Shadow Attacks based on Password Reuses: A Quantitative Empirical Analysis

Weili Han, *Member, IEEE,* Zhigong Li, Minyue Ni, Guofei Gu, and Wenyuan Xu, *Member, IEEE*

Abstract—With the proliferation of websites, the security level of password-protected accounts is no longer purely determined by individual ones. Users may register multiple accounts on the same site or across multiple sites, and these passwords from the same users are likely to be the same or similar. As a result, an adversary can compromise the account of a user on a web forum, then guess the accounts of the same user in sensitive accounts, *e.g.*, online banking services, whose accounts could have the same or even stronger passwords. We name this attack as the shadow attack on passwords. To understand the situation, we examined the state-of-the-art Intra-Site Password Reuses (ISPR) and Cross-Site Password Reuses (CSPR) based on the leaked passwords from the biggest Internet user group (*i.e.*, 668 million members in China). With a collection of about *70 million real-world* web passwords across four large websites in China, we obtained around 4.6 million distinct users who have multiple accounts on the same site or across different sites. We found that for the users with multiple accounts in a single website, 59.72% reused their passwords and for the users with multiple accounts on multiple websites, $33.16 \pm 8.91\%$ reused their passwords across websites. For the users that have multiple accounts but different passwords, the set of passwords of the same user exhibits patterns that can help password guessing: a leaked weak password reveals partial information of a strong one, which degrades the strength of the strong one. Given the aforementioned findings, we conducted an experiment and achieved a 39.38% improvement of guessing success rate with John the Ripper guessing tool. To the best of our knowledge, we are the first to provide a large-scale, empirical, and quantitative measurement of web password reuses, especially ISPR, and shed light on the severity of such threat in the real world.

Index Terms—Password, Cross-Site Password Reuses, Intra-Site Password Reuses, Shadow Attack, Empirical Analysis, Quantitative

1 Introduction

Password-based authentication [1] is one of the most widely used methods to authenticate a user before granting accesses to secured websites. The wide adoption of password-based authentication is the result of its low cost and simplicity: a user can enter his or her passwords anywhere by a keyboard or a touch screen without any other extra devices. The popularity of passwords and the proliferation of websites, however, lead to a concern on password reuses between accounts on different websites [2] or even on the same websites. Moreover, the recent numerous high-profile password leakage events did not make the password situation better, and we ask the questions: *What do password reuses mean to accounts between websites and even the ones within the same websites*? *What is the implication of a compromised website or account to others*? How easy are shadow attacks, i.e., an adversary compromises an account utilizing the passwords of other accounts that are either on the same site or from other sites? To find out the answers, in this paper we analyze password reuses and shadow attacks empirically.

It is well-known that passwords are usually reused by a user across different websites [2][3], yet little work has been devoted to understanding passwords being shared among multiple accounts of the same user on the same website. Since both password reuses within the same website and across multiple ones can enable shadow attacks, in this paper, we analyze the both scenarios: (*i*) a user creates accounts with the same password on the *same* websites, which we term as Intra-Site Password Reuses (ISPR), and (*ii*) a user creates accounts with the same password across *different* websites, which we term as Cross-Site Password Reuses (CSPR). While having the same passwords for multiple accounts is simple and convenient to users, it raises security concerns, *e.g.*, if a password on one website is leaked, an adversary can have an enhanced chance to crack the other accounts of the same user, regardless of whether the accounts are on the same or different websites. We note that account ownership can be identified by the registered email addresses. As a result, we argue that users' accounts with passwords of higher security level could be relatively easily compromised, given the knowledge of the passwords at a lower security level, *e.g.*, web forums.

Although the password reuses are known to researchers for years, a large-scale in-depth empirical analysis of password reuses is still absent so far. Das *et al.* [2] leverage 6,077 distinct accounts to answer the question of *How often does a user reuse the same password across multiple sites?* Our work is along the same line. Yet we conduct a first-of-its-kind in-depth empirical study on web password reuses (both ISPR and CSPR) at a much

- *W. Han, Z. Li, M. Ni are with Software School, and Shanghai Key Laboratory of Data Science, Fudan University, Shanghai, P. R. China 201203.*
- *G. Gu is with the Department of Computer Science and Engineering Texas A&M University.*
- *W. Xu is with the Department of Electronic Engineering, Zhejiang University.*

larger scale. We leverage a collection of more than *70 million* real-world leaked web passwords in cleartext to investigate the fine-grained patterns and threats of password reuses. These leaked passwords are from four main-stream websites with millions of users in China: `CSDN` [4], `Tianya` [5], `Duduniu` [6], `7k7k` [7][1]. Luckily, two websites allow users to register multiple accounts using the same email address. This provides a valuable opportunity to study the ISPR, which has never been studied in the literature [2], to the best of our knowledge.

In total, we have gathered accounts of *2,671,443* distinct users (based on their email addresses) each of whom has at least two accounts on the same website (for ISPR analysis), *2,306,055* distinct users each of whom has accounts on at least two websites (for CSPR analysis), and *350,849* distinct users that are the intersection of the above two sets. Based on the above users' accounts, we answer the following questions in this paper:

Q1: *What percentages of users have reused their passwords among their intra-site and cross-site accounts?*

Q2: *What are the differences between the CSPR and ISPR passwords? Are their strength same?*

Q3: *What are the differences between reused passwords and all passwords? Are reused passwords stronger or weaker than any passwords?*

Q4: *For all passwords belonging to the same user, if they are not exactly the same, do they share similar patterns?*

Q5: *How much can we improve the efficiency of password guessing with the aforementioned findings?*

These questions are important, because they provide insights through analyzing the effects of shadow attacks on passwords: given a user's password(s) on a website, how likely can an adversary crack other account(s) of the same user?

The main contribution of this paper is that we analyze a large number of users' accounts to understand the threat of web password reuses (both ISPR and CSPR) and obtain a set of interesting results. Interesting findings include (but not limited to) the following:

- For the users who have accounts on different websites, according to our research, $33.16 \pm 8.91\%$ of users use the same passwords across two sites (CSPR). This percentage is lower than the ones (43-51%) reported in the literature of Das *et al.* [2], because we took an conservative approach to process data and may have excluded a few reused passwords. For the users who have multiple accounts on a website, in our research, 59.72% of them reused their passwords (ISPR). This percentage is higher than the upper bound of the CSPR rate reported by Das *et al*. This suggests that users tend to reuse their passwords on the same websites than across multiple websites.
- We further investigate the security strength of the *reused passwords* in terms of how easily they can be guessed correctly by an adversary with dictionaries. With the same metrics (*e.g.*, α-guesswork, α-workfactor) used by Bonneau [8], we find that the *reused passwords* across sites are stronger (*i.e.*, harder to guess) against *online password guessing attacks* than all passwords, while intra-site reused passwords perform similarly to all passwords against *online password guessing attacks*. When we conducted offline password guessing attacks, all reused passwords perform weaker than all passwords.
- Even though some users use different passwords for their accounts across different websites, their passwords are sometimes created using the same building blocks. For example, among the users who use different passwords on the four websites, 15.36% of them add prefix to create passwords and 9.03% of them add suffix. The definitions of prefix and suffix patterns are described in Section 3.2.4.
- Utilizing our findings to facilitate password guessing, we achieve a 39.38% improvement of password guessing success rate based on the JtR (John the Ripper) tool. By cracking a user's weaker passwords first, an adversary greatly improves his chances of successfully guessing a stronger password of the same user. This suggests that the strength of a user's passwords are somehow determined by the weakest one. Thus, shadow attacks can undermine the strength of relatively strong passwords.

The rest of this paper is organized as follows: Section 2 introduces the background of the password leakage events and our collected password data. Section 3 quantitatively answers **Q1**-**Q4** questions. Section 4 shows our experiment that improves a password guessing tool and then answers **Q5**. Section 5 discusses the limitations and implications of our empirical study, especially on the impact of using only Chinese websites. Section 6 summarizes the related work. Section 7 concludes the paper and introduces our future work.

2 Password Corpora

In December 2011, more than 70 million web accounts from four popular websites in China were accidentally leaked to the public. The incident is also known as "*`CSDN` Password Leakage Incident*", because the first victim website was `CSDN`, one of the largest web communities for IT professionals in China. The `CSDN` leakage contains over six million accounts. Immediately following the `CSDN` leakage, a significant number of accounts of `Tianya`, `duduniu`, and `7k7k` were leaked to the public in a similar manner.

As shown in Table 1, the total number of accounts leaked from these four websites is more than 70 million and the total number of distinct accounts after data preprocessing (as described in Section 3.1) is 51,233,384.

[1] Two of these websites are among Alexa Top 500 global sites. Such a large-scale dataset of cleartext passwords from multiple diverse real-world websites provides us the first opportunity to understand the current situation of web password reuses among real users.

TABLE 1
Basic Statistics of Leaked Passwords on Four Websites. Note that 7k7k has 8,825,710 accounts whose usernames are email addresses.

	Site Address	Amount	Valid Accounts	Data Type
CSDN	www.csdn.net	6,428,629	6,418,661	Username, Password, Email
Tianya	www.tianya.cn	30,179,474	26,337,242	Username, Password, Email
Duduniu	www.duduniu.cn	16,282,969	13,429,816	Username, Password, Email
7k7k	www.7k7k.com	19,138,270	5,047,665	Username (*Email*), Password
Total		**72,029,342**	**51,233,384**	

The leaked data from CSDN, Tianya, Duduniu include usernames, passwords, and email addresses, while the data from 7k7k contain usernames and passwords. The usernames of 8,825,710 accounts in 7k7k are email addresses.

In this section, we introduce background information of the four victim websites and their user base:

- CSDN [4] ranks first among all Chinese IT professional communities (one could consider it as a combination of MSDN.com and Slashdot.org). CSDN is a website announcing and reporting technology events as well as a technical forum. CSDN has more than 18 million registered individual users. The majority of its user base is programmers and IT developers. It is currently ranked 473 in Alexa Top Global Sites (August 2015).
- Tianya [5] claims to be one of the largest Chinese online forums and blogs. Tianya has more than 65 million registered individuals and is known as one of the most influential Chinese forums. It is currently ranked 60 in Alexa Top Global Sites (August 2015).
- Duduniu [6] is a company site who mainly sells management platforms to Internet cafes (which provide Internet access to the public for a fee and are popular in China). Duduniu's services include billing tools and wholesales of vouchers for online games. The registered members of Duduniu are mainly owners or managers of Internet cafes.
- 7k7k [7] is a website collecting and sharing small flash games. Founded in 2003, 7k7k has become one of the top 50 popular Chinese websites as of September, 2009. The majority of its user base is young people. It is currently ranked 4,021 in Alexa Top Global Sites (August 2015).

According to our investigation, these websites do not enforce strict password policies. For example, CSDN allows a password with only five digits, even after the password leakage event, and Tianya allowed any passwords of six characters for many years.

3 Empirical Analysis of Web Password Reuses

We analyze web password reuses from two perspectives: First, we investigate the strength of passwords, including the reused passwords and the different passwords that belong to the same user; Second, we examine the user behaviors by categorizing users into multiple groups, e.g., VIP (paid) users, academic users, Chinese users, and international users. The first part analysis will answer **Q1**-**Q4** mentioned in Section 1, and the second part will show the differences of CSPR in various user groups.

3.1 Dataset Setup

We setup six datasets to analyze the web password reuses.

3.1.1 Terminologies

We call the passwords that are used more than once by a user (either ISPR or CSPR) in our dataset as *reused passwords*, and the pair of different passwords used by the same user as *diverse password pairs*. For example, if Bob uses *123456*, *abcde*, and *abcde* as his passwords, then *abcde* is a *reused password*, and {*123456*, *abcde*} are considered as a *diverse password pair*. We will analyze the diverse password pairs to understand the strength of distinguish passwords belonging to the same users.

In this paper, we consider that a person can register several accounts on websites. If their registered email addresses are the same, we believe these accounts belong to the same user. We note that a person may use multiple email addresses to register multiple accounts, and addition information could be obtained to link these email addresses, *e.g.*, a user's corresponding friends may be aware of the linkage or it can be identified by the same email name but different email domain names (weilihan@google.com and weilihan@hotmail.com). To simplify the data processing, in this paper, we only utilize identical email addresses to identify users. Luckily, two websites Tianya and Duduniu allow a user to register multiple accounts with the same email addresses, which made our ISPR analysis possible.

3.1.2 Preprocessing

We follow the common practices in the field and collected the leaked password data from public domains for research purposes (as discussed and compared in Section 6). Especially, the data sets used in our experiments are already used in other published research literatures [2][9][10][11][12]. Although there is no IRB in

China, we processed the data with great care and did not cause any more harm than what has already happened. In particular, we did not perform any other operation other than understanding user behaviors. This processing is the same as in the research literatures [2][9][10].

In order to ensure that all evaluated accounts are valid and map to real users, we pre-processed the leaked password data sets by removing rogue accounts before experiments. Firstly, the accounts with blank passwords were all removed from our data sets. Secondly, in our experiments, email addresses are used to identify users, so we deleted invalid accounts whose email addresses are invalid (e.g., empty email usernames). Thirdly, we have discovered that there are over 4 million intersecting accounts that share the same email addresses and passwords for both `Tianya` and `7k7k`. However, several confusing evidences show that these accounts were copied either from `Tianya` to `7k7k` or the other way around. Because we cannot validate whether these accounts belong to either `Tianya` or `7k7k`, we removed all accounts from both `Tianya` and `7k7k`. We admit such a step could reduce the password reuse rate, but our analysis can serve as a lower bound of the password reuses. Additionally, according to the conclusion made in prior work [3] that the number of valid email addresses on the same website should be smaller than 25 on average, we removed all accounts whose email addresses had been used for more than 25 times on one website. Finally, we found that `Duduniu` and `CSDN` contained some accounts with the same emails and usernames but different passwords. We believe this is caused by changing passwords. Since we could not identify which record is the latest one, we deleted all these data from `Duduniu` and `CSDN` (about 950,000 distinct emails for `Duduniu` and 40 for `CSDN`).

After removing rogue accounts, we obtained 51,233,384 accounts, as detailed in Table 1. Then, we imported them into MySQL for further analysis.

3.1.3 User Classification

All four websites record users' email addresses, and thus we used email addresses as the users' identification. That is, if two accounts, regardless of whether they are from the same website or different ones, have the same email addresses, then these two accounts are considered as belonging to one user. We extracted the following three types of accounts:

- *Users each of whom has at least two accounts on the same website.* `Tianya` and `Duduniu` allow users to register for multiple accounts with the same email addresses (This is not true for `CSDN` and `7k7k`). This provides us an opportunity to study ISPR. As shown in Figure 1, in total we have obtained 2,671,443 distinct users for ISPR analysis, in which 1,796,717 users (67.26%) have two accounts, 548,071 users (20.52%) have three accounts, and 149,171 users (5.58%) have four accounts on the same website. We observed a tail of the account numbers, and only 0.10% of users have more than 20 accounts after we have deleted all these accounts whose emails had been used for more than 25 times on one site.

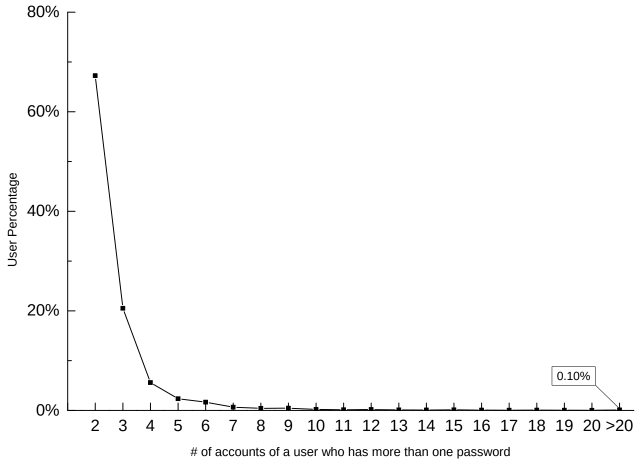


Fig. 1. Users for the Analysis of Intra-Site Password Reuses

- *Users each of whom has at least two accounts across different websites (cross-site users).* The detailed account information is show in Table 2, where we obtained 2,306,055 distinct users in total and 4,963 users that have accounts on all four sites. Note that, in the data preprocessing we removed the duplicate accounts from both `7k7k` and `Tianya` that have same email addresses and passwords, but kept the ones that have the same email addresses but different passwords. Thus, a few users have accounts on all four websites.
- *Users that belong to the intersection of the previous two data sets (for both ISPR and CSPR analysis)*: We obtained 350,849 users of this type, who have multiple accounts within a site and across sites.

After classifying the users into three types, we further divide the passwords into the following sets.

- D_{cspr}: The distinct reused passwords used by one user across sites, *e.g.*, across two, three, or four websites. The size is 726,860.
- D_{ispr}: The distinct reused passwords used by one user within the same site. The size is 1,665,137.
- D_{total}: All passwords associated with the accounts of four websites: `CSDN`, `Tianya`, `Duduniu` and `7k7k`. The size is 51,233,384.
- D_{td}: The passwords associated with the accounts of

TABLE 2
Users for the Analysis of Cross-Site Password Reuses

# of Accounts	Number	Percentage
2	2,180,771	94.57%
3	120,321	5.22%
4	4,963	0.22%
Total	2,306,055	100.00%

Tianya and Duduniu. The size is 39,767,058. This dataset is used to analyze the intra-site *reused passwords*, since ISPR is only available for the accounts of Tianya and Duduniu.

- D_{csdp}: The diverse password pairs used by one user across sites. The size is 2,569,813.
- D_{isdp}: The diverse password pairs used by one user on one site. The size is 2,768,842.

In the above datasets, D_{cspr}, D_{ispr}, D_{total} and D_{td} are designed to measure the strength of passwords in different situations. Here, D_{total} is the baseline for all other three sets. D_{td} is the baseline for D_{ispr}, because only Tianya and Duduniu allow multiple accounts registered with the same email addresses. The last two datasets, D_{csdp} and D_{isdp} are designed to measure the similarity of different passwords, and conduct the experiment of how leaked weaker passwords can reduce the strength of stronger passwords.

3.2 Quantitative Analysis of Web Password Reuses

This section will quantitatively analyze the password reuses based on the processed datasets as described in Section 3.1.2. Our analysis includes four aspects: the rates of CSPR and ISPR, which will answer **Q1** mentioned in Section 1; the strength of the passwords, which will answer **Q2** and **Q3**; patterns in the passwords and similarity of the diverse passwords created by the same users, which will answer **Q4**.

3.2.1 Rates of Password Reuses

We firstly calculated the reuse rates between any two websites (except the one between Tianya and 7k7k). It means that among the users who have accounts on both sites, how many of them reuse their passwords. With 95% confidence, the reuse rate on average is: $33.16 \pm 8.91\%$. Here, we assume that we have sampled the CSPR rates between two sites, and obtain a dataset of five available entries shown in Table 3.

When we look into Table 3 which lists the rates of password reuses between any pair of websites, the numbers of users are shown in the parentheses. We note that resulting from removing all duplicate records during data preprocessing, the reuse rate between Tianya and 7k7k is 0.00%. Among the reuse rates of the rest pairs, the reuse rate and the number of users who have multiple accounts between CSDN and Duduniu are the lowest. This is probably because CSDN is a website for IT professionals while Duduniu is a commercial website, whose accounts contain information at different sensitive levels. Thus, users tend to choose different passwords to ensure their security requirements. In general, our CSRP results (Table 3) are smaller than the lower bound of reuse rate reported by Das *et al.* [2], *i.e.*, 43%. This is partially caused by the four websites we studied, which are smaller than the number of websites in the work of Das *et al.* [2]. In addition, all users who have reused their passwords on Tianya and 7k7k were removed completely during data preprocessing. As a result, the rate is a lower bound of CSPR.

For ISPR, We calculated all the users who have multiple accounts in Tianya and Duduniu. The rate of users who reuse passwords intra-site is 59.72%. Note that we were fortunate enough to obtain this insight, and our results show how severe the password reuses are. Typically, websites forbid a user to register multiple accounts with the same email address, even though they can still use different emails to register for multiple accounts and their password reuses become almost impossible to analyze.

Note that, when we calculate the rate of ISPR, we do not sample the data set due to the limited number (two) of sites. That is, all data of ISPR in two websites are mixed together to calculate the rate of ISPR.

The rate of ISPR is higher than the upper bound of CSPR (51%) reported by Das *et al.* We suspect that this is because users who register multiple accounts on the same website may attempt to win a voting or lottery, *etc*. Thus, they might not care about the security of these accounts, resulting in such a high reuse rate.

Thus we answer **Q1** mentioned in Section 1 as follows:

> **A1**: *The percentage of ISPR is 59.72%, and the percentage of CSPR between any two websites is* $33.16 \pm 8.91\%$ *in our datasets. Compared with the results (43-51%) of CSPR reported by Das* et al.*, our rate of CSPR is lower than their lower bound, and our rate of ISPR is larger than the upper bound.*

3.2.2 Password Strength Analysis

We first compare the strength of passwords of D_{cspr}, D_{ispr}, D_{td} and D_{total} in terms of the resistance to adversaries' guessing in two scenarios: *Online guessing* where adversaries can try limited numbers of guesses, and *off-line guessing* where adversaries can guess as many times as possible. To measure the password strength, we adopt the same metrics used by Bonneau [8], namely, min-entropy, marginal success rate (β-success-rate), guesswork, α-guesswork, and α-work-factor. The first two metrics (min-entropy, marginal success rate) are mainly useful for measuring *online guessing attack*, and the other three are commonly used for measuring *off-line guessing attack*. These metrics are defined as follows:

- Min-entropy, H_∞, measures the likelihood that an adversary can guess a user's password within one

TABLE 3
Rates of CSPR between Two Sites.

	Tianya	Duduniu	7k7k
CSDN	33.29% (745,451)	27.10% (203,791)	35.69% (239,974)
Tianya	-	30.74% (497,772)	0.00% (416,514)
Duduniu	-	-	38.96% (468,010)

guess. Usually, an adversary will try the most frequently used password to launch the first guessing. Assume that the frequency of the most frequent password is p, then $H_\infty = -\log_2(p)$.

- Marginal success rate or *β-success rate*, λ_β, represents the expected success rate that an adversary can correctly guess the password of an account given β guesses. In addition, $\tilde{\lambda_\beta} = \log_2\left(\frac{\beta}{\lambda_\beta}\right)$, which is the representation in units of bits. $\tilde{\lambda}_{10}$ quantify how successful the adversary can be, when an adversary uses the top 10 frequent passwords to guess a user's password. Usually, it is an important indicator for an online guessing.
- Guesswork G represents the expected number of sequential guesses to find the password of an account if an adversary proceeds in an optimal order, where the entries in a dictionary are ordered in a descending sequence based on the frequency of passwords in the target password set. Typically, instead of directly using G, we use $\tilde{G} = \log_2(2\cdot G - 1)$ as the metric.
- α-guesswork, a.k.a. G_α, reflects the expected number per account to achieve a success rate α. Similar to the case of $\tilde{G}$ for G, we typically use $\tilde{G}_\alpha = \log_2\left(\frac{2\cdot G_\alpha}{\lambda_{\mu_\alpha}} - 1\right) + \log_2\left(\frac{1}{2-\lambda_{\mu_\alpha}}\right)$.
- α-work-factor (μ_α), a.k.a. marginal guesswork, measures how difficult it is to crack a proportion α of passwords, when an adversary knows all password distribution of the password set, and launches a dictionary attack based on a dictionary whose entries are ordered in a descending sequence of the frequency of passwords.

The measurement results with min-entropy, marginal success rate (β-success-rate), guesswork, and α-guesswork are shown in Table 4. The results of α-work-factor with various values of α are shown in Figure 2. From the results, we draw the following conclusions.

- As shown in Table 4, the passwords in D_{cspr} are stronger than those in D_{ispr} against *online guessing attacks*. The first two metrics indicate that the occurrence of the most frequent passwords in D_{cspr} is lower than the ones in D_{ispr}. This result confirms that compared with ISPR users, CSPR users might be aware that naive passwords can be a threat to the security of their accounts, so they create their own passwords for their accounts instead of using common passwords (e.g., passwords, 123456, or iloveyou). However, they typically follow the prefix or suffix patterns to create their passwords, as is shown in Section 3.2.4. Thus, the passwords in CSPR are not always stronger than those in ISPR against *offline guessing attack* as shown in Figure 2.

TABLE 4
Resistance to Guessing

	H_∞	$\tilde{\lambda}_{10}$	$\tilde{G}$	$\tilde{G}_{0.25}$	$\tilde{G}_{0.5}$
D_{cspr}	6.52	8.50	18.80	16.88	18.49
D_{ispr}	4.77	7.13	19.34	14.81	18.34
D_{td}	4.99	6.88	23.13	15.66	20.77
D_{total}	5.11	7.20	23.51	16.27	21.37

Note that, a higher value means the security strength is stronger.

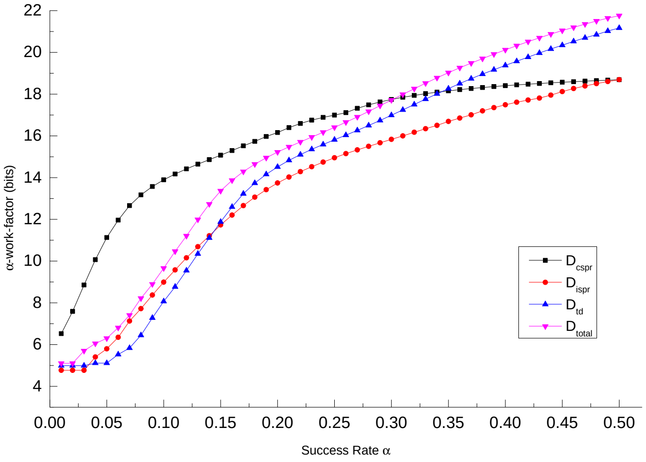


Fig. 2. α-work-factor of Passwords (a higher value means a stronger security strength)

- We can also see in Table 4 that compared with general passwords in data sets D_{td} and D_{total}, the passwords in D_{cspr} can better resist against *online guessing attack*. However, when it comes to *offline guessing attacks*, the passwords in both D_{cspr} and D_{ispr} are not as strong as the general passwords.
- As shown in Figure 2, the passwords in D_{cspr} performs better than other datasets when cracking a small portion of passwords (i.e., α is small), because these passwords reused across sites could be carefully composed by users. They paid attention to create a relatively stronger passwords to improve account security. In Table 4, the statistic results of D_{cspr} show better resistance against *online guessing*. However, for $\tilde{G}$, the *reused passwords (cross-site)* in D_{cspr} perform the weakest for guessing resistance. This situation is the same in Figure 2 when the *success rate* is 0.5. That means the choices of passwords for different sites are limited and less than other data sets, because the metric of $\tilde{G}$ depends on the choices of password creation. That is, if a user group chooses more distinct passwords, the $\tilde{G}$ is larger.

Thus we answer **Q2** and **Q3** as follows:

> **A2**: *The passwords in CSPR are stronger than the ones in ISPR against* online password guessing attacks, *but are weaker against* offline password guessing attacks.
> **A3**: *The passwords in CSPR and ISPR are stronger than all passwords against* online password guessing attacks, *but weaker than all passwords against* offline password guessing attacks.

TABLE 5
Keyboard Patterns

	Same Row	Same Row (Digit-only)	Zig-Zag	Snake
D_{cspr}	3.42%	3.21%	0.16%	0.19%
D_{ispr}	8.85%	8.39%	0.19%	0.21%
D_{td}	8.15%	7.58%	0.15%	0.19%
D_{total}	8.57%	8.00%	0.16%	0.20%

Note: The same-row (digit-only) column stands for the passwords that are digit-only and belong to the same-row pattern. For example, only 0.57% (= 8.57%-8.00%) passwords of D_{total} belong to the same-row pattern and are not digit-only.

3.2.3 Keyboard Patterns

While appearing random, passwords with keyboard patterns are easy to remember [13]. We will explore and compare three keyboard patterns between *reused passwords* (both cross-site and intra-site) and the whole set of passwords (D_{td} and D_{total}).

- *Same Row*, a sequence of contiguous keys in the same row. For example, *123456* belongs to this pattern, while *123567* does not.
- *Zig-Zag*, a sequence of contiguous keys from two rows. For example, *qazsed* belongs to this pattern, while *qzectb* does not.
- *Snake*, a sequence of contiguous keys which does not belong to the two patterns above. For example, *qwerfgh*.

In all four datasets, the proportions of digit-only passwords are similar, which are between 51% and 55%. But as shown in Table 5, we can conclude that D_{cspr} has the lowest percentage of passwords that have the keyboard pattern of Same Row (Digit-only). This phenomenon shows that users will create passwords with more security concerns because these passwords are reused across websites.

3.2.4 Patterns in Diverse Password Pairs

Patterns, or mangling rules, are the tricks that users leverage to create new passwords according to existing ones. We study six patterns here:

- **Suffix**, **Prefix** and **Middle**: These three patterns are substring patterns. For example, a user uses *12345*, *a12345*, *12345a* and *a12345a* as passwords. Then, (*12345*, *a12345*) belong to the **Prefix** pattern , (*12345*, *12345a*) belong to the **Suffix** pattern, and (*12345*, *a12345a*) belong to the pattern **Middle**.
- **Double**: Diverse password pairs like (*12345*, *1234512345*) belong to the **Double** pattern. We remove these password pairs from the **Prefix** and **Suffix** patterns to avoid double counting.
- **Case Transformation**: If two passwords are just different in letters' cases, they belong to this pattern, such as (*cRazy2duck*, *cRazy2duCk*).
- **Reverse**: The **reverse** pattern reverses one password to create another, such as (*12345*, *54321*).

TABLE 6
Patterns in Diverse Password Pairs

	D_{csdp}	D_{isdp}
Prefix	15.36%	4.61%
Suffix	9.03%	4.74%
Middle	0.57%	0.31%
Double	0.41%	0.09%
Case Transformation	0.34%	1.43%
Reverse	0.02%	0.07%

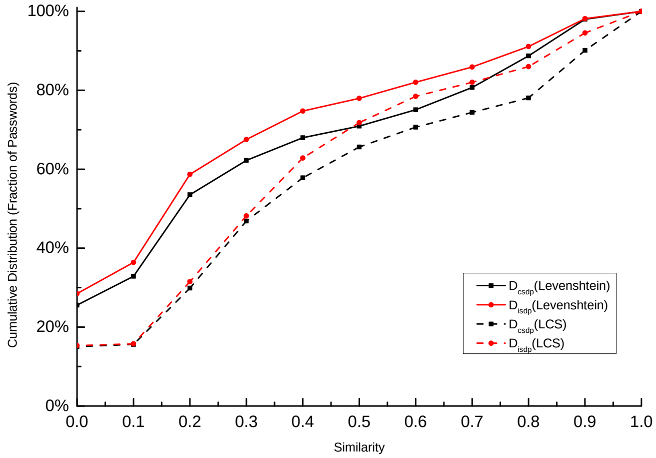


Fig. 3. Similarity between Diverse Password Pairs

The results are shown in Table 6. We can conclude that:

- Compared with D_{isdp}, a larger percentage of passwords in D_{csdp} share similar patterns between accounts on the same website.
- Lots of password pairs in D_{csdp} belong to pattern **Prefix** and **Suffix**. We list the mostly used ten N-gram, where N refers to the numbers of characters, prefixes/suffixes from D_{csdp} in Table 7. We leverage these prefixes and suffixes to improve the efficiency of a password guessing tool in Section 4.

Thus we answer **Q4** as follows:

> **A4**: *Both prefix and suffix are popular ways to create new passwords, when a user generates two different passwords across websites. In addition, the patterns of prefix and suffix are more popular in CSPR than in ISPR.*

3.2.5 Similarity of Diverse Password Pairs

We measure the similarity of *diverse password pairs* based on two algorithms as follows:

- *Levenshtein* distance [14]: The *Levenshtein* distance between two words is the minimum number of single-character edits (insertions, deletions and substitutions) required to change one word into the other. Let d denote the distance, l_1 and l_2 denote the length of two words, the similarity is defined as $1 - \frac{d}{max(l_1,l_2)}$.
- *Longest Common Subsequence(LCS)* function [15]: The LCS function finds the longest common subsequence of two words. Let d denote the length of

TABLE 7
Mostly Used N-gram Prefixes/Suffixes

	Prefix			Suffix		
	Unigram	Bigram	Trigram	Unigram	Bigram	Trigram
1	0 (61.77%)	00 (22.49%)	000 (12.42%)	a (21.68%)	78 (15.42%)	789 (15.97%)
2	a (14.64%)	19 (12.39%)	123 (3.10%)	1 (15.17%)	00 (9.52%)	123 (13.53%)
3	q (3.76%)	11 (5.42%)	asd (1.50%)	0 (9.32%)	11 (4.12%)	520 (3.93%)
4	z (3.26%)	qq (4.82%)	liu (1.44%)	. (4.59%)	12 (3.12%)	456 (2.14%)
5	w (2.44%)	AA (2.15%)	abc (0.13%)	q (4.36%)	aa (3.02%)	abc (1.90%)
6	l (1.96%)	li (1.47%)	qwe (0.69%)	8 (3.93%)	qq (2.72%)	521 (1.71%)
7	8 (1.47%)	zx (0.70%)	lin (0.66%)	9 (2.90%)	88 (2.60%)	000 (1.69%)
8	y (1.11%)	as (0.70%)	aaa (0.60%)	z (2.88%)	99 (1.13%)	110 (1.10%)
9	x (1.06%)	zz (0.69%)	wei (0.53%)	6 (2.84%)	23 (0.94%)	asd (1.04%)
10	h (0.98%)	zy (0.65%)	111 (0.51%)	7 (2.80%)	22 (0.92%)	111 (1.03%)

the LCS, l_1 and l_2 denote the length of two words, the similarity is defined as $\frac{2d}{l_1+l_2}$.

The results of cumulative distribution are shown in Figure 3. We can conclude that passwords in D_{isdp} are a little less similar than those in D_{csdp}.

3.3 Web Password Reuses in Different User Groups

Because the domain name of email addresses may help us identify the types of users, we are able to study the differences of password reuses in different user groups.

We divided users into four categories according to the domains of their email addresses, and then we calculated the cross-site password reuse rates and compared the password patterns among those categories. The four categories are defined as follows:

- *VIP users (VIP for short)*, the VIP (Very Important Person) email addresses are usually not free and have annual fees. Based on this criterion, all the users with the following domain are classified into this group: *@vip.qq.com, @163.net, @263.net, @vip.sina.com, @vip.163.com, @vip.sohu.com*.
- *EDU users (EDU for short)*, the academic email addresses are provided by academic organizations in China. We extracted 26 domains which have *edu* in the domain names, such as *@fudan.edu.cn, @pku.edu.cn*. We envision that the EDU users are typically better educated and should have stronger passwords.
- *Chinese email service users (Chinese for short, excluding VIP and EDU users)*, besides the email services with fee, there are a large set of free email service providers in China. The selected email domains include *@163.com, @126.com, @yeah.net, @qq.com, @sina.com, @sohu.com, @tom.com, @21cn.com, @tianya.cn*.
- *I18n email service users (I18n for short)*, these users utilize the free email boxes provided by International email service providers. The selected email domains are *@hotmail.com, @gmail.com, @msn.com, yahoo.com*.

3.3.1 Password Reuse Rates of Different User Groups

Using the aforementioned categories, we calculated the rates of cross-site password reuses for each group, and summarized results in Table 8, from which we have the following conclusions.

- The rate of CSPR is the lowest for users with education email addresses, and the number is smaller than the general rate of CSPR (26.13% *vs* 33.16%). This result confirms our hypotheses that users in academic organizations are better educated with web security than common users and tend to use different passwords for accounts in different websites. Another reason may be that users incline to reuse passwords when registering with low-valued or easily replaceable email accounts. Academic emails, however, are difficult to be replaced.
- On the contrary, it is interesting to find out that users with international email addresses are most likely to reuse their passwords cross-site. Surprisingly, VIP users, those who would pay annual fees for their email addresses, also have a high rate of cross-site password reuses, which is second to I18n users.

3.3.2 Patterns of Passwords of Different User Groups

Just like Section 3.2.4, we also calculated the percentages of patterns of diverse password pairs in the four categories as shown in Table 9. We can make the following conclusions:

- Although more VIP users than others reused their passwords across multiple websites as shown in Section 3.3.1, the least percentage of VIP users chooses the listed six popular patterns to create new passwords.

TABLE 8
Reuse Rates of CSPR of Different User Groups

Email Category	# of Reuse Accounts	# of All Accounts	Reuse Rate
VIP	7,063	20,442	34.55%
EDU	712	2,725	26.13%
Chinese	614,989	1,970,522	31.21%
I18n	40,164	114,734	35.01%
Total	662,928	2,108,423	31.44%

TABLE 9
Patterns of Passwords of Different User Groups

	VIP	EDU	Chinese	I18n
Prefix	14.26%	24.00%	16.22%	15.62%
Suffix	8.55%	12.51%	10.31%	9.22%
Middle	0.53%	0.36%	0.56%	0.58%
Double	0.30%	1.11%	0.63%	0.41%
Case Transformation	0.30%	0.31%	0.37%	0.35%
Reverse	0.00%	0.04%	0.03%	0.02%

- On the contrary, more academic users have chosen these six simple patterns. This phenomenon indicates that although students and staff from academic organizations are aware of the threat brought by cross-site password reuses, they tend to use well-known patterns to construct a password, which is not an effective way to create a strong password.

4 Shadow Attack Evaluation

This section will examine how effective it is to leverage the results of above analysis to imporve guessing. Here, we try to improve the guessing efficiency of John the Ripper (JtR) community-enhanced 1.79 [16]. JtR has a quick guessing speed using the wordlist mode and pre-installed rules.

4.1 Experiment Setup

To evaluate shadow attacks, we use the diverse password pairs in D_{csdp} to perform the experiment, and diverse password pairs are distinct passwords of cross site accounts of the same users. In addition, we use the weaker passwords (compared by entropy [17]) in the diverse password pairs to guess the stronger ones. This shows the danger of the widely adopted users' behavior: using weaker passwords in low-valued accounts and stronger but similar ones in high-valued accounts.

The methods being tested include the following.

1) JtR_default: Using weaker passwords in the diverse password pairs as a dictionary to guess the stronger passwords, with JtR default rules.
2) JtR_uni: Using weaker passwords in the diverse password pairs as a dictionary to guess the stronger passwords, with added unigram prefix/suffix rules.
3) JtR_bi: Using weaker passwords in the diverse password pairs as a dictionary to guess the stronger passwords, with added unigram and bigram prefix/suffix rules.
4) JtR_tri: Using weaker passwords in the diverse password pairs as a dictionary to guess the stronger passwords, with added unigram, bigram and trigram rules.

The added prefixes/suffixes are listed in Table 7. Note that in the latter three methods, we delete the default prefix/suffix rules pre-installed in JtR. In addition, the patterns *double*, *case transformation* and *reverse* already exist in JtR default rules.

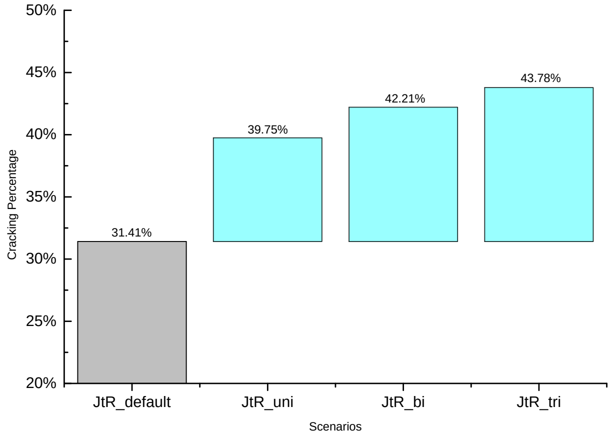


Fig. 4. Guessing Results of John the Ripper after We Utilize our Findings

4.2 Results

As is shown in Figure 4, we can conclude that:

- After adding the unigram prefix/suffix rules, the efficiency increases much more compared with bi-gram and trigram prefix/suffix rules. It shows that most users only add one character at the beginning/end of a password to create another.
- From JtR_default to JtR_tri, we increase the efficiency by 39.38% ($= \frac{43.78\%-31.41\%}{31.41\%}$) for guessing passwords across sites in total. This result shows that given weak passwords and the patterns, adversaries have a high chance to guess the stronger ones successfully.

The results show that shadow attacks have its practical concerns: The users with high security concerns may choose weak passwords for low-valued accounts, which is different from their strong passwords in high-valued accounts, *e.g.*, electronic commercial accounts. However, our experiment shows that the adversaries may has an improved chance to guess the stronger passwords based on the weaker passwords, which could be used on web forums.

Thus we answer **Q5** as follows:

> **A5**: *The patterns found in this paper significantly improve JtR by 39.38% when we guess users' passwords using weaker ones of the same users.*

5 Discussion

In this section, we discuss the limitations and usages of our empirical analysis.

5.1 Limitations

Quality and number of datasets: Our password datasets are from four Chinese websites. Although Chinese Internet users accounts for a large portion of the entire Internet users, our study mainly reflect the password reuse patterns of Chinese users. Our data pre-processing steps may have caused underestimation of password reuses. The password pre-processing step involves removing noisy data, such as accounts with invalid email addresses, and all duplicate accounts shared by `Tianya` and `7k7k`. When removing about 4 million duplicate users that have the same email address and passwords for both `Tianya` and `7k7k`, we admit that we underestimate the password reuse percentage and obtain a lower bound of the password reuses. In addition, our analysis is based on the limited amount of leaked data rather than standard sampling. Thus, we present major results with average numbers. Although the way we obtain data is simple, the results, including the improved guessing, are significant enough to shed light on the severity of such threat in the real world.

Mapping between persons and users: In our research, we did not analyze the scenario where a person registered as multiple users on sites using different email addresses, because we do not have enough information to perform this analysis. Although we may merge several accounts with the same complex passwords dto one human user, we cannot apply this method to all accounts in our analysis.

5.2 Concerns of Regional Features

Passwords have strong regional features according to the results of the literature [10][11]. Sequentially, the results in our paper reflex insights more about Chinese than the people in other nations. Nevertheless, our results in this paper have values, because: (1) our datasets contain users from a similar crowd (i.e., Chinese). This analysis maps to real scenarios, where the adversary tends to obtain passwords of the user groups in the same region to guess passwords of other users. (2) the security concerns of Chinese are similar to English users. Research [8] has shown that users in each region prefer their own character set, but the strength of passwords can be measured independent of these preferences. To confirm the prior research conclusion, we calculate the resistance [8] to password guessing for both the Chinese websites (the four data sets) and for an English website (`Rockyou`), which includes 32 million leaked passwords of English users in cleartext. As is shown in Table 10, the strength of passwords is similar. Although Chinese users do prefer a different set of character set (*e.g.*, digits) than English-speaking users (*e.g.*, who prefer letters), they both create passwords at the similar strength [10].

TABLE 10
Resistance to Guessing

	$\tilde{G}$	$\tilde{G}_{0.25}$	$\tilde{G}_{0.5}$
`CSDN`	21.29	15.60	20.29
`Tianya`	22.28	15.01	19.39
`Duduniu`	22.42	19.10	21.52
`7k7k`	20.64	15.42	19.26
`Rockyou` [8]	*22.65*	*15.88*	*19.80*

Because of this reason, our major analysis results should be applicable to other user groups or helpful to understand the password reuses in other user groups. In addition, given that there are 668 million netizens in China [18], Chinese users do play a major role in the statistics and thus our findings in this paper are general and valuable.

5.3 Implications of Our Findings

Our empirical analysis can improve the efficiency of password guessing: First of all, when an adversary obtains a password and the corresponding email from a website, if there exist accounts on other websites registered with the same email, he or she is able to crack another account with a success rate of $33.16 \pm 8.91\%$. Second, if an adversary obtains the passwords of an account, the adversary would have the success rate of 59.72% to crack another account from the same user with a different username. Furthermore, the users tend to choose weaker but random passwords for accounts on the same website than the ones for another website. Thus, the adversary can leverage different guessing strategies to crack passwords on the same website or on another website given the knowledge of web password reuses. Finally, when an adversary guesses a different account on another website, the adversary may leverage the substring patterns of *prefix*, *suffix* and other patterns to improve the efficiency of guessing. Figure 4 shows that we can obtain an improvement of about 39.38% for guessing efficiency when we leverage patterns and use the weaker passwords to guess stronger ones.

That is, before guessing the password of a user account, an adversary can retrieve this user's other accounts to greatly improve the guessing efficiency, for the user will leave the shadow of the target password in other accounts. Although this attack method is common for many researchers, this paper offers a quantitative empirical view with a large scale of real data.

5.4 Security Suggestions

Managing passwords is still challenging, especially when the number of distinct passwords is large. Florencio *et al.* [19] even proposed that a user should reuse their passwords in similar accounts, because they argue that it is impossible for a user to remember so many passwords, and input them in correct user interfaces. We thus suggest:

- A user should have stronger security concerns to protect their accounts, especially some high-valued accounts, from the threat of ISPR and CSPR. For example, they should not reuse their passwords of some forum sites in their online banking accounts. Especially, some easy patterns, such as prefix, should not be applied yet. The two behaviors are both dangerous for the high-profit accounts.
- When a webmaster wants to measure the strength of passwords, he or she should consider the threat of ISPR and CSPR. That is, when a similar website

leaks their passwords, the relevant accounts should be notified and their passwords should be reset. The strength meters of passwords should also be designed partially based on the threat of these password reuses rather than passwords themselves [17].

- A password manager [20] could be a good helper to manage a large number of passwords, although some threats or vulnerabilities still exist [21][22]. In addition, multiple factors should be popular in the nearly future. Then the dynamic combination method of authentication factors might offer more user-friendly experiences [23].

6 Related Work

How to manage passwords is a hot topic in the areas of information security [24][25][26][9]. Passwords are one of the most sensitive data of users on websites. Howe *et al.* [27] studied the user behaviors of home computer users and pointed out many issues about passwords. Passwords usually suffer from various attacks [28], *e.g.*, phishing [29], dictionary attacks, heuristic password guessing, and even brute force attacks.

However, it is hard to conduct empirical studies on passwords [30][31], due to the absence of large amount of real-world passwords, specifically in cleartext. Morris *et al.* studied the password habits of Unix users, but their dataset only contains 3,289 users [1]. Gaw *et al.* [32] investigated the password management strategies for online accounts based on the study of 49 undergraduates. Yan *et al.* [30] researched the password memorability and security based on their user study on 288 students. Although Florencio *et al.* [3] reported a study of web password habits, the involved users were only 544K, and there were no detailed patterns and threat analysis of web password reuses in the literature. Finally, even though Das *et al.* studied the threat of password reuses, they only used 6,077 distinct accounts. Their datasets mainly include sites that serve English-speaking users.

Bonneau [8] studied almost 70 million `Yahoo!` users' passwords. With the availability of the large-scale passwords, the corresponding demographic factors, and account history factors, Bonneau was able to analyze the correlation between password strength and a few factors, which include genders, regions, and languages.

Kelly *et al.* [33] studied 12,000 actual passwords from several perspectives including the strength of passwords, the guessability of passwords against different password-guessing algorithms, as well as the correlation between the entropy of passwords and the strength of passwords. Their experiment results show that some password policies are superior to others against password attacks although they are treated as equally important. Their experiments also show the importance of the choice of dictionaries in improving the security of passwords.

Furthermore, Sharma *et al.* [34] conducted an empirical study on the strength of passwords with several state-of-the-art password attack methods. They proposed that each attack method has its strength in cracking passwords of certain strength. They also pointed out that the probability of guessing a correct password will decrease exponentially as the search space grows up, which is consistent with our experiment results.

One of the famous websites, `LinkedIn`, had approximately 6.5 million encrypted passwords stolen in 2012. A blog focused on cyber security [2] gave brief analysis on the decrypted passwords' length and the most common passwords used by LinkedIn users. Similarly, other blogs also gave their analysis of guessing the plain text of the passwords and the most commonly used passwords [3] [4].

Different from the above studies, this paper performed a large-scale empirical study on *2,671,443* distinct users whose passwords are in cleartext and each of whom has at least two passwords on one website, and *2,306,055* distinct users each of whom has at least two passwords across websites in China. The results from our study are interesting, highlighting the severe threat of web password reuses. Especially, different from the research of Das *et al.* (6,077 users), our research is a large-scale empirical study on web password reuses based on a large volume of passwords. Secondly, we examined the two types of password reuses: ISPR and CSPR, which were not mentioned in prior work. The rate of ISPR is greater than the upper bound of the rate of CSPR reported by Das *et al.*

Due to several issues associated with existing password schemes, many voices have called for password replacement or enhancement. Bonneau *et al.* [35] listed and described many ancillary means to replace the current password-based authentication mechanism. Florencio *et al.* [19] proposed that a user should group their accounts when he or she has many different passwords.

7 Conclusion and Future Work

To the best of our knowledge, this is the first empirical study on web password reuses by analyzing a large number of sample data. Although the web password reuses are known to researchers and Internet users, it is yet to perform a large-scale empirical study. We obtained *2,671,443* distinct users each of whom has at least two accounts from the same site, and *2,306,055* distinct users each of whom had at least two accounts from different websites. We also obtained *350,849* distinct users who has at least two accounts on the same site and across sites simultaneously.

We empirically studied the phenomenon of web password reuses (both ISPR and CSPR) utilizing the large password corpora, and manage to answer the five questions listed at the beginning of the paper (Section 1). The quantitative answers shed lights on the serious threat

[2] http://cyberarms.wordpress.com/2012/06/07/analysis-of-passwords-dumped-from-linkedin/

[3] http://boingboing.net/2012/06/07/preliminary-analysis-of-linked.html

[4] http://inavneetsingh.com/blog/internet/tips/30-worst-passwords-analysis-by-hacked-linkedin-passwords-infograph/

of web password reuses, i.e., password shadow attacks, where an adversary may attack an account of a user using the same or similar passwords of his/her other less sensitive accounts.

As a future direction, we would study CSPR from both adversaries' and defenders' points of view, leveraging the logs or activities that are available in the public domain. In addition, we will evaluate how the password policies affect CSPR after understanding the policies of these four websites. Last but not the least, we plan to study the impact of single sign-on tools on password reuses.

ACKNOWLEDGEMENT

This paper is supported by NSFC (Grant No. 61572136, 61472358). The authors would like to thank all anonymous reviewers for their insightful comments.

REFERENCES

[1] R. Morris and K. Thompson, "Password security: A case history," *Communications of the ACM*, vol. 22(11), pp. 594–597, 1979.

[2] A. Das, J. Bonneau, M. Caesar, N. Borisov, and X. Wang, "The tangled web of password reuse," in *NDSS'2014*, 2014.

[3] D. Florencio and C. Herley, "A large-scale study of web password habits," in *WWW'07 Proceedings of the 16th international conference on World Wide Web*, 2007, pp. 657–666.

[4] CSDN, "http://www.csdn.net/company/about.html."

[5] Tianya, "http://help.tianya.cn/about/history/2011/06/02/166666.shtml."

[6] Duduniu, "http://baike.baidu.com/view/1557125.htm."

[7] 7k7k, "http://www.7k7k.com/html/about.htm."

[8] J. Bonneau, "The science of guessing: Analyzing an anonymized corpus of 70 million passwords," in *2012 IEEE Symposium on Security and Privacy (SP)*, 2012, pp. 538–552.

[9] J. Ma, W. Yang, M. Luo, and N. LI, "A study of probabilistic password models," in *Proceedings of IEEE Symposium on Security & Privacy*, 2014.

[10] Z. Li, W. Han, and W. Xu, "A large-scale empirical analysis of chinese web passwords," in *23rd Usenix Security Symposium*. San Diego: USENIX, 2014.

[11] W. Han, Z. Li, L. Yuan, and W. Xu, "Regional patterns and vulnerability analysis of chinese web passwords," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 2, pp. 258–272, 2016.

[12] D. Wang, H. Cheng, Q. Gu, and P. Wang, "Understanding passwords of chinese users:characteristics, security and implications," https://www.researchgate.net/, July 2014.

[13] D. Schweitzer, J. Boleng, C. Hughes, and L. Murphy, "Visualizing keyboard pattern passwords," in *Visualization for Cyber Security, 2009. VizSec 2009. 6th International Workshop on*. IEEE, 2009, pp. 69–73.

[14] Wikipedia, "Levenshtein distance," http://en.wikipedia.org/wiki/Levenshtein_distance, May 2014.

[15] ——, "Longest common subsequence problem," http://en.wikipedia.org/wiki/Longest_common_subsequence, May 2014.

[16] J. the Ripper, "John the ripper password cracker," http://www.openwall.com/john/, May 2014.

[17] W. E. Burr, D. F. Dodson, E. M. Newton, R. A. Perlner, W. T. Polk, S. Gupta, and E. A. Nabbus, "Nist special publication 800-63-1 electronic authentication guideline," 2006.

[18] CNNIC, "The 36rd survey report on chinese internet development," http://www.cnnic.cn/hlwfzyj/hlwxzbg/hlwtjbg/201507/P020150723549500667087.pdf, July 2015.

[19] D. Florncio, C. Herley, and P. C. van Oorschot, "Password portfolios and the finite-effort user: Sustainably managing large numbers of accounts," in *23rd USENIX Security Symposium (USENIX Security 14)*. San Diego, CA: USENIX Association, Aug. 2014. [Online]. Available: https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/florencio

[20] R. Chatterjee, J. Bonneau, A. Juels, and T. Ristenpart, "Cracking-resistant password vaults using natural language encoders," in *2015 IEEE Symposium on Security and Privacy, SP 2015, San Jose, CA, USA, May 17-21, 2015*, 2015, pp. 481–498. [Online]. Available: http://dx.doi.org/10.1109/SP.2015.36

[21] Z. Li, W. He, D. Akhawe, and D. Song, "The emperor's new password manager: Security analysis of web-based password managers," in *23rd USENIX Security Symposium (USENIX Security 14)*. San Diego, CA: USENIX Association, Aug. 2014. [Online]. Available: https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/li_zhiwei

[22] D. Silver, S. Jana, D. Boneh, E. Chen, and C. Jackson, "Password managers: Attacks and defenses," in *23rd USENIX Security Symposium (USENIX Security 14)*. San Diego, CA: USENIX Association, Aug. 2014. [Online]. Available: https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/silver

[23] W. Han, C. Sun, C. Shen, C. Lei, and S. Shen., "Dynamic combination of authentication factors based on quantified risk and benefit," *Security and Communication Networks*, no. 7, p. 385C396, 2014.

[24] P. Wang, Y. Kim, V. Kher, and T. Kwon, "Strengthening password-based authentication protocols against online dictionary attacks," in *ACNS'05 Proceedings of the Third international conference on Applied Cryptography and Network Security*, 2005, pp. 17–32.

[25] K. P. Yee and K. Sitaker, "Passpet: convenient password management and phishing protection," in *SOUPS'06 In Proceedings of the second symposium on Usable privacy and security*, 2006, pp. 32–43.

[26] Q. Yan, J. Han, Y. Li, and R. H. Deng, "On limitations of designing usable leakage-resilient password systems: Attacks, principles and usability," in *Proceedings of 19th Annual Network & Distributed System Security Syposium (NDSS 2012)*, 2012.

[27] A. Howe, I. Ray, M. Roberts, M. Urbanska, and Z. Byrne, "The psychology of security for the home computer user," in *2012 IEEE Symposium on Security and Privacy (SP)*, 2012, pp. 209–223.

[28] T. Holz, M. Engelberth, and F. Freiling, "Learning more about the underground economy: A case-study of keyloggers and dropzones," in *ESORICS'09 Proceedings of the 14th European conference on Research in computer security*, 2009, pp. 1–18.

[29] G. Xiang and J. I. Hong, "A hybrid phish detection approach by identity discovery and keywords retrieval," in *WWW'09 Proceedings of the 18th Internation Conference on World Wide Web*, 2009, pp. 561–570.

[30] J. Yan, A. Blackwell, R. Anderson, and A. Grant, "Password memorability and security: empirical results," *IEEE Security Privacy*, vol. 2, no. 5, pp. 25–31, 2004.

[31] S. Ji, S. Yang, X. Hu, W. Han, Z. Li, and R. Beyah, "Zero-sum password cracking game: A large-scale empirical study on the crackability, correlation, and security of passwords," *IEEE Transactions on Dependable and Secure Computing*, 2016. [Online]. Available: http://dx.doi.org/10.1109/TDSC.2015.2481884

[32] S. Gaw and E. W. Felten, "Password management strategies for online accounts," in *SOUPS'06 Proceedings of the second symposium on Usable privacy and security*, 2006, pp. 44–55.

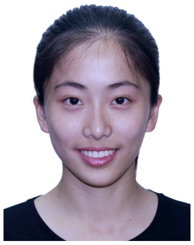
[33] P. Kelley, S. Komanduri, M. Mazurek, R. Shay, T. Vidas, L. Bauer, N. Christin, L. Cranor, and J. Lopez, "Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms," in *2012 IEEE Symposium on Security and Privacy (SP)*, 2012, pp. 523–537.

[34] R. Sharma, A. Datta, M. DeH'Amico, and P. Michiardi, "An empirical study of availability in friend-to-friend storage systems," in *2011 IEEE International Conference on Peer-to-Peer Computing (P2P)*, 2011, pp. 348–351.

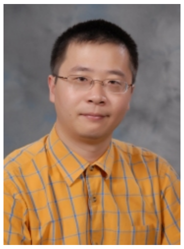
[35] J. Bonneau, C. Herley, P. van Oorschot, and F. Stajano, "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes," in *2012 IEEE Symposium on Security and Privacy (SP)*, 2012, pp. 553–567.

Weili Han (M'08) is an associate professor at Fudan University. His research interests are mainly in the fields of Access Control, Digital Identity Management and IoT security. He is now the members of the ACM, SIGSAC, IEEE, and CCF. He received his Ph.D. at Zhejiang University in 2003. Then, he joined the faculty of Software School at Fudan University. From 2008 to 2009, he visited Purdue University as a visiting professor funded by China Scholarship Council and Purdue University. He serves in several leading conferences and journals as PC members, reviewers, and an associate editor.

Zhigong Li is a graduate student with Software School, Fudan University. His research interests focus on password security, systems security.



Minyue Ni is a graduate student with Software School, Fudan University. Her research interests focus on systems security, visualization.



Guofei Gu is an associate professor in the Department of Computer Science & Engineering at Texas A&M University. He received his Ph.D. degree in Computer Science from the College of Computing, Georgia Tech, in 2008. He is a recipient of 2010 NSF CAREER Award, 2013 AFOSR Young Investigator Award, Oakland'10 Best Student Paper Award, and ICDCS'15 Best Paper Award. He is currently directing the SUCCESS (Secure Communication and Computer Systems) Lab at TAMU. His research interests are in network and system security, software-defined networking (SDN) security, and mobile/smartphone security.

Wenyuan Xu is a professor in the College of Electrical Engineering at Zhejiang University. She received her B.S. degree in Electrical Engineering with the highest honor from Zhejiang University in 1998, an M.S. degree in Computer Science and Engineering from Zhejiang University in 2001, and the Ph.D. degree in Electrical and Computer Engineering from Rutgers University in 2007. Her research interests include wireless networking, network security, and embedded system security. Dr. Xu received the NSF Career Award in 2009. She has served on the technical program committees for several IEEE/ACM conferences on wireless networking and security, and she is an associated editor of EURASIP Journal on Information Security.