International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 05 | May -2017 www.irjet.net p-ISSN: 2395-0072

Integrated Encryption of Passwords for Enhanced Security

Nirosh P[1], Dr. Jitendranath Mungara[2]

[1]*Student, Department of Information Science and Engineering, New Horizon College of Engineering, Karnataka, India*
[2]*Professor and HOD, Department of Information Science and Engineering, New Horizon College of Engineering, Karnataka, India*

Abstract - *The present scenario poses a situation where a user needs to login to multiple websites and is expected to remember many user names and passwords for a variety of different applications. Remembering the passwords of many applications is a key convolution. The principle is to provide password vault programs that have been designed with a single interface capable of storing the usernames and passwords respectively. Users are required to remember the master password of the vault application in such situations. Subsequently, many security algorithms and security keys can be introduced to make it more difficult for hackers to crack the master password by encrypting the passwords and to enhance the overall strength and build of such applications.*

Key Words: Username, Password, Security Algorithm, Encryption.

1.INTRODUCTION

Every web application is designed in such a way that the login user always creates an account within the website that he/she launches. This will help in better maintenance of the website and helps track activities of each user. On day to day basis users launch multiple websites for reference and are required to create their login username and password for multiple accounts. It is always difficult to remember each password and username for these accounts as the complexity level of the password may vary from one website to another.

To overcome these difficulty users can store the usernames and passwords in their local machines in the form of text pads and local files. However, the saved files may get lost due to a machine format or due a virus attack or may even pose a bigger threat to the integrity of the user if his machine is hacked by external factors. In such cases if the user has stored some sensitive information such as bank passwords, account details, net banking details he may incur heavy losses.

How do we tackle this scenario where users are not exposed to security risks, yet they should be able to store the usernames and passwords in a single place? The answer to this lies in the password vault application. The application acts as a single interface where users can store information about 1) Credit Cards 2) Wireless Routers 3) Servers 4) Email Accounts 5) Bank Accounts 6) Databases 7) Driver License 8) Passport 9) Social Security Number 10) Software License etc. [1]. The users can store the information and maintain just a single master password for the application. This reduces the overhead of users needing to remember usernames and passwords for multiple accounts.

Although as a short-term solution many web browsers offer to store the usernames and passwords, there are many dis advantages of saving information on these browsers. Firstly, what if the user's machine is used by someone else, then they can access sensitive information of the other person without any permission. If the cache of the browser is cleared accidentally, then all the information is lost. The passwords saved here may or may not be encrypted hence may cause data leaks. The temporary database that the browsers use may not be designed specifically to store encrypted information hence may easily be hackable by external forces. Keeping all these factors in mind the password vault application is designed with some of the best security algorithms and with security keys (public and private keys) to make life difficult for the people who try to hack and fetch sensitive information.

Paper is organized as follows. Section 2 describes how the password vault applications have come into use and cannot be hacked into easily. A brief description of the 256-bit encryption is also described to show proof for the same. Section 3 describes some of the existing password vault applications that have aided the users on a large scale. Section 4 presents the conclusion.

2. RELATED WORK

Many password vault applications have been designed and are existing in the real world. Millions of online users are reaping the benefits of such applications and the benefits include 1) Users don't need to maintain a text pad to store the username and passwords 2) Users don't need to store the information on their mobiles and tablet devices (which might get lost or be hacked into) 3) User don't need to remember the information 4) They don't need to worry about hacking as these applications are designed using bit encryption technology like AES256.
To give a brief description of how 256-bit encryption works refer below:

256-bitencryption [2] uses 256-bit key to encrypt and decrypt information that is stored in these password vault applications. This means that a hacker will need to implement 2*256 different types of combinations to decrypt any information that is encrypted with this key. This is a big overhead for any hacker and is literally impossible for anyone or for even super-fast computers to crack the information. Previously 128 and 192-bit encryption existed, but the 256-bit encryption is the most sophisticated encryption that is existing as of now.

Typically, the 256-bit encryption is useful when doing online transactions where data is transmitted from one place to another and it cannot be hacked by middleware programs. Sensitive government information, online bank transactions and military information shared across borders all use this technology.

Table -1: Possible combinations

Key Sizes	Possible combinations
1-bit	2
2-bit	4
4-bit	16
8-bit	256
16-bit	65536
32-bit	4.2×10^{3}
56-bit	7.2×10^{16}
64-bit	1.8×10^{19}
128-bit	3.4×10^{38}
192-bit	6.2×10^{57}
256-bit	1.1×10^{77}

Table -2: Time to track the information encrypted using 256-bit encryption

Key size	Time to crack
56-bit	399 seconds
128-bit	1.02×10^{18} years
192-bit	1.872×10^{37} years
256-bit	3.31×10^{56} years

3. RESULTS

Some of the applications like 1Password [1] and RoboForm [4] that exist have been using the 256-bit encryption to store data. All that the users need to do is login to these websites and enter their email ID. After which the users need to verify their email ID accounts and a onetime master password needs to be set by the user. As the user sets the onetime master password for the application, the strength of the password entered is validated then and there, after which the users are notified. In this way, the users are helped throughout the creation of the account.

When the user finishes creating an account on these websites he simply needs to navigate through the application and select the kind of information that needs to be stored. These applications have inbuilt operations which allow the users to select the category under which the information needs to be stored. Some of the categories include:

1) Credit Card
2) Wireless Router
3) Servers
4) Email Account
5) Bank Account
6) Database
7) Driver License
8) Passport
9) Social Security Number
10) Software License.

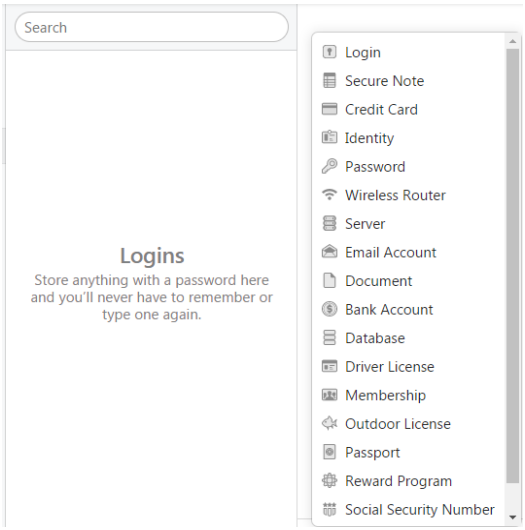

Fig -1: Some of the options available to the user

Once the information is entered by the user it is automatically stored within the application's database which is designed using sophisticated design technologies. Hence the databases that these websites use are safe and cannot be cracked open easily. Apart from storing information these databases provide additional security by storing the information in an encrypted format and data can be read only by decrypting the information.

As an additional security feature the master password can be changed after a specific time out period. Here the user doesn't need to change the password of the individual accounts, but just needs to just change the master password.

4. CONCLUSION

Even though there are multiple browsers which offer to save the usernames and passwords within their inbuilt database tree it poses many security risks as they may not be designed in an effective way by implementing all the security features which are available. Hence, the password vault applications are a big sigh of relief for the users to store the username and passwords with enhanced security.

REFERENCES

[1]1Password. Automatic Syncing Using Dropbox. http://help.agilebits.com/1Password3/cloud_syncing_with_dropbox.html.

[2]https://www.techopedia.com/definition/29703/256-bit-encryption.

[3]AgileBits, Inc. 1password agile keychain design. http://help.agilebits.com/1Password3/agile_keychain_design.html.

[4]Siber Systems, Inc. RoboForm. http://www.roboform.com/.

[5]A. Belenko and D. Sklyarov. \Secure Password Managers" and \Military-Grade Encryption" on Smartphones: Oh, Really? Technical report, Elcomsoft Co. Ltd.,2012. http://www.elcomsoft.com/WP/BH-EU-2012-WP.pdf.

[6]M. Bellare and C. Namprempre. Authenticated Encryption: Relations among Notions and Analysis of the Generic Composition Paradigm. J. Cryptology, 21(4),2008.

[7]D. Bernstein. The Salsa20 Family of Stream Ciphers. In New Stream Cipher Designs - The eSTREAM Finalists. Springer-Verlag, 2008.

[8]G. Blasko, C. Narayanaswami, and M. Raghunath. A Wristwatch-Computer Based Password-Vault. Technical report, IBM Research Division, 2005.

[9]J. Katz and Y. Lindell. Introduction to Modern Cryptography. Chapman & Hall/CRC, 2008.