ISSN:2249-5789
Gaurav Arya et al , International Journal of Computer Science & Communication Networks,Vol 2(3), 430-435

Hacking of Passwords in Windows Environment

C.K. GOEL and GAURAV ARYA*

Professor of Mathematics, Amity University, NOIDA, * Dept of Mathematics CCS University, Meerut (UP)

Abstract: Hacking is so simple! Not only the operating system's loop holes offers opportunities to hackers but also the applications like Skype and Google Chrome developed for the operating systems are quite attractive to hackers. In this paper I present the various ways in which the passwords like user account's passwords stored by the operating system or the passwords required by different applications are stored on the system and can be hacked by intended hackers. This paper presents in depth research of the password storage mechanisms implemented in various versions of Windows and various application software and can be exploited by hackers.

Keywords: Hacking, Windows, SAM, Skype

Introduction

Passwords can be login passwords for operating systems like Windows or login password for any application like yahoo messengers etc or login password for any web site like email login passwords. We will study the password storage mechanisms and analysis of their strengths for Microsoft Windows operating system and the applications developed for it.

Microsoft Windows is the name given to the family of operating systems developed by the the US based company Microsoft. Microsoft first introduced an operating environment named Windows 1.0 in November 20, 1985 [1]

In this paper, we will discuss Windows 98/ME, Windows NT/XP and Windows 7. We will also study how actually the passwords of various applications like Web Browsers store the passwords on local drives.

Password Storage Mechanism for Windows operating system

Windows-based computers utilize two methods for the hashing of user passwords, both having drastically different security implications. These are LAN Manager (LM) and NT LAN Manager version 2 (NTLMv2). A hash is the result of a cryptographic function that takes an arbitrarily sized string of data, performs a mathematical encryption function on it, and returns a fixed-size string. Windows Typically use RC4 and MD5 encryption algorithms to encrypt the passwords before storing.

Windows 98/ME

In Windows 98/ME passwords are stored in password list (.pwl) files. The name of the pwl file is the name by which we logon to the system. Encryption algorithms involved in the storage of passwords in pwl files are RC4 and MD5. All *.pwl files are generally stored in the C:\WINDOWS folder. We can find all the *.pwl files on the system using the operating systems find option.

These .pwl files are readable in any text editor like Notepad, but they are definitely not understandable. A typical example [2] of the contents of a .pwl file is:

ISSN:2249-5789
Gaurav Arya et al , International Journal of Computer Science & Communication Networks,Vol 2(3), 430-435

ã,...-

ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ

ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ

ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿ ÿÿÿÿÿÿÿÿÿÿÿÿÿÿÿR

p u.ÐX+□ |rÐq"±/2³ Êå¡hCJ,D × `ÍY¥□ !íx}(□ qW¤ãÆ±<!?àÜ6šá˜ôæ4+3/4 õ+%E°ËÔýmÇÔ ÞI», B à×œøÐ...'@

Windows NT/XP/Vista/Windows 7

SAM Database

Majority of the different versions of Windows like Windows NT, Windows 2000, Windows XP, Windows Vista and Windows 7 uses Systems Account Manager (SAM) to store user's credentials. SAM is implemented as a registry file to store user's passwords [3]. A registry file is a hierarchical database that stores configuration settings and options on Windows Operating Systems [4]. It contains the information about system hardware, installed programs and settings, and profiles of each of the user accounts von your computer [5]. All the registry entries are store in (key,value) pairs. Each Key can contain sub keys. Keys are referenced with syntax similar to Windows' path names, using backslashes to indicate levels of hierarchy. Each sub key has a mandatory name, which is a non-empty string that cannot contain any backslash, and is not case sensitive. The registry keys can be accessed from a known Root Key Handle. To refer to the SAM, the handle used is HKEY_LOCAL_MACHINE (HKLM). HKLM key contains a sub key called SAM. The registry for SAM is stored at location:

%SystemRoot%\System32\config\

It is used to refer to full SAM database for all domains and users. Each SAM database contains all built in accounts and configured accounts (all user and administrative accounts) for all domains. It notably contains the user names that can log on to that domain, a cryptographic hash of each user's password and the location of storage of their user registry keys i.e. HKLM etc. [4]. The SAM registry file is locked for exclusive use while the OS is running.

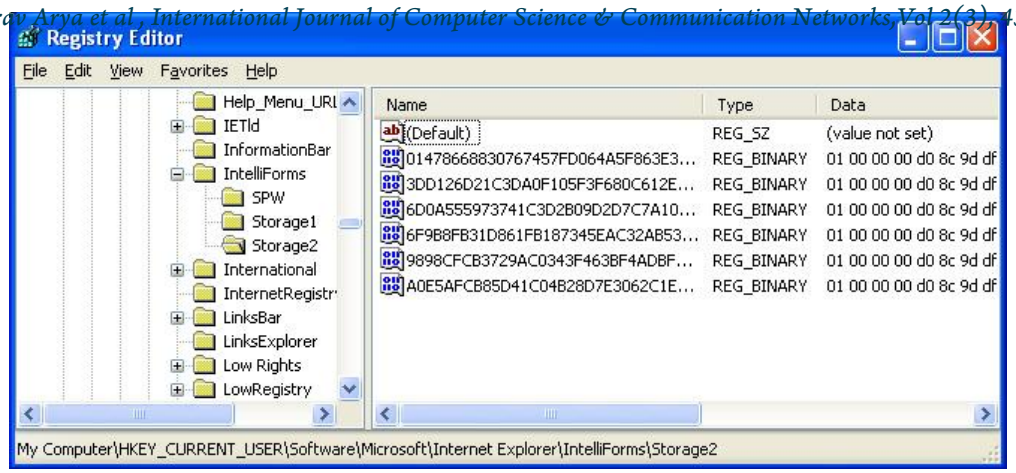
The SAM directory contains the user's passwords in either old LM Hash for windows prior to Windows NT Service Pack 4 (SP4) or NTLM hash which is in use from Windows NT SP4 till date including Windows 7 Because the SAM stores its information in the SAM database, we can assume that NT is only as secure as its SAM data.

Password Storage Mechanisms for Applications

Internet browser applications

Internet Explorer (IE):
IE saves two types of passwords: sign-on passwords and HTTP basic authentications (generally proxy and router configuration) passwords.

IE below version 7 stores both the passwords in encrypted form in the secure location known as 'Protected Storage' at the following registry location:



HKEY_CURRENT_USER\Software\Microsoft\Protected Storage System Provider

Windows introduced the secure 'Protected Storage' location to allow applications like IE/Outlook etc to store the secret credentials securely in an encrypted format.

With version 7 onwards IE uses a new mechanism to store the sign-on passwords. The encrypted passwords for each website and auto complete passwords are stored along with hash of the website URL in the registry location:

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\IntelliForms\Storage2

The HTTP basic authentication passwords are stored in the 'Credentials store' at following location based on the operating system:

For Windows XP:

C:\Documents and Settings\[username]\Application Data\Microsoft\Credentials

For Windows Vista and Windows 7:

C:\Users\[username]\AppData\Roaming\Microsoft\Credentials

The typical windows registry for IE looks like:

Instant Messengers

Google Talk (GTalk):

GTalk stores all remembered account information at following registry location:

HKEY_CURRENT_USER\Software\Google\Google Talk\Accounts

For each account separate registry key is created with the account email id as name. Account passwords are encrypted using Window's Cryptography Functions and are stored at the above registry.

GooglePasswordDecryptor is a free tool to decrypt and obtain the GTalk usernames/passwords in plaintext.

Skype

Skype does not stores the passwords directly. It computes the encrypted hash of the password and stores in config.xml present in skype's user profile directory. Typical location of the user profile directory is:

For Windows XP:

C:\Documents and Settings\<user_name>\Application Data\Skype\<account_name>

For Windows Vista & Windows 7

C:\Users\<username>\AppData\Roaming\Skype\<account_name>

The config.xml configuration file contains <Credentials2> tag which contains encrypted hash of the password. Skype uses MD5 hash of string "username\nskyper\npassword" for authentication. If user has set the 'Remember password' option then this MD5 hash is encrypted using AES-256 & SHA-1 algorithms and finally saved into the 'Config.xml' file [6].

Hacking Passwords

Windows 98/ME

The pwl files cannot be easily edited, but can be overwritten. However, we can delete the existing pwl files and the next time we log on to the system, we will be prompted to enter our username and password, and this new information will be stored in a new *.pwl file. We can also copy pwl files from one machine to another. Thus to hack a computer, we just need to boot the system using some bootable cd and copy the existing pwl file in the c:\windows directory. Immediately we can now logon using the new user name and password. Thus once we boot the system using bootable CD, we can follow either of the follwing approaches:

a) Delete existing pwl file: In this approach, once the system is restarted after deleting existing pwl files, the system will ask for a new user name and password. So the system is hacked.

b) Copying existing pwl files: In this approach, the new user accounts as specified in the pwl file being copied are automatically created in the operating system. Hence the hacker can login with his choice of user name and password.

Replacing existing pwl files: In this approach, the existing user accounts will be deleted and the new user accounts as specified by the new pwl file are automatically created. Hence again the system is hacked.

Windows NT/XP/Vista/Windows 7

NT stores a permanent working copy of the SAM database on the hard disk that can be accessed via the HKEY_LOCAL_MACHINE Registry hive under the SAM key by either writing a program or using a Registry editor (e.g., regedt32.exe). Ordinarily, users can't directly access the SAM key with a Registry editor because NT limits the permissions on the key to the built-in SYSTEM account, but administrative users can trick NT into providing SAM-key access under the user context of the SYSTEM account.

When you forget user passwords,if you know the theory as above,you can change the SAM file by following the steps below. These steps can also be used by any hacker/cracker to breach into the computer if he/she has physical access to the computer running on Windows NT.

Step 1:Login to a Computer that has Windows XP system.

Step 2:Copy the SAM file to a floppy disk.

Step 3: Then turn to your locked pc and insert the floppy disk Reboot the PC and enter into MS-DOS.

Step 4:In dos,type : del c: windowssystem32configsam ,then you will delete the SAM file.

Step 5: type : Copy a:sam c: windowssystem32config,copy the other's SAM file to your PC.

Internet Explorer (IE):

IE version 7 and above use Credential Store to store HTTP basic authentication passwords. The same Credential Store is used to store the network credentials like proxy/router configuration usernames/passwords.
However its easy to distinguish between the two as the passwords stored by IE begins with the identifier text 'Microsoft_WinInet' and they are of type 1 while network credentials do not begin with iden 'Microsoft_WinInet' and do not have type 1.
The passwords are encrypted using the Windows Cryptography functions (as defined by Microsoft Developer Network) after salting them with the text generated from the GUID 'abe2869f-9b47-4cd9-a358-c22904dba7f7'.

To traverse through the secret credentials, window's function CredEnumerate defined in WinCred.h can be used. Once the encrypted passwords are obtained by using CredEnumerate function, they can be decrypted, as illustrated by SapporoWorks, by using CryptUnprotectData defined in Wincrypt.h function as shown in the below code example.

```
// wincred.h is included in Platform SDK.
// To use CryptUnprotectData, it is necessary to enlink Crypt32.lib.

#include <windows.h>
#include <wincrypt.h>
#include <wincred.h>

void main(int argc,char *argv[])
{
DATA_BLOB DataIn;
DATA_BLOB DataOut;
DATA_BLOB OptionalEntropy;
short tmp[37];
char *password={"abe2869f-9b47-4cd9-a358-c22904dba7f7"};
for(int i=0; i< 37; i++)
tmp[i] = (short int)(password[i] * 4);
OptionalEntropy.pbData = (BYTE *)&tmp;
OptionalEntropy.cbData = 74;

DWORD Count;
PCREDENTIAL *Credential;

if(CredEnumerate(NULL,0,&Count,&Credential)){
for(int i=0;i<Count;i++){
DataIn.pbData = (BYTE *)Credential[i] ->CredentialBlob;
DataIn.cbData = Credential[i] ->CredentialBlobSize;

if(CryptUnprotectData(&DataIn,NULL,&OptionalEntropy,NULL,NULL,0,&DataOut)){
printf("Type : %dn",Credential[i] ->Type);
printf("TargetName : %sn",Credential[i] ->TargetName);
printf("DataOut.pbData : %lsn",DataOut.pbData);
        }
}
CredFree(Credential);
}
}
```

If we run the above code, the result looks like:

```
C:>sample_1.exe
Type : 1
TargetName : Microsoft_WinInet_enter.nifty.com:443/Service
DataOut.pbData : user-id:password

Type : 1
TargetName : Microsoft_WinInet_192.168.0.1:80/test-server
DataOut.pbData : test:123456
```

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/skypef/default.asp, 3rd June 2012.