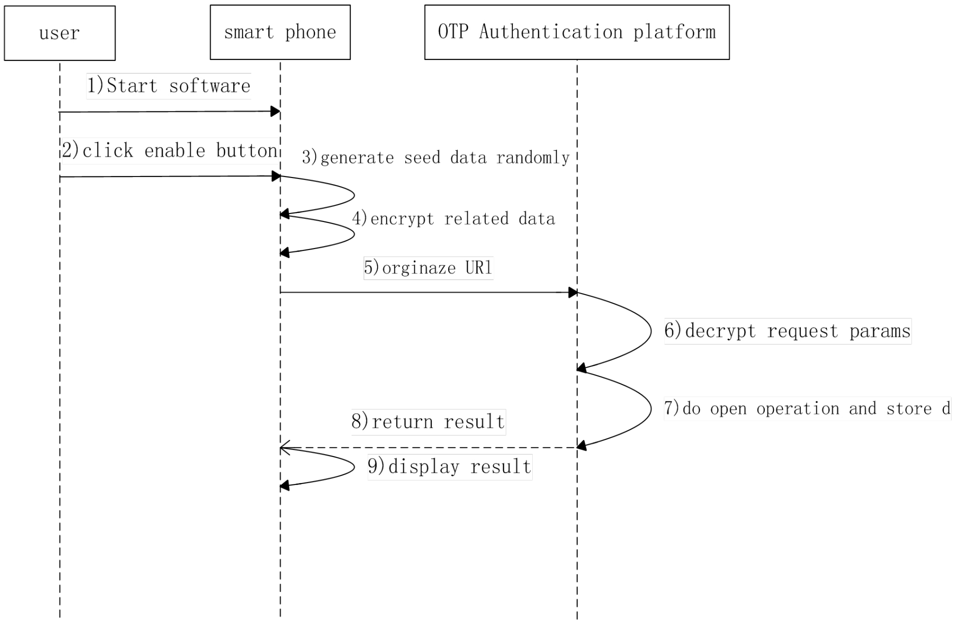

Fig. 3.1 opening

1) Start the dynamic password software;

2) Click on the enabled menu;

3) Generate random seed data, terminal software can use any algorithm which can generate a string of hexadecimal digits to generate a 24-character string of hexadecimal digits, saved in client as seed data for later using;

4) Using the public key of the dynamic platform to encrypt phone number and the seed data;

5) Organize the opened request URL and send a request to the dynamic password platform;

6) Decrypt the request parameter to get the random seed data and phone number;

7) Implement the enabled logic, store data to the database;

8) Organize the result which is in XML format;

9) The dynamic password terminal software performs different operations according to the result.

3.2 *The Design of Single Sign-on Scheme*

This paper designs a single sign-on scheme in broker mode based on Cookie. The scheme's core idea: using unified authentication and management platform's token-C as the identity of login and store the identity in the client's Cookie; if subsystem do not have a Token-S, it will visit unified platform to complete authentication and generate a Token-S . Exit and assign permissions are not specifically introduced. Figure3.2 show the flow of the dynamic password opening.

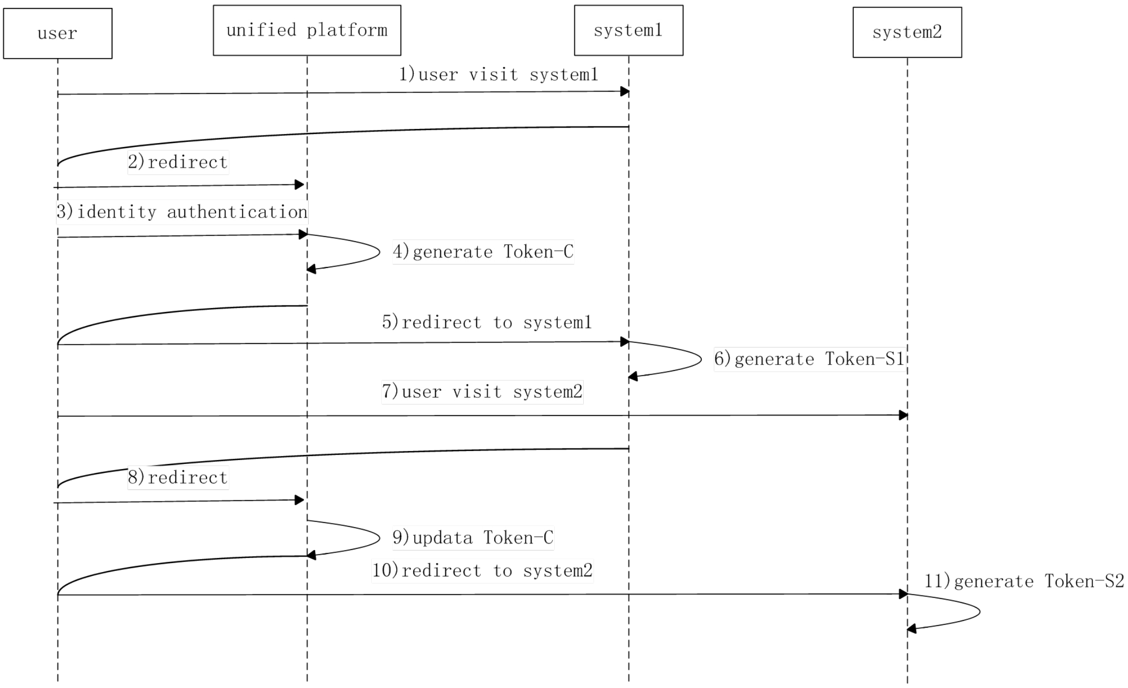

Fig. 3.3 sign-on scheme

1) The user access platform system at first time

2) System 1 does not have token-S1. So system1 sends a request to the unified authentication and management platform, and redirects the user to the platform.

3) The user successful login in the platform in accordance with the process of authentication.

4) Cookie if the user is legitimate, unified authentication and management platform generates Token-C and writes it to the client Cookie

5) Unified authentication and management platform returns information about the user to system 1

6) System 1 generates the Token-S1 and stores it in Session. the user ’ certification in system 1 has completed, Then the user can do any relevant functional operation. Step1 to6 is the process of the first certification

7) The user accesses system 2

8) System 2 determines whether the user holds a valid Token-S2. If not, the system 2 sends a request to the unified authentication and management platform for authentication.

9) Token-C unified authentication and management platform determine whether the user holds a valid token-C. If any, unified authentication and management platform updates Token-C

10) Unified authentication and management platform sends the authentication information to the system 2 and redirects the user to the system 2

11) System 2 generates Token-S2 for the administrator, users finished certification in the system 2.So users can do relevant functional operation. Step 7-11 is subsequent authentication process.

3.3 The Dynamic Password Algorithm

OTP authentication is a kind of abstract authentication. This paper uses 3DES algorithm to encrypt original data. 3DES is designed to provide a relatively simple method, by increasing the length of the key of DES to avoid similar attacks. Hash function is a irreversible process that different input will get different output, but the same output do not mean the same input. This paper uses sha1 algorithm to generate a different 20-character abstract. Finally, digitize the hash results in order to achieve OTP.

Algorithm description: The client uses seed (k) to encrypt SID (phone number) and CH (the challenge code). Then the client use sha1-hash algorithm to encrypt the result. Finally, the client digitizes hash results to 8-10 bit hexadecimal digits.

The user gets the change code from website and enters the change code into Mobile. Mobile phone gets an ASCII code and converts ASCII code to hex.

1. Seed data is the key to encrypt

2. 3DES's input must be an integral multiple of eight bytes. So complete the original data

$$PM=PKCS5\_PAD(SID+CH) . \qquad (1)$$

PKCS5_PAD：add based on PKCS5

3. Calculate encrypted information

$$EM=3DES\_CBC(PM) . \qquad (2)$$

4. Do sha1-hash,get SM String

5. Generate a 4 bytes string

$$Sbits=DT(SM) . \qquad (3)$$

6. Generate number 0-2^(31)-1

$$Snum=StrToNum(Sbits) . \qquad (4)$$

7. Generate final OTP

4 Analysis

The security of this platform is based on dynamic password. First, the communication between OTP authentication platform and smart phone is safe, because the data transmission is encrypted. 3DES algorithm ensures the ciphertext will not easily reversed by others to get plaintext. Second, 3DES-hash Algorithm is used to generate OTP. 3DES algorithm is an upgraded version of the DES. So it is hard to achieve the key and source. This system brings other benefit-convenient. Using software token is not like importing hardware token which will cost a lot in buying equipment. The user only needs to download software from the platform and open OTP business, then to bind their account with the software. Now they can use dynamic password to login the system. On the other hand, Smart phone as carrier undoubtedly make using OTP convenient. You can use it anytime and anywhere without extra equipment. For old system upgrading, Single Sign-on this paper proposes is also easily imported.

5 Conclusion

Summarizing the advantages and disadvantages of related technologies, This paper puts forward a kind of unified authentication management platform which employs intelligent mobile phone as the carrier, challenge code as the uncertain factor of dynamic password generation mode, and Single sign-on in the broker mode based on Cookie technology as an authentication management platform. This platform has the following advantages: provide a much better enterprise information security and a more convenient user management system; single sign-on, do not remember much account password, also saves the cost of development for more efficient use of system resources.

Acknowledgments. the work presented in this paper was supported by National Great Science Specific Project (Grants No.2011ZX0300200301) .

References

1.Jinying, Z. (2006) The Design and Implement of Identity Authentication Based on Dynamic Password. Southwest Jiaotong University,Cheng du,1-56

2. Zhigao, Z., ShengQiu, Y (2009) The Design of Double Factors Authentication Based on ECC.Computer Engineering.35(9):124–127

3. Xi, Y., Yiru, Y., Qin, C (2010) The Implement of Dynamic Password Authentication System Based on the Mobile Token.Computer Systems & Applications.19(10):32–37

4. Hang, Q., Yong, Q (2003) Research and Design of Single Sign-on System Based on Kerber0S.Computer Applications.23(7):142-144

5. Sumalatha Adabala,A.Matsunaga (2004) Role-based Access Via Delegation Mechanisms UsingShort-lived UserIdentities.Paralleland Distributed Processing SymPosium. Single Sign-on in In-VIGO.1(2):22-23