Global Information Assurance Certification Paper

Password Management Applications and Practices

GIAC (GSSEC) Gold Certification

Author: Scott Standridge, scotts985@gmail.com
Advisor: Rob Vandenbrink
Accepted: 2/15/2016

Abstract

Passwords are fundamental for information security. They are used as a first-line defense in securing almost all electronic information, networks, servers, devices, accounts, databases, files, and more. Most of us now have a multitude of passwords we need to somehow track and remember. This paper will cover the latest recommendations for secure password management practices including the use of third party password management applications. It will provide an overview of how password management applications work, the security they provide, and the benefits and risks of using them. It will then take a deeper dive into the options, technical implementation, and potential security vulnerabilities of three of the most popular password applications: Last Pass, Dashlane, and Keepass.

1. Introduction

Password compromise is still the root cause behind many cyber breaches. In 2014 two out of three breaches involved attackers using stolen or misused credentials (Higgins 2014). Yet, the majority of internet users still do not follow secure password management practices (Rubenking 2015).

Secure password management requires that unique passwords be used for each and every account. Passwords must be both long and complex; comprised of numerals, mixed-case letters, and special characters. They also should not be words, or be names of anything which could be associated with their owner. Finally, passwords must be changed frequently.

Secure password practices result in numerous cryptic passwords which are very difficult to keep track of. It is impossible for most people to consistently remember more than just a few of them. Yet, according to a recent survey conducted by Google, over fifty percent of users report that they rely on memory alone to keep track of their passwords. The fact that they rely solely on memory is a clear indication that they are not following secure password practices, because if they can remember all of their passwords then they must be creating simple passwords, or reusing passwords for multiple accounts, or both (Ion, Reeder, and Consolvo, 2015).

Password management applications are one answer to the problem. These applications fulfill all the secure password management requirements. They create complex passwords that are very difficult to guess or crack. They can remember an unlimited number of passwords. They are fast, efficient, easy to use, and most include additional functionality such as auto-fill to speed up or eliminate the data entry required for an online purchase or account registration. Although there are other methods to remember and track passwords, none of them offer the convenience that password management applications provide.

Scott Standridge, scotts985@gmail.com

2. IT security experts recommend password management Applications

Password management applications are recommended by the vast majority of IT security experts. Yet the vast majority of non-experts do not use them to manage their passwords. A recent survey of both security experts and Non-expert web users conducted by Google revealed some interesting differences between the two groups. According to the Google survey, seventy-three percent of security experts use a password manager themselves; compared to only twenty four percent of non-experts. Both experts and Non-experts agree it is very important to follow secure password practices, but they disagree on the benefits of using a password management application for this purpose. Forty eight percent of the security experts polled ranked the use of password management applications as one of the top things people can do to stay safe on the internet; while only three percent of non-experts thought that this was an important practice to follow. It seems that the average web user is either unaware of the benefits gained by using a password management application, or that they do not trust them to keep their passwords secure (Ion, et al., 2015).

3. Manual Password Management Methods

Besides password management applications, there are also manual methods that can be used to track passwords.

3.1. Use of notebook or paper

One manual method for password management is to manually write the passwords down in a notebook or piece of paper. Although this method seems primitive, it does have its merits. Keeping your passwords offline protects them from the myriad of internet based attacks; although the passwords are still susceptible to physical compromise should the paper be viewed, lost or stolen. The biggest drawback of this method, however, is its inconvenience. It requires a great deal of manual effort; the storage medium must be carried from place to place, passwords must be manually copied to be used, and the printed material must be kept up to date. It is the amount of labor and the inconvenience of this method that makes it impractical for the average user to use securely.

Scott Standridge, scotts985@gmail.com

3.2. Storing passwords unencrypted in a file on a connected device

Another method is to store the passwords unencrypted in a file on the devices from which they will be used. Although this is more convenient then the paper based method above, it is not a very secure option. Besides being vulnerable to physical theft, this method also exposes the passwords to all the various internet attacks and malware. It is also not portable, because the passwords cannot be accessed from other devices.

3.3. Storing passwords using browsers

Browsers can also be used to store passwords. Chrome, Firefox, and Internet Explorer all have built-in password managers. But both Chrome and Internet Explorer store the passwords unencrypted on the device. Mozilla Firefox, however, does have an option which allows you to encrypt your saved passwords and to protect them using a master password. This is very similar to how Password Managers store your password, except that Firefox cannot create new passwords for you, and has very limited syncing capabilities (Hoffman, 2015).

4. Overview of Password Management Applications

There are many password management applications to choose from. Choosing the best one depends upon the needs of the individual. According to recent reviews conducted by PCMAG, Life Hacker, and Digital Trends, Lastpass, Dashlane, Roboform, and KeePass are all among the top rated password manager applications available today. All four of these applications provide the following features, except where noted (Rubenking, 2015).

4.1. Create unique passwords

These password management applications can provide unique passwords for each account. They have the capability to create and save an unlimited number of passwords. This greatly reduces the potential damage if one account is breached and the password is compromised, because the stolen password cannot be used to access any other account.

4.2. Create strong passwords

All of them can create secure passwords which provide protection from password cracking attacks, such as brute-force, dictionary or rainbow table attacks. The format of the password is configurable. All three of these managers allow you to select the length and type of characters to be used for the generated passwords.

4.3. Safely store passwords

The applications store your passwords using strong encryption. The passwords are never stored in plaintext. This helps to protect them because even if they are stolen they are still useless to an adversary unless he can decrypt them. The key needed to protect and decrypt them is called the master password. The master password is not stored anyplace. It is the one password which still needs to be remembered.

4.4. Bookmark web sites

The URLs, user ids and passwords are all stored together in the password database. The URL must match exactly or the credentials will not be supplied. This can help to alert the user to phishing attacks because the user id and password for a site will not be provided by the application unless the URL is an exact match of the saved URL.

4.5. Auto log-in to websites

There is no need to type your user id and password, once it has been saved by one of these applications. The applications can log you in from a single click on a saved URL. This in not only very convenient and efficient, but it also helps to protect against key logger attacks because passwords do not need to be re-typed at the keyboard.

4.6. Allow additional information to be saved in the password database

The password database can also be used to save other personal information, such as credit card numbers, PINS, name, address, telephone number, etc. This additional feature provides a convenient way to secure your other important information on-line.

4.7. Auto fill forms

Besides passwords, the managers can also auto fill information on common forms. For example, common information which is needed to make purchases on line, such as credit card information, name, home address, and email addresses can all be auto-filled from the database.

4.8. Synchronize your password across devices

All, except Keepass, offer the ability to synchronize your passwords across other devices. The encrypted passwords and management software can be downloaded from the manager site or the cloud to any other device supported. Keepass users can also synchronize their passwords across devices, but they need to use an outside service, such as Dropbox, to do it.

4.9. Provide access to your passwords from a public device

Lastpass, Dashlane, and Roboform, allow access to your passwords through their websites. On a computer where the password manager is not installed the passwords can be retrieved from the password manager website. The decryption of the passwords in this case is carried out locally through client scripts which are embedded in the webpage. KeePass, however, does not have this feature. It is a local database only. To retrieve passwords from KeePass they must either be carried on a USB device or through a third party application.

4.10. Password Strength Report

Three out of four of these applications will rate the strength of your current passwords. The exception is ROBOFORM, which does not have this capability at the time of this writing.

4.11. Export passwords and user IDs

All of them allow you to export your passwords in various formats.

4.12. Multi-Factor Authentication

All of the managers offer some means of multi-factor authentication.

4.13. Password Sharing

All of them except Keepass offer the ability to share passwords with friends or family. Passwords are shared securely using TLS for transport and are sent in their encrypted form only. To share passwords, Lastpass and Dashlane use public / private key technology**.** Each user is assigned a public and private key when they first install the applications. The private key is encrypted using the vaults encryption key. To share a password, the sender enters the email address (User ID) of the person he wishes to share the key with. The password to be shared is then encrypted with the public key of the recipient. The password is decrypted on the recipient device using the private key.

5. Password Managers Mobile Phones

Be careful before choosing to use a password management application on a mobile phone, however. Most of them use the copy and paste function of the clipboard to pass credentials between the Password Manager and the websites or applications. The clipboard is not a secure means of transfer. It can be accessed by any other application which is installed and running on the device. This means your password could be stolen by any one of these applications if it contains the necessary malware (Goodin, 2015). At the time of this writing Lastpass, Dashlane and Roboform use the clipboard on both Android and IOS phones. The latest mobile version of Keepass, Keepass2 for Android, however, does not. Keepass2 has an Android Keyboard which can pass credentials to applications and Websites without using the clipboard (Crawford, 2014). Another password manager that can avoid this vulnerability is 1Pasword. 1Password offers a built in browser for both operating systems which allows the passing of credential to websites directly. In addition, they also have a new beta-version for Android 5 (Lollipop) which uses the new application interface of this operating system to pass credentials to applications without making use of the clipboard (Goldberg, 2014).

6. Lastpass

The following provides a deeper dive into the specifics of the Lastpass application. We will look at some of its additional features, the technology it uses for security, its security vulnerabilities, and the reported data breaches it has endured.

6.1. Overview

Lastpass is currently the most widely used password manager with over seven million users and 15000 businesses. It was founded in 2008, and was just recently acquired. A company by the name of Logmein acquired Lastpass in October of 2015 for about 110 million dollars (Perez, 2015).

6.2. Pricing

Lastpass on a single device is free. But the cost is twelve dollars per year to use it across multiple devices.

6.3. Additional features

Lastpass has many additional features that are not offered by the other password applications. Three of them are as follows:

6.3.1. Multifactor authentication

Lastpass includes many additional options for multifactor authentication.

1. *Web Authentication Applications*

It supports many web authentication applications such as Google Authenticator, Microsoft Authenticator, Authy, Duo Mobile, and Transat.

2. *Physical Grid*

This option uses a printable GRID to provide an additional PIN for 2 factor sign-on.

3. USB

Lastpass supports Yubiko and Sesame USB based authentication.

4. *Fingerprint*

LastPass has support for various fingerprint readers, including Windows Biometric Framework.

6.3.2. One time passwords (OTP)

A One Time Password (OTP), as the name implies, is a password which can only be used once. These passwords are to be used instead of the master password when there is more of a risk that the master password may be stolen. Lastpass recommends using them for access from a public computer or a public network.

6.3.3. Recovery of the account for forgotten master passwords

Recovery of the password vault is a feature that allows a user to recover his password vault should he forget his master password.

6.4. Security premise

The Lastpass slogan is the "Last Password you will ever need to know". The last password that is referred to in the slogan is the master password. The master password is used to derive the encryption key for the password database. The password database is referred to as the vault. The vault is protected because it is stored using very strong encryption and the master password is required to decrypt it. Lastpass does not store this password anywhere. The only storage of the master password is in the memory of the owner. The premise is that your master password cannot be stolen from Lastpass because Lastpass does not know it (Lastpass 2015).

6.5. Encryption key derivation

To convert the master password into an encryption key, Lastpass uses Password-Based Key Derivation (PBKDF2) with SHA-256. PBKDF2 is a standard function which is part of the Public-Key Cryptography Standards (PKCS). The PBKDF2 function

requires a seed, a salt, number of iterations, a hashing algorithm and the plain text master password to derive the key. Lastpass uses SHA-256 as the hashing algorithm, the user id as the salt, and a random number as the seed value. The number of iterations is a configurable value that for windows currently defaults to 5000. The master password is supplied by the owner at the time of the initial login. The entire key derivation process takes place on the local device. The master password is never sent over the network in plain text form. The key can only be derived locally on the client machine because this is the only place and time in which the master password is known. The final derived key is the symmetrical key used to encrypt and decrypt the password vault (Lastpass 2015).

6.6. Authentication key derivation

The master password is also used to derive the authentication key. The authentication key, as the name implies, is used to authenticator a user when she logs into LastPass. To derive the authentication key, the derived encryption key undergoes an additional single round of PBKDF2. The formula for this additional round of encryption uses the master password as the salt value and the encryption key as the password value (Vigo, 2015).

6.7. Server key encryption

Finally, on the server side, Lastpass uses the PBKDF2 function again with a large number of rounds to encrypt the authentication key for storage on the server. The specific number of rounds used is not published for security reasons (Lastpass 2015).

6.8. Vulnerabilities revealed at the BlackHat conference November 2015

As one of the oldest and most popular password management application, Lastpass has undergone extensive scrutiny, analysis, and penetration testing from various security experts. Two of these experts are Martin Vigo and Alberto Garcia who revealed the following vulnerabilities at the Black Hat European Conference in November of 2015:

6.8.1. Client Side Vulnerabilities

The following client side vulnerabilities can only be exploited if an attacker is able to gain access to a victim's computer, although root access is not required.

1. *Recover the account vulnerability*

Vigo and Garcia showed how the Account Recovery feature of Lastpass could be compromised to gain access to a victim's password vault. The Account Recovery feature is implemented using a special type of a One Time Password that enables a user to login and decrypt their password vault. The researchers were able to show how they could retrieve this recovery one-time password (ROTP) from local storage and then use it to login and access a victim's password vault. The victim does not even need to be actively logged in, as the ROTP is always available from storage. To make matters worse, once the ROTP is obtained, the login can be performed from anywhere because the ROTP also bypasses both multifactor authentication and IP validation (Vigo, 2015).

2. *Obtaining the vault encryption key through Cross Side Scripting*

Another vulnerability revealed at the conference was the stealing of the vault encryption key from the victim's computer while the victim is currently logged into Lastpass. The researchers discovered that the key to the database is stored on local storage in encrypted form. They were able to demonstrate how the key could be lifted and decrypted using a combination of cross side scripting (CSS) and cross side request forgery (CSRF) (Vigo, 2015).

3. *Bypassing multifactor authentication*

The presentation also showed how Lastpass multifactor authentication could be bypassed. The trust token used to validate the second level authentication is stored locally in plaintext in the browser plug-in and the DOM. This token does not change and once obtained it can be used along with a compromised master password to log-in to the victim's password vault (Vigo, 2015).

Scott Standridge, scotts985@gmail.com

4. Remember master password option

Although this vulnerability was previously reported by Vigo and Garcia, it was included in this presentation as well, and does still exist. If the user selects the option, "store password," then the user id and master password is stored locally in the browser plug-in where it can potentially be stolen by an adversary**.** Although the master password must first be decrypted before it is useful, the researchers were also able to show how they could accomplish this. Lastpass now includes a warning when this option is invoked. The warning was added in late 2014 in response to the fist announcement of this vulnerability (Vigo, 2014).

6.8.2. Server side vulnerabilities

Server side vulnerabilities can only be exploited if there is a major breach at Lastpass. The adversary would need access to the servers. The following server side vulnerabilities were presented:

1. *Potential to steal account credentials*

The researchers showed that if an adversary could modify the victim's password vault on the Lastpass server, then they would be able to retrieve the user id, password, and session cookies for each account. They discovered that Lastpass includes a parameter, "custom_js", for every account in the vault. The purpose of this parameter is to inject a JavaScript pay load in the login pages to pass the user id and password. However, if the script is modified by an adversary it could be used instead to steal the login credentials (Vigo, 2015).

2. *OTP vulnerability*

To implement One Time Passwords, Lastpass stores the encryption key on the server. Although it is encrypted before it is stored, having the key that can decrypt the password database on the server is in itself a potential security risk. Vigo also discovered that the encryption method used to encrypt the key is not as strong as it should be. It does not use PBKDF2. As stated by Vigo, "the formula to derive this key is *SHA256(SHA256(username+OTP) + OTP)* where OTP are 16 random bytes. Given that the

username is known, and that there is no PBKDF2 used to derive the key, anyone on the Lastpass side would have to brute force only the OTP (128 bits) rather than 256." Although he goes on to admit that brute forcing 128 bits is not easy, it is much easier than guessing a 256 bit key (Vigo, 2015).

6.8.3. The vault is only partially encrypted

The vault is also only partially encrypted. The URLs are in clear text allowing an adversary or an employee at Lastpass with access to the database to see them (Vigo, 2015).

6.8.4. Outside attack using GOOGLE

Although not a vulnerability with the Lastpass software, the researchers also showed how the GOOGLE search engine could be used to find Lastpass user ids and passwords. They simply searched for "extensions.Lastpass.loginpws" which is the fieldname used by the Firefox plug-in to store their passwords. This search brings up dumps of data that people have sent to various forums and other websites. In many cases when they posted this data, they unknowingly also exposed their user ids and passwords (Vigo, 2015).

6.9. Lastpass response to the BlackHat conference November 2015

A week after the conference, Last Pass posted on their blog that they were made aware of these vulnerabilities in 2014 and they have been working to remediate them. Among other fixes they do now offer the option to disable account recovery and another option to better secure it. They also have published a list of recommendations which can be followed to better secure your usage of Lastpass (Gott, 2015).

6.10. Lastpass breaches 2011 and 2015 (Attacks on the Server or Cloud)

The Lastpass password manager was breached in 2011 and again in 2015. Neither of these compromises was deemed to be critical, however, because the actual passwords stored in the password databases were not exposed. In 2011, the email addresses and the

hash values of master passwords may have been compromised. In 2015, email addresses, salt values, and the hash values of master passwords were once again compromised. But according to the CEO of Lastpass and several other security experts the encryption is strong enough that the only clients at risk are those who may have used a simple master password which could be susceptible to cracking techniques. That said, Brian Krebs does suggest at the end of his report on the breach that "If you entrust all of your passwords to Lastpass, now would be a terrific time to change your master password" (Krebs, 2015).

6.11. Lastpass Support

Lastpass has good user documentation and adequate technical documentation. There are also forums and various third party articles describing their technical implementation. Lastpass does also accept and answer support questions by email. Although my personal experience with regard to their support I cannot rate highly; I asked Lastpass a support question regarding the use of the clipboard on Android, and although they did respond to my inquiry, they did not answer the question. I was instead directed to documentation on the auto-fill feature which only explains how to use the feature, but not how it is implemented.

6.12. Lastpass Summary

Despite the recently found vulnerabilities and breaches, some experts still consider Lastpass to be a safe and viable option for password management. The company has fixed some of the issues reported and has recommended safe practices as a work around to the remaining ones. Vigo and Garcia noted in their blog that they still regard Lastpass as a solid tool and as a safer option than using weak or the same passwords. They point out that they only scrutinized Lastpass and it is possible that other web management applications have similar vulnerabilities (Vigo, 2015). Another security expert, Bob Covello, agrees with them. He states in his blog post, "Lastpass is still safe," and "any password manager is safer than the current password practices used by most folks" (Covello, 2015).

7. Dashlane

The following provides a deeper dive into the specifics of the Dashlane application. We will look at some of its additional features, the technology it uses for security, and its potential security vulnerabilities.

7.1. Overview

Dashlane is one of the newer password management applications. It was founded in 2011, and in three short years it had exceeded 2 million customers. One reason for its quick acceptance may be due to the reputation of its co-founder, Bernard Liautaud. Bernard is highly regarded by many in the industry as he was also the founder of Business Objects, which he later sold to SAP for about seven billion dollars (Lunden, 2014).

7.2. Pricing

Dashlane is free for a single device. But if you want to synchronize your passwords across multiple devices then the current cost is $39.99 per year**.**

7.3. Additional features

The following are three unique features offered by Dashlane

7.3.1. Password Changer

Dashlane has a password changer feature which allows all the passwords in the database to be changed automatically. Dashlane can login to each website on behalf of the user, and change the password.

7.3.2. Emergency Contact

Dashlane also allows you to set up an emergency contact that can gain access to your passwords in the case of emergency or death. This feature follows the same logical flow as sharing passwords, except the sharing is scheduled to occur in the future after a pre-defined waiting period. If there is no activity on the share request before the end of the

waiting period, then the passwords will be shared with the emergency contact. The process is as follows:

1. An email is sent to the person designated as the emergency contact. This person must accept this role, and must install Dashlane if they are not currently a Dashlane user. (They can install just the free version, however.)
2. Dashlane will then provide them with a private key and it will store this key in their password vault.
3. At the next log-in to Dashlane, all the passwords will be encrypted using the public key of the emergency contact and stored on the Dashlane server.
4. The person designated as the emergency contact can now request access to the passwords. If they request access (presumably at the time of an emergency) then a request will be sent to the database owner. If this request is not rejected within the specified waiting period, then access will be granted.

7.3.3. Breach Notification

Dashlane sends an email notification if any of the websites in the password database has been breached.

7.4. Security

The Dashlane security premise is similar to Lastpass. The password vault is protected by an encryption key which is based upon a master password known only to the user. The master password is never stored or sent. The implementation of the security, however, is not the same.

7.5. Encryption key derivation

The encryption key, like Lastpass, is derived using the master password with PBKDF and SHA-256. The number of iterations is not configurable and is about 10000.

The encryption key is derived on the client machine only. But unlike Lastpass it is not stored or sent in any form. (Dashlane, 2015).

7.6. Authentication key derivation

The Authentication key is independent from the master password. It is derived from a device key which is composed of a secret pin and the device attributes. Dashlane creates a unique pin for each device at the time of device registration. This key is stored and encrypted locally in the password vault database along with the other web site passwords.

7.7. Server key encryption

No master password or payment information is stored on the server side. The Device key on the server is encrypted using the Dashlane private key. Communication between the browser and Dashlane is secured using AES256 with the OpenSSL.

7.8. Vulnerabilities

7.8.1. Password Changer

The optional password changer feature is implemented on the server side. This is the one case where your passwords are sent to and from the Dashlane server not encrypted by the encryption key, although under the protection of SSL. The passwords may be vulnerable to compromise on the Dashlane server during this change process. Dashlane does state, however, that all passwords are deleted after the process is complete (Fowler, 2014).

7.8.2. Breach Notification

Although the technical implementation of this feature is not available in their documentation, the fact that Dashlane can send breach notifications for any sites visited indicates that the URLs in the password database are stored in clear text. This would allow an adversary or an employee at Dashlane with access to the database to see them.

7.9. Dashlane Support

Dashlane provides good user documentation and excellent technical documentation. Dashlane also accepts and answer support questions by email. I asked Dashlane two technical questions regarding the use of the clipboard on the mobile platform. Both questions were answered by them within 24 hours. They were honest and forthcoming regarding their use of the clipboard on both Android and IOS.

7.10. Dashlane Summary

Dashlane is one of the top password management applications. It is a full featured solution with solid security, no reported breaches, and few potential security vulnerabilities. As Yarra Lancet of PCWorld stated in her review of Dashlane, "With its simple interface and myriad of features, Dashlane is a powerful password manager anyone should consider" (Lancet, 2013). Unlike Lastpass, Dashlane never stores any form of the database encryption key on their servers. Although this means that you cannot recover from a lost master password or use a one-time password, it results in tighter security and avoids two server side vulnerabilities found with Lastpass. The only two potential vulnerabilities known at this time are the use of the clipboard on Android and IOS, and the passing of passwords to the server when using the change password feature.

8. Keepass

The following provides a deeper dive into the specifics of the Keepass application. We will look at some of its additional features, the technology it uses for security, its security vulnerabilities, and the reported data breaches it has endured.

8.1. Overview

Keepass is a free and open source (FOSS) password management application. It was one of the first password management applications. It was created and released in 2006 by Dominik Riechl (Rubenking, 2012).

8.2. No built in Synchronization

Unlike Lastpass and Dashlane, Keepass uses a local database only. There is no web application to log into, and it does not support the synchronization of passwords over the internet. Passwords can be shared using a USB drive, or other methods such as Dropbox, however.

8.3. Additional features

8.3.1. Choice of how the password database is protected

Keepass offers a choice as to how the password database is protected. The choice is a master password, a key file, or both. On a windows machine you it can also be configured to use the windows account credentials.

8.3.2. Secure Desktop Option

Keepass offers a secure desktop option which if enabled will turn off tracing software such as keyloggers when prompting for the master password of key file.

8.3.3. Configurable Password Generation

Keypass allows for more detail in the configuration of generated passwords. It has separate configuration values for dashes, underscores, and brackets, instead of lumping them together under special characters. It can generate special passwords and keys that the other password management applications cannot.

8.4. Security

Keepass does not have a server or cloud component. It only exists locally on the client device. The master password and encryption key is never saved on a server or sent over the internet. Keepass also offers an option to use a key file, instead or in addition to the master password. The key file is an additional layer of security which can either be stored on the device or externally on a USB drive.

8.5. Encryption key derivation

Keepass also uses SHA-256 to derive the encryption key. If the master password is used in conjunction with the key file, then the formula is as follows: SHA-256 (SHA-256 (password), key file contents). The number of iterations defaults to a value of up to

6000 depending upon the device, but this number is configurable. The salts and random seed are derived from a long list of values including date and time, current tick count, performance counter, mouse cursor position, various process and thread IDs, and random bytes provided by the system's default random generator (Keepass, 2016).

8.6. Authentication key derivation

Keepass has no need for a separate authentication key because it does not have a web site in which to log into.

8.7. Server key encryption

Keepass has no need for a server key because it has no server.

8.8. Vulnerabilities

A vulnerability in the export function of Keepass was revealed in late 2015. Not only was the threat publicized but an open source hacking tool, called KeeFarce, was also released to exploit this vulnerability. The tool uses DLL injection to call an existing Keepass export method, which copies the contents of a currently open KeePass database to a CSV file. The resulting file contains the user names, passwords, notes, and URLs which were stored in the database in plain text. The file can then be uploaded to the site of an adversary (Goodin 2015).

This is a serious and very dangerous vulnerability but it is not an easy one to exploit. The device must first be compromised and controlled by an adversary before this malware could be executed. As one security expert points out in his review of the threat, it is also important to think in terms of risk. Although the impact of this risk is high, the likelihood of your local computer to be attacked by this malware is low because it first requires an adversary to have admin rights on your device (Bursell 2015). DLL injection is also not a vulnerability that is unique to Keepass; it is quite possible that other password manager application may also be vulnerable to similar attacks (Goodin, 2015). If an adversary can obtain admin rights to your computer then it is also open to a wide variety of other attacks.

8.9. Keepass Support

Keepass is open source and does not have a paid staff to answer questions. They do have a forum, excellent documentation, and tutorials, however.

8.10. Keepass Summary

Keepass is a solid password management application and a good choice for someone that does not want to store their passwords on the server of a password manager. The fact that it is open source is also a plus because with open source there are no secrets. One can be certain of how it is implemented by looking at the source code. Even if you can't personally understand the source code yourself, you can be confident that others in the open source community have reviewed it carefully. Keepass, as noted above, is also one of the few password managers that have a work-around for the Android clipboard vulnerability found with most other password managers.

9. Conclusion

In this digital age, where more and more of our transactions are sent over the internet, it has never been more important to follow safe and secure password management practices. Passwords are used to protect our on-line information including bank accounts, emails, medical records and more. The breaches in 2015 at Target, Home Depot, TJX, and Heartland Payment systems alone should be enough to convince anyone of the importance of using unique passwords for every on-line account. The need for complex passwords is also clear. Simple passwords can be cracked by modern day programs in a matter of seconds.

Most security experts recommend the use of password management applications as the most practical and secure way for people to follow secure password practices. Although they are not infallible and like all other web applications they are susceptible to attack, the majority of security experts do believe that it is much safer to use a password management application then not to use one.

We reviewed three popular password managers, but there are many others to choose from. Choosing the best one depends upon the requirements of the individual. Some requirements to consider include the need to synchronize

passwords across devices, the use of mobile devises for secure website and application login, and desired features. There are many reviews of password managers available on the internet. These can be valuable sources, but it is also important to conduct additional research. The applications continually evolve; new releases may include patches for existing vulnerabilities and make other improvements.

Scott Standridge, scotts985@gmail.com

References

Betters,E. (2013, October 11). *Password Managers Explained The Best Apps Available And Why You Need One* Retrieved December 7, 2015 from: http://www.pocket-lint.com/news/124283-password-managers-explained-the-best-apps-available-and-why-you-need-one

Bursell,J. (2015, November 9). *Concerned about KeeFarce? Don't be. Why you should still use a password vault* Retrieved December 21, 2015 from https://www.pentestpartners.com/blog/concerned-about-keefarce-dont-be-why-you-should-still-use-a-password-vault/

Covello,W.(2015,Noveber 16). *A LastPass Hack with a Happy Ending* Retrieved December 7, 2015 from http://www.tripwire.com/state-of-security/security-awareness/a-lastpass-hack-with-a-happy-ending/

Fakhrou, M. (2014, July 20). Retrieved January 3, 2016, from http://www.martani.net/2014/07/thoughts-on-dashlane-password-sharing.html

Fowler, G. (2014, December 9). *A Quick Fix for Poor Passwords*. Retrieved January 2, 2016, from http://www.wsj.com/articles/a-quick-fix-for-poor-passwords-1418126603?KEYWORDS=dashlane

Franceschi-Bicchierai,L. (2015, November 20) *Flaws In Password Manager Lastpass Expose Users' Passwords* Retrieved December 22, 2015 from http://motherboard.vice.com/read/flaws-in-password-manager-Lastpass-expose-users-passwords

Goldberg,J. (2014, November 22). *Avoiding the clipboard with 1Password and Lollipop* Retrieved January 31, 2016 from https://blog.agilebits.com/2014/11/22/avoiding-the-clipboard-with-1password-and-android-lollipop/

Goodin,D. (2014, November 21). *Using a password manager on Android? It may be wide open to sniffing attacks* Retrieved January 31, 2016 from http://arstechnica.com/security/2014/11/using-a-password-manager-on-android-it-may-be-wide-open-to-sniffing-attacks/

Goodin,D. (2015, November 2). *Hacking tool swipes encrypted credentials from password manager* Retrieved December 21, 2015 from

Scott Standridge, scotts985@gmail.com

http://arstechnica.com/security/2015/11/hacking-tool-swipes-encrypted-credentials-from-password-manager/

Gott, A. (2015, November 18). *Protecting Yourself on a Compromised Computer*. Retrieved December 29, 2015, from https://blog.Lastpass.com/2015/11/protecting-yourself-on-a-compromised-computer.html/

Henry,A. (2015, November 11). *Five Best Password Managers* Retrieved December 8, 2015 from http://lifehacker.com/5529133/five-best-password-managers

Higgins,K. (2014, April 22). *Stolen Passwords Used In Most Data Breaches* Retrieved December 5, 2015 from http://www.darkreading.com/stolen-passwords-used-in-most-data-breaches/d/d-id/1204615

Hoffman, C. (2015, September 9). *Why You Should Use A Password Manage And How To Get Started* Retrieved November 23, 2015 from http://www.howtogeek.com/141500/why-you-should-use-a-password-manager-and-how-to-get-started/

Ion, L., Reeder, R., & Consolvo, S. (2015, June 20). *"...no one can hack my mind": Comparing Expert and Non-Expert Security Practices.* Retrieved December 13, 2015, from https://www.usenix.org/system/files/conference/soups2015/soups15-paper-ion.pdf

Krebs, B. (2015, June). *Krebs on Security.* Retrieved December 22, 2015, from https://krebsonsecurity.com/2015/06/password-manager-Lastpass-warns-of-breach/

Last Pass User Manual . (n.d.). Retrieved December 30, 2015, from https://helpdesk.Lastpass.com/

Perez, S. (2015, October 9). *LogMeIn Acquires Password Management Software Lastpass For $110 Million.* Retrieved December 22, 2015, from http://techcrunch.com/2015/10/09/logmein-acquires-password-management-software-Lastpass-for-110-million/#.xkiavb3:l0bP

Lunden, I. (2014, May 19). *Dashlane Passes 2M Users, Collects $22M For Its Client-Based Password Manager*. Retrieved January 2, 2016, from

Scott Standridge, scotts985@gmail.com

http://techcrunch.com/2014/05/19/dashlane-raises-record-22m-for-its-cloud-based-password-manager-after-clocking-2m-users/

Keepass. (n.d.). Retrieved January 3, 2016, from http://keepass.info/help/base/security.html

Roberts, P. (2012, June 27). *Researcher Warns Of Security Hole In KeePass Password Manager*. Retrieved January 3, 2016, from https://threatpost.com/researcher-warns-security-hole-keepass-password-manager-062712/76738/

Rubenking, N. (2012, August 3). *KeePass.* Retrieved December 1, 2015 from http://www.pcmag.com/article2/0,2817,2408063,00.asp

Rubenking, N. (2015a, March 4). *Survey: Hardly Anybody Uses a Password Manager* Retrieved December 1, 2015 from http://www.pcmag.com/article2/0,2817,2407168,00.asp

Rubenking, N. (2015b, November 13). *The Best Password Managers for 2015.* Retrieved December 28, 2015, from http://securitywatch.pcmag.com/security-software/332517-survey-hardly-anybody-uses-a-password-manager

Vigo, M. (2014, September 18). A *look into Lastpass - Martin Vigo.* Retrieved December 22, 2015, from http://www.martinvigo.com/a-look-into-Lastpass/

Vigo, M. (2015a, June 15). *About today's Lastpass breach - Martin Vigo*. Retrieved December 26, 2015, from http://www.martinvigo.com/about-todays-Lastpass-breach/

Scott Standridge, scotts985@gmail.com