Ethan F Ludden

IT 104 - 009

03/14/2024

Password Managers - Benefits, Risks, and Encryption advancements

"By placing this statement on my webpage, I certify that I have read and understand the GMU Honor Code on https://catalog.gmu.edu/policies/honor-code-system/ and as stated, I as a student member of the George Mason University community pledge not to cheat, plagiarize, steal, lie, or do anything unethical in matters related to academic work. In addition, I have received permission from the copyright holder for any copyrighted material that is displayed. This includes quoting extensive amounts of text, any material copied directly from a web page, and graphics/pictures that are copyrighted. This project or subject material has not been 2 used in another class by me or any other student. Finally, I certify that this is not for commercial purposes, which is a violation of the George Mason Responsible Use of Computing (RUC) Policy posted on https://universitypolicy.gmu.edu/policies/responsibleuse-of-computing/ web site."

“I also certify that no citation will be left to chance and will be critically evaluated for credible and reliable information or important statistical evidence per the statement above.”

Introduction & Background

A password manager is a computer program that stores and manages passwords for an internet user. It can be built in or provided as an extension for certain web browsers. A study from the University of Connecticut shows that internet users may choose to have a password because of increased security and not needing to memorize so many passwords (Fagan et al., 2017). Password managers can store over 100 unique passwords, measure their strength, alert users to data leaks, and encrypt passwords. However, some users fear using a password manager compromises their accounts because of weak or no encryption. This study explains the benefits of password managers, their legal, ethical, social, and security concerns, how the concerns are handled now, and further required research for improving them.

Benefit of Password Managers

According to a CNN news report, the average user has 100 online accounts (Kelly, 2024). Most are password-protected. Some users often reuse passwords for multiple accounts because they can only remember a few passwords at a time. However, this puts them at high risk of having a lot of personal information stolen. If one password is compromised, all accounts with the same password are compromised (Dale & Lewis, 2020). By using a password manager, a user can save a unique password for all accounts without the need to remember it. A user only needs to memorize its master password, log into the password manager, and the passwords will be accessible via autofill or copy and paste.

Legal & Ethical Issues

Even though certain laws prevent stealing personal information, – I.E. Virginia State Law prohibits examining private financial or employment records (*§ 18.2-152.5. Computer Invasion of Privacy; Penalties*, 2022) – some hackers may not comply. Therefore, according to the

SECEPP software engineering principles, a password manager must be safe for all users (Gotterbarn, 2001). To address this ethical issue, password managers should ensure all stored passwords are strong and have not been leaked. To measure password strength, LastPass uses a strength meter (Steel, 2012). The strength meter marks passwords as weak, moderate, or strong based on the following factors: not a common word or phrase, number of shared access, number of characters, and if it contains any special characters – lowercase letters, uppercase letters, symbols, and numbers. To detect data leaks, LastPass uses a process called "dark web monitoring." LastPass monitors users' email and alerts them if their accounts have been compromised (Bachmann, 2020). Password managers that implement dark web monitoring and strength meters together provide users with increased security by having strong and secure passwords.

Security & Social Concerns

Some password managers apply encryption is when one user shares a password with another trusted user. According to Nell Dale and Dr. John Lewis, most shared passwords are easily accessible to hackers (2020). In essence, the encryption is either nonexistent or weak. Therefore, sharing passwords with other users is a major security concern. In a study from the University of Tennessee, most password managers – including LastPass – use AES-256 encryption (Oesch, 2021). This method hashes a password 14 times with 256-bit characters, using a substitution box each round (Wenceslao, 2018). By hashing, LastPass makes a password less prone to brute force attacks.

Another security concern is hackers gaining access to a user's master password, especially when stored on another password manager. This can also happen when someone shares the master password. When that happens, all the user's stored passwords are

compromised. Some password managers, like LastPass, use two-factor authentication to address this concern. But even though two-factor authentication prevents a hacker from accessing stored passwords, encrypting the master password, again, makes it harder for hackers to obtain. In a nutshell, a more advanced encryption algorithm is needed for both master passwords and stored passwords.

Further Required Research & Conclusion

Although password managers provide a strong security, further research is needed to find more advanced encryption methods for stored passwords. In a study from Northern Ilolio State University, Computer Scientist Felicisimo Wenceslao proposes a modification to the AES-256 algorithm. This method uses multiple substitution boxes (Wenceslao, 2018). the first S-Box is the original (Wenceslao, 2018). The second box is created by rearranging the substitution bytes in each row and XORing them, then replaces the first (Wenceslao, 2018). The process repeats for every hash. Other methods involve increasing the number of hashes or bit representation of the keys. People use a password manager to remember over 100 unique passwords. So, finding a stronger encryption method for password managers key to enhanced user security.

References

Bachmann, L. (2020, August 20). *What do I do when I receive a lastpass dark web alert?* The LastPass Blog. https://blog.lastpass.com/2020/08/receive-lastpass-dark-web-alert/

This source describes a process called Dark web monitoring. Dark web monitoring is a process used by LastPass to detect data leaks. Data leak detection is one of the key ethical issues with password management systems as it helps ensure the safety of all internet users. The concept of data leak detection also addresses another area where further research is required. In the event of a data leak, the user is just alerted to change their password manually. One area where further research may be required is finding a method to change a user's password in case of a data leak.

Dale, N., & Lewis, J. (2020). *Computer science illuminated* (7th ed.). Jones & Bartlett Learning.

Nell Dele is a computer scientist –with a Ph.D. from the University of Texas, Austin – who spent 25 years in the field of Computer Science. Dr. John Lewis is a professor of Computer Science at Virginia Tech. In this textbook, Dale and Lewis explore the essentials of computer science, which includes information on computer networking, Boolean logic, AI concepts, computer security concepts, etc. This textbook provides information on password criteria, as well as password management guidelines – both of which can help describe factors LastPass uses when measuring the strength of stored passwords for an internet user. The password management guidelines – especially the one that advises against reusing the same password for multiple accounts – also help emphasize the reason why some internet users prefer to have a password manager based on a study conducted at the University of Connecticut.

Fagan, M., Albayram, Y., Khan, M. M. H., & Buck, R. (2017). An investigation into users' considerations towards using password managers. *Human-Centric Computing and Information Sciences*, *7*(1). https://doi.org/10.1186/s13673-017-0093-6

In this study from the University of Connecticut, Dr. Michael Fagan –a computer scientist with a Ph.D. in Computer Science from the University of Connecticut – and his colleagues interview internet users who do and don't use a password manager. The most important research question in this study is "What are the main reasons behind using password managers (Fagan et al., 2017)?" Using the answer to this research question can help emphasize the introduction by answering the following research questions in the introduction: "What is a password manager?" and "Why do some people choose to use a password manager?"

Gotterbarn, D. (2001). Software engineering code of ethics and professional practice. *Science and Engineering Ethics*, *7*(2), 231–238. https://doi.org/10.1007/s11948-001-0044-4

In this scholarly article, Donald Gotterbarn – a retired Computer Science professor who last worked at East Tennessee State University – Dr. Keith Miller – A Computer Science Professor at the University of Iowa, Simon Rogerson – a retired Computer Science professor who last worked at De Montfort University, and Steven Barber – A manager of TIBCO Streaming products – outline the SECEPP engineering principles. The Software Engineering Code of Ethics and Professional Practice (SECEPP) is a code for how software engineers should ethically handle software. The code consists of eight principles about how software engineers should develop their software ethically and beneficially. Out of the eight principles outlined in the SECEPP principles of engineering, ensuring the safety of the public plays a critical role regarding legal and ethical issues of password managers. Overall, the principle of ensuring the

public's safety lays the foundation for understanding how LastPass measures the strength of certain passwords for all internet users, as well as what to do in the event someone's master password gets leaked. The SECEPP principles of engineering can also help with further required research on password managers since engineers must ensure that internet users are extra secure with them.

Kelly, S. M. (2024, February 26). *We each have an average of 100 online accounts. here's how to make sure they aren't a nightmare for your family if you die | CNN business*. CNN. https://www.cnn.com/2024/02/26/tech/digital-legacy-planning-personal-technology/index.html

Samantha Kelly is an author for CNN about how technology impacts our lives. In this article, Kelly illustrates how technology impacts our lives and ways to preserve accounts when an internet user dies. Although password management has nothing to do with preserving information of a dead internet user, Kelly does mention two key details about password managers in a section. One key detail Kelly mentions is the fact that it's less of a burden to memorize 100 passwords. The other important piece of information Kelly mentions is that having a password manager allows passwords to be shared with other family members when their loved one dies. Together, these pieces of information help establish some background information on why people choose to use password managers and help establish the idea of further research required for encrypting passwords stored in a password manager. When passwords are encrypted in a password manager, they become harder for hackers to access when shared between two or more users.

Oesch, T. (2021). *An analysis of modern password manager security and usage on desktop and mobile devices* .

In this study from the University of Tennessee, Knoxville, Dr. Timothy Oesch – a cybersecurity researcher – explores how strong password managers are. In the section on password encryption, Dr. Oesch covers the types of encryption algorithms most password managers use – the most common one is AES-256. Understanding how password encryption algorithms work not only helps understand how information that is shared is protected, but it also influences a need to conduct further on stronger encryption algorithms. If an encryption algorithm is weak, then a shared password may become easily accessible to hackers.

Steel, A. (2012, February 8). *Resolutions with lastpass: #10 strengthen your master password*. The LastPass Blog. https://blog.lastpass.com/2012/02/resolutions-with-lastpass-10-strengthen-your-master-password/

In this article, Amber Steel – an author of The LastPass blog – illustrates the idea of creating a strong password. Although Steel focuses on creating a strong, unique master password that you can remember by heart, her idea can also be applied to passwords internet users store in their password manager. Steel points out an essential password strength feature in this article: LastPass' "How strong is your master password?" feature, also called the strength meter – which is also used on passwords stored in LastPass. By measuring the strength of a password, LastPass is ensuring the public's safety by letting the user know if a password needs to be changed – taking four factors into account. Understanding how LastPass measures password strength helps address the ethical issue of ensuring the safety of all internet users according to the public interest based on SECEPP engineering principles.

Wenceslao, F. (2018). Enhancing the performance of the advanced encryption standard (AES) algorithm using multiple substitution boxes. *International Journal of Communication Networks and Information Security (IJCNIS)*, *10*(3).

Creating a more advanced encryption system is one part of password managers where further research is needed. More advanced encryptions will decrease the vulnerability of passwords that are shared between two or more internet users. In this article, Felicisimo Wenceslao – who has a B.S. in Computer Science – illustrates the concept of the AES algorithm that is used by most password managers when encrypting a stored password. Wenceslao also creates a proposed algorithm by using multiple substitution boxes – which hash one character in the password for another. This means some characters will be hashed into characters from one substitution box, while other characters will be hashed from a different box. Increasing the number of substitution boxes on the current AES algorithm is one possible research solution for enhancing the security of password managers as it will make it more difficult for a hacker to decrypt.

§ 18.2-152.5. Computer invasion of privacy; penalties. (2022). Virginia.gov. https://law.lis.virginia.gov/vacode/title18.2/chapter5/section18.2-152.5/#:~:text=A%20person%20is%20guilty%20of

Since the audience is in Virginia, using Virginia state laws as an example could help underscore the legal issues of hacking into internet user accounts. Although hacking without authority is a criminal offense, most hackers don't comply - regardless of whether a hacker is a black hat, white hat, or grey hat. Therefore, password managers take the ethical issue of

protecting internet users into account. In essence, understanding how the legal issue of hacking isn’t enough alone helps establish the ethical issue of protecting password manager users.