A Practical Password Management Scheme based on Computer Hardware Information and IC card

Jie Xu¹, Zhongtian Jia¹,²*, Bo Zhang¹,² and Minyao Ma³

¹School of Information Science and Engineering, University of Jinan, Jinan 250022, China
²Provincial Key Laboratory for Network Based Intelligent Computing, University of Jinan, 250022 Jinan, China
³School of Mathematics and Computer Science, Guizhou Education University, 550018 Gui-yang, China

ABSTRACT

Since the twenty-first Century, the Internet has brought great convenience to our life, following with a large number of network accounts registered on kinds of websites or Internet systems. The management of these accounts and their passwords has become a public problem needed to be solved. Recently, there have been a lot of works trying to answer this question in the literature. However, there isn’t a practical method suitable for a variety of occasions. In this paper, we propose a novel password management scheme to address this issue by binding the computer hardware’s identifier and an IC (Integrated Circuit) card. The accounts and passwords of the third-party systems are stored in a secure repository of a computer. Any manipulations of the accounts and passwords must be authenticated, in which only the user who can provide the computer, the IC card and the management password is accepted by the system. Therefore, with only one password, which is called management password, the administration of all the other accounts and passwords can be achieved. Additionally, we can login into a third-party system automatically if its’ login API is public. Practicability and security analysis show that the proposed scheme is practical and secure, and can be applied in many situations.

INTRODUCTION

Network technologies have been brought great convenience to our daily life. For example, you are almost able to buy daily necessities on the Internet without going out home. You can video chat through a Gmail account with friends from all over the world. However, in order to get the service provided by an application, one must register with it in advance, in which one needs to define an account name and provide a secure password for later login [1]. Therefore, the number of the account and password pairs that one should maintain are increasing continuously. Recent studies show that the average number of the account and password pairs managed by a person is more than ten. It is a commonplace to forget the password or even the account name ever registered on a website. Thus, how to manage the account and password pairs is becoming a challenge [2].

To avoid forgetting passwords, some people try using simple passwords, such as 123456, hello world, 19980818, etc. These methods are vulnerable for malicious
dictionary attacks. Some people adopt generic password, which is maybe very strong, for every account registered on the Internet. Regrettably, it is easy to become the target of the library hit attack [3]. This means all the accounts using the generic password will be in the risk of masquerade attacks [4]. Additionally, there are other people like to keep all their passwords in a notebook or computer file. This method looks simple and convenient because it can help people remind the registered accounts and their corresponding passwords. Nevertheless, once a password-recorded notebook or computer file is lost or stolen, then all accounts and their passwords will be in the risk.

![System Architecture](image)

Figure 1. System Architecture.

To solve this problem, we propose a practical password management scheme based computer hardware and IC card in this paper. The architecture of the proposed method is shown in Fig.1. First, an ID (Identification) information is drawn from a computer’s hardware, such as CPU, motherboard, memory etc. Then, an IC key is extracted from the ID information and written into the IC card. Along with the IC key, a few random numbers are also written into the IC card, which will be used for encryption key’s generation subsequently. The third party’s accounts, their corresponding passwords and login entrances are stored in a secure repository of the computer. Any access to the secure repository must be authenticated. To authenticate an access, the IC card should be inserted into the computer. Then, IC key is recalculated on the basis of the computer’s hardware. If the recalculated IC key is equal to that read from the IC card, the access is allowed. Else, the access is denied. In addition to the account and password management, the system provides automatically login the platform of the third party according to the corresponding address stored in the secure repository. The contribution of the paper has three aspects: 1) propose a password management scheme based on computer’s hardware and IC Card, through which all kinds of passwords can be administrated with one management password and an IC card; 2) present a method to login to the third party’s system; and 3) analyze the practicability and the security of the proposed scheme.

The remainder of the paper is organized as follows. We review the related works in section II. Then, the novel password manager is proposed in section III. Section IV discusses the practicability and the security of the proposed scheme. Finally, conclusions are drawn in section V.
RELATED WORKS

Recently, there are a large number of works about online password management in literature. As early as 1998, the password management idea had been proposed by Michael for communication network, in which one of the communication parties maintained a list of passwords and adopted a scheme to distribute them among the other parties to obtain secure communications[5]. But this is not the real meaning of the user account and password management program for the Internet applications studied in this paper.

It was not until 2005 that how to administrate the accounts and passwords became a problem and began attracting the interest of researchers [6]. Kerr et al. proposed such a method related to user accounts and their corresponding passwords management. Their patent utilized a universally accessible location to store the accounts and their passwords. To obtain adequate security, both the client side and server side were encrypted. However, investigations done by Chiasson, van Oorschot and Biddle showed that many password management proposals were lack of formative and summative usability tests and not practical. Users do not feel they are needed or provide greater security [7].

In 2007, Vu K. P. L. presented a method and a series of recommendations to improve the online password security and memorability. However, tries to strengthen password security and memorability just by generating such a kind of passwords [8]. In the same year, Jeff Yan also discussed the contradictory of password security and memorability. He believed that it should depend on the application system itself to help users to select a strong and easy memorable password [9].

In 2010, Al-Sinani and Mitchell investigated the problem and presented a design for account and password management using Windows CardSpace [10]. The followed analysis, presented by Li et al. in 2014 [11], showed that the main popular Web based password manager were all vulnerable in diverse aspects, such as logic and authorization mistakes, misunderstanding of the Web security model etc. Zhao, and Yue also analyzed the website base password managers. They not only uncovered their vulnerabilities and showed how to exploit by the attacker to steal users’ passwords, but also proposed a password administration method based on cloud computing for Web based applications [12]. Then, Stajano et al. proposed a semantic labels method in 2015, in which the password manager could extract the meaning of the form on the web page and parse their password policy [13]. By these designs, they tried to improve the functions of the password manager embedded in the web browser.

In order to improve the facility and security of the web based password manager, Yuchen et al. gave out an approach using a hardware trusted platform module in 2016 [14]. Additionally, some researchers attempted to define a new password keeping architecture by utilizing multiple device control. In 2012, McCarney et al. proposed a more solid scheme for password management by leveraging a desktop computer and a smartphone. They claimed that even in the occasion of one device was stolen, the stored passwords were still secure [15]. Then, Eggimann and Gloor presented a new password manager using the secret sharing theory. The password manager split a password into multiple pieces stored in multiple devices respectively. A password can be uncovered by putting some of the split pieces together [16]. It is really a very secure password management method. But we should maintain many devices to get enough security.
this paper, we propose a more convenient method which is discussed in the following sections.

THE PROPOSED SCHEME

In this section, we discuss our scheme in the following five subsections: \( A, B, C, D, \) and \( E \).

Assumptions and Security Aims

ASSUMPTIONS

- The IC card issued by the system must be kept secretly;
- The password, called management password in the proposed scheme, is secure.

SECURITY AIMS

- Anyone can’t access the accounts and passwords if the computer, the issued IC card or the management password is absent;
- The user can access the accounts and passwords if he can provide the computer, the issued IC card and the management password.

Identifier Extraction

In order to construct a secure area in a computer’s hard disk for sensitive information, necessary encryption is indispensable. Therefore, how to generate the encryption key is the critical factor. In our design, the third party’s sensitive information, such as accounts and passwords are encrypted and stored in the hard disk of a given computer. Accordingly, any access to these data can only be performed on this given computer. Hence, the proposed scheme extracts an ID information from the computer’s hardware, including CPU, motherboard, hard disk, memory, etc. Firstly, the information read from the CPU should include the serial number, the number of cores, and the default frequency. Secondly, the information fetched from the motherboard should contain the serial number, date of manufacture. Thirdly, the information drawn from the hard disk should have the serial number, the storage capacity, cluster size. Finally, the information extracted from the memory should cover the serial number and capacity. The ID information extraction phase includes the following two steps.

**Step1:** Fetch hardware information from the CPU, mother board, hard disk and memory, and assign them to four variables \( M_1, M_2, M_3, M_4 \), respectively.

\[
M_1 \leftarrow CPUInfo, \\
M_2 \leftarrow MotherBoardInfo, \\
M_3 \leftarrow HardDiskInfo, \\
M_4 \leftarrow MemoryInfo.
\]

**Step2:** Calculate the ID information \( IDInfo \) as an identifier of the selected computer.

\[
IDInfo = M_1 \parallel M_2 \parallel M_3 \parallel M_4 \tag{1}
\]

Here, \( \parallel \) represents string concatenation.
IC Key Generation

In this subsection, we discuss the IC key generation module as the following six steps. At first, the generation process needs to call the Identifier extraction module, through which an ID information based on a given computer is extracted. Then, the ID information and the management password are hashed using a hash function. The hashed value is written into a blank IC card. Additionally, some random numbers are also written into the blank IC card as well. The IC key and the random numbers will be used in the authentication module and the password management module, subsequently. The hashed ID information stored in the IC card, is called an ICKey in the remainder parts of this paper. Finally, the IC key generation module must be destroyed from the current computer. The ICKey variable should be deleted. The memory storing of this module must be overwritten. These manipulations intend to prevent any possible potential key leakage and key tempering.

Step1: Execute subsection B to get the ID information: IDInfo.
Step2: Get the user-input password, which is called management password, and assign it to the variable UPASSWORD.
Step3: Compute the IC key using a hash function.
\[ ICKey = H(IDInfo \parallel UPASSWORD) \] (2)
Here, \( H(\cdot) \) is hash cryptography algorithm.
Step4: Generate several of random number using a pseudo-random function.
\[ r_1 = \text{rand}(), \ r_2 = \text{rand}(), \ldots, \ r_T = \text{rand}(). \] (3)
Here, \( r_1, r_2, \cdots, r_T \) is random numbers. \( T \) is system parameter, and \( \text{rand}() \) is a pseudo-random function.
Step5: Write the ICKey and the \( r_1, r_2, \cdots, r_T \) into the IC card.
Step6: Destroy the IC key generation module and empty corresponding variables and memory from the current computer.

Authentication Module

The authentication module includes the following three steps.
Step1: Execute subsection B get ID information: IDInfo'.
Step2: Recalculate the IC key according to the IDInfo' and the input password: UPASSWORD'.
\[ ICKey' = \text{hash}(IDInfo'|\parallel UPASSWORD') \] (4)
Step2: Insert the IC Card into the computer.
Step3: Compare ICKey' with ICKey stored in the IC card, if the two values are the same, allow the user to execute Password Management Module. Else, Denied.

Password Management Module

This module refers to how to manage user’s accounts and passwords of the third-party’s service providers. It includes three functions: 1) how to store the third-party’s accounts and passwords, 2) how to access these passwords, and 3) how to login to the system of third party. In the proposed scheme, all the third party’s accounts and passwords, along with the URL (Uniform Resource Locator) of their corresponding login entrance, are stored in the hard disk of a computer. The one who wants to
manipulate the account information, should own the computer, the IC card issued by
this system, and the management password and pass the system’s authentication.

PASSWORDS SECURE STORING

The steps of password storing for third party’s system is discussed as the following.

Step1: Authenticates the user according to the steps given in subsection D. If he/she
passes the authentication, the user is permitted to do the following steps. Else, Denied.

Step2: Encrypts the accounts and passwords using a symmetric cryptographic
algorithm.

\[
\begin{align*}
    c_1 &= E_k[U_1||P_1] \\
    c_2 &= E_k[U_2||P_2] \\
    \vdots \\
    c_n &= E_k[U_n||P_n] \\
    k &= H(IDInfo||r_i)
\end{align*}
\]

Here, \(U_i\) \((0 \leq i \leq n)\) is the account name of the third-party system. \(P_i\) \((0 \leq i \leq n)\) is the
ciphertext of \(U_i\) and \(P_i\). || is string concatenation operator. \(IDInfo\) is the identifier
information of the special computer generated in the subsection B. \(r_i\) \((0 \leq i \leq T)\) is
random number reading from the IC card. \(H(\cdot)\) is a hash function. \(E_k\) is a secure
symmetric cryptography algorithm.

<table>
<thead>
<tr>
<th>TABLE I. STORING FORMAT.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Landing Entrance</td>
</tr>
<tr>
<td>(L_1)</td>
</tr>
<tr>
<td>(L_2)</td>
</tr>
<tr>
<td>(\vdots)</td>
</tr>
<tr>
<td>(L_n)</td>
</tr>
</tbody>
</table>

Step3: Store the landing entrances and the ciphertexts of the accounts and
passwords in the hard disk of the computer as shown in TABLE I.

Here, \(L_i\) \((0 \leq i \leq n)\) is the landing entrance of third-party’s system. \(c_i\) \((0 \leq i \leq n)\) is the
ciphertext of \(U_i\) and \(P_i\). If the user has more than one account in a same system,
which means \(c_i\) and \(c_j\) are for the same system, then \(L_i = L_j\) \((i \neq j)\).

PASSWORDS ACCESSING

If the user just wants to search an account or a password that has been registered in a
certain site, he should insert his IC card into his computer, which is used for the secure
storing, and accept the authentication of the system. The operating steps are as follows.

Step1: Inserts his IC card into the computer and accepts the system’s authentication
as subsection D. If he/she passes the authentication, he/she obtains the access rights.
Else his access is denied.

Step2: User locates the entrance \(L_i\) of the third-party’s system.

Step3: The system calculates the decryption key base on the \(IDInfo\) and the random
number \(r_i\) as formula (6). Then decrypts \(c_i\) and recovers \(U_i\) and \(P_i\) to the user.
THIRD PARTY SYSTEM’S LOGIN

When the user needs login to the third-party’s system, the IC Key and Random Number in the IC Card are used for system authentication and decryption. The account and it corresponding password are filled in the blanks of the application program or login interface of the third-party’s system and login to the system after the user makes the login command. The specific operation steps are as follows.

Step1: As Step1-Step3 in the above subsection after authentication and get the plaintext of $U_i$ and $P_i$.

Step2: Confirm the login account. If it is not a suitable one, the user should examine the other entrance in the repository table and look for the intend account.

Step3: The account and password are filled in the blanks of the third-party’s system login interface automatically.

Step4: login to the system according to the user’s login command.

PRACTICABILITY AND SECURITY ANALYSIS

Practicability and security are two key factors to a password management method. In our design, the IC card acts as a private credential like the key of a lock. Accounts and passwords of the third party are stored in a computer. Only the one who owns the computer, the IC card and the management password can manage the third party’s accounts and passwords. This kind of design separates the storage and the authorization spontaneously. It has three merits: 1) the accounts and passwords usually does not need to be carried with you and only be accessed when you forget the password, 2) credentials to be kept secretly are very simple, and 3) the secret is sharing in computer hardware, IC card and the managing password. Usually, when we register a new account on one site or system, it needs to access the secure repository and insert the new account, password, and system entrance to the repository. If we want to login to a site or system, we just insert the IC card and manipulate as described in section E. Therefore, the system, which uses fewer cryptographic calculations as shown in TABLE II, is very practicable.

| TABLE II. NUMBER OF ENCRYPTION USED IN EACH PROCESS. |
|---------------------------------|-----------------|-----------------|
| Identifier Extraction           | 1               | 0               |
| IC Key generation               | 1               | 0               |
| Authentication Module           | 2               | 0               |
| Passwords Secure Storing        | 1               | 1               |
| Passwords Accessing             | 4               | 1               |

Additionally, security is ensured by cryptography technology. It can be divided into two sides: 1) storing security, and 2) accessing security. At first, the third party’s accounts and passwords are encrypted with a symmetric algorithm using a key extracted from the hardware ID information and random number saved in the IC card. Without the computer, in which the IC key is extracted from, and the IC card, anyone can not decrypt the ciphertext of the third party’s accounts and passwords. Second, any accessing to or manipulation of the third party’s accounts and passwords needs an
authentication as discussed in subsection III.E.b. Anyone who has not the computer, the IC card or the management password will be denied by the system authentication. Hence, the security can also be ensured.

CONCLUSIONS

In this paper, we propose a novel password management scheme for the third party’s accounts. The third party’s accounts, passwords, login entrances are stored in a computer securely. Any accessing to the accounts and passwords must be authenticated by a trinity protective measure which requires verifying the computer, the IC card, and the system management password. The method not only solves the memorability problem of passwords, but also prevents the risk of passwords leakage. In practice, if the third party can open its API interface, the proposed system can help user login to his/her third party’s system automatically. By such design, it can increase the convince of login process of the third party’s platform and protect the security of the accounts and passwords as much as possible.

ACKNOWLEDGEMENT

This work is supported by the Natural Science Foundation of Shandong Province (No. ZR2013FL003, ZR2014FL011), the Science and Technology Foundation Project of Guizhou Province (No. QianKeHeJiChu[2016]1115), the Youth Science and Technology Talent Project of Guizhou Provincial Education Department (No. QianJiaoHe-KY-Zi[2016]220), the “YiTiiLiangYi” Special Project of Guizhou Education University (No. 2016YTLY10).

REFERENCES


