Longfei Xi ([redacted])

A Hash-Based Password Management System

Abstract

From past to present, password management is always a popular topic in information and Internet security. There is always a contradiction between safety and convenience regarding password management. Using strong passwords, instead of convenient but easy-to-guess passwords, is strongly recommended by many parties to ensure the safety of informational assets. However, it is usually not convenience for users to remember and use strong passwords, especially in the cases when strict password policies are being used. Users tend to use inappropriate practices to try to ease the burdens regarding passwords, which usually pose security risks. A lot of unique security products exist to try to solve this problem. However, they either have high costs, or are not yet usable for production environments.

Regarding this challenge, this proposal tried to present a different way of password management system design, with the consideration of adapting to different situations in which the passwords are used. This design utilizes three core pieces of data (keyword, personal salt, random salt) and four core algorithms (salt insertion algorithm, hashing algorithm, password string extraction algorithm, and an optional special character insertion algorithm) to generate strong passwords. These algorithms provide a way to make passwords adapt to various situations that have different password requirements, while keeping complexity and strength of passwords.

The design ensures the safety of passwords by creating and storing all data in different manners, utilizing only basic human memories and standard security features to migrates and scatters the common risks of password management and avoid single point of failure. This design also provides a way to quickly replace current passwords with new one in urgent situations like undergoing data leaks or attacks. Moreover, the design is flexible enough to be able to integrated with existing solutions. Any systems that have ways to extend over the existing authentication mechanisms can utilize the proposed design to provide a simpler login and authentication experience.

With all the facilities, this design attempted to find an optimized balance point between the information safety and user convenience. An implementation from the design allows a user to effectively use different strong and secure passwords in different situations without burdens of memorizing and managing excess load of information.

Introduction

A hash-based password management system utilizes several pieces of data, managed by both users and organizations (in enterprise environments) or solely users (in single-user environments), to generate passwords for different situations. All the generated passwords are strong, secure, but also unique to what the data are given as inputs describing the scenarios of password uses. This system is an attempt to solve the existing problem that strong passwords are hard to remember and to ease the burdens on user's side. To understand how and why the system is designed as is, a brief introduction of the development of passwords and password management techniques is necessary.

Longfei Xi ([redacted])

Text-based passwords have been widely used as a method of authentication for a long time. People use passwords to protect their own sensitive information, and to gain access to certain services or information that is hosted by third parties. Nowadays, an individual probably has multiple passwords for different purposes, such as a PIN (Personal Identification Number) for accessing its bank account information, a password to access its social accounts on the Internet, to access the resources in school's learning system, or to log into the internal network of an organization. No matter what purpose is, it is reasonable to expect that a certain service or resource that involves sensitive information, which is related to a person's identity or properties in any forms, is protected by passwords. Even though the biometrics-based authentication started to become more and more popular, and the two-factor authentication integrating with personal mobile devices and other mechanisms is getting recommended to use in many situations, text-based passwords will still be the main mechanism of authentication in a long, foreseeable time period, thanks to its easy implementation as a part of security control. This applies to creation and replacement of passwords, which are both low-cost activities compared to other authentication methods [Shay et al. 2010; Inglesant and Sasse 2010].

Because of the important role the passwords act in modern computing and information infrastructure, they are the most obvious targets wanted by attackers who seek for access to resources and services maliciously all over the world. Hence, it is crucial for all the individuals and organizations to ensure the safety of the passwords in order to protect their information assets. There are many articles, documents, and guidelines regarding information security having introduced secure password best practices, such as using long and complex passwords instead of short and easy passwords to make passwords hard to guess, and using different passwords in different places to prevent massive compromises when having a data breach. Some publications also described more systematic and advanced password practices for enterprise environment, such as setting up the password complexity, password expiration, and lockout policies within a system or an organization [Karen (Karen Ann) Kent 2009]. For the users who need to access services and resources containing sensitive information, and the hosts who provide them, these practices are supposed to help them enhance the safety regarding information storage, processing, and transmission.

However, even though these best practices have been released in public domain for many years, and supposed to make the information technologies more secure, there are still a lot of indications showing the opposite facts because of poor security practices. One of them is the use of weak passwords consisted of common dictionary words and personal information. Many users tend to use weak passwords because they feel the strong passwords are too complicated to remember, and such passwords cause them a lot of inconveniences, especially in the occasion when a single user has to use multiple passwords in different places [Shay et al. 2010; Herley 2009; Laptyeva et al. 2011; Stobert and Biddle 2014]. A strong and complicated password is also hard to type. This could annoy the user in a busy learning or working environment. Another issue represents the poor security is the use of same passwords in different places to reduce the burden of remembering [Shay et al. 2010; Stobert and Biddle 2014]. It increases the risk and the area of data compromises greatly, regardless of the password complexity, if passwords were stolen by attackers or a massive data breach on the Internet happened.

For the users who are in an environment that has enforced the password policies and used complicated and strong passwords, the risks posed by weak passwords can be avoided. However, complicated passwords may cause unexpected changes of user behaviors, which could also put the information systems in danger. They include writing down passwords onto paper or saving them in a computing device, and sharing or reusing the same passwords among different people or departments [Shay et al. 2010]. It creates the window for social engineering attacks and increases the risk of breach in the organization. Additionally, if high-frequency password expiration policy is applied, the users also may not be able to remember the passwords very well. It increases the cost of the organization, because the needs of resetting passwords often cause higher workload of IT administrators and interruptions on normal task [Shay et al. 2010].

All these issues reflect the conflicts in reality between the information safety posed by the strong and complicated passwords and the user convenience. This indicates the importance of password management. Password management is a crucial part of information and Internet security, and has been discussed over the years [Karen (Karen Ann) Kent 2009; Stobert and Biddle 2014]. There are already several mature password management systems in information security market, which are usually named password managers. Most of them provide features like password list by different websites or applications, random password generator, password safe or vault, automatic form filling, automatic login, and cloud-based synchronization [Siber Systems, Inc. n.d.; LastPass n.d.; Symantec Corporation n.d.]. Even though these systems try to reach the balance between safety and convenience for users, they still have issues. Users must input all their passwords manually, and depend on these third-party applications to have access to them. Also, even though the cloud-based synchronization among different devices makes the use of passwords more convenient, it raises up the question of the safety on these cloud services themselves. This is especially important in enterprise environment, since there are few ways to know if the passwords were securely stored and they would not be seen by others or not. The password manager apps on the devices themselves also may have vulnerabilities, such as program bugs, open to attackers. Thus, they may not be a good solution from information safety perspective.

Some new developments utilize different mechanisms to try to ease the difficulty of strong passwords. For example, pictures can be used to replace the text-based passwords, or assist the creation of the password text [Stobert and Biddle 2014; Zach Pace, Steven Sinofsky n.d.]. This is based on the fact that the characteristics of meaningful pictures are easier to remember than plain text passwords without meanings [Stobert and Biddle 2014]. However, while picture-assisted passwords are much safer, such forms of passwords are not widely used yet, due to the complexity in implementations and the hardness of integrations with other systems. Hence, for most systems, addressing the issues around text-based passwords is still an emphasis in information safety fields.

Regarding the issues described above, which focus on making passwords secure without burdens of memorizing, this paper proposes a password management system based on hashing algorithms, coordinated with selection and insertion algorithms during the password generation process to attempt to achieve the balance of safety and convenience. This system uses three pieces of information: keyword, personal salt, and random salt, with a selected password length.

Utilizing all pieces of information as the input of a series of algorithms performing salt insertion, hash, symbol insertion, and selection operations, it is able to generate a password that is strong but unique by keyword and salt information. Users can choose long meaningful sentences as keyword and personal salt. This enables a user to ease the burden of remembering passwords, but still maintains the information safety in a high standard. It also can prevent the use of same passwords in different places. For organizations, this system provides large enough varieties for different purposes by different combinations of keywords and salts. The only stored data is the random salt, and other information is depending on personal memories or other forms of management. In emergency situations or yearly routine practices, the organization can replace the whole set of passwords all in once by changing the salts, which simplifies the IT management work. Since the system is a local system, it is not depending on any cloud or online services. Using a hash algorithm that is sensitive to input changes, having partial information will not lead to the actual passwords. Hence, it disperses the source of risks of data compromises and enhances information safety within the organization.

This paper is organized as follows. The next section performs a review on the related work addressing password security issues, existing solutions, and the base algorithms of the proposed system. Then, it follows the structure and design of the system, as well as the description of the different algorithms. Finally, the objectives and expect results from password security tests on complexity and duplication will be discussed.

Literature Review

Users are the weakest link in security [Herley 2009]. This has been proved by many research studies in information security over the years. Passwords are mainly designed to be used and managed by humans, hence a large portion of the security of passwords directly depends on its user's behaviors. In theory, it is expected for users to be fully aware of the security issues and know how to use or manage passwords properly, so that the information security can be achieved and ensured. This is a viewpoint that password security is a responsibility of users. However, this is just a perfect condition that is impossible to reach. In reality, it is more complicated than such a perfect condition. In order to maintain security of information with passwords, it is not feasible and safe for an organization to solely rely on its users to achieve security without any external measurements [Ur et al. 2016]. These measurements include best or recommended security practices, policies, standards, procedures, and actual hardware or software regarding the management of organization's information and passwords. Many agree that these measurements greatly helped organizations and users to manage their passwords and information in a practical and reasonable way, and many professionals treat these measurements as effective ways to establish information security.

However, even the external measurements can be much more complicated than what they look like in a glimpse. It is surprising and interesting to see a lot of unexpected effects and feedbacks to and from the users who use and manage passwords, because of some parts of measurements that seem reasonable but are impractical to implement or incorporate in reality [Herley 2009]. Some of them may even lead to new security vulnerabilities, which are against the original purposes of these measurements. Regarding such unexpected effects and feedbacks, many recent research studies continued to dig into the origins, trying to find their patterns and derive

solutions from them. At the same time, due to the awareness of the challenges of password management for individuals and organizations, some major players of password management existed in the security markets, most of which are commercialized password managers, also evolved to address the issues from these unexpected effects and feedbacks related to password users. However, such password managers also have their own weakness and disadvantages need to be solved, because they only addressed non-human factors of password management issues. As users continue to use passwords as main ways of authentication, users are still the weakest link in information security.

In this section, a list of research studies and related works related to the root of password management will be discussed. The following paragraphs will introduce them by their focusing topics, which are categorized as: password management practices in personal and enterprise environments, password complexity and strength, user factors for password management, and password policy and its side effects.

Password Management Practices

There are many resources providing guidelines and instructions about the best practices of password management formally or informally. Among them, NIST released a very comprehensive guide regarding password management in enterprise environment [Karen (Karen Ann) Kent 2009]. Even though it was in draft form and not an officially released document, it provides a comprehensive introduction of passwords and password management and lays a solid foundation on common practices regarding password security. To organizations and people who emphasize the importance of information security, it is clear that password management takes a critical role in protecting sensitive information and valuable resources. In specific, password management helps individuals and organizations maintain confidentiality, integrity, and availability of passwords, so that authorized users can use passwords to access the information and resources they need successfully, while preventing unauthorized users from seeing or using them. It includes a number of security controls and procedures as well as policies and standards to achieve such a goal. The NIST guide indicates, however, that it may be challenging to establish strict rules, such as making users use strong and complex passwords. Such rules may cause inconvenience to users, which instead increases risks of insecure password storage [Karen (Karen Ann) Kent 2009, p.12]. Hence, even though best practices can help enhance the information security, the balance between security and user convenience still must be put into consideration when implementing these practices as policies or standards.

The NIST guide on password management also introduces the strategies to migrate the common risks associated with passwords, which summarizes the common used and secure ways to handle passwords in various situations. One common risk is that passwords can be captured in storage or during the transmission. Also, they can be captured from careless users. The storage and transmission involves encryption. The transmission also involves using secure tunnels between two parties. Other than them, users can be the cracks to initiate a password capturing, such as using social engineering means. A number of solutions are available for such attacks, even though some of them involve other aspects of internal management within the organization or individual's matters [Karen (Karen Ann) Kent 2009, pp.14–17]. They fall into the categories of enhancing IT infrastructure by using secure technologies and algorithms, and enhancing user educations.

Another risk can be the password cracking, which is directly related to password complexity and strength. The guide provides some common ways to prevent such attacks, like setting up a password with enough complexity and length by certain standards, and avoid using common words or personal information [Karen (Karen Ann) Kent 2009, p.17]. Especially, the guide provides a usable mean to measure password strength [Karen (Karen Ann) Kent 2009, pp.19–21], and several practical methods to make passwords more complex while still being easy to remember [Karen (Karen Ann) Kent 2009, pp.21–23]. Additionally, to prevent attacks from outside, the guide also touches the configuration of operating systems. Particularly, it is recommended to change all the default passwords existing in a system. Regarding enterprise environments, the guide also discusses some unique issues about local administrator passwords. For such passwords, it is recommended to use random password generation based on network interface addresses, and utilize central password storage to ensure their safety from unauthorized use The guide also discusses about the password recovery and password expiration policies in general, providing guidelines to prevent hackers from performing brute-force or other forms of attacks based on these mechanisms [Karen (Karen Ann) Kent 2009, pp.24–28].

In the end, the guide introduces and compares several password management solutions, including single sign-on, password synchronization, and local password management, from usability perspective [Karen (Karen Ann) Kent 2009, p.32]. In summary, single sign-on method has its advantage of reducing user's burdens on password management and authentication, but it is expensive to implement due to the requirements of multiple authentication servers. And it has the risks of man-in-the-middle attacks if system was implemented incorrectly [Karen (Karen Ann) Kent 2009, p.29]. Password synchronization, otherwise, is less expensive and easier. But it has the risk of single-point failure, i.e. a single password used on multiple locations, which if leaked, a significant amount of compromises would happen. It also has a potential problem that is utilizing "lowest common denominator" approach to guess the password strength, which different location's password requirements could yield the lowest password strength available to users, so that hackers could use the information to plan attacks [Karen (Karen Ann) Kent 2009, p.30]. The last method, local password management, utilizes password manager software. While it is convenient for users to use in many situations, some security considerations must be made regarding master passwords and software designs themselves, because the overall security of password storage depends on the software design. Once used, the organization or person must live with software whenever they need to access the passwords. It may pose additional costs. Also, the guide indicates that password managers cannot prevent attacks by key loggers or compromised machines[Karen (Karen Ann) Kent 2009, pp.30–31]. Some hardware-form password mechanisms are also discussed in the guide as an appendix [Karen (Karen Ann) Kent 2009, pp.33–34].

As a summary, this guide provides lots of information to help organizations plan for their security infrastructure and measurements and migrate potential risks.

Password Complexity and Strength

As a comprehensive material, the NIST guide to enterprise password management provides easy methods to estimate a password's strength and its hardness to be cracked. For ideal situations, which the characters in a password has equal probability to be used, a table of comparison of

password strength in different character sets and lengths is shown. However, the guide also indicates that in practical cases, the probability of each character to be shown is not equal [Karen (Karen Ann) Kent 2009, p.20]. Hence, some human factors, such as user's interests, contribute to the complexity of password strength measurements.

This guide also provides several methods for users to make a strong password while keep them easy to remember. It is noticeable that the provided methods were for public comments. But they still provide guidelines on how to convert an easy-to-remember phrase or word into a strong password. The guide also indicates the disadvantages of these methods, particularly the vulnerability to brute-force or social engineering attacks and hardness of remembering [Karen (Karen Ann) Kent 2009, pp.21–23].

In summary, the NIST guide provides basic information about password complexity. However, there are more research papers covering the topic. A formal framework to measure password complexity and strength is available [Sahin et al. 20151217]. Specifically, password complexity is defined as the size of the set that contains smallest amount of alphabets by combining and using the rules given. And password strength is defined as FAT-strength based on FAT-Security Experiment, which attempts to output an analogous finite string within time threshold over the given alphabets and rules.

In addition, recently password guessability is also being used in some research studies as a metric to password complexity, which represents the ability of resisting guessing cracks from specific password crackers using certain training data, quantitatively in a metric form of guess number, i.e. the number of guesses the password cracker takes under certain condition [Mazurek et al. 2013]. These metrics of password complexity and strength lays down a foundation for the further research studies regarding password management issues.

User Factors in Password Management

Many password management issues have user factors involved. There are several research studies focusing on such factors. One factor is the user perception of password security. According to Ur et al., because of the wide user education on password security in recent years, it is a surprise that users' perceptions on password security match the development of password cracking, which overturn the common sense that users did not know much about password security. However, users still have unrealistic expectations on some aspects, such as the emphasis of password length increase and the uses of common phrases. Many users do not realize how popular some inappropriate behaviors and practices about passwords are over the crowd. This seems to be one of the root causes of bad password creations. Also, it leads to difficulties for users to understand the true image of forms of password cracking and attacks [Ur et al. 2016].

Another user factor, which is more important, is the attention to information users received. Depending on individuals, it may be the case that users mainly focus on their primary tasks and make compromises on unrelated affairs. From a perspective of cost, because a user has limited resources like money and time, the user must choose to do things that bring the maximum benefits corresponding to the cost. This is mostly an implicit process. Hence, when users have primary tasks, it means that such tasks will bring them maximum benefits. Password security,

for most users, is not one of such tasks. A research study shows that for different groups of entities, the direct costs and indirect costs of online financial frauds are different. While such frauds have direct and indirect costs on victims and banks, for non-victim users, there is no direct cost, but indirect cost of user education applies. When educating users about online financial frauds, an important part of it is the password security, since modern financial assets are mostly protected by various forms of passwords. The study indicates that, users may consider about the information they received, and choose to pay attention to specific one, based on the cost assessments in mind [Herley 2009]. If expands the cost perspective further, the user perception of password security can also be regarded as a representation and a result of cost assessments, due to the fact that an individual can only learn a limited set of information, while the total amount of information may be close to unlimited.

Password Policies and Side Effects

Because of the existence of user factors, password policies may lead to unexpected results. Recently, a lot of research studies become aware of the impractical password policies and their effects. Herley's research study focus on the cost. From the perspective of cost assessment, users may reject to put such policies into practice, because the indirect cost for them is high, even though such policies are designed for protect users from paying direct costs for data asset losses. In other words, the direct cost due to the loss of information assets is much less than the indirect cost from the efforts users have to take to meet the requirements of password policies. In order to prevent security leaks, password policies in an organization usually cover aspects such as password strength and ways of password handling. The result of such policies is to make users create unique, complicated but secure passwords and memorize them. This definitely creates pressures on user's side in addition to the main tasks. Even though they may have benefits, like password strength policies for better protection of information assets, the amount becomes very little after the policies exceed the minimum requirements and cooperate with lock-out systems. Hence, to make policies productive, it is better to understand the extent of actual harms, which are different from worst-case scenarios. Based on this understanding, user education should be controlled within a certain rate consistent with actual harms. Rather than enforcing password policies on users, it is better to prioritize the best practices and advices to users to ease the burden caused by indirect costs. When creating password policies, it is necessary to analyze the actual risks and threats, as well as putting user's time and efforts into consideration [Herley 2009].

The cost of password policies becomes clear when user factors are put into consideration. According to Inglesant and Sasse, there is a conflict between password policies or requirements and user' needs. Also, changing a password, making a password according to compliances, remembering a password, or even situations after forgetting a password create burden on users. Hence, users may treat them as interruptions. Users know some extent of password security, but they do not always know the best ways to manage, because the cost of password policies depends on the context within the organization. A policy that works in an organization may not fit other organizations due to the difference of contexts. Hence, a policy emphasizing password strength and changing frequencies may be inappropriate to help password security while keeping users productive in an organization [Inglesant and Sasse 2010].

Longfei Xi ([redacted])

Conclusion

As a conclusion to related research studies, the password management policies provided by NIST are comprehensive, and represent commonly praised knowledge regarding password security by many researchers and professionals. Especially, password complexity and strength are well regarded as important factors for password security. However, such policies do not make password security fully established automatically, because as the weakest link of the security, users and their behaviors also play an important role. Because of user factors, it is possible that an inappropriate password security policy that is supposed to protect the information assets can yield opposite results, i.e. users tend to use insecure ways to try to meet the requirements of the policy. Thus, when establishing policies and associated guidelines or procedures, it is crucial to know the needs of users and the whole organization to avoid the side effects of inappropriate policies and maximize the benefits of password security practices.

Methods

In this section, a password generator design will be proposed and explained in detail. Also, a set of general measurements and data analysis steps of password strength and complexity verification will be discussed for the purpose of password generation performance evaluations. By using them, it is possible to verify the strength and complexity of generated passwords from the proposed password generator, and get a clear idea about how different components in the password generator corporate.

Ethical Considerations

To protect the privacy and meet the compliances, all the tests of password generations and strength / complexity evaluations will be performed in test environments instead of production environments. During the process, no real personal information will be collected, saved, and used. A set of input data will be specially designed to ensure the validity of test results while avoiding using personal information in reality.

Data Subjects

The proposed password generator design focuses on two types of data. One is the inputs to the password generator to generate a password. They contain the following data fields:

- Keyword
    - A user-selected phrase, usually representing or describing an entity, a location, or a purpose which the password is used for. Despite the name "keyword", its length is not limited to word's length. Users of the password generator can select and use anything they feel comfortable and easy to remember for this field. The input in keyword field will be used as a base to the input of hashing algorithm to get generated passwords as a result.
    - For example, a user can use the sentence “The quick brown fox jumps over the lazy dog” as the keyword. A web address such as “https://www.youtube.com/” is also acceptable.
- Personal Salt
    - A user-selected phrase, same as keyword. The difference between them is that personal salt is supposed to be used to identify the user itself, and be hidden from others. The role of personal salt is similar to PIN codes. However, the

purpose of personal salt is to provide randomness to keyword using salting algorithm before perform hashing operations.

Both keyword and personal salt are not limited to English. Because they are designed to be Unicode strings, any languages supported by Unicode can be used as well.

- Random Salt
    - A computer-generated string without semantic meanings. The length can be adjusted, but at least 64 characters. It is different from personal salt due to its characteristic of auto-generation. Random salt will randomize the keyword further in addition to personal salt. But a more important reason to have two types of salts is the consideration of centralized password management. An organization could replace random salt to replace all passwords without user's involvements. The random salt can be automatically updated to users' devices. Users can still use their keywords and personal salts to access the system without interruptions.

All these data will go through the following algorithms, listed below by processing order:

- Salting Algorithm: Mix keyword with salts. One example is to insert characters of salts into keyword at certain positions, calculated by selected password length
- Hashing Algorithm: Get hash value from result from salting algorithm, such as SHA-2 algorithm set
- Cropping Algorithm: Pick characters based on given password length by users, and capitalize some of them randomly
- Special Character Insertion Algorithm: This is an optional step. If used, this algorithm will replace some characters with special characters in the result from cropping algorithm. This is for the adaption of different situations, since some places are not allowing special symbols as a part of passwords

The result of these input data is the generated password, which is generated by a series of steps with algorithms involved. The password strength and complexity evaluation and verification measurements introduced below will focus mainly on the generated passwords.

Test Preparations

The test presented in this proposal focus mainly on password strength and complexity. A set of input data based on a common organizational structure will be designed for the proposed password generator performance evaluation. The input data will cover two basic user roles: administrators and normal users. It is also possible to add other roles into the input.

The test input data will have a uniformly distributed data set, mixing with following characteristics:

- Keyword: Same amount of words and sentences
- Personal salt: Same as keyword
- Random salt: Minimal size (64 characters) and extended size (128 characters)

And the algorithm choices will be:

- Salting Algorithm: Alternatively select characters, one at a time from keyword, personal salt, and random salt
- Hashing Algorithm: SHA-1 and SHA-2 (SHA256 and SHA512)
- Cropping Algorithm: Based on given password length, choose characters at certain locations from the result of salting algorithm
- Special Character Insertion Algorithm: Insert special characters based on given password length, then crop the result to remove redundant characters

Also, the target password length will be set to reflect the use in reality, i.e. 8-20 characters. In the evaluation, the target lengths will be chosen by 2, i.e. 8, 10, 12, 14, 16, 18, 20 characters.

Lastly, to formally evaluate the performance of password generator, a set of rules will be set as the input of evaluation framework indicated in [Sahin et al. 20151217]. Such inputs include:

- Minimum and maximum allowed password length in a simulated organization
- Rules of passwords and their priorities
- Other necessary restrictions apply to passwords

In evaluation, the generated passwords will also be one part of inputs to the evaluation functions.

Protocol Design

The performance evaluation will be performed as follows:

1. Choose at least 20 words and 20 sentences, which describe common entities a person usually will use
2. Cut words and sentences half and assign as candidates of keyword and personal salt
3. Generate random salts to match the amount of candidates of keyword and personal salt, each with two forms: minimal size (64 characters) and extended size (128 characters)
4. Form combinations of keyword, personal salt, and random salt from the candidates by randomly choosing. Form at least 40 combinations with uniformly distributed keyword, personal salt, and random salt choices
5. Use proposed password generator to generate result passwords by target password lengths (8-20 characters, stepping by 2)
6. Measure password lengths and analyze the data to evaluate password generator's performance

Measurements and Calculations

The performance of proposed password generator will be based on the strength and complexity of result passwords. A common password checker (for example, https://howsecureismypassword.net/) will be used to check if the generated passwords are secure. Furthermore, a more precise measurement definition of password strength and complexity will be used, based on [Sahin et al. 20151217]. Specifically, in such framework, the passwords and the set of rules in preparation phrase will be used as inputs in the framework described in the paper to get results of password complexity and strength data. All the result data will be evaluated and analyzed independently.

Data Analysis

The result data will be analyzed to check following aspects:

- The average strength and complexity of passwords generated
- The existence of weak generations, i.e. a certain generated password is weaker than other generations
- The effects of results using different algorithms but same data inputs

Each password will get two types of result data. One is the result from the password checker, and another one is from the formal password strength and complexity framework's outputs. All the data will be combined and analyzed altogether in order to find the inner relations between password strength and complexity indications and numeric data.

Future Work

Some additional tests may be performed to evaluate the proposed system further. Such tests may include the following categories:

- Algorithm: this is to find out the best combinations of algorithms that make the generated passwords secure while being efficient on performance of computation
- Usability: a conduction of user interaction experiments may contribute to this category in order to validate the actual uses in real environments
- Integration: the system is designed to be flexible and is supposed to be able to integrate with any systems that have extensibility on authentication. However, further tests and evaluations are needed to find out the optimal ways of implementations of the design and algorithms involved
- Weakness: although the system is designed with considerations of safety, it is still possible to have weaknesses. More tests and evaluations may help find such weaknesses on design itself and the generated passwords. Also, it may also help evaluate if reverse cracking is possible for the system (i.e. using only partial data, such as a generated password with one type of salts, to get other ones that can lead to other generated passwords)

Summary

Through the design and measurements described above, it is expected to see the structure of proposed password generator, and how different components corporate to generate passwords based on inputs. The performance of the password generator regarding the strength and the complexity of generated passwords will be also evaluated in a formal way. The methods presented above are focusing on the results of password generator. However, more aspects such as the integration of proposed password generator into existing system may also be worthy as directions of further work.

References

1. Cormac Herley. 2009. So Long, and No Thanks for the Externalities: The Rational Rejection of Security Advice by Users. In *Proceedings of the 2009 Workshop on New Security Paradigms Workshop*. NSPW '09. New York, NY, USA: ACM, 133–144. DOI:https://doi.org/10.1145/1719030.1719050

2. Philip Inglesant and M. Sasse. 2010. The true cost of unusable password policies: password use in the wild. (2010), 383–392. DOI:https://doi.org/10.1145/1753326.1753384

3. Karen (Karen Ann) Kent. 2009. *Guide to enterprise password management (draft): recommendations of the National Institute of Standards and Technology* Draft., Gaithersburg, MD: USDeptof Commerce, National Institute of Standards and Technology.

4. T.V. Laptyeva, S. Flach, and K. Kladko. 2011. The weak-password problem: Chaos, criticality, and encrypted p-CAPTCHAs. *EPL Europhys. Lett.* 95, 5 (2011), 50007. DOI:https://doi.org/10.1209/0295-5075/95/50007

5. LastPass. Features | LastPass. Retrieved December 3, 2016 from https://lastpass.com/features/

6. Michelle L. Mazurek et al. 2013. Measuring Password Guessability for an Entire University. In *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*. CCS '13. New York, NY, USA: ACM, 173–186. DOI:https://doi.org/10.1145/2508859.2516726

7. Cem S. Sahin, Robert Lychev, and Neal Wagner. 20151217. General Framework for Evaluating Password Complexity and Strength. (20151217).

8. Richard Shay et al. 2010. Encountering Stronger Password Requirements: User Attitudes and Behaviors. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*. SOUPS '10. New York, NY, USA: ACM, 2:1–2:20. DOI:https://doi.org/10.1145/1837110.1837113

9. Siber Systems, Inc. RoboForm Features. Retrieved December 3, 2016 from https://www.roboform.com/features

10. Elizabeth Stobert and Robert Biddle. 2014. A Password Manager That Doesn'T Remember Passwords. In *Proceedings of the 2014 Workshop on New Security Paradigms Workshop*. NSPW '14. New York, NY, USA: ACM, 39–52. DOI:https://doi.org/10.1145/2683467.2683471

11. Symantec Corporation. Password Manager & Online Identity Security | Norton Identity Safe. Retrieved December 3, 2016 from https://identitysafe.norton.com/

12. Blase Ur, Jonathan Bees, Sean M. Segreti, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2016. Do Users' Perceptions of Password Security Match Reality? In *Proceedings*

of the 2016 CHI Conference on Human Factors in Computing Systems. CHI '16. New York, NY, USA: ACM, 3748–3760. DOI:https://doi.org/10.1145/2858036.2858546

13. Zach Pace, Steven Sinofsky. Signing in with a picture password. Retrieved December 3, 2016 from https://blogs.msdn.microsoft.com/b8/2011/12/16/signing-in-with-a-picture-password/