Scientific and Practical Cyber Security Journal (SPCSJ) 1(2):1-6
Scientific Cyber Security Association (SCSA), 2017 ISSN: 2587-4667

PASSWORDS AS A MEANS OF PROTECTION IN ORGANIZATIONS

O. Kovalchuk

Kyiv National University of Trade and Economics

ABSTRACT

Personal data of users is subject to damage, viruses, natural disasters, theft. Digital thieves are constantly looking for vulnerabilities that will allow them to steal valuable data. Attempts to steal information have different purposes: some scammers get money from bank accounts or credit cards, and others can sell information to a third party. The password is the simplest and cheapest way to authenticate. Restrictive password policies can cause some user actions, such as writing passwords, reusing them for different accounts, or sharing passwords with friends, can compromise security. The password security policy should balance directly between security and ease of use. The article proposes the worked out recommendations for the balance of security and user convenience.

KEYWORDS: password, security, organizations, protection, usability.

РЕЗЮМЕ

Персональные данные пользователей подвержены повреждениям, вирусам, стихийным бедствиям, кражам. Цифровые воры постоянно ищут уязвимости, которые позволят украсть ценные данные. Попытки украсть информацию имеют разные цели: одни мошенники - получают деньги с банковских счетов или созданных кредитных карт, а другие могут продавать информацию третьей стороне. Пароль является самым простым и дешевым способом аутентификации. Ограничительная политика паролей может привести к тому, что некоторые действия пользователей, например, записывание паролей, повторное использование их для разных учетных записей или совместное использование паролей с друзьями, могут поставить под угрозу безопасность. Политика безопасности паролей должна балансировать непосредственно между безопасностью и удобством использования. В статье предложены разработанные рекомендации для баланса безопасности и удобства пользователя.

Персональные данные пользователей подвержены повреждениям, вирусам, стихийным бедствиям, кражам. Цифровые воры постоянно ищут уязвимости, которые позволят украсть

ценные данные. Попытки украсть информацию имеют разные цели: одни мошенники - получают деньги с банковских счетов или созданных кредитных карт, а другие могут продавать информацию третьей стороне. Пароль является самым простым и дешевым способом аутентификации [1].

Пароли защищают личную информацию - информацию, которую мы не хотим передавать или не каждый должен знать. В нашей личной жизни это означает финансовую информацию, медицинские данные и частные документы. В профессиональном контексте это может охватывать все, что считается решающим для успеха организации: коммерческие секреты, финансовые данные, интеллектуальная собственность, списки клиентов и т.д. Создание пароля, по сути, привычное дело для пользователя, но далеко не каждый достаточно серьезно подходит к решению этого вопроса [2].

Рассмотрим разные вариации паролей со стороны безопасности и удобства использования.

1. 123456	**11.** 123123	**21.** mustang	**31.** 7777777	**41.** harley
2. password	**12.** baseball	**22.** 666666	**32.** flower	**42.** zxcvbnm
3. 12345678	**13.** abc123	23. qwertyuiop	**33.** qazwsx	**43.** asdfgh
4. qwerty	**14.** football	**24.** 123321	**34.** Jordan	**44.** buster
5. 123456789	**15.** monkey	**25.** 1234…890	**35.** Jennifer	**45.** andrew
6. 12345	**16.** letmein	**26.** princess	**36.** 123qwe	**46.** batman
7. 1234	**17.** shadow	**27.** superman	**37.** 121212	**47.** soccer
8. 111111	**18.** master	**28.** 270	**38.** killer	**48.** tigger
9. 1234567	**19.** 696969	**29.** 654321	**39.** trustno1	**49.** charlie
10. dragon	**20.** michael	**30.** 1qaz2wsx	**40.** hunter	**50.** robert

В таблице представлено 50 самых популярных паролей. Ни один из них не является достаточно хорошим или безопасным паролем, но они довольно простые для запоминания. По сути, это говорит нам, что при создании паролей предпочтение пользователя состоит в том, чтобы их было легко запомнить.

Хотя пароли являются жизненно важным компонентом системной безопасности, их можно легко взломать или сломать. Существует 5 проверенных способов:

1) *Запрашивание.* Является наиболее распространенным способом получения доступа к чьему-то паролю. То есть, для того чтобы узнать чей-то пароль, нужно просто попросить об этом (часто в связи с чем-то другим). Люди часто рассказывают свои пароли, совсем не беспокоясь о своей безопасности. Эта проблема не решится пока пользователи не начнут осознавать последствия таких своих действий.
2) *Угадывание.* Достаточно распространенный метод взлома. Большинство людей выбирают пароль, который легко запомнить, и самые простые - это те, которые связаны с вами как с личностью. Такие пароли легко угадать, зная минимальный объем информации о человеке, чей пароль запрашивается. Для предотвращения взлома данным способом, рекомендуем выбирать пароль, не имеющий отношение к пользователю как к человеку.

3) *Атака «грубого взлома».* Это обыкновенный перебор различных вариантов и комбинаций. Например, если у вас пароль «*sun*», программа попытается войти в систему, используя «aaa, aab, aac, aad ...sul, sum, *sun*». То есть – самые элементарные наборы цифр и букв. Эта программа способна в кратчайшие сроки перебрать огромное количество комбинаций. Единственное, что останавливает такую атаку - это сложность и более длинные пароли.
4) *Атака через общие слова.* Подобно атаке «грубого взлома», хакер пытается выполнить вход в систему, но уже используя список похожих слов, вместо комбинаций букв. Например, «sum, summer, summit, sump, *sun*».
5) *Атака по словарю.* Выполняется аналогично предыдущей атаке, единственное отличие заключается в том, что хакер теперь использует полностью весь словарь.

Первые два способа атак невозможно предотвратить только с помощью пароля, но есть возможность защитить систему от других форм атак [3]. Хакер обычно разрабатывает автоматизированный сценарий или программу, которые выполняют работу для него. Также система безопасности должна установить количество запросов на пароли, которые может сделать автоматическая программа - например, в секунду. Возможны разные варианты, но большинство веб-приложений не смогут обрабатывать более 100 запросов на вход в секунду. Это, по сути, и влияет на скорость взлома.

К примеру, если в качестве пароля используется:

- Любые цифровые комбинации, например, дата рождения - «15021986» - программа затратит около 2-х секунд на расшифровку;
- Именные пароли с маленькой буквы (anna, oleg) потребуют около 4-х секунд;
- Пароли, в которых используются имена с большой буквы (Anna, Oleg) – около 4-х минут;
- Более сложные комбинации с использованием цифр «1d2d3s4a8c» программа расшифрует за 4 дня;
- Пароли из серии «HSU5-BHJDa» будут расшифрованы через 12 лет;
- И комбинацию «J4fS<2» программа расшифрует через 219 лет.

Но означает ли это, что ИТ-отделы и компании по обеспечению безопасности правы, когда часто напоминают нам о том, что мы должны использовать сложные пароли, поскольку они являются более безопасными? Нет, это просто значит, что пароль с 6 символами не будет работать. Никто хочет запоминать пароль типа «J4fS<2», и, очевидно, что он будет записан в заметки.

Ограничительная политика паролей может привести к тому, что некоторые действия пользователей, например, записывание паролей, повторное использование их для разных учетных записей или совместное использование паролей с друзьями, могут поставить под угрозу безопасность. Другим нежелательным побочным эффектом определенной политики паролей является забывание паролей. На самом деле вред, причиненный пользователям после чрезмерно ограничительной политики паролей, может быть больше, чем вред, предотвращаемый этой политикой.

Соблюдение некоторых простых правил значительно облегчит жизнь пользователей, и решит проблему использования сложных паролей:

1) Прежде всего, в паролях нужно использовать слова, которые легко запоминаются, что-то простое и то, что можно быстро набрать (но это не должно быть связанно с пользователем как с личностью).

2) Также, когда в пароле используется не одно, а два простых слова, - это значительно увеличивает безопасность (для взлома пароля с одного слова программа потратит приблизительно 4 минуты, на пароль из двух - 2 месяца). Но, используя уже 3 слова, получается чрезвычайно безопасный пароль, для взлома которого понадобятся тысячи лет (в табл. 2 продемонстрированы примеры).

Type	Password	Method	Time	Security level
2 common word password	yellow bicycle	Common word	2 month	Low risk
3 common word password	tell the truth	Common word	2,537 years	**Secure forever**

3) И последнее, стоит пользователю придумать пароль с необычными словами, или же использовать больше 3-х коротких фраз, уровень защиты и время, которое понадобится для взлома, достаточно сильно возрастают (табл.3).

Type	Password	Method	Time	Security level
3 uncommon word password	pragmatic is realistic	Dictionary	39,637,200 years	**Secure forever**
5 uncommon word password	Du-bi-du-bi-dub	Brute-force	531,855,448,467 years	**Secure forever**

Исследования показывают такие результаты, так почему ИТ-департаменты заставляют нас ломать головы и пытаться запомнить очень сложные пароли? Если же присмотреться к офисным столам сотрудников любого департамента, с легкостью можно заметить, по крайней мере, несколько мониторов или столов, украшенных красочными пост-заметками с множеством паролей. Это признак того, что ИТ-администраторы ошиблись в своей политике паролей. И решение с точки зрения юзабилити заключается не в том, чтобы люди использовали заметки на столах или менеджеры паролей, а в том, чтобы сделать пароли более удобными.

Политика безопасности паролей должна балансировать непосредственно между безопасностью и удобством использованиях [4]. А система паролей будет более безопасной,

если пароль будет более удобным. Это объясняется как человеческим, таки компьютерным факторами. Для поддержания баланса мы рекомендуем:

1. *Обеспечить базовое обучение пользователей.* В первую очередь, этот принцип должен помочь сократить количество взломов под воздействием человеческого фактора (т.е. предотвратить угадывание и прямые запросы паролей). Беспрерывные нарушения безопасности происходят в результате человеческих ошибок или небрежности. В организациях нужно создать корпоративную культуру, которая подчеркивает безопасность компьютеров посредством учебных программ, предупреждающих о рисках небрежного использования паролей и неосторожного использования сетей, программ и устройств.
2. *Обратить внимание на энтропию (сложность) пароля*. Сложность пароля в компьютерной индустрии обычно измеряют в битах. Вместо количества попыток, которые необходимо предпринять для угадывания пароля, вычисляется логарифм по основанию 2 от этого числа, и полученное число называется количеством «битов энтропии» в пароле. Например, набор случайных символов, таких как «Tr0ub4dor&3», выглядит как супер безопасный пароль. Такой пароль имеет 2^{28}битов энтропии. Согласно формуле, при увеличении длины пароля на один бит количество возможных паролей удвоится, что сделает задачу атакующего в два раза сложнее. То есть, длинная цепочка запоминающихся для нас слов, например, «correct horse battery staple» имеет 2^{44} битов энтропии и является не только удобной, но и безопасной с технической стороны.
3. *Ограничить количество попыток входа.* В примерах выше устанавливали стандартное количество запросов на пароли, которые может сделать автоматическая программа - 100 запросов на вход в секунду. Но если администратор сократит количество попыток входа до 1 запроса на 5 секунд, и, более того, еще добавит штрафной период после 10 неудачных попыток, безопасность системы и ее взлома кардинально изменится, при этом не сильно повлияет на удобство использования (табл.4).

No of attacks	Password	Time	Security level
100 times per sec	yellow bicycle	2 month	Low risk
1 time every 5 sec	yellow bicycle	63 years	Secure
1 time every 5 sec with a 1 hour penalty period after 10 attempts	yellow bicycle	1,889 years	Secure forever

Очевидно, что пароль - всего лишь одна часть головоломки. Другие части – это политика безопасности, обучение пользователей и техническая составляющая обеспечивают гораздо более глобальную защиту в контролируемой корпоративной среде, чем пароли. Но в тех областях, где единственным способом контроля пользователей является ПИН или пароль, самое лучшее, что можно сделать, это знать о рисках безопасности и подобрать безопасный пароль.

Использованная литература

1. Dustin Van Der Haar, Basie Von Solms, "The poor man's biometric: Identifying cost-effective biometric system criteria for SMMEs", *IST-Africa Conference Proceedings 2014*, pp. 1-10, 2014.
2. M. Bellare, R. Canetti, and H. Krawczyk. A Modular Approach to the Design and Analysis of Authentication and Key Exchange Protocols. STOC ’98.
3. National Institute of Standards and Technology, "Digital Signature Standard," Federal Information Processing Standards Publication 186, May 1994.
4. Captcha development problems // Modern technics and technologies. 2015. № 7 [Electronic journal]. URL: http://technology.snauka.ru/en/2015/07/7577