International Journal of Complex Systems – Computing, Sensing and Control
Vol. 1, No. 1-2, pp. 119-124, 2013

RESEARCH ON THE SECURITY PROBLEMS EXISTED IN INFORMATIZATION MANAGEMENT OF LIBRARIES

QINGE XU
Inner Mongolia People's Hospital
Inner Mongolia, P. R. China
E-mail: nmgqingexu@163.com

ABSTRACT—Along with widely application of the network and information techniques, the level of informatization in libraries has been developed, however, the security problems also become severe. Based on the analysis of current security condition of library network and the key factors by which security disasters can be induced, a lightweight authentication protocol is proposed, ensuring only the legal users can access into the digital library. The analysis indicates that the protocol is both efficient and secure.

Key Words: Digital Library; Information Security; RSA Cryptosystem; Lightweight Authentication; Denial of Service

1. INTRODUCTION

In recent years, internet techniques has become mature, and the application of network also rapidly developed which has been widely used in almost every corner of our daily life, including government, bank, factory, university and so on. The modern digital library also cannot live without the network[1-5]. Pitifully, the global network environment is complicated and risky. The attackers online are ready for stealing, tampering and forging information at any time.

There are several security problems during the management process of digital library[6-9].

- **System vulnerability.** The security flaws maybe existed in the operation system and software, such as IE loophole. If they are not fixed timely, they will be utilized by the attackers to intrude the system. Sometimes it will result in the damage of information resource in library.
- **Virus.** Computer virus is a procedure which can be self-duplication and spread. If the library system is infected by the virus, the transactions will be disturbed, even the data in library is going to be destroyed, or the hardware system will be stayed on paralysis.
- **Leak of the password.** The administrator may leak the password of its account occasionally, and someone can use it to obtain the information which he cannot get it through a legal way.
- **Malicious attacks.** This kind of attack can be generally divided into two categories: active attack and passive attack. The former one means the attackers use all kinds of methods to crack the target information, making it invalid or un-integral. The latter one means the attackers steal the information in premise of not to affect the usual working process. The malicious attacks are great threats to the network security.

Based on the security problems above-mentioned, a lightweight authentication protocol is proposed for securing the process of authenticating, enabling the registered users to log in the library server efficiently.

2. PRELIMINARIES

The proposed protocol is based on RSA cryptosystem[10], which is consisted of the following three stages.

Key Setup

To set up a user's key material, the user performs the following steps:

1) Choose two random prime numbers p and q such that $|p| \approx |q|$; (this can be done by applying a Monte-Carlo prime number finding algorithm)
2) Compute $N = pq$;
3) Compute $\phi(N) = (p-1)(q-1)$;
4) Choose a random integer $e < \phi(N)$ such that $\gcd(e, \phi(N)) = 1$, and compute the integer d such that $ed \equiv 1 \pmod{\phi(N)}$; (since $\gcd(e, \phi(N)) = 1$, this congruence dose have a solution for d which can be found by applying the Extended Euclid Algorithm)
5) Publicize (N, e) as its public key, safely destroy p, q and $\phi(N)$, and keep d as its private key.

Encryption

To send a confidential message $m < N$ to the receiver, the sender creates the ciphertext c as follows

$$c \leftarrow m^e \pmod{N} \tag{1}$$

(view by the sender, the plaintext message space is the set of all positive numbers less than N, although in fact the space is Z_N^*)

Decryption

To decrypt the ciphertext c, the receiver computes

$$m \leftarrow c^d \pmod{N} \tag{2}$$

In the next section, we will propose a authentication protocol based on the RSA cryptosystem.

3. A LIGHTWEIGHT AUTHENTICATION PROTOCOL

In the most of digital library, the kind of password-based mechanism is utilized for the users to access into the data resource and the administrator to manage the library. But as we know, this mechanism is easy to crack and poses significant risk. In this section, we present a lightweight authentication protocol to solve this problem. The user/administrator and the digital library server just need to interact on a little registered information with a few lightweight operations to complete the validation of identity, which almost have no negative influence on the efficiency. The protocol is on the basis of TTP (Third Trusted Party). That is, the TTP is in charge of

generating the ultimate public/private key pairs (N, e, d) for the mechanism through the RSA cryptosystem[10]. Then, in order to protect the security of the interaction process between the digital library server and the user, we design a mean to divide the original key into two pieces, and distribute them to each party respectively.

3.1 Key Generation

TTP randomly selects d_u as the user's private key, and computes $d_s = d \,.\, d_u^{-1} \bmod \phi(N)$ for the digital library server, and then sends (N, e, d_u) and (N, e, d_s) to the user and the server respectively through secure channel.

In the following description, let pw denotes user's password, $\oplus$ denotes XOR operation, $h(\ )$ is a collision resistant hash function, $E_k(m)$ denotes a encrypting execution on message m by a symmetric key k.

3.2 User Registration

The user submits its registration information $\{ID, h(b \oplus pw)\}$ to the server through secure channel, with b is a random number generated by user itself, which is stored on its own device. When the server receives the information, it computes:

1) $T = h(ID \oplus x) \oplus h(b \oplus pw)$, with x is a secret key which is long enough to ensure the security of the registration, and the server keeps it for all the registered users;
2) $sk_s = (e, N, d_s)$, $SK_s = E_x(e, N, d_s)$;
3) Compute $C_T = (T)^{e.d_s} \bmod N$, and then send it to the user.

Then store the information $\{ID, N, SK_s\}$ for each registered user. The user can recover T through computing $T = (C_T)^{d_u} \bmod N$.

3.3 Authentication

Authentication: Before accessing into the library, the user needs to interact with the server to complete authentication.

1) User: sends $y = h(b \oplus pw) \oplus T$ to the front end;
2) Server: checks if $y = h(ID \oplus x)$ holds or not. If so, the authentication is passed, otherwise, reject it.

3.4 Change the password

The user can change its password in an efficient way.

1) User: completes the authentication process in Section 3.3;
2) User: chooses its new password pw_{new}, and computes $h(b \oplus pw_{new})$, then sends it to the server.

3) Server: updates the value of T, $T_{new} = T \oplus h\left(b \oplus pw_{old}\right) \oplus h\left(b \oplus pw_{new}\right)$, and return $C_{T_{new}} = \left(T_{new}\right)^{e.d_s} \mod N$ to the user.

3.5 Correctness

The correctness of the recovery process can be proved as follow:

$$\begin{aligned} T &= \left(C_T\right)^{d_u} \mod N \\ &= \left(\left(T\right)^{e.d_s}\right)^{d_u} \mod N \\ &= \left(T\right)^{e.d} \mod N \\ &= \left(T\right)^{\phi(N)+1} \mod N = T \end{aligned} \tag{3}$$

4. SECURITY ANALYSIS

The security of the protocol is based on RSA cryptosystem, and split of the RSA key will not compromise the security of RSA. (The detailed proof is provided in our paper [11]). Here we consider the security of the system in the following attack.

1) The server suffers attack

The attacker can obtain x and the partial keys d_s storing for all users, but the matched d_u is kept by the user, so the decryption key d is not revealed. We just need to ask TTP to reproduce new pieces of d for the user and the front end, then re-initialize the system.

2) Leak of password

We don't need to worry about the leak of password. The password is always combined with b in the calculating process, which is only stored on the user's device. So the attacker cannot launch any attack by utilizing the password. Furthermore, the user can change its password efficiently following the steps in Section 3.4.

3) Denial of service (DoS)

This is a very common attacking fashion. By introducing lightweight but effective authentication, all the services of digital library will be provided only the authentication is passed, so the protocol can resist DoS in a great extent.

5. EFFICIENCY ANALYSIS

Let X, H, SE/D, and ED respectively denote XOR operation, Hash operation, Symmetric encryption/decryption, and modular exponentiation. Table 1 lists amounts of calculation needed in each process of our protocol. User registration (UR), Authentication (AU), Change the Password (CP). User (U), Server (S).

Through the analysis in Table 1, only a few lightweight calculations, including XOR, Hash, and Symmetric encryption/decryption, need to operate in each process, except the user and server need to do one modular exponentiation in UR and CP. So our protocol is feasible in computational efficiency.

Table 1. Amounts of Calculation Needed in Each Process of Our Protocol

Calculation	UR		AU		CP	
	U	***S***	***U***	***S***	***U***	***S***
X	1	2	2	1	3	2
H	1	1	1	1	2	1
SE/D	--	1	--	--	--	--
ED	1	1	--	--	1	1

6. CONCLUSIONS

Based on the analysis of the security concerns of digital library, a lightweight authentication protocol was proposed, allowing the registered user/administrator logging in the library effectively, and then the data resource of library can be accessed and managed securely. The security of the proposed protocol is based on RSA cryptosystem. During the authentication process, the users just need to manipulate 2 XOR and 1 Hash operation, so it is practical for the digital library in reality.

REFERENCES

1. C. Cheng, Discussion on the Problems Existing in the Informatization Development of University Library, Sci-Tech Information Development & Economy, 2009, 19(12): 56-58.
2. X. J. Tan, Reflections on the wave of Digital Library, The Journal of the Library Science in China, 2002, 28(137): 12-14.
3. J. R. Yang, Considerations about Automation of Library in China, Journal of Information, 2002, (6): 75-76.
4. X. R. Mao, Process and Prospect for Automatic Construction of Library in China, Journal of Hefei University of Technology, 2002, 16(5): 117-120.
5. X. P. Fan, A Discussion about the Development of Digital Libraries in China, Library and Information Service, 2001, (3): 82-84.
6. G. Xing, Y. Q. Zhang, and D. G. Feng, Study of Management Platform for Network Security, Computer Engineering, 2004, 30(10): 129-131.
7. H. Q. Zhang, Network and Information Security, Beijing: Tsinghua University Press, 2002.
8. Y. X. Yang, X. X. Niu, Network Security: Theory and Technology, Beijing: Posts & Telecom Press, 2003.
9. H. X. Wang, Z. J. Zhao, and J. P. Liu, The Analyze of Firewall Technology, Computer Engineering and Design, 23(2): 14-17.
10. R. L. Rivest, A. Shamir, L. Adleman. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM, 1978, Vol.21(2): 120-126.
11. F. Xu, X. Lv, R. Y. Jiang. Online Public Key Cryptographic Scheme for Data Security in Bridge Health Monitoring. Intelligent Automation and Soft Computing, 2010, Vol. 16 (5): 787-795.

ABOUT THE AUTHORS

Q. Xu is a librarian in Inner Mongolia People's Hospital. Her main research interests are library management, network information security and information science.