International Journal of Security and Its Applications
Vol.9, No.11 (2015), pp.403-418
http://dx.doi.org/10.14257/ijsia.2015.9.11.37

Mechanism on Computer Access Permission Management Based on the Proposed Dynamic Password Algorithm

Jiujun Cheng[1, 2], Yang Yang[2, *], Jianyu Shao[2], Jingxue Liao[2]

1 Department of Computer Science and Technology, Tongji University, Shanghai 201804, China
2 Key Laboratory of Embedded System and Service Computing of Ministry of Education, Tongji
chengjj@tongji.edu.cn;
yy_tongji@163.com;
jianyutj@gmail.com;
liaojingxue1201@163.com

Abstract

With the rapid development of information technology, personal computer privacy and permission management are becoming more and more important. Based on RSA encryption algorithm, we design a dynamic password encryption and codec algorithm, and propose a mechanism on computer access permission management which is capable of dealing with situations both online and offline. In the offline mode, administrators can authenticate users by matching their contact information to that registered in administrators' mobile terminal. Generated by the co-work of a personal computer and a mobile terminal, the dynamic password makes cracking the password a trickier task. Permission control information is also added into the dynamic password, and file filter system will be loaded once the screen is successfully unlocked, so as to protect private directories or files from being accessed without authorization. In online mode, the system provides real-time video for identity verification, which makes the system more secure and convenient. Experiment results show that this dynamic password based mechanism on computer access permission management is efficient in dealing with existing problems in personal privacy and access permission management.

Keywords*: Privacy Protection; Access Permission Management; RSA; Dynamic Password*

1. Introduction

With the wide use of computer technology, a large number of data stored in computers are accessed every day. Therefore, the access permission management on personal computers becomes very important. The common practice of computer protection is to set up a login password, which can only ensure the owner who has the authority to access this computer.

You might have come to this kind of situation: a friend of yours is in urgent need to borrow your computer, while you happen to be away. Of course he or she could call you for your password but you are unwilling to tell, since the password is kind of privacy, it is very important to you and you don't want certain information be seen by others. But you wouldn't mind if the friend is just in need of some not-so-private-or-important data. You still want to be a nice colleague.

* Yang Yang[2] is the corresponding author.

ISSN: 1738-9976 IJSIA

The most common solution is the user control system provided by operating systems such as Windows or Linux. They provide various users or user groups for computer access control. But they need to create an account for other users in advance, since the old systems do not suit for temporary authorization. What we need is to conveniently give the users a temporary authority to use the computer and remotely remove it afterward. Another general method to solve this problem is to use dynamic password encryption algorithm to encrypt our private password. Dynamic password encryption algorithm was proposed by L. Harn [1] *et al*., who combined the public key with user's password to reduce the password leakage risk which is caused by storing an encrypted password file. Chen *et al*. [2] processed a "fair" password authentication system, which can find the real reason of the failure in the identity authentication in advance. For network with poor security, Liao and Lee [3] proposed a password authentication scheme that can support Diffie-Hellman key agreement protocol [4]. In their schemes, users can use the session key to encrypt or decrypt their communications. Generally speaking, traditional dynamic password encryption uses time seed method to generate dynamic password. Han and Zhang [5] adopted time seed to encrypt a same plaintext to get different cipher to resist the plaintext attack, but this approach has two shortcomings: first, if the dynamic password generation algorithm has been made public, anyone can work out the dynamic password based on time, which will damage the system's security; Second, this approach cannot guarantee the time synchronization between mobile terminals and personal computers, and it will make the password useless if time is not synchronized. Chang [6] proposed a remote password authentication scheme based on the quadratic residue theorem. Intruders cannot obtain any public confidential information or intercept any password message in this scheme. Das [7] used user authentication based on dynamic password encryption in wireless sensor network, and the emulation experiment indicated that the algorithm has high efficiency and security, and the effect of concealing is very good. On the basis of Das's work, Turkanovic and Holbl [8] proposed an enhanced version of user authentication based on dynamic password encryption. The new authentication strategy overcame some deficiencies in practical use and removed some redundant elements in Das's method. Wang [9] thought that Das's method did not achieve mutual authentication and can't resist simulation remote server attack, so he proposed an enhanced password authentication scheme while maintained the advantages of Das's scheme.

But the algorithms mentioned above [2-9] need the machine to work online, and if not, it's hard for the system to deliver the encrypted password. What we want to achieve is to have a way to pass the secret messages between two terminals, no matter in what network conditions these terminals are. In order not to repeat the defect in traditional privacy protection and access permission methods, we propose a mechanism of computer access permission management based on dynamic password, which combines mobile terminals with personal computers, so as to realize dynamic password encryption and delivery regardless of network conditions. It allows the other individuals except for the administrator to use the computer, while limiting their access permission. Therefore, it improves the protection of user privacy.

In this paper, we focus on the proposed mechanism for computer access permission management based on dynamic password, the implement of an effective permission access management and remote authorization system. The rest of this paper is organized as the following. Section 2 presents our improved RSA-based dynamic password encryption algorithm. Section 3 presents the computer access permission manage mechanism. Section 4 shows and discusses about the experiment results. Finally, we conclude our works in Section 5.

2. The RSA-Based Dynamic Password Encryption Algorithm

RSA [10] is an asymmetric cryptosystem based on number theory. If the length of RSA's key is longer, the encrypted cipher text is more secure and the password is more difficult to be breached. However, with the increase of the key's length, the encryption process needs more time and resources such as CPU and memory. The public key and private key encryption of RSA can fight against decryption attack because it is based on the factorization difficulty of big prime number. Therefore, RSA is mainly used in digital signature, encryption area, *etc*.

Our dynamic password encryption is designed to realize the function of encrypting and decrypting administrator's password, operation permission, time limitation and other information. It mainly includes two parts: the section of the information encrypt terminal and the section of information decrypt terminal. The former combines the public key provided by the latter with administrator password, time and access permission information to generate dynamic password using specific algorithm. The latter implements functions such as code generation, dynamic password decryption, extract and parse the message information and so on. For security consideration, it will generate a random pair of public key and private key each time the request is made. And convert the public key into printable strings for the encrypt terminal. This process can greatly enhance the anti-attack capability of the system. In terms of the problem of massive calculation of the password system, we recommend to put key generation and decryption on the computer side, because this algorithm is mainly designed for personal computers (PC) and mobile terminals and the performance of mobile equipment is limited. So the mobile terminal only needs to encrypt password. This can reduce the hardware demand of mobile devices.

Dynamic password encryption algorithm is shown as the follow four.

Algorithm 1: Integer to String encode

Input: Integer i
Output: converted string str

```
str <= empty string
While i ≧ 64
temp <= i mod 64
If 0 ≦ temp < 10 Then
str.append('0' + temp)
Elseif 10 ≦ temp < 36 Then
str.append('A' + temp – 10)
Elseif 36 ≦ temp < 62 Then
str.append('a' + temp – 36)
Elseif temp = 62 Then
str.append('#')
Else
str.append('*')
Endif
i <= ⌊i/64⌋
Endwhile
```

Algorithm 2: Random Verification Code generation

Input:

Output: generated RSA private key and public key converted as printable string (defined as verification code)

```
1.  seed <= rand() * (clock() + 1) * time(NULL)
2.  rand <= SFMT[11]::FeedSeed(seed)
                                .Rand(1, INT_MAX)
3.  rand <= BBS[12]::Rand(rand)
4.  While not MillerRabinTest(rand)
5.      seed <= rand() * (clock() + 1) * time(NULL)
6.      rand <= SFMT[11]::FeedSeed(seed)
                                .Rand(1, INT_MAX)
7.      rand <= BBS[12]::Rand(rand)
8.  Endwhile
9.  Return rand
10. repeat 1-9, generate secret key(sk_p, sk_q)
11. phi_n <= (sk_p – 1) * (sk_q – 1)
12. Do
13.     repeat 1-9, generate pk_b
14. While pk_b ≦ sqrt(phi_n) or pk_b ≧ phi_n
15. Use algorithm 1 to convert pk_b => v_b and pk_n => v_n
16. VerificationCode <= concat(v_b, v_n)
```

Algorithm 3: Dynamic password encrypt algorithm

Input: to be encrypted information, verification code
Output: dynamic authentication code string (auth_code, defined as authentication code)

```
1. Reverse use algorithm 1 to VerificationCode => public key pk_b + pk_n
2. plain_text <= Concat(password, control_information)
3. cipher_text <= RSA::encrypt(plain_text, pk_b, pk_n)
4. Use algorithm 1 on cipher_text => auth_code
```

Algorithm 4: Dynamic password decrypt algorithm

Input: dynamic authentication code string(auth_code)
Output: management password and other control information

```
1. Reverse use algorithm 1 to auth_code => cipher_text
2. RSA decode(sk_a, cipher_text) => plaintext
3. parse(plaintext) => (password, control_information)
4. parse(control_information) => machine representation
```

In Algorithm 2, we use SFMT random number generation algorithm and Millier-Rabin primality testing algorithm, they can ensure that the public key can be generated more quickly, more randomly, and no fixed rules to follow. Therefore, it ensures that the dynamic encryption mechanism can be realized smoothly and safely. Besides, in algorithm 3 and algorithm 4, the generated public key has been encoded as printable string using algorithm 1. In algorithm 2, the output printable string is defined as verification code. While in algorithm 3, the output string is defined as authentication code. Using these codes, we can deliver public key and the encrypted messages through various ways including text messages of a cellphone. What's more, the algorithms we proposed is also suitable for encrypt and decrypt other secret information besides password.

3. Mechanism on Computer Access Permission Management Based on the Proposed Dynamic Password Algorithm

Our mechanism is intent to serve the remote authentication between personal computers and mobile terminals. In order to make it work correctly regardless of the network condition between personal computers and mobile terminals, we designed both offline mode and online mode to make it function correctly in both offline and online network conditions.

3.1. User Authentication Based on Dynamic Password

Process of user authentication based on dynamic password is shown in Figure 1. User requests to generate a key pair on computer client dynamically. Then computer converts the public key into verification code and user sends the verification code to the administrator. The administrator starts their own mobile terminal client, and encrypts administrator's password, operation permission and time control information, yielding the encrypted cryptograph. This process is equivalent to an affine encryption. Then the administrator uses mobile terminals to encrypt the encrypted cryptograph by the RSA-based dynamic password encryption algorithm we've mentioned in section 2, combining with the verification code, and send the encrypted message back to the user. This process ensures that only the administrator knows the correct password, and unauthorized users trying to break this system is extremely difficult because of the security of RSA cryptosystem. If users pass the authentication, their operations will be limited by the granted permission. Therefore, this authentication module fully guarantee the safety of the system.

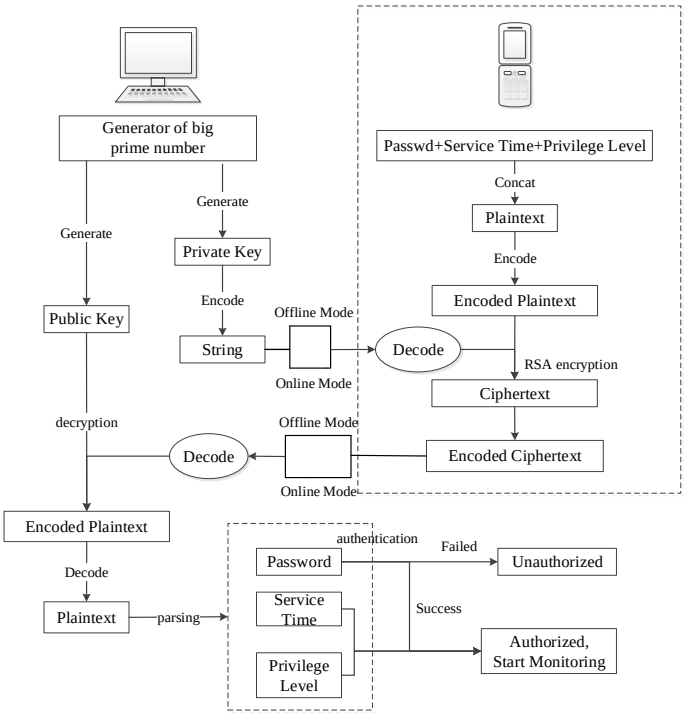


Figure 1. Process of user authentication

In the offline mode, the dynamic verification code can be sent to the administrator via SMS or telephone voice. The administrator can confirm the identity of the visitor by SMS

or telephone numbers. In the online mode, users can send the dynamic verification code to the administrator through the internet, and the administrator can also confirm the identity of the users through the real-time video. Therefore, the process of authentication further enhances the security and usability of the system.

3.2. Permission Control Information Encryption

On the basis of proposed dynamic password encryption algorithm, we define the control information as permission control information and time limitation. When a user request to use the computer, the computer generates a verification code using algorithm 2. And the user uses a cellphone to send it to the administrator. The administrator get the verification code and use the dynamic password encryption algorithm to encrypt the password along with the chosen control information which is consist of permission control flags, including the information of file access permission and computer access time limitation, and send the dynamic authentication code back. Once the temporary users get the authentication code, they can enter it on computer. We provide a function to decrypt the encrypted information and get the control information on the PC side. This process can ensure the concealment of permission control information. The client of computer side will parse the control information and limit the users within the granted permission. Permission control process is shown as Algorithm 5.

Algorithm 5: Algorithm of permission control process

Input: plaintext of administrator passwords(pwd), permission and time control information

Output: results of permission and time control information

1. PC generate verification code using algorithm 2
2. Send verification code to mobile terminal
3. Administrator choose granted permission level
4. Mobile terminal convert permission level into permission flags
5. Mobile terminal use algorithm 3 to encrypt pwd, permission and other information through verification code to generate dynamic authentication code
6. Send the dynamic authentication code back to PC
7. PC use algorithm 4 to decrypt dynamic authentication code, generate plaintext of pwd, permission and time control information
8. **If** pwd correct **Then**
9. Set the permission and deadline, unlock the screen, open the timer
10. Timeout, lock screen, withdraw authentication
11. **Else**
12. Echo error information
13. **Endif**

3.3. Permission Control Mechanism

Permission control [13, 14] made it possible to restrict user's operations to computer files and improved the system protection grade of sensitive documents. In the implementation of our mechanism which we will cover in section 4, we use Mini-Filter Installable File System [15] that are recommended by Microsoft. When turned on the filter, users can only obtain the corresponding folders' or files' operating authorization. Permission control algorithm of files is shown as Algorithm 6.

Algorithm 6: Control of file access permission

Input: Private files or folders
Output: Authorization success or authorization failed

```
1.  Administrator login the system
2.  Administrator set the private files or folders
3.  Private files and folders path => Database
4.  User unlock screen
5.  If  has administrator permission Then
6.      Return permission granted
7.  Else
8.      If  operate private file or folder Then
9.          Return permission denied
10.     Else
11.         Return permission granted
12.     Endif
13. Endif
```

Time control model can be implemented by using operating system's built-in timer and time control flags are extracted from the permission control flags, and use it to index the corresponding time in the schedule. Specific algorithm is shown as Algorithm 7.

Algorithm 7: Time control

Input: Time control information
Output: Service time

```
1.  Administrator set the service time
2.  User unlock screen
3.  The Client on PC parse service time flag => srv_time
4.  Pop up notification box of srv_time
5.  Set timer update interval to 1 second
6.  While srv_time > 0
7.      If Timer update Then
8.          srv_time <= srv_time – 1
9.          Refresh notification box
10.     Endif
11. EndWhile
12. Lock screen, withdraw authentication
```

3.4. Different Access Permission Management Mode

3.4.1. The Offline Mode: In the offline transmission mode, the verification code and generated authentication code is designed to be transmitted by SMS or voice over the phone. And the administrator can identify the user by the cellphone number and the contacts information registered in the mobile terminal. The offline identity authentication algorithm is shown as Algorithm 8.

Algorithm 8: Offline identification

Input: SMS or voice contained verification code
Output: encrypted unlock information, file access permission and time control information

```
1.  User request for offline identification
2.  PC client generate verification code
3.  User send verification code through SMS or voice audio.
4.  Contact_info <= contacts(cellphone_number)
```

```
5.  Administrator identify Contact_info
6.  If agree to authorize Then
7.     If SMS Then
8.        verification_code <= parse(SMS)
9.     Else
10.       verification_code <= administrator identify
11.    Endif
12.    Adminstrator set the plaintext of pwd, operation
          permission and time control flags
13.    Encrypt(plaintext, verification_code) =>
                                                  auth_code
14.    Send auth_code back to user via SMS
15.    Return permission granted
16. Else
17.    Return permission denied
18. Endif
```

3.4.2. The Online Mode: In the online mode, the mechanism is designed to capture more information about user to further enhance system security. The implemented system should capture the video of the temporary user, compress the video stream and send it to the mobile terminal through the Internet. The mobile terminal should support the same video codec to decompress the stream and show the vision. In the online mode, verification code and generated authentication code are also transmitted through the Internet in order to improve the usability. The online identity authentication algorithm is shown as Algorithm 9.

Algorithm 9: Online identification

Input: PC：Video stream; mobile terminal：manage password(pwd), file access permission and time control information

Output: unlock information, file access permission and time control information

```
1.  User request for online identification
2.  PC client generate verification code
3.  PC client send the request to administrator's mobile terminal via TCP protocol
4.  If administrator agree to identification Then
5.     Open camera on PC, open video stream
6.     Send verification code to administrator's mobile
          terminal via TCP protocol
7.     Send video stream to administrator's mobile
          terminal via RTP protocol
8.     Administrator watch the video stream and identify
          the identity of the user
9.     If agree to authorize Then
10.       Administrator set the plaintext of pwd,
             operation permission and time control flags
11.       Mobile terminal encrypt pwd, file access
             permission and time control information => auth_code
12.       Send auth_code to PC via TCP protocol
13.       PC decrypt auth_code => plaintext
14.       Parse(plaintext) => pwd, file access
             permission and time control information
15.       If pwd correct Then
16.          Set operation permission and time
                control flags , unlock screen, open timer
17.       Else
18.          Echo error information
```



```
19.        Endif
20.     Else
21.        Return permission denied
22.     Endif
23. Else
24.     Return permission denied
25. Endif
```

4. Performance Testing and Results Analysis

4.1. Experiment Environment

Our implemented system consists of three parts: PC client, server and the mobile terminal client. The experiment environment is shown as Figure.2, and the specific process is described as follows.

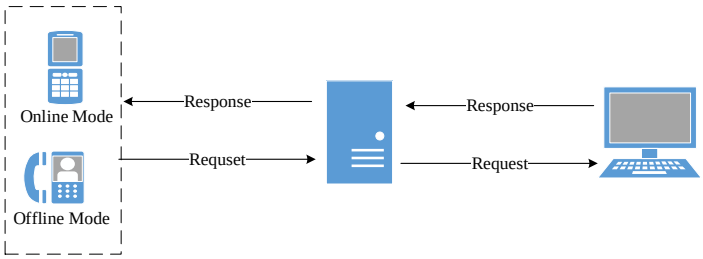


Figure 2. Experiment Environment

The mobile terminal can work on two modes: online mode and offline mode. In the offline mode, the broadcast receiver of android application is used to receive SMS sent by the PC user. The administrator's password encryption can be achieved by using proposed dynamic password encryption algorithm. Dynamic password can be firstly generated with the permission information and time control information set by computer owner. And then the administrator can send dynamic password back to the PC user.

In the online mode, when you are logging in, mobile terminal program would send your network account and password to the server for authentication and association. If not succeed, you need re-enter information until a successful login. Then you can get video identification by using socket-based TCP and RTP protocol to transmit control information and video stream between PC and mobile terminal. If you do not want the requester to use your computer, you can reject the request. At the same time, the computer will transfer verification code to the mobile terminal by server. A dynamic password can be created using verification code, combining with password, operation permission and time limitation information. And then the dynamic password will be sent from the server to PC for unlocking the screen.

The main role of the server is to connect PC with mobile terminal. All of the services, such as the process of user login and transmission of verification code, dynamic password and video stream, rely on the program running on the server.

4.2. Analysis of Experiment Results

4.2.1. Dynamic password Encryption: We experiment our system with the following three steps.

1) We choose two password, one is correct while the other is not. Combines with different authority and time limitations, we use the mobile terminal to generate different dynamic

authentication codes. Send them back and enter them in the textbox of login screen which is shown as Figure. 3.
2) Change the length and composition of the admin password, then do the same work as the first step and observe results.
3) After the correct admin password was input to the mobile terminal, we input false authentication codes to the PC and observe results. Dynamic password generation module is shown as Figure. 4.
4) We give the false verification code to the mobile terminal, and input the generated authentication code to the PC and observe results.

The testing results show that, only when we send the correct verification code to the mobile terminal and use it to encrypt the correct password and enter the exact authentication code generated by the mobile terminal can we unlock the screen. Otherwise, it's not likely to enter the system via other ways or brute-force the authentication code. Besides, the generated authentication codes seem to have no literal relationship between the original passwords. Attackers can't calculate the password through the dynamic authentication code. And with different verification codes, we generate different authentication codes for the same password. So our mechanism can help unlock the computer remotely without exposing our private password.

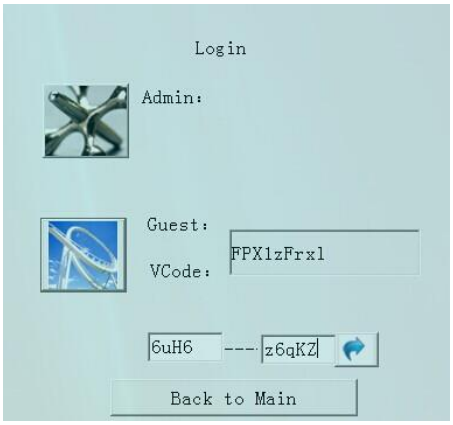


Figure 3. User Login Interface

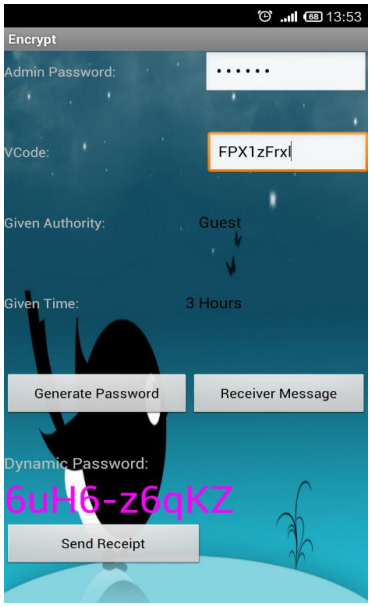


Figure 3: Dynamic Password Generation Module

4.2.2. File protection : When our system locked the screen, select the offline mode. Then we enter the offline mode screen lock interface. We choose to grant the administrator and the guest permission to test our system separately, with the service time setting to 60 minutes.

1) Grant guest permission. Visitors do the following operations to ordinary files, folders and private files, folders: read, write, delete, rename, copy, and so on.

2) Grant administrator permission. Visitors do the following operations to ordinary files and private files, folders: read, write, delete, rename, copy, and so on.

The experiment results show that, when we grant guest permission, visitors can only access ordinary files successfully. In the meantime, they can't do any operations to private files or folders. When we grant administrator permission to the mobile terminal, visitors can do any operations to both ordinary files, folders and private files, folders. One experiment result is shown as Figure. 5.

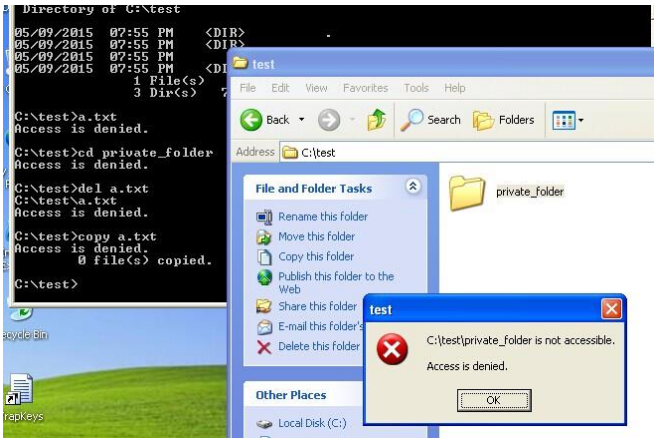


Figure 4: File Protection Test

Besides, our implemented system can also control the available time. When we unlocked the screen, a tooltip showed up in the upper right corner of the desktop, displaying remaining time countdown which is shown as Figure 6, When the countdown finished, system would relocked the screen automatically.

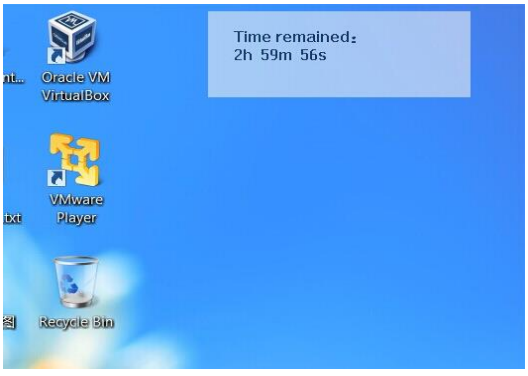


Figure 5: Time Control Module

4.2.3. Video Transmission in the Online Mode: When our system locked the screen, select the online mode, then we can enter the online identification and unlock interface. In the meantime, we need open mobile terminal program and select online mode as well.

Register an account which is used to login to the server, then video authentication can be carried out after a request from PC. Figure 7 shows the video stream captured and displayed on PC client. Figure 8 shows the video stream transmitted to mobile terminal through the Internet and displayed on the mobile screen. Based on different video content, the owner can determine as follows.

1) Grant to login and input the correct password. Set different permission and time control information and observe the changes in the computer.
2) Reject the request.

The experiment results show that, in the online mode, we can get the requester's video captured by the camera of the computer and send the video stream to the mobile terminal. The mobile terminal displays the video in real-time. The verification codes and authentication codes are transmitted through the Internet, which is more convenient than the offline mode.

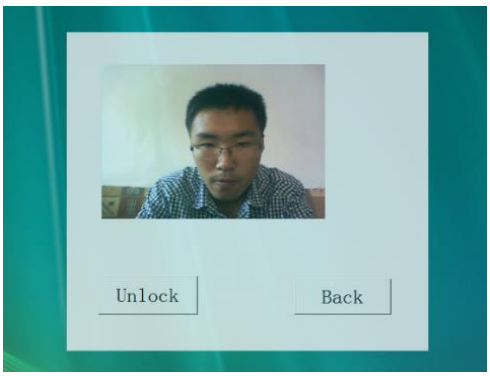


Figure 6. Video Captured and Displayed on PC

Figure 7: Video Stream Displayed on Mobile Terminal

In conclusion, we adopt the improved RSA encryption and authentication to guarantee the system security in the offline mode. On the basis of the offline mode, we add video authentication module in the online mode. It can further improve the security and the reliability of system. Our implemented system usually runs in the background. And we found that the CPU utilization is always below 5% after a long time running. Obviously, the system only need low computer configuration, and consumes less system resources. The experiment results show that the system can provide proper access permission to visitors. And it can also protect user's data and privacy at the same time, which provides solid safety and practicality.

5. Conclusion

Problems of the security and privacy protection have become more seriously in our daily life. Traditional methods that only use login password will be a risk in terms of computer security and privacy, especially when the user's computer is borrowed. In order to solve this problem, we propose, in this paper, a mechanism on computer access permission management based on dynamic password. It aims to solve security and privacy problems when others use the owner's computer. First of all, it uses a new dynamic password mode, combining string coding with RSA encryption algorithm for dynamic password, adopts SFMT algorithm to avoid security problems of dynamic password generated by time seed algorithm and improves the system security; secondly, it extends the function of the dynamic password by adding control information; finally, our implemented system also provides file access protection with a file protection driver module. This module limits user's access permission and improves the system protection grade of sensitive documents. The computer access permission management mechanism based on dynamic password can effectively solve the problem in personal privacy and access permission. At the same time, it can also be extended to other password management area. Unlike traditional computer access control systems provided by operating systems such as Windows or Linux, our mechanism has the following advantages.

1) Owner of the computer does not have to grant certain authority in advance to the user. The user can be given temporary access which can be changed conveniently through mobile terminal.

2) Compared with the algorithm [2-9], our mechanism provides a way to transmit the secret encrypted message between computers and mobile terminals in both online and offline mode.

3) Our mechanism provides various ways to help the owner identify the identity of the user in different network conditions. This improves the usability and security of the system.

4) Our mechanism considers the limitation of the using time and file access permission. And it's also very convenient in extending modules to limit other forms of authority.

Acknowledgements

This work was supported in part by NSFC Grant No.61472284, No.61472004 and No.61202384, by Natural Science Foundation Programs of Shanghai Grant No.13ZR1443100, and by ISTCP Grants No.2013FM10100.

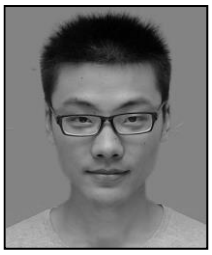
References

[1] H. Lein, "A public-key based dynamic password scheme", Proceedings of the 5th International conference of the Symposium On Applied Computing, **(1991)** April 3-5; Kansas, USA, pp.430-435.
[2] C. Y. Chen, C. Y. Gun, and H. F. Lin, "A fair and dynamic password authentication system", Proceedings of the 2nd International conference of Artificial Intelligence, Management Science and Electronic Commerce, Zhengzhou, China, **(2011)** August 8-10;, pp.4505 - 4509.
[3] Liao, I-En, Cheng-Chi Lee, and Min-Shiang Hwang, "A password authentication scheme over insecure networks", J. Journal of Computer and System Sciences **(2006)**, Vol.72, No.4, pp.727–740.
[4] D. Whitfield, and H. Martin E, "New Directions in Cryptography", J. IEEE Transactions on Information Theory **(1976)**, Vol.22, No.6, pp.644 - 654.
[5] D. Han, Q. Zhang, J. Li, "The Dynamic key and implementation of Rijndael algorithm", Proceedings of the 5th International conference of Multimedia Technology, **(2011)** July 26-28; Hangzhou, China, pp.5610 - 5613.
[6] C. Chin-Chen, S-M Tsu, and C-Y Chen, "Remote scheme for password authentication based on theory of quadratic residues", J. Computer Communications, vol.18, no.96, **(1995)**, pp.936-942.
[7] A. K., Das, P.Sharma, S. Chatterjee , and J. K. Sing, "A dynamic password-based user authentication scheme for hierarchical wireless sensor networks", J. Journal of Network and Computer Applications, vol.35, no.5, **(2012)**, pp.1646-1656.
[8] M. Turkanovic,, and M. Holbl, "An improved dynamic password-based user authentication scheme for hierarchical wireless sensor networks", J. Elektronika ir Elektrotechnika, vol.19, no.6, **(2013)**, pp.109-116.
[9] Y. Wang, J. Liu, F. Xiao, and J.Dan, "A more efficient and secure dynamic ID-based remote user authentication scheme", J. Computer Communications vol.32, no.4, **(2009)**, pp.583-585.
[10] R . Rivest, A, Shamir,., and L. M Adleman,., "A Method For Obtaining Digital Signatures And Public-Key Cryptosystems", J. Communications of the ACM vol.21, no.2, **(1978)**, pp.120-126.
[11] S., Mutsuo, and M. Matsumoto, "SIMD-oriented fast Mersenne Twister: a 128-bit pseudorandom number generator", Monte Carlo and Quasi-Monte Carlo Methods 2006, Springer-Verlag, Berlin Heidelberg, vol. 2, **(2008)**pp.607-622.
[12] G., Kaustubh, and M.Mundle, "Various Implementations of Blum Blum Shub Pseudo-Random Sequence Generator", Project Report **(2001)**.
[13] R. S, Sandhu, E. J, Coyne, H. L., Feinstein, and C. E Youman,., "Role-based access control models", J. Computer , vol.29, no.2, **(1996)**, pp.38-47.
[14] J. Ai Hua, and D. F. Chen, "A Study of User Permission Control Based on RBAC Model on.NET Platform", J. Journal of Hubei University of Technology ,vol.23, no.3, **(2008)**, pp.29-30.
[15] S. Gao, A. Hu, Y .Song, "Remote forensics system based on Minifilter", Proceedings of the 2nd International conference of Computer Science and Network Technology (ICCSNT), **(2012)** December 29-31; Changchun, China, pp.1381– 1385.

Authors

JiuJun Cheng, he received his Ph.D. degree from Beijing University of Posts and Telecommunications in 2006. He is presently an associate professor of Tongji University, Shanghai, China. In 2009, he was a Visiting Professor at the Aalto University, Espoo, Finland. He has over 40 publications including conference and journal papers. His research interests span the area of mobile computing and social network with a focus on mobile/Internet interworking, Network security, and Internet of Vehicles.

Yang Yang, he is a postgraduate at the College of Electronics and Information Engineering, Tongji University Shanghai, P.R.C. His main research interests are in the field of mobile Internet and Internet security. Email: yy_tongji@163.com



JianYu Shao, he is a postgraduate studying in Key Laboratory of Embedded System and Service Computing of Ministry of Education, Tongji. His research area mainly includes mobile internet and internet of vehicle. Email:jianyutj@gmail.com

JingXue Liao, he is a postgraduate studying in Key Laboratory of Embedded System and Service Computing of Ministry of Education, Tongji. Hisresearch area mainly includes mobile internet, internet of vehicle, mechanics, *etc.* Email:liaojingxue1201@163.com