

Similarly, Window's cryptographic functions as defined by Microsoft Developer Network can be used to decrypt and obtain the auto complete passwords in plain text form.

Skype

Since the HASH of the password is saved, it is not possible to directly get the password. Instead one has to use dictionary or brute force approach to find out the right password from the hash. This approach may take days or months together based on the length & complexity of the password.

Last Bit Software developed a tool called 'Skype Password'. It is a free tool used to recover Skype passwords. This tool applies universal password recovery methods like Brute Force Attacks/Dictionary Attacks at a very high speed of 200 lacs per second on a modern CPU [7]. However if the password is complex, this tool will still take lot of time. The approximate time for recovering the Skype password using 'Skype Password' tool can be obtained by another tool called 'Password Calculator'. This tool cannot be termed as a hacking tool as it need to be installed and can recover the password of only the user who has logged onto the system. However, in near future, one can expect some malware that might run without the knowledge of the logged on user.

Conclusion

We have seen in this paper that the password for any version of windows operating system including windows 9x, XP, NT, Vista and Windows 7 are not guaranteed to be hack-proof. Also we have seen that the passwords for all the major application software like Internet Explorer, Skype etc can be decrypted and obtained

bin plain text by using specific techniques. We have seen that every application that needs username/passwords, stores them using its own techniques at a unique location in the system. The security of some applications like Google Chrome depends on the security of the user's System's login passwords. Even though the passwords are strong, we have tools available that can apply universal password recovery methods like Brute Force Attacks and Dictionary Attacks at a very high speed. Thus storing of the passwords in some files, let it be registry file, on the local machine opens up the opportunities for hackers.

References

1. "A history of Windows". Windows, Microsoft Corporation. <http://windows.microsoft.com/en-us/windows/history>, 10th May 2012
2. "Windows Password", Vitas Ramanchauskas, downloaded from <http://www.thenetworkadministrator.com/hack/WindowsPasswords.htm>, 10th May 2012
3. "Security Accounts Manager", Wikimedia Foundation, https://en.wikipedia.org/wiki/Security_Accounts_Manager, 20th May 2012
4. "Windows Registry", Wikimedia Foundation, https://en.wikipedia.org/wiki/Windows_registry 20th May 2012.
5. "What is Registry?", Microsoft Corporation, <http://windows.microsoft.com/en-US/windows7/What-is-the-registry>, 20th May 2012
6. Fabrice DESCLAUX and Kostya KORTCHINSKY , "Vanilla Skype part 2", RECON2006, Suresnes, FRANCE, June 17th 2006
7. "Skype Password", Last Bit Software, <http://lastbit.com/skypepf/default.asp>, 3rd June 2012.