Project Report:
Password security in practice

With focus on password management and weaknesses

Grupp: 001A - Joel Strömblad & Tim Österlund

Abstract

This report highlights the differences and similarities in the thought process between security experts and regular people. We did this with the help of a survey, which show that when our control-group is faced with a security critical situation they tend to read up on the problem and at least do as asked. The survey did test how they chose passwords given different choices, and password memorability seems to be favored. We also see a tendency to not trust third party password management solutions.

Introduction

The purpose with this project is to find out how todays password handling and security works. It will also check, with the help of a survey, how ordinary people handle their own passwords. How often they change them, their view on how secure the passwords are and if they use tools to help keep changing and handle their passwords. Many different tools are available to help users create and handle their passwords but how secure are theses "password management"-tools in reality? In this project, a few selected password management and generator programs will be tested to see how they work. Is it something that's easy to use and what advantages does it bring to everyday users, in regard to letting oneself keep the control of the passwords?

The results of the survey, regarding user view on password security, will be compared with information regarding how one should reason to create secure passwords. One can find a lot of advice from both companies and experts on how a secure password should look like. Do people use these advices and how do the information reach the everyday user?

Assignment setup

The goal with the project is to derive an answer to the following questions

- How does today's password management work? What is done to make it trustworthy?
- What weaknesses exist in today's system and how are they exploited?

To achieve this we broke down this into three parallel smaller areas:

- Experts, state of the art
- Normal users
- Third party solutions

Experts, focuses on what exactly does the people working with password security and password management think. Where are the weaknesses of passwords today? Is it the users which is the problem or has the focus shifted? This analysis will be mainly based upon published materials.

Normal users, what exactly does people think about password security and password management? A normal user is defined as a person who doesn't necessarily work with security-related issues. It was decided a survey should be made in order to first and foremost check security-awareness. Through an analysis of the survey the goal was to deduct if the ideas of experts had any roots in reality or if computer-science-theory is far ahead of computer-science-in-practice.

Third party solutions, last but not least it was decided that we will make a case study of 2 password management solutions in order to determine if a password safe, a password management solution, is a viable option to individually remember every single password or somehow compromise them in other ways like writing them down in order to remember all of them.
The survey is divided into four parts. Each part handles certain areas regarding passwords and password handling as well as user view on management tools. The four parts are the following:

- Password security in practice. This part looks into how user act and think when constructing their passwords. The participants were also asked to choose a password from a given list. It also asks how one reacts when information surfaces, claiming a site to be insecure with the users passwords. Do they care?
- General rules. How does a user think when creating a password? Do they use certain rules, tools or do they only randomize their passwords to the degree they feel safe.

How often do everyday users change their password?
- Memorability. How well do users remember their password? This is based on a previous question where the participant had to choose a password from a list and then remember it.
- Password management tools. Is the participant currently using a password management application? How is their view on the applications? The participants also had the possibility to write down more describing comments regarding the subject.

Results

Experts

Today there exists many different ways how to construct a "secure" password. One can find methods and advice on the internet as well in technical magazines. In this part we're going to explain how some of the methods work.

One way[1] to start is to simply choose a word that one can easily remember. The next step would be to spell it backwards, making it more stable against dictionary attacks, attacks that use dictionaries in order to crack the password. Using a set of combined words in a password is no longer considered secure even though the advice still circulates on the internet. The next step is to replace some of the letters in the password. It can be done by turning letters into capital letter or substituting letters with numbers or special characters (an "0" instead of "o" or "@" instead of "a"). However, one should strive to not making standard changes, exchanging "e" for a "3" is still something that's very obvious or predictable to hackers. The important thing to do is to make changes that make sense to oneself. By following these steps and keeping in mind that by having greater variation of letters and symbols, the password will only get stronger.

Another way[2] to create a secure password is the use of passphrases or acronyms. Simply choose a long sentence and use only the first letter in each word and combine them. Then make changes to it by using the method mentioned earlier. This is a method that might be easier to connect to one's daily life and thus making it easier to remember. One should however keep in mind to not use too much personal information when creating passwords (for example names, birthdays etc.). Quite a bit of information can be found about oneself on the internet and can easily be used to deduct how one constructs his/her passwords in some cases.

In the end, all passwords are hackable. Doesn't matter how advanced one try to make it, it can be hacked. However, the raw computer power needed and sought efficiency is the factors that in many cases decide if the password will be hacked. The longer the password, with great variation, the longer it will take. That makes it quite inefficient and not worth the time for attackers to find out your password.

Bruce Schneier suggests[3] the use of password management programs. Programs that helps to generate random passwords, most times random alphanumeric passwords, and which stores them in either its own database using various encryption methods. In this project we have included a case study[4] regarding two password management solutions, looking into their functionality and usage toward the users.

Jeff Yan, Alan Blackwell, Ros Anderson and Alasdair Grant has done a study on password memorability and security[5] and found that random passwords is harder to remember and passwords based on memory-phrases are harder to guess than "naively selected passwords". They also found that "Naively selected passwords" and memory-phrases are about the some in remember-difficulty.

Survey

The number of people who took part in our survey was 37. (Updated 12/5 -14)
The survey, which was done in Swedish, and its result can be found in Appendix A, but here follows the result which was most interesting. We asked our participants to pick a password for a bank service. They divided quite equally into 2 main groups. The

[1] "Password Protection: How to Create Strong Passwords", Eric Griffith

[2] "A Really Good Article on How Easy it Is to Crack Passwords", Bruce Schneier

[3] "A Really Good Article on How Easy it Is to Crack Passwords", Bruce Schneier

[4] See section "Case study" on page 5

[5] "Password Memorability and Security: Empirical Results", Jeff Yan, Alan Blackwell, Ross Anderson Alasdair Grant

first favored memorability and the other favored password strength. The password which featured some of both got without argument the most picks, about 50%. 20% would pick a strong password without a previously set way of memorizing the password and 30% would pick a weak, compromised or a password which gives a false sense of security due to combo-attacks.

Furthermore about 60% of the asked would read up on a published problem (problem announced by bank or newspaper) to see what they can do to help make their information be more secure and only 10% would completely ignore the issue. This shows that a majority has a certain sense about password security but improvements can be made. The major issue would be that there exists a lot of information about password construction but this never really reaches the everyday user. It could be because new research only get published in technical articles which is not designed to explain the concept for other experts, not the end users. This lead to that only the people actively interested in password security or more technical people has the latest knowledge.

When looking into what password traits the participants chose in the survey, two traits stood out. The first one was that when it came to passwords on more important places (for example banks, social media etc.), a unique password would be used. When it came down to places of less importance, toward the user, less secure passwords tended to be used and in less variance than before. It shows that awareness exist and is important to people but only to a certain degree.

Something far more disturbing is that our survey group has a tendency to only change password if they are notified that account information has been leaked or when they forget their login-information. About 25% is actively changing their password without being asked and 10% never changes. However, 70% of the participants would choose to change their password in the cases where they think their password information had been leaked. Still, 30% remain that seemingly don't think there is any real security risk in it. One of the many reasons might be that even though information gets leaked, the companies or distributors often claim that due to encryption the information will still be secure. Changing ones password only stands as an advice.

As far as we can tell, the main reason for not using third party password management solutions is trust. Almost 50% of our participants indicated that they would not use a password management solution because of they do not trust the application. A reason for this distrust might be the lack of understanding on how the security is implemented. In many cases, only the methods are mentioned without extensive information. Without education/insight this leads to a lack of proper understanding, due to technical terms and leads the users to use their own methods.

An alternative reason can be the messages different experts promote. For instance Bruce Schneier is very enthusiastic towards password safes.

"Better, though, is to use random unmemorable alphanumeric passwords (with symbols, if the site will allow them), and a password manager like Password Safe to store them".
- Bruce Schneier

Others[6], for instance Imperva, recommends not to trust in any third party with your passwords.

"Never trust a 3rd party with your important passwords (webmail, banking, medical etc.)."
- Imperva

The survey was published and written in a way so that there would be no way to identify the person behind the responses as information security and more importantly password security is sensitive matter, so it was decided that unidentifiable answers were better than no answers. However, we used social media to spread our survey so we could assume that it is our friends and our friend's friends which potentially have answered the survey. This probably means students or mostly people without security education.

Case study

We chose to investigate the two password management solutions, KeePass and LastPass. We began with looking at the published technical details, then walk-through installation and setup, and end with testing the application. A technical specification can be found in Appendix B, which includes chosen encryption, storage and platform-support.

Installation and usage of LastPass

- Quite easy to install.

[6] "WP Consumer Password Worst Practices", Imperva

- Requires additional installments of plugins to your web browser(s).
- Requires you to set up a LastPass-account.
- Offers a recovery solution if you lose your password.
- Opens in a web browser tab which gives the feeling of a messy webpage, not a proper password security solution.
- Once added, easy to order passwords into groups for easier management.
- Synchronization between device-databases.
- No control over sync-data.
- Basic password control functionality and password generation.

Installation and usage of KeePass

- Portable, removes the need to install.
- Gives full control over database-file.
- Asks if you have a database-file or if you like a step-by-step setup-guide.
- Allows for drag-and-drop control of passwords making management extremely easy.
- No synchronization between devices.
- Integration with web browser is not guaranteed.
- Basic password control functionality and password generation.

The experience
When KeePass and LastPass is running simultaneously you get to very different feels to what program you are using. KeePass feels like a small, minimalistic, password safe. KeePass is designed as a window-application with a lot in common with a normal file-explorer window. Compared with the in-browser application of LastPass, LastPass have more in common with the router setup-page as it includes other types of filters and connection blockers.

Analysis

Users and passwords

Our study shows that our participants have a healthy distrust towards passwords which can be associated with a compromising event. They also tend to keep themselves updated. It can be deduced that they change their own security policy to fit the current situation based on the importance of the security issue. This is possibly also shown in the lack of trust in a third party password management application.

Given a choice, we can also see that memorability is favored over password-strength even if a relatively strong password is favored as long it's possible to remember it. We believe this can be considered as "proof of awareness" even if it doesn't tell us anything about the thought process in a "live"-environment. This suggests that the majority of our participants have a basic understanding of password security and follows the commonly accepted norm on what is a good password. The reluctance towards password management solutions seems to be a lack of trust towards the company or creators behind it. The question however remains, is this only a healthy distrust towards giving away credentials or just a marketing problem for the company pr organization behind it?

Password managers

With the results from the survey in mind, any password-manager application will need to pressure the issue of no "third party insight" while giving the user full control of everything from how and where security is enforced. In concrete examples the user will need to have access to security mechanisms and how this is implemented. Through explanation and more importantly simplification, the security process must be explained in order for users to start trusting in a program being responsible for their passwords.

Another important issue is device transference. Can you trust a company which holds your passwords for synchronization between devices even if they are encrypted? Or is a different solution required for trust? The case study gives two very different solutions. One asks you to trust in them to store an encrypted copy of your password-database, to allow you to access your passwords from an application on any device. For the users, the condition that one must install this application every time one uses a new device, might lead to it being complicated in regard to having one's password written down. The other solution, KeePass, only allows for manual database transfer. However, it's portable so it can be placed on a USB-stick which essentially turns the solution into a single password with a token. Mistrust still exist with this method as to what happens if someone else would acquire the USB-stick, is it something the user feels comfortable with even though it's encrypted? Both solutions require additional plugins with the main program in order to work integrated with web-browsers. This could be a deciding factor, due to the case one must install it on every new device one has.

Conclusions

How does today's password management work? What is done to make it trustworthy?

People in general seem to be somewhat aware of the issues and reacted in such a way that the most important passwords are unique and for the most part secure.

Focus is starting to shift from education "good choice of password" towards other problems and techniques to eliminate the need to remember all of them. Those that work with password security either focuses on the "server-side", trying to secure the usage of passwords or focuses on password management solutions in order to give the user the option to only remember one password.

What weaknesses exist in today's system and how are they exploited?

As always, the greatest weakness is the human factor. In password related terms this means social engineering. If the attacker can make you give up your credentials, you're sold.

Another important aspect is how the server-side password-database is stored. Reports about databases stored as plaintext or password hashes being downloaded is no new thing. These hashes are vulnerable because of what is called an offline combination attack, which essentially means the hacker can sit, at home, and guess without anyone knowing.

So why aren't more advanced security measures implemented to prevent these types of exploits? They exist, but are too expensive for the affected party to really care. Expensive in aspects of hardware and permutation-time, productivity is more important than security in most cases.

Password management solutions

Password management in theory is a very good concept. But until the concept has gained some trust it won't become widely spread. Insight and no middle-man can be considered important aspects in solving the trust issues as well as finding a solution to the several devices problem. For instance, a feature to tunnel a database-transfer between known devices combined with a way to allow for temporary public access.

Discussion and final thoughts

We understand that the small number of participants doesn't allow us to say anything which can be considered statistically correct. However we can use our data to anticipate trends and compare these against the result of others[7]. With this in mind we think we got a result which is better than expected. As, based on our data, we can still motivate why password is one of the most commonly used passwords even if our study shows it wouldn't be used to access a bank.

As part of the project we looked into password management applications, which almost weren't touched in the analysis and conclusion because our study showed a clear reluctance towards the idea. This means we could not draw any real conclusions in the respect. However, after checking more closely on password management solutions, we feel it might be worth to start to use at least to some extent. However we believe that some things must be done to really make the idea of password management application a valid one in everyone's mind. The main thing is that the user must always feel as he or she is always in control, and there can't be allowed any room for the feeling of "a man in the middle" to fall through. Yet personal accessibility can't be limited as it will be needed for every device to available for the user intends to use.

Appendix - Survey and References

Appendix A - Survey

link to survey

https://docs.google.com/forms/d/1gzvbk5w8yawSQ8BZkpk7yVwkKxZnGAQUIth4yboAN9U/viewform?usp=send_form

link to survey results

https://docs.google.com/a/student.liu.se/forms/d/1gzvbk5w8yawSQ8BZkpk7yVwkKxZnGAQUIth4yboAN9U/viewanalytics

References

Where you find KeePass and information about it

[7] "WP Consumer Password Worst Practices", Imperva

http://keepass.info/
Where you find LastPass and information about it
https://lastpass.com/

"A Really Good Article on How Easy it Is to Crack Passwords", Bruce Schneier, https://www.schneier.com/blog/archives/2013/06/a_really_good_a.html

"Password Protection: How to Create Strong Passwords", Eric Griffith, http://www.pcmag.com/article2/0,2817,2368485,00.asp

Appendix B – Technical specification

	LastPass	KeePass
Encryption	AES-256-bit encryption with routinely-increased PBKDF2 iterations	• Supports AES-encryption • Uses Twofish algorithm to encrypt database • Uses SHA-256 for hashing master password
Other protection		In-memory password protection: means that the system cache won't store information in plaintext
Password Generator	Built-in, with personal preferences	Built-in, with personal preferences
Storage	Uses LastPass servers to sync passwords between your installed devices, the communication is encrypted and can't be read by the company.	Comes in a portable version and allows the database to be stored on an encrypted file. Which means the application and the database file can be transferred to a desired device through normal file transfer.
Code	Company trade secret	Open source
Support	Multiple platforms	Portable to multiple platforms