RSA Algorithm for User Authentication System

Byung-Ho Song and Sang-Hyun Bae

** Dept of Computer Science & Statistics Graduate School, Chosun University, Korea*
***Dept of Computer Science & Statistics, Chosun University, Gwangju, 375, Korea*
Tel : +82-062-6623 Fax : +82-062-234-4326
E-mail: cssstar@hanmail.net,shbae@chosun.ac.kr

Abstract: For the effective use of information in the information society, information should be protected and outflow of information by illegal users should be prevented.

This study sets up user authentication policy, user authentication regulations and procedures for information protection and builds information protection key distribution center and encryption user Authentication system, which can protect information from illegal users.

1. Introduction

Researches for information protection have made rapid progress in information protection system and information communication system. It is considered as the result of recognizing an importance of information security in the process of secrecy protection and save. This study is to cope with the various threats of information protection system by using information protection and encryption algorithm in information protection system and information communication system as a part of these researches.

Encryption technique to implement information protection system is used to protect major information from illegal outflow or not allowed users using information communication network, foster the realization of information society and minimize a threat factor of information[1][2]. Information protection system cannot eradicate damages of information, but it can be the most fundamental technique to prevent information crime in distributed computing environment, minimize damage and restrict committing a crime.

Existing user authentication system depends on verification and access control through several steps, which is vulnerable to several attacks and has a weakness of saving ID and password. In addition, since user authentication system is built on network environment, it has a potential to make a normal work performance from intentional prevention and threat by illegal users impossible. Information protection key distribution system and encryption user authentication system suggested for settling these problems can protect information protection system against illegal attacks, outflow of information by illegal users and illegal service demands.

2. Authentication Mechanism

Authentication can be divided into user authentication, message authentication and certification of integrity of public key. The former confirms identification using ID and password and the latter guarantees integrity through signature of authorized certification agency, which gives a foundation for using public key safely. For the purpose of protection and integrity of information resources, information protection system monitor must recognize that user is the party concerned to decide access approval when a user has an access to information protection system resources and such a process of revealing user's identity is authentication[3][4].

User authentication is the process of confirming a valid user with user's ID, password, network address, etc. In addition, it is to guarantee that user involved in generation, processing, transmission and storing of information in information protection system is the right user. Message authentication is to guarantee that information is not changed and forged by a unlicensed third party, which includes integrity of message and user authentication. integrity of message includes methods detecting whether a transmitted message is forged or not and it is tapped by a wiretapper and the method of preventing data forgery or tapping. Certification of integrity of public key offer a means to solve certification problem of public key in Public Key Infrastructure. Its components include certification agency, registration agency, user and repository.

User authentication system model is built on web based user authentication system according to information protection system environment, user authentication system using digital certificate and user authentication system using client/server, but it should be based on building interlocking system[5]. Process related to user authentication is user information of directory server and digital certificate and in case of user of client/server environment, user authentication and safe data transmission are ensured by means of encryption ID and password. This user authentication system can ensure user authentication by having an access to information protection system only when user's certificate should be verified by authentication server.

3. Information protection Policy

3.1 User Security Management

The objects of user security management include direct or indirect users of user security system and management resources are composed of computing resource, communication resource and information resource. For the effective utilization of these resources, the information

protection system environment must establish a user security policy to keep the following regulations.
- Only the manager entrusted with the authority can access user security system and manage and control this system.
- Only the user entrusted with the authority can access security system and perform his services.
- Only the user entrusted with the authority can access user security system from distance and revise information.
- Operated applications are examined in approved operation group and processing and saving information are prohibited without the approval of security manager.

3.2 User Security Rregulation

User security regulation describes the regulations to be applied to develop user security procedures within user security system environment. It has the consistency with user security policy and does not conflict with other management policies and procedures. In addition, it is a subset of user access control required for implementing user security policy. For this environment, the regulations are divided into user access regulation, user ID, password management regulation and confidentiality control regulation.

3.3 User Security Procedure

User security procedure is established for implementing user security regulation and it is just a procedure of higher level. A detailed procedure is varied depending on platform operated in user security system, operation network, network components and application.

User Access Procedure : User must have ID (password) of security system first to obtain an access authority. This ID should be made to give users concerned an access authority of proper level. Also the procedure to eliminate user's access authority should be followed. These procedures refer to giving and eliminating user's access authority and complete ID generation. (Fig. 1) shows the procedure of giving users an access authority in user security system.

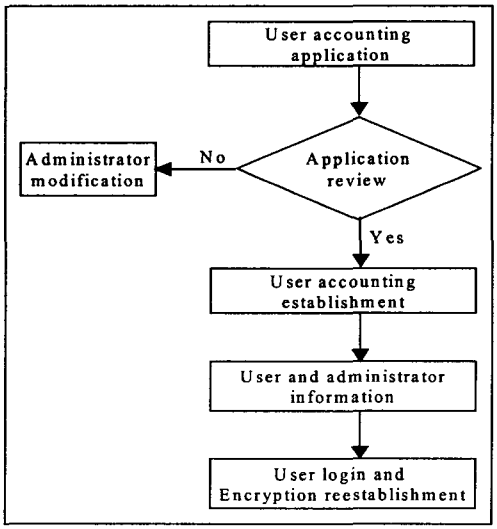


Figure 1- User access authority

Password Management Procedure : When a user inputs a new password, password generation utility requests password compliance check routine automatically to confirm whether length and composition of password meet the whole regulations or not. If a password is accepted from compliance, the password is registered on database with date.

Confidentiality Management Procedure : When a user accepts confidentiality required for access to an application, confidentiality is the time stamped. When system hours exceed the hours of adding confidentiality time stamp and life, confidentiality is withdrawn. Additionally, each application listens to the active users' activities. If a fixed time passes without any activities, an application requires a new certificate required for user login again after a fixed time without any activity and disconnects with user.

4. Information Protection Key Distribution System(IPKDC)

Users making user authentication system must do authentication work that user concerned is a legal user in registering service code and requesting service. Information protection key distribution system is a reliable key distribution server which shares a common symmetrical key between user systems composed of many users and information protection server. User system and information protection service are distributed to user concerned through information protection key distribution center and user performs encryption technique through distributed key.

4.1 Composition of IPKDC

Information protection key distribution center distributes keys for authentication between user system and information protection server based on symmetrical key playing a role of encryption key. IPKDC is made of five modules as shown in (Fig. 2) and functions of these modules are as follows.

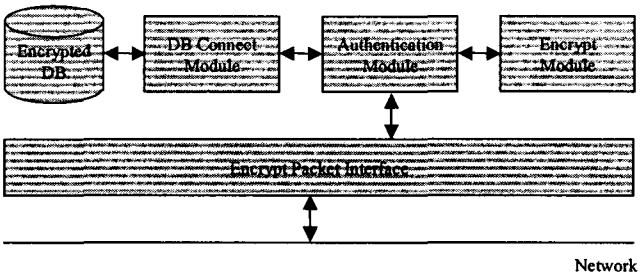


Figure 2- Information protection key distribution center

User makes encoded packet for the request of symmetrical key by work object user. Then information protection key distribution center uses encoded packet interface modules for receiving encoded packet. Transmitted encryption packet sends authentication module and transmits user's symmetrical key of user requested following the authentication process. Encryption packet used in transmitting and receiving uses packet of system defined by authentication protocol.

Authentication module analyzes encryption packet transmitted from its interface and confirms authentication

of user requesting work. Encryption technique used in doing this is encryption module. When user authentication is confirmed, user's demand is performed by means database link module. Encryption packet transmitted to user is also through encryption work by authentication protocol.

Encryption module is based on encryption technique used for making and reading encryption packet. Encryption techniques within encryption module include RSA, DES, ElGamal, oval password and MDS. This study uses RSA algorithm.

Encryption database stores symmetrical key of the whole users making information protection system, and stored symmetrical key is offered to users through authentication and stores a symmetrical key of a newly registered user. User accesses database using query language. Also user performs encryption and decryption using authentication modules. encryption, decryption and database use database link module.

This study tries linkage using consolidation of security of user authentication, maintenance of encryption of secret data itself, security function of database and database character.

4.2 Key Distribution Method of IPKDC

User requires symmetrical key of information protection server for performing work with information protection server. Therefore confirm authentication of user first before requesting symmetrical key of information protection server to information protection key distribution center and performing the user's demand for symmetrical key. If user's authentication is not confirmed, request of work required is not performed and if user's authentication is confirmed, symmetrical key of information protection server is retrieved in its own encryption database, it is encoded and transmitted. User requires work using symmetrical key of information protection server from information protection key distribution center.

4.3 IPKDC Authentication Protocol

Users having information protection system use user authentication protocol(UAP) in registering and requesting service to confirm its authentication with information protection server.

4.3.1 UAP in Registering Service

User performs process of authentication using information protection key distribution center in order to register his own service code to information protection server. Then registration of service code to information protection server means that user concerned can play a role of component of information protection system. Accordingly, information protection key distribution center confirms registration of user requesting service code registration and if he is not registered user, store it to encryption database newly and if he is renewed user, store revised symmetrical key information to encryption database.

4.3.2 UAP in Requesting Service

When information protection server or user requests a work, user whose work is requested performs the work after confirming authentication of user concerned. If user requests a work to information protection server, user requests symmetrical key of information protection server to information protection key distribution center. Information protection key distribution center transmits symmetrical key of information protection server after confirming authentication of user and user transmits work request packet using symmetrical key of information protection server.

5. User Authentication System

Proposed system is designed for keeping independence and security and easy application to user authentication and database. Also it is designed not to use information by unlicensed users. User authentication table is made by encryption of user ID and password with basic key.

5.1 Generation of Encryption User Authentication Table

Encryption user authentication system which can show validity of users' access to information protection server and prevent illegal uses of data and illegal modification of data table is designed. Composition of table for information protection server system authentication is as follows.

User authentication is achieved by inputting user ID and password, but this study encodes and stores ID and password in making user authentication table and confirms it with RSA code algorithm in user authentication. Generation and registration procedure of encryption user authentication table are as follows;

(1) Generate decimal of appropriate figures using decimal generation program.
(2) Select decimal of different figures over two, p, q and then does p-1, q-1 with large prime factor and ged (p-1, q-1) with small prime factor.
(3) Calculate modular n = p, q and select Ek (public key) smaller than lcm (p-1, q-1).
(4) Calculate Euler function ϕ (n) = (p-1)(q-1) and reverse modular of Ek ϕ (n) using Euclid algorithm, and set secret key Dk to be a pair with Ek, the key selected in (3).
(5) Set two keys to secret key Dk and public key Ek.
(6) Use user name as basic key in user registration table and store password value by encoding with server encryption key.
(7) Store ID and password to table by encryption, delete p, q, Ek used after making user authentication table and complete the work after keeping Dk by an individual.

Registration of user authentication table with initial value by performing the above algorithm shows this.

(Table 1) Registration of user authentication table

ID	Password	Ek	Dk	n	p	q
Cssai	1234	67	1886827	15811997	2029	7793
Cssai2	4567	17	7133489	13483693	1789	7537
Cssai3	7890	79	1401271	8521307	3743	2549

Cssai4	0123	61	17853541	21791339	6829	3191

ID and password are encoded and stored in table, p, q and Dk are deleted after making user authentication table and Ek is kept by an individual.

(Table 2) Registration of user authentication table

ID	Password	Ek	n
Cssai	1234	67	15811997
Cssai2	4567	17	13483693
Cssai3	7890	79	8521307
Cssai4	0123	61	21791339

5.2 Implementation of Encrypted User Authentication System

Proposed system is designed for keeping independence and security and easy application to user authentication and database. Procedure of encryption user authentication is as follows;

(1) User encodes ID and password and sends them to server.
(2) Server compares ID and password sent and if password is the same, encode message and send it to user.
(3) User decodes sent and sends it to server.
(4) If server receives response of the same content as message sent, allow user authentication.

If user encodes ID and password, compares it to user authentication database and confirms user authentication, he uses information. But if user authentication is not confirmed, he cannot use information. Scene of performing encryption user authentication is as follows;

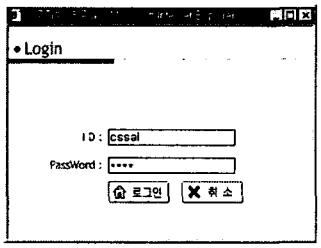


Figure 3- Normal user

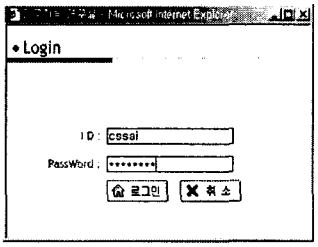


Figure 6 - Abnormal user

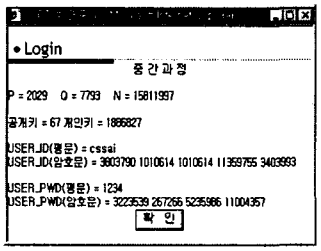


Figure4-Authentication process

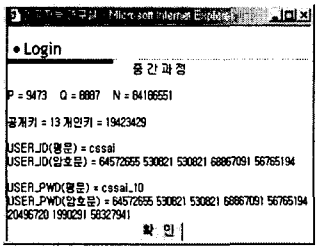
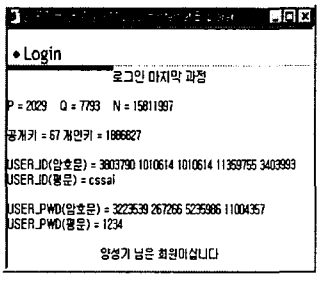


Figure7- Authentication process



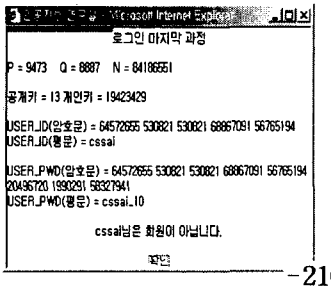


Figure5- User authentication *Figure8 - User authentication*

6. Conclusions

Information protection key distribution system presented in this study did mutual verification work between user system and server system and builds information protection key distribution system to distribute symmetrical keys of encryption user authentication system. Information protection key distribution center distributes symmetrical key required for job demand to server system by user system and sends encryption packet based on the symmetrical key. Therefore, encryption packet give and taken between encryption user authentication systems can prevent the reading by illegal users or outflow of information through altered message.

Also, encryption user authentication system using information protection key distribution system is the method complementing existing user authentication system. Encryption method pursues simple ID and password method and encodes ID and password applying RSA encryption algorithm, which keeps the secrecy of information. Encrypted ID and password are sent to information protection server, protects user ID and designs and implements encryption user authentication system for a gradual application of resources after user verification.

References

[1] Schneier, Bruce. (1995). "Applied Cryptography : Protocols, Algorithms, and Source Code in C" .
[2] Alfred J. Menezes, PaulC. (1996). van Oorschot, ScottA. Vanstone "Handbook of Applied Cryptography" .
[3] Charles P.Pfleeger. (1989). Security in Computing, Prentice-Hall. International Editions.
[4] W. Diffie, P.C.van Oorschot, and M.J,Wiener. (1992). "Authentication and Authenticated Key Exchanges", Designs, Codes, and Cryptography, vol.2 pp107~125.
[5] Seoung-Pil Hong, Je-Wook Ko. (1998). "Technical and Implementation of Information Security", powerbook.