# How to Set and Manage Your Network Password: A Multidimensional Scheme of Password Reuse

Yang Cheng, Zhao Qi



# How to Set and Manage Your Network Password: A Multidimensional Scheme of Password Reuse

Yang Cheng[1,2]✉, Zhao Qi[2],

[1] China's Research Centre for Payment System
[2] School of Economic Information Engineering, Southwestern University of Finance and Economics, Chengdu 611130, China
Yangcheng@swufe.edu.cn

**Abstract.** The rapid development of the Internet and highly decentralized network services, prompting the majority of Internet users continue to register more accounts, and cause a high incidence of password reuse, which makes the user information leakage risks facing the domino-style. Based on the data of Internet password leak door at the end of 2011 as well as the college students' online survey, the paper analyzed the structural characteristics and reuse behavior of netizen passwords in detail, and thus designed a multidimensional password scheme that infused into the information dimensions and classified management. This scheme, based on the structure of "seed - reuse code", includes three dimensions: the content dimension contains multi-independent "information factor", which constitutes the main part of the password; the formal dimension is responsible for conversion formatting, in order to enhance the complexity and security of the password; and space-time dimension is targeted designed to protect the password timeliness and reusability. Through comparative analysis and quantitative analysis, the new password scheme not only has good memorability and convenience, and can effectively resist the violent attacks and acquaintances attacks.

**Keywords:** Password Security, Password Reuse, Seed Password, Difference code, Multidimensional Password Scheme.

## 1 Introduction

With the rapid expansion of the Internet, the network has been closely together with people's life, become an indispensable part of life. In order to fully enjoy the convenience of the Internet, such as business transactions, information access, communication and network entertainment, users need to register account more and more. At present, the most common site authentication mechanism is still the username and password combination model (ID-PWD). Although the mode has the obvious disadvantage of [1][2][3] in terms of safety compared with biometrics, smart cards and other methods, but it is easy to be accepted by users, and low cost, thus no one mature authentication mechanism can replace it so far, because of the convenience and practicality. Network certification will be mainly ID-PWD model [4] for a long period.

As the ID-PWD model is not perfect in the protection of network information security, so users often have to face the problem that account password was stolen and personal information been leaked, or distress. According to the CNNIC "twenty-eighth times Chinese Internet development statistics report" [5] data shows, the number of Internet users who had account or password stolen reached 121000000 at the first half of 2011, account for 24.9 percent of the total number of Internet users. At the end of this year, Chinese Internet outbreak a large-scale user data leaks. From the 6400000 user data leakage of the programmer website (CSDN.net), to the 30000000 user password leakage of Tianya (Tianya.cn), and Renren (renren.com), duowan (duowan.com), 7K7K network (7K7K.com), baihewang (baihe.com), mop (maopu.com) and other famous sites have been stolen. So far, a large number of the big and famous website in China has been involved, about hundreds of millions of users. Not only the amount is amazing, and the leaking data is a plaintext password, non-encrypted storage, so the "secret door" caused a panic of the password security in china. In the user information leak incident, password reuse behavior of Internet users play an important role, causing huge losses to the majority of Internet users.

The so-called "password reuse" refers to the user's behaviors that choose the same password between multiple different accounts. Cognitive psychology indicate that this behavior is rooted on human memory limitations [6]: ordinary users can remember a meaningless, random, high-intensity password composed of numbers, letters and special characters after training, but after multiplied by 10 or more human mind will reach the physiological memory limit. Therefore, the design of ID-PWD combination would face trade-offs between memory and security. Based on the specificity and sensitivity of password data, there has little research about this kind of behavior, also not deep enough, and the domestic is almost a blank, but the hidden danger lead to network security is a consensus: using a small amount of password at numerous sites repeatedly would face security risk, if a combination of ID-PWD leaked it may cause the user to lose many other accounts [3] [6] [7] [8] [9]. For example, the protection of the user account information is different as different websites; especially some small and medium-sized website may become a short board password protection, which leads to the large websites' pay went up in smoke, because of funding, technology limitations. So, in order to avoid further spread of password reuse phenomenon, put forward a reasonable imminent, efficient password design and management are strategy, based on a large amount of empirical research we attempt to do some exploration in this respect.

## 2 Analysis the structure of passwords

The serious user data leak which occurred at the end of 2011 is the sorrow of the entire Internet industry. On the other hand, it also provides researchers priceless data with which to study the password security and password feature. At present, similar studies are often limited by the objectivity and representative of data, because the data before are got either from a small scale questionnaire survey or from the little leak data of a single website, thus there has never have a study that involves so many sites, cross category, large scope user password data. More importantly, most of the existing literature on the user password feature is about the English speaking world, but

these user password data are usually related with the culture and language of the country, for example, we have found a lot of unique characteristics of Chinese in our research, such as Chinese Pinyin. In addition, as the password data involve a number of different categories of representative sites, we can get the value sequence of these kinds of websites and the empirical research of reusable data through the correlation analysis. Therefore, in this section we will analyze some of the leak data and the students password reuse behavior, to study the universal ways users design the password, including structure features, application habits and reuse mode, so as to bring forward the password design scheme and management strategies.

### 2.1 Structure

In the analysis of password structure in this section, we select the most representative leaked data of Tianya community as the main analysis object, while other data for comparative analysis and verification, this is because the Tianya community uses blog, micro-blog as a basic way to exchange, human emotion as the characteristics of the integrated virtual community and large social networking platform, it is the most influential global Chinese online home, while the user groups are widely distributed, including different age, different class, different occupation of Internet users. At the same time, Tianya is also the website who has been stolen the most data in this incident, thus, it is suitable to select it as the analysis object.

This leaked data of Tianya is backup data for 2009, a total of 29865731 account records, each record contain the account ID, password and E-mail information, so we can quickly get some basic structure characteristics of the Internet users password using some simple SQL statements.

For example, length, two thirds of the passwords range from 6 to 8, where the average is 7.94, the ratio of number and letter is about 3:1. About structure, 63.8 percent of the accounts are pure digital password; while 10.3 percent are pure alphabetic password. On the other hand only 24 percent are mixed, and the choice of the special character for the password is lower than 1.9 percent (the last two numbers in the Myspace users are respectively 81% and 8.3%) [10]. Visible, China users prefer digital password; password security awareness is generally low.

To analyze the commonly used password, we found a lot of difference from the western caused by the unique characteristics of Chinese culture. In addition to the highest frequency of 1, 2, and0, the number eight ranked fourth (the pronunciation is similar to "death "); while the number four is the least frequently used number (the pronunciation is similar to "making fortune ").

In addition, due to the differences in culture and modes of thinking, Western Internet users are different from their Chinese partner in the choice of 26 letters (case insensitive) as the password character. Through the statistics the frequency of each letter used in four different application environment (English text, Western password, Pinyin text and Chinese password), and calculate the space cosine angle between the four groups of data, we found that the correlation of China users' password and Chinese characters Pinyin text is 0.928, far higher than the English one 0.841, showing that people in the password design used to reference the pinyin. [11] This point is also reflected in these commonly used Chinese Pinyin characters: Ang, Jia, Hao, Wan and Xiao with a frequency of 0.5 percent, while the frequency of password, baby, ball,

boy and other strings are often appeared in the Western passwords are below 0.005 percent, only ABC and love have a frequency close to 0.5 percent. Further studies revealed that the frequency of consonant characters are higher in Pinyin. This reflects that people like use Mnemonic Phrase-based Passwords, for example, with reference to the idiom " Man proposes, God disposes ", the password may be set to "m4zrc4zt".

### 2.2 Reusability

In this section, we select the leak data of four websites Tianya, CSDN, 7K7K and Renren as the research object, to establish the association table across the sites account for a common mailbox, and study the phenomenon of password reuse. These four sites belong to different subject categories, in addition to the previously mentioned Tianya, CSDN is the largest (6428631 records) technology forum for programmers, 7K7K is one of the most professional casual games website (19138451 records), Renren is a famous social networking sites (4768600 records). They are the leader in their categories, has a huge and representative registered users.

**Table 1.** Analysis of Password reuse between any two of the four sites

| | full password | | | | root password | | | |
|---|---|---|---|---|---|---|---|---|
| | Tianya | CSDN | 7K7K | Renren | Tianya | CSDN | 7K7K | Renren |
| Tianya | - | 34.10% | 91.60% | 51.70% | - | 19.80% | 3.30% | 6.90% |
| CSDN | 34.10% | - | 36.00% | 29.30% | 19.80% | - | 21.90% | 22.30% |
| 7K7K | 91.60% | 36.00% | - | 57.50% | 3.30% | 21.90% | - | 5.30% |
| Renren | 51.70% | 29.30% | 57.50% | - | 6.90% | 22.30% | 5.30% | - |
| Average Val | 59.10% | 33.10% | 61.70% | 46.20% | 10.00% | 21.33% | 10.17% | 11.50% |

Account association table “Relation (Email, Tianya_PWD, CSDN_PWD, 7K7K_PWD, renren_PWD)” has a total of 4718269 records; each of them is at least email registered at two different sites. Through the table we found that, in addition to password reuse, there are a large number of multiple password corresponding with the same email exist only minor differences, they are from the same root password (PWD-Seed) and derived, this should be regarded as an extension of the password reuse. In order to accurately measure the multiple correlation relationship, we use the standard LCS algorithm. The standard LCS algorithm was adopted here to calculate password similarity from the same users on different websites:

$$sim(PWD1, PWD2) = \frac{2 \times len(lcs(PWD1, PWD2))}{len(PWD1) + len(PWD2)} \quad (1)$$

*len*(x) returns the length of the string X; *lcs*(X, Y) returns the longest common substring of X and Y, such as, *lcs*(‘12345678’, ‘a13458’) =’345’. In the formula, “Sim=1” indicates that users use the same passwords on multiple websites and “Sim=0” indicates that the passwords used in different websites are totally different. Therefore, “0.75< Sim<1” indicates that passwords used in unique websites are basi-

[1] Function Description: *len* Returns the length of the string, *lcs* Returns the longest common substring, for example, *lcs*(‘12345678’, ’a13458’)=’345’.

cally the same. Table 1 shows the average Sim between the four sites of two values, namely password reuse rate of different websites.

Table 1 indicates that in these four sites more than half of the public user password existing reuse phenomena between any two sites (the sum of two reuse patterns between any two sites are larger than 50 percent), where Tianya and 7K7K have a proportion of more than 90 percent are completely password reuse, with password basically the same is more close to 95 percent. In the two reuse mode, ordinary users tend to use fully password reuse is simple, but has the background of IT users (CSDN) tend to relatively complex password reuse. Further analysis showed that, in the multiply site registered users, nearly 80% (79.1%) users existing a behavior of password reuse (4 password corresponding to the same Email are at least 2 identical), including 4 password identical up to 33.9 percent, which is more than one to three users.

Usually, password reuse rate between websites are related to many components, the value of website and its user component structure are the two most important. For example, in four sites in Table 1, CSDN has the highest value, followed by Renren, the two passwords are unique compared with others, to prevent theft; while Tianya and 7K7K account value is relatively low, more likely to share the password, to facilitate the application. As the user structure, network safety consciousness of the four in descending order: CSDN user has the background of IT technology, Renren to college students, while Tianya and 7K7K are relatively popular. The above two rea-sons, jointly determined the password reuse of four big websites and its representative categories with a sort: CSDN (IT) < Renren (SN) < Tianya (BBS) < 7K7K (GAME).

Finally, the generalized password reuse should also include different users use the same password. It is embodied in the high-frequency password. In the case of Tianya, there have an average 1.5 people sharing a same password per 1000000 people, of which there are more than 4% accounts use "123456" as the password, the top 20 high-frequency password account proportion reached 8.42 percent, 100 reached 11.38 percent, while the first 10 percent password should cover more than forty percent (41.11). Obviously, the security of these passwords is relatively low, when faced with force attacks; it is very likely that they are the first to be compromised.

### 2.3 Behaviors study for students

In order to analyze users' password reusing habits, we developed an online re-search of 123 students majoring information manager, which received 118 effective questionnaires (including 25 boy-students, 93 girl-students). These participants having better knowledge of computer science and network safety realization, and we tried to find some valuable devise thought through their reusing behavior.

By the previous interview, we surveyed and sifted 29 website which always visited by college students (or website software), including QQ, Alipay, the ABC online bank （blank cooperated with college）, 163 mailbox, Sina Web，Worry-free future，Baidu Library and so on, which can roughly divide into 6 kinds: online classes, communication kind，forum kind，job wanted kind, datum kind and entertainment kind, and add to an daily “starting up password”. Subjects involved were asked to visit these website from the first one, and fill out one typical figure one/two/three..., and the website which having reusing password use one public figure to mark，

unregistered website use zero to mark. For the survey using anonymous way, and didn't involve material password data, or privacy reveal, so the data of this survey are relative real and objective.

By analysis, we found that almost all 118 students interviewed having reusing password behavior (94.9%), and among them 56.8% used the root password mode. The average account number is 10.6 for each student (between 3 and 28), however the independent password number is only 4.6 (between 2 and 8). Using the number of registered website and independent password of each student, we calculated all interviewers' average rate of reusing password is 2.6(between 1.0 and 6.5). This meaning, when the password of a reusing website leaked, an average of 2.6 websites facing a potential threat. Compared with the previous survey，we found that some data is coincide. For example, Florencio and Herlry analysis 500,000 users found that the average number of password is 6.5, the reusing rate of password is 3.9; Brown and others researched 218 students from American universities found similar result: each student had the average number of password is 4.45, and the reusing rate of pass-word is 1.84[13].

Researchers always use reusing rate to measure the potential threat level of password system, but Youngsok and some others thought this data ignored users' bias of password use, that is, it reflected the unbalance of reusing password on the account. They construct passwords on the base of graph theory, and put forward a new kind of Vulnerability Index [14],

$$VI = \sum_{i=1}^{m} (\frac{n_i}{N})(\frac{n_i - 1}{N - 1}) \quad (1)$$

$N$ is the total number of register website, $m$ is the number of independent password(that is, the number of reusing subnet, $m \leqslant N$), $n_i$ is the number of websites included in reusing subnet.

Using this formula, we calculate 118 students' average value of VI is 0.33, that is, when one website leaked, averagely 1/3 of remaining website facing threat, compared with 2.6 before is much higher. Figure 1 shows the reusing rate and VI value of all students interviewed, from which we can found that, the VI value is very different with same reusing rate. For example, the reusing rate of student A and student B is 3.0, but the VI value of them is 0.67 and 0.20. It's thus clear that, using reusing rate only to measure Vulnerability Index is not enough, it also need independent password distribution in reusing network to evaluate it.

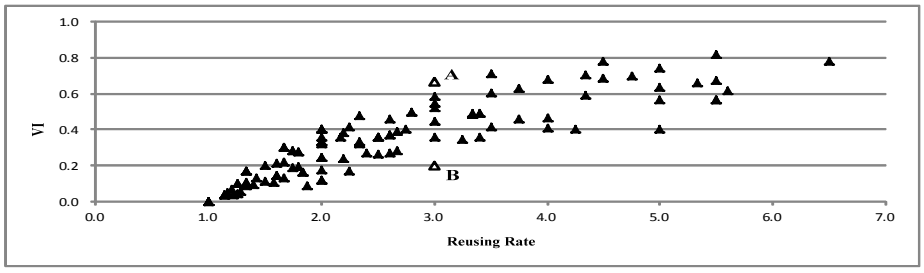


**Figure 1. P**assword reuse rate and VI value of interviewed students

However even so, we recognized VI value is still not exact enough, it ignored the value difference among websites: the same leak information, the loss of different value account is very different. Although the registered websites number of users is large, but most of them have low value, and the high value accounts only a little part. The value of websites is also observed "two-eight principle", this phenomenon reflected by our survey data.

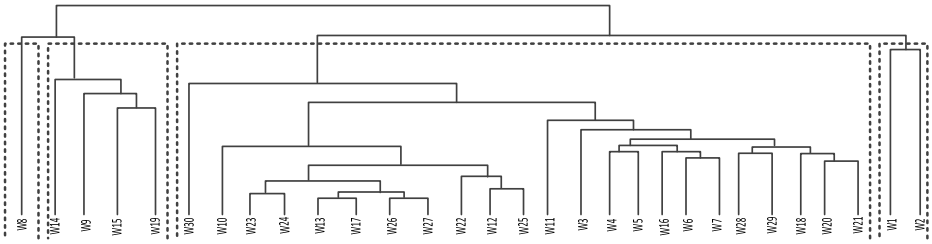


**Figure 2.** Clustering pedigree chart of 30 surveyed sites

According to the data of all users' passwords, Clustering of 30 websites: firstly, numbered all websites with w1.w30[2], secondly, make a table [30*30] by the original data, the data in the table is the number of users having reusing password between two websites, and last, using "the longest distance way" in R software make cluster analysis, figure 2 is hierarchical diagram. The figure showed, the interviewers' reusing password having obvious classified phenomenon: the password similarity of w1(the ABC online bank)and w2(alipay) is higher; w8(QQ)is an independent class; however the passwords of w9(Fetion), w14(Renren), w15(Sina Weibo) and w19(Baidu Library ) are similar; and the remaining 23 websites is a class. Obviously, the two classes previously belong to high useful website, and the number is very small; the number of latter class more than 2/3 of the total number, but for college students, they belong to small useful website. This classification can meet the real need of large password use, is a worthy mirror in our password design system.

## 3. Multi-dimensional password

For the phenomenon of reusing the same password for multiple websites, there are two better solutions usually: one is using "one website one password" pattern, setting a random password for each password; the other is using hash function pat-tern, using the name and other feature of website as dependent variable，generating independent passwords. Obviously, the former needed wonderful memory, but the latter needed the same wonderful mental ability. Since the memory and mental ability of people is limited in the reality, these two schemes would entrap the dilemma of weak password or with the aid of tools for storage/calculation. So, on the problem of multiple website

[2] 30 sites(w1..w30): ABC online banking, Alipay, Ali Wangwang, Amazon, Jingdong Mall, Ctrip, VANCL, QQ, Fetion,Gmail mailbox, 163 mailbox, 126 mailbox, The Farm, RenRen, Sina Weibo, Douban, Tianya Forum, CSDN, Baidu library, Douding network, DaoKe Baba,51job,ChinaHR,Street site, The recruitment of Chile, Youku, Tudou, The most liked online games, The most liked game sites, power-on password.

password design, lots of scholar considered pessimistic cannot meet the memory and security at the same time. But there are some scholar considered that memory and security are opposite actually, so finding suitable solution meeting the real demand is possible, and they presented principle thought: (i) the quality of initial passwords; (ii) the memory of passwords; (iii) the complexity of passwords [15].

The short-term memory survey of American psychologist Miller indicated that, the capacity of short-term memory had inner relationship with the quality of memory material and individual material processing, the memory limitation of general people is around $7\pm2$ chunk. Here the chunk is the unit of short-term memory, it's the process of uniting several separate stimulation into meaningful, larger information unit, that is stimulation of information recoding，this can effectively improve the capacity and effect of short-term memory. And short-term memory through repeated collection, changed into long-term memory. [16] For this, we imagined a password encoding way: changing a long password string into the suitable combination of several small "information factor" , and each information factor is a sub-string through the designer considered deeply, containing rich personal information, and having closed relationship with the experience of designers. In this way, it remained the complex and multiple form，at the same time improved the durability of memory.

Concretely, we referenced "Dimension of Information" concept in Information Theory, extended it and then proposed" Multiple Dimensions Password System" designed way. In Information Theory, dimension of information is a measure to estimate the effective value of information, including dimension of content, dimension of form and dimension of time, to measure the relationship of content, the rationality of form and the effective of time separately. Expanded into multiple dimension system, dimension of content corresponded several independent information factors, constituted of the memorial main part of password; dimension of form responded to the form change, improving the complexity and security of pass-words; and dimension of time reflected specific design, ensuring the effect and importance of passwords. The following is a detailed instruction for each latitude.

Dimension of Content：It's the base of the entire password system, and it can be any personal information of users, such as name, date, address, telephone number, motto, pet phrase, or liked poetry, proverb and so on.

Designing the dimension of password, we should avoid the case of single "information factor". Such as, analyses the Tianya passwords, we found lots of simple mnemonic passwords, they often from a poetry or proverb. Designed in this way could solve formal violence attack, but couldn't avoid friend attack. When content dimension contained several information factors, it could be recoded, changed it into a entire, meaningful information unit, improving the effect of memory further. For example, a dog named "diandian", and its mother was born at 62, and it wanted to go to "Vienna", so the content could be designed as"Dot-62-Vienna", memory point: diandian went to Vienna at 62.

Dimension of Form: It was effective guarantee of password security; it included both password type diversity, and its changed complexity.

The Dimension of Space-time: it was the key of multiple password system reusing, including the content of time and space.

By selecting the content dimension and form processing, we got the password having excellent performance in memory and security. Besides that, compared with the independent password problems, the design of multiple websites password system should consider the ease problem. In section 2.2, mentioned password reuse phenomenon except for complete reuse patterns, also had root mode, which is especially obvious in Internet population with higher security awareness. It was not hard to find that, the root password reuse is actually compromise of “one network one password” and “multiple websites one password”, it enabled users to meet certain safety while took the least amount of time and energy in the design, memory and application of the password. This also conformed to the American Harvard professor G.K.Z put forward “Principle of least effort”, namely, all people have the nature of streamline save and pursuit of benefits, always want to obtain the maximum benefit with the minimum cost (including current and expected). But studied the leaked data in-depth found that, the reuse of code (that is, the different part of the outside of the root password) design were too simple, they were more attached to the root password in the form of a prefix or suffix, and on content used multiple websites pinyin initials and digits as simple encoding. This design might be meet the security requirements of a single password, but as a password system, this faced the threat of collapse once a point breakthrough. For once the interpreter got two or more passwords of the same account, he would easily analysis the root password, and easily guess the user’ password for other websites.

To avoid the password system domino collapsed, the reuse of code must be based on the personalized design, it should be diversified, no rules, and should not be stereotypes and unified. Formally, although the multiple information factors’ order of root password relatively fixed, but the reuse of code can be inserted into the information factors, it could be integrated and also could be spread; and on content, it was not only related to the public information of the websites, but also related to the user’s personal experience of the website, which was joint coding based on the two parts of information (Net-Public, Net-Private). Such as alipay website, Net - the Public can be zfb (alipay), ali (alibaba), ww (ali wangwang), 82 (taobao TB phone stretchable latex pinyin) and so on, even $, EC (electronic commerce) and characters contacted with alipay, such as Net private could be the time of the user shopping online, one of the most expensive online, or the nickname or avatar of ali wangwang,or...any private information associated with "alipay" . For example, the same root password “.62Vie”, its alipay password could be designed for “67.62$Vie” (67, the user usually shopping on weekend), and sina blog password could be designed as "eCat. 62 Vie" (e with sina logo similar big eyes; the Cat, the user's blog, nicknamed "big Cat") or "M24.62 Vie" (24, sina's top two vowels; M, with big Cat logo shape).

At last, drew lessons from the results of the survey in 2.3, we need to divide websites into 3-4classes by the value degree, designed different root password, and constituted different password system for classified management. This classification not only reflected the value difference among websites, more was that it could en-hence the security of the entire password system further, especially be conducive to protect small amounts of high value accounts. This was because, on subjective the user had stronger sense of security for high value accounts, would pay more attention to the environmental security, reduced the possibility of self-leak; On objective, ac-count of the high value often correspond to some large websites, which could provide more

capital and technology for the client data protection, isolated such accounts could avoid safe hidden trouble caused by the short board effect. Therefore, balance d the convenience and safety, users classified managed the Internet accounts ac-cording to the value, for online banking, alipay, QQ and other first or second high value should be focused on protected, let the root password contained more information factors, and carefully constructed to reuse code; And for the last class of account with low value or zero value, should focus on convenience, using relatively simple root password and reuse code, and even didn't need reuse code.

## 4. Security analysis

Compared with the traditional password, multi-dimensional password system has obvious advantages in memory and convenience, and in this section we will analyze the quantity of safety. Usually, password attack was mainly divided into two kinds, hackers and acquaintances hack. The former attack is more widely, while the latter has a higher success rate. In the system scheme of this paper, the hacker attack is still decided by the password length and alphabet size, while acquaintance attack is decided by the number and form of the root password information factors and the privacy levels of the reused string in the password.

As Shirley and Edward [3] conducted a survey in 2006; their purpose is to find who poses a biggest threat to their password in the eyes of the users. They considered the population in risk and the ability of hackers, on the basis of computer ability and the relationship with the attacker, the population in risk was divided into 6 categories. Similarly, we have classified test on the security of password system, also divided into 6 types: $SN^0$, $SN^1$, $SN^2$ and $AN^0$, $AN^1$ and $AN^2$, according to the revealed password number (not leak, one leakage as $N^0$, $N^1$, revealing 2 and above as $N^2$) and the degree of closeness (strangers and acquaintances remembered as S and A).

We propose that the length of multidimensional password is at least 10 or more, because it will be unable to contain enough information factors and enough number of reusable codes if it is shorter than that, thus affecting the security of the password. Table 2 take a password with 3 information factors and the minimum length of 10 characters as an example, to analyze the 6 cases safety. At this time, the multidimensional password usually has 3 kinds of structure mode: 6-4 (6 root passwords, 4 reuse codes), 7-3 and 8-2. Table3 estimated the number of possible combinations in a conservative way, to reveal the worst safety case: assuming that risk groups are "Acquaintances" and the hacker is very understanding, knowing that the possible 100 information factors (10 classes, each class contains 10 items of information), and 10 common formal transformation, namely each factor about 1000 value. In the reuse of code, Net-Private is highly personal, similar to another information factor, while the Net-Public is limited to specific sites, equivalent to a large class of "weak" information factor, set the value as 100 (10 items of information *10 forms transformation). In addition, Table2 also provides a reference system: simple mnemonic type reuse passwords. This kind of password generated by a mnemonic phrase and simple reuse code, its essence is a simple combination of a single factor and Net-Public.

As shown in Table2, multidimensional password was significantly better than the simple mnemonic type password in safety; in any case it has several orders of magni-

tude higher than the latter. If the simple mnemonic type password was good for violent attack, then it is almost completely transparent when encounters an acquaintance attacks, especially under the condition that the attacker got multiple passwords. For multidimensional password system, not only it can effectively resist all kinds of pure technology attacks, but also close to 8 bit random password when faced "Acquaintances". Even the highest $AN^2$, the most conservative estimate, it also had a combined million species. The current online login mechanism, such as incorrect password restrictions and additional parity check code, can effectively ensure the security.

**Table 2.** Multidimensional password system security quantify table

| type | combination | simple mnemonic | description |
|---|---|---|---|
| $SN^0$ | $94^{10}, O(10)$ | | Available password characters 96. |
| $SN^1$ | $C_{10}^6 \times 7^4 \times 94^4 + C_{10}^7 \times 8^3 \times 94^3 + C_{10}^8 \times 9^2 \times 94^2$ $O(6.9)$ | $2^2 \times (94^4 + 94^3 + 94^2)$ $O(4.3)$ | Randomly selected 6-8 root password, reuse code can appear in any position in the multidimensional system, and only in the simple mnemonic is a former suffix. |
| $SN^2$ | $7^4 \times \frac{94^4}{8^3} \times \frac{94^3}{9^2} \times 94^2$ | $2 \times \frac{94^2}{2} \times \frac{94^3}{2} \times 94^2$ | Known the root password, three Numbers corresponding structure in turn 6-4/7-3/8-2 |
| $AN^0$ | $1000^2 \times 1000 \times 100 \times 4^2$ $O(7.7)$ | $2 \times 1000 \times 100$ $O(2.7)$ | Information factors (including Net - Public and Net - Private) is the basic unit of the constructing multi-dimensional password, usually does not make the split |
| $AN^1$ | $4^2 \times 1000 \times 100$ | $2 \times 100$ | Known the root password and every information of the factor (the worst possible) |
| $AN^2$ | $4^2 \times 1000$ | 2 | Net - Public encoding be cracked (worst possible) |

Note: $O(x)$ represent password combinations of equivalent to the length of x random password

In addition, Table2 also shows that when faced the high risk acquaintance attack, the security of multidimensional password system is mainly determined by the number of information factor and private levels, and has no direct relationship with its characteristic length. Therefore, suggests that high value sites contain at least more than 3 information factors, while the reusing code should be not less than 3 characters, in order to ensure system security after particular individual password leaked.

## 5. Discussion

Based on the survey data and the leaked data, we designed and created the multidimensional password system, “root password - reuse code" as the structure, involved the information dimension and the classification thought. After comparison and quantized analysis, which not only has a good memory and convenient, but also can effectively resist brute force attack and acquaintance attack. Although the complete website authentication mechanism contains two parts: ID and PWD, many researchers have suggested using different ID in secure password system, but we think that the essence of ID is the password extension, it is not recommended to do too much change in the account. Because most of the formal sites were required to pro-vide email when the users register, or even mobile phone number, for confirmation of registration and retrieve password and other services, and users often fill in. And it is often the key to judge whether it is the same user, rather than ID itself. Therefore, too much account transform can do nothing but increase the burden of memory, meaningles to reduce the risk of reuse.

Notable is, password scheme in this paper is only for network user. And a good password security system needs three aspects to cooperation: users, Internet companies and policy makers. Especially for the enterprise, safe storage and encryption transmission problems need to be solved for user data. If these data were stored in plain text, once encounter "drag library", and then the password was also in vain even if it designed perfectly.

## References


1. de Rodrigo L G, Carlos A L, Atman A, et al. Biometric identification systems [J]. Signal Processing, 2003, 83(12): 2539-2557.
2. Halderman J A, Waters B, Felten E W. A convenient method for securely man-aging passwords[C]. Proceedings of the 14th international conference on World Wide Web. ACM, 2005: 471-479.
3. Shirley G, Edword W F. Password management strategies for online ac-counts[C]. Proceedings of the second symposium on Usable privacy and security. ACM, 2006: 44-55.
Pinkas B, Sander T. Securing passwords against dictionary attacks[C]. Proceedings of the 9th ACM conference on Computer and communications security. ACM, 2002: 161-170.
4. China Internet Network Information Center (CNNIC). The 28th Statistical Report on Internet Development in China [EB/OL]. (2011.7.19). http://www.cnnic.net.cn.
5. Zhang J, Luo X, Akkaladevi S, et al. Improving multiple-password recall: an empirical study [J]. European Journal of Information Systems, 2009, 18(2): 165-176.
6. Notoatmodjo G, Thomborson C. Passwords and perceptions[C]. Proceedings of the 7th Australasian Conference on Information Security. Australian Computer Society, Inc., 2009[98]: 71-78.
7. Devi S M, Geetha M. OPass: Attractive presentation of user authentication protocol with resist to password reuse attacks [J]. International Journal of Computer Science and Mobile Computing, 2013, 8(2): 174-180.
8. Ives B, Walsh K R, Schneider H. The domino effect of password reuse [J]. Communications of the ACM, 2004, 47(4): 75-78.
9. Schneier.B. Real-world passwords [EB/OL]. Schneier on Security, 2006, 12.
10. http://www.schneier.com/blog/archives/2006/12/realworld_passw.html

11. Cheng Yang, Jui-long Hung, Zhangxi Lin. An analysis view on password pat-terns of Chinese internet users [J]. Nankai Business Review International, 2013, 4(1): 66-77.
12. Florencio D, Herley C. A large-scale study of web password habits[C]. Proceedings of the 16th international conference on World Wide Web. ACM, 2007: 657-666.
13. Brown A S, Bracken E, Zoccoli S, et al. Generating and remembering pass-words[J]. Applied Cognitive Psychology, 2004, 18(6): 641-651.
14. Bang Y, Lee D J, Bae Y S, et al. Improving information security management: An analysis of ID–password usage and a new login vulnerability measure [J]. Inter-national Journal of Information Management, 2012, 32(5): 409-418.
15. Sasse M A, Brostoff S, Weirich D. Transforming the 'weakest link' — a human/computer interaction approach to usable and effective security[J]. BT Technology Journal, 2001, 3(19): 122-131.
16. Lisman J E, Idiart M A. Storage of 7+/-2 short-term memories in oscillatory subcycles[J]. Science, 1995, 267(5203): 1512-1515.