Proceedings of FIKUSZ '15 Symposium for Young Researchers, 2015, 121-130 pp Published by Óbuda University http://kgk.uni-obuda.hu/fikusz

Life is Short. Have another Affair – Password Security

Keszthelyi András

Óbuda University, Keleti Faculty of Business and Management, Budapest, Hungary
Keszthelyi.Andras@kgk.uni-obuda.hu

This summer Ashley Madison the online dating site was hacked and many gigabytes of data was downloaded from the site and published, including user records. Amongst these data more than 11 million user passwords were revealed. In this paper I investigate the case from the sysadmin's (or the management's) point of view on the basis of publicly known circumstances: what is the best practice to properly handle user passwords.

Keywords: data security, password, data loss

JEL code: L-86 Information and Internet Services; Computer Software

1 Introduction

Living in the Age of Computer Networks when the internet is part of our everyday life, the amount of digitally stored data increases day by day and what is more: our dependency on these data also becomes stronger day by day – we speak about a new paradigm, we have virtual personalities and we act in a virtual world (too). In such a situation information security is more important than ever.

At the beginning identifying users was not a too important task of security – at those times nobody thought that the time would come when everybody will use computer networks as part of everyday life. The more the computer networks spread the more important user identification became. Nowadays it is of critical importance. There are different methods for identifying users and each of them has its advantages and disadvantages compared to the others. Among these methods the use of passwords is the oldest and simplest way.

What are the possible aims of intrusions into computer systems? They cannot be enumerated fully but they can be classified into two groups: they can be direct and indirect ones.

Direct purposes are to be mentioned first: money, revenge, political protests, classical spying, industrial espionage, or whatever you can even imagine. Attackers will use directly and in most cases immediately what they could steal from the targeted system.

After these direct aims there may be some indirect ones. Among these possible indirect ones now the stealing of real-life passwords are interesting for us. The bigger set of real passwords you have and analyse the more realistic knowledge you will have about password selecting habits (Keszthelyi, 2013). Analysing password selecting habits of real users of present one can improve a lot on password cracking methods, so future attacks will be more efficient.

In the past few years there were some significant intrusions into different computer systems that resulted in getting a (very) large number of user passwords published. Among them the data breach of the cheating site Ashley Madison is the last. In this paper I investigate the publicly known circumstances of the case to get the conclusion: what is the best practice of handling passwords at server side.

2 What happened?

Ashley Madison, The Ashley Madison Agency in full, was founded in 2002 in Canada. It is a commercial web site for online dating, especially for people who are married or in a relationship. The slogan of the site is "Life is short. Have an affair". On the basis of traditional ethical values it is far from what we could call as normal. The site had (has?) nearly 40 million members from more than half a hundred countries and realized a yearly income of about 100 million US dollars. (CBS, 2015/A) The site charged a 19 US dollar fee for deleting a user account. Site said this "full delete" option was to include all the personal data of the user, such as photos, site usage and search history, sent and received messages etc. (Chideya, 2015)

In the middle of July 2015 some hackers who called themselves as "The Impact Team" could successfully get into the system of the site and downloaded the user database, including the real names of the users, their home addresses, their search history and bankcard transaction data. (Thomsen, 2015) The Impact Team announced the successful attack on 15 July and demanded the site to be shut down immediately and permanently unless the owners want the user records published. The site was not closed (and is working even today) and the tons of user data was published via BitTorrent. Soon it came to light that the permanent deletion of user profiles was a humbug, attackers could reveal data records that were considered as deleted. "Despite promising customers to delete their user data from the site for a $19 fee, the company actually retained the data on ALM's servers, the hackers claimed. «Too bad for those men, they're cheating dirtbags and deserve no such

discretion,» the hackers wrote. «Too bad for ALM, you promised secrecy but didn't deliver.»" (Zetter, 2015)

Among the published user records there were thousands of official government and military email addresses, belonging to members of the US army and government offices (email addresses ending with .gov, .mil). (Gibbons-Neff, 2015) This attack can be compared to the celebrity photo hack in 2014.

3 Password cracking – background

There are some well-known methods to find out other people's passwords. These methods are so logical and so well-known that it is an interesting question: "Why people use so stupid passwords?" Because of user irresponsibility there are some easy ways to reveal users' passwords. If users are responsible and apply the most important and basic password selecting rules then attackers have to go on harder ways. Let's have a look on these methods.

The most irresponsible password selection methods are when users pick up "basic" passwords (or leave factory default ones unchanged) such as 123456, password, etc. For more examples try Google search expression "top 100 passwords". Among Ashley Madison users the most frequent password was 123456, used by more than 120 thousand users (1,03%) out of the 11,7 million whose passwords have been successfully cracked. The top ten passwords are listed in Table 1. (Collins, 2015)

password	*number*	*proportion*
123456	120 511	1,03%
12345	48 452	0,41%
password	39 448	0,34%
DEFAULT	34 275	0,29%
123456789	26 620	0,23%
qwerty	20 778	0,18%
12345678	14 172	0,12%
abc123	10 869	0,09%
pussy	10 683	0,09%
1234567	9 468	0,08%
(sum)	335 276	2,87%

Table 1

The top ten passwords of Ashley Madison

It is also an irresponsible password selection method when there is a connection between the password and a) the person (date of birth, name of favourite actor/actress), b) the login name as strings (admin – admin, admin – admin!admin), c) the login name in the meaning (ashley – madison).

These kinds of passwords can easily be guessed in a few turns, even online and personally. Barack Obama's Twitter account was hacked this way in 2010. (Mesquita, 2010) If a password cannot be found by these ways the next step is the classic dictionary attack, when a program tries out all the words from a given list (dictionary). On the basis of the results of analysing the structure of millions of real passwords a so-called advanced dictionary attack may be performed. In this case not only the basic words from the list are probed but their variants similar to the most common structures as well (e.g. a two digit number appended at the end of the word). A brief analyses I made on rockyou.com passwords can be found in (Keszthelyi, 2013).

The last possibility of an attacker is the brute force method when a program tries out all the possible character combinations. In this case the password will be found for sure, the only question is: When? Three years ago, at the end of 2012 Jeremy Gosney presented his machine designed to crack passwords with brute force. It was running the HashCat password cracking program on 25 AMD Radeon GPUs. He could provide an unbelievable 348 billion tries/sec (NTLM password hashes), which means that a 14 character long WinXP password, for example, could be cracked just in six minutes. (Paul, 2012) (Soulskill, 2012)

Advanced dictionary and brute force attacks can normally (?) be performed offline, after the attacker has successfully stolen the shadow passwords from the target system. What are shadow passwords? To store the passwords of the users in plain-text form is a serious security flaw. If anyone, in any way, can get access to the plain-text password file then s/he could personalize each and any users of that system. Instead of plain-text passwords, normally, their hashes, the so-called shadow passwords are stored. Hash functions are one-way mathematical functions that calculate a fixed length string from the input. If the hash function consists of a large number of calculations the brute force method would need a very long time to be finished even if you have a very large calculation performance (petaflops or more).

4 Best practice

The security level passwords can provide us depends on both the user(s) and the system administrator and/or the management who makes the security rules. As we know from revealed password lists, too, the weakest link in the chain of security is the human factor, i.e. the irresponsible user. In such a circumstance the

management and/or the system administrator should be more careful because they do have the necessary knowledge (or at least: they ought to have it).

The first step is to improve security in general, obviously. The security level of every system is as high as that of its weakest link. In addition, if you are also responsible for the privacy of your users, you must act that attackers should have the least chances even if the shadow passwords are stolen. And shadow passwords can be stolen, there are more than enough examples for that.

Now let's focus on password handling on server side. Considering the fact that a lot of users pick up their passwords irresponsibly we conclude that we must check the password selection of our users. Having a look on the above mentioned methods to get others' passwords the following rules ought to be applied.

New passwords should be checked against a regularly updated blacklist of the most common passwords. For details do a Google search for the expression of "top 100 passwords", or the top 1000. Keeping in mind the existence of the advanced dictionary attack, the new password chosen by the users must be checked not only against the simple blacklist but against the commonly prefixed-suffixed-concatenated words of the blacklist as well. For more details on common password structures, see for example (Keszthelyi, 2013).

The next step is deciding the function that calculates the password hashes to be stored. There are a lot of hash functions, with very big differences in computing power they need. The more computing power a hash function needs the better it stands against brute force. Supposing the above described machine developed by Gosney in 2012 we get the results for some hash functions in Table 2. (Paul, 2012) (Soulskill, 2012)

algorythm	*tries/sec*
NTLM	348 billion
MD5	180 billion
SHA1	63 billion
LM	20 billion
bcrypt (05)	71,000
sha512crypt	364,000

Table 2
Gosney's cracking speed

It is clear that if you use bcrypt instead of NTLM than a successful brute force attack will last for about five million times longer. As Gosney demonstrated that an NTLM-hashed WinXP password could be cracked in six minutes max, if the hash function was bcrypt instead of NTLM it would last for about half a century. This is a really big difference.

In addition to use a strong hash function passwords should be "salted". "Salt" is some random data the plain password is concatenated to before hashing. This

method results in different hashes even for the same passwords. As we can see from the Ashley Madison password statistics (Collins, 2015) there are a lot of people who pick up the same – too simple – password at Ashley Madison, too. If the password is not salted then the same hash will belong to the same passwords. It means that if an attacker can probe the most common passwords, for example trying 123456 will result in finding the password for more than 120 thousand accounts in one step. If the passwords are salted, at most one password can be found in one step.

A very important rule that passwords themselves must not be stored, not even in an encrypted form. What you have encrypted someone may decrypt. Adobe did it and 135 million user passwords came into light. (Ducklin, 2013) In case of Ashley Madison the reason why so many passwords (more than 11 million) could be revealed was that they were stored not only in bcrypt hashes but in md5 hashes as well. "A blogger who went after the the bcrypt hashes recovered only 4000 passwords in a week. In contrast, CynoSure Prime recovered the passwords for over 11 million of the MD5 hashes in about 10 days." (Ducklin, 2015)

In addition to the technical requirements and possibilities you can (try to) teach your users how to properly chose and use passwords. It may be easier and more efficient if the users are your employees, naturally.

The possible ethical and business aspects also should be mentioned here. Users are (ought to be) interested in security in general, in the proper use of their passwords in particular. Yet they are usually not on top of things. So because the master of the system has (or should have) the professional knowledge and tools, they have more responsibility regarding the security (as well). A user may have a perfect password: it will not work if the master is not careful enough, or directly careless. As the master is interested in running the business in the future, too, it is he who must do the most for the proper operation.

5 Teaching and learning

In our so-called information age, when we depend on the increasing amount digitally stored data stronger and stronger security is a very important field both in business and in private life. As a teacher of IT I must tell that IT security is not the problem of the IT sector only but it is (should be) an important problem if the education system, too. As we must teach our children how to properly take part in the city traffic as early as possible, in the same way we ought to teach our children how to properly take part in the virtual traffic of the virtual world, too. The young generation should exercise themselves in the typical situations practically and when it is possible they must be taught also to the theoretical background. It cannot be done too early, because if you investigate the skills and knowledge of

the university students in computer sciences in Hungary and in Central Europe you will find an alarming situation. (Kiss, 2012/A) (Kiss, 2012/B) Educating, teaching and training is a good idea but may not be enough. The culture of security ought to be developed, for it means less possibility for risky behavior. (Lazányi, 2015)

The minimal requirement would be at least not to teach false things or anything worse than the best. "Using numbers, symbols and mix of upper and lower case letters in your password makes it harder for someone to guess your password. For example, an eight-character password with numbers, symbols and mixed-case letters is harder to guess because it has 30,000 times as many possible combinations than an eight-character password with only lower case letters." (Google, 2015)

The situation is that that the length of the password is a significantly more important factor than the number of char types. Increasing the number of elements in the basic char set used in passwords will result in the polynomial growth of the possible char combinations and so the time needed for a successful brute force attack while increasing the length will result in an exponential growth. Let's calculate with a cracking speed of 10^{12} tries/sec. If the password may contain any of 80 different chars and the length is 8 chars, it would need less than half an hour to crack it. Let's increase the number of the chars in the basic char set from 80 to 100 (25% growth), the time requirement will grow only to less than three hours. Leaving the number of elements in the basic char set at 80 and increasing the length also by 25% to 10, the crack would need about four months!

Stanford University, which is listed among the top ten universities in all over the world suggests to its users a very simple password building procedure, the result of which is also very simple. (Stanford, 2015) They suggest to select four simple words and concatenate them into a passphrase. Their example is orange+eagle+key+shoe. Calculating with quite a big dictionary of eight thousands basic words we get that it would need 68 minutes to crack such a password. If the dictionary contained only 2 thousand words the time requirement would be only 16 seconds. Not too convincing.

But what we can wait for in a world where, for nearly 20 years, the launch code for the US nuclear missiles was eight zeros? (Vaas, 2013)

6 Conclusion

The conclusion of the data breach of Ashley Madison cheating site can be very short.

From the point of view of those who run the (a) service: above general security rules and improvements use a strong hash function and salt to calculate the password hash. Do not let users select weak passwords as well as too short ones. Never store passwords, not even in an encrypted form. Teach and train your users if it is possible. Take part, more generally, to develop the culture of security. Don't take for granted what others state about security in general, about passwords in particular: trust – but check!

From the point of view of users: knowing what a good password is and how to select such one is vital. Knowing that your privacy depends on not only your consciousness but on that of the service provider, too, men had better not register to such sites. Instead of that they had better treat their own family. Especially in light of the fact that most women records were fake at Ashley Madison...

References

[1] CBS (2015/A). Ashley Madison hacked, users threatened with exposure, 20.07.2015. CBS News, http://www.cbsnews.com/news/ashley-madison-hacked-users-threatened-with-exposure/

[2] Chideya, F. (2015). Some Dude Created an Ashley Madison Account Linked to My Gmail, and All I Got Was This Lousy Extortion Screen, The Intercept, 21.07.2015. https://theintercept.com/2015/07/21/ashley-madison-breach-why-am-i-getting-their-emails/

[3] Collins, K. (2015). The top 100 passwords on Ashley Madison, Quartz, 14.09.2015. http://qz.com/501073/the-top-100-passwords-on-ashley-madison/

[4] Ducklin, P. (2013). Anatomy of a password disaster - Adobe's giant-sized cryptographic blunder, 04.11.2013. Naked Security Award winning computer security news from Sophos, https://nakedsecurity.sophos.com/2013/11/04/anatomy-of-a-password-disaster-adobes-giant-sized-cryptographic-blunder/

[5] Ducklin, P. (2015). 11 million Ashley Madison passwords cracked in 10 days, 10.09.2015. Naked Security Award winning computer security news from Sophos, https://nakedsecurity.sophos.com/2015/09/10/11-million-ashley-madison-passwords-cracked-in-10-days/

[6] Gibbons-Neff, T. (2015). Thousands of .mil addresses potentially leaked in Ashley Madison hack, The Washington Post, 19.08.2015. https://www.washingtonpost.com/news/checkpoint/wp/2015/08/19/thousands-of-mil-addresses-potentially-leaked-in-ashley-madison-hack/

[7] Google (2015). Creating a strong password, https://support.google.com/accounts/answer/32040?hl=en

[8] Keszthelyi, A. (2013). About passwords, ACTA POLYTECHNICA HUNGARICA 10:(6) pp. 99-118., http://www.uni-obuda.hu/journal/Keszthelyi_44.pdf

[9] Kiss, G. (2012/A). Measuring Computer Science Knowledge Level of Hungarian Students specialized in Informatics with Romanian Students attending a Science Course or a Mathematics-Informatics Course / TOJET: The Turkish Online Journal of Education Technology, Volume 11, Issue 4. ISSN: 2146 – 7242, pp. 222-235.

[10] Kiss, G. (2012/B). Comparison of the Programming Knowledge of Slovakian and Hungarian Students. In: Procedia of Social and Behavioral Science Journal, volume 64, 09.11.2012., pp. 169–178., http://www.sciencedirect.com/science/article/pii/S187704281204997X

[11] Lazányi, K. (2015). A biztonsági kultúra [The culture of security], In: TAYLOR: GAZDÁLKODÁS- ÉS SZERVEZÉSTUDOMÁNYI FOLYÓIRAT: A VIRTUÁLIS INTÉZET KÖZÉP-EURÓPA KUTATÁSÁRA KÖZLEMÉNYEI 7:(1-2) pp. 398-405. (2015)

[12] Lee, M. (2015). Ashley Madison hackers follow through on threat, dump user database online, 19.08.2015. Naked Security Award winning computer security news from Sophos, https://nakedsecurity.sophos.com/2015/08/19/ashley-madison-hackers-follow-through-on-threat-to-expose-users/

[13] Mesquita, R. (2010). Frenchman convicted for hacking Obama, Boston Globe, 25.06.2010. http://www.boston.com/business/technology/articles/2010/06/25/frenchman_convicted_for_hacking_twitter

[14] Paul (2012). Update: New 25 GPU Monster Devours Passwords In Seconds, The Security Ledger, 04.12.2012. http://securityledger.com/new-25-gpu-monster-devours-passwords-in-seconds

[15] Soulskill (2012). New 25-GPU Monster Devours Strong Passwords In Minutes, SlashDot, 05.12.2012.

http://it.slashdot.org/story/12/12/05/0623215/new-25-gpu-monster-devours-strong-passwords-in-minutes

[16] Stanford (2015). Which characters are required in my password? https://weblogin.stanford.edu/pwstrength.html

[17] Stockley, M. (2015). What Ashley Madison got right, 31.08.2015. Naked Security Award winning computer security news from Sophos, http://localhost/~kea/sql/ujcedula/leszedettek/inf/2015_III/nakedsecurity.sophos.com_car_AshleyMadison_pwd.html

[18] Thomsen, S. (2015). Extramarital affair website Ashley Madison has been hacked and attackers are threatening to leak data online, Business Insider, 20.07.2015. http://www.businessinsider.com/cheating-affair-website-ashley-madison-hacked-user-data-leaked-2015-7

[19] Vaas, L. (2013). For nearly 20 years, the launch code for US nuclear missiles was 00000000, 11.12.2013. Naked Security Award winning computer security news from Sophos, https://nakedsecurity.sophos.com/2013/12/11/for-nearly-20-years-the-launch-code-for-us-nuclear-missiles-was-00000000/

[20] Vaas, L. (2015). Cheating site Ashley Madison breached by hackers threatening to expose users, 20.07.2015. Naked Security Award winning computer security news from Sophos, https://nakedsecurity.sophos.com/2015/07/20/cheating-site-ashley-madison-breached-by-hackers-threatening-to-expose-users/

[21] Zetter, K. (2015) Hackers Finally Post Stolen Ashley Madison Data, Wired, 18.08.2015. http://www.wired.com/2015/08/happened-hackers-posted-stolen-ashley-madison-data/