Analysis the Structure of SAM and Cracking Password Base on Windows Operating System

Jiang Du and Jiwei Li

Abstract—**Cracking Windows account password is critical to the forensic analyst. The general methods of decipher password include clean the password, guess by social engineering, mathematical analyzing, exhaustive attacking, dictionary attacking and rainbow tables algorithm. This paper provides the details about the Security Account Manager(SAM) database and describes how to get the user information from SAM and cracks account password of Windows 10 that the latest operating system of Microsoft.**

***Index Terms*—SAM, decipher password, crack password, Windows 10.**

I. Introduction

In the process of computer forensic the analyst need to enter the Windows operating system by cracking windows account password to collect evidence at times. Within the family of Windows operating systems, like mostly used Windows 7, Windows 8 and the latest Windows 10, the Security Account Manager(SAM) database was used to store user's login information and passwords which encrypted by NT-hash [1]. This paper analysis the structure of the SAM that come from Windows 10 and makes an experiment to obtain the user's account information from the SAM and crack the account password. During the research and experimentation stage, the following software will be utilized:

1) VM ware Workstation 9.0.0 build-812388 was used to create a virtual machine;
2) Mount image pro v5.0.6 was used to mount E01 disk image file as a physical disk;
3) Red Hat Enterprise Linux Server release 7.0 was created by VMware Workstation to run the programs;
4) Access Data FTK imager 3.0.0.1443 was used to create an E01 disk image file from Microsoft Windows 10 operating system;
5) The SAM file is come from the Windows 10 which mounted by Mount image pro v5.0.6;

II. Windows Registry Overview

The Windows registry is a central hierarchical database used in the entire operating system of Microsoft to store users' information, applications and hardware devices [2], like the mostly used in Windows XP, Windows 7, Windows 8 and the latest Windows 10, the registry contains information that Windows continually references during operation, such as profiles for each user, the applications installed on the computer and the types of documents, property sheet settings of folders and application icons, what hardware exists on the system, and the ports that are being used [3]. On disk, the Windows registry is not only a large file but a set of discrete files called hives. Each hive is a hierarchical tree which identified by a root key to provide access to all sub-keys in the tree up to 512 levels deep.

III. Security Account Manager (SAM)

Security Account Manager (SAM) is a database used to store user account information, including password, account groups, access rights, and special privileges in Windows operating system. In the registry, all of the users include the general users and the administrators can not read the SAM file except the users who gain the system privileges. So if the general user and administrator want to read the SAM file they have to gain read access by changing the access control list of those registry keys with the permission of the administrative privileges. And the file can be found in %SystemRoot/system32/config/SAM% and it mounted on HKLM/SAM and HKLM/SE-CURITY/SAM which is all the same in these two nodes.

IV. The Structure of SAM

Security Account Manager (SAM) is a HIVE file which is consists of HBINs and CELLs. In this section, the data structure of SAM will be analyst.

A. The HIVE Header

The HIVE file header is the first block of hive which is also named base block. Table I list the content of the HIVE header.

TABLE I: HIVE Header

Offset	Size	Name	Notes
0×00	4	regf_id	signature " regf "
0×04	8	timestamp	last modify date
0×0C	4	version	HIVE version
0×10	4	ofs_rootkey	offset of 1st key record
0×14	460	name	filename and path
0×1E0	4	checksum	checksum

B. HBIN

HBIN is the storage units of HIVE internal data files and always use block (4KB size) as allocation unit. When expanding the HIVE file for the CELLs, the real allocation

Manuscript received January 4, 2016; revised April 12, 2016.

Jiang Du and Jiwei Li are with College of Computer Science and Technology, Chongqing University of Posts and Telecommunications, Chongqing 400065, China (e-mail: clouddu@163.com, cloudleejw@163.com).

doi: 10.18178/ijfcc.2016.5.2.455

storage space will be extended to the border of next block [3], [4]. Table II shows the content of HBIN.

TABLE II: HBIN CONTENT

Offset	Size	Name	Notes
0×00	4	hbin_id	signature " hbin "
0×04	4	ofs_self	offset to itself
0×08	4	ofs_next	relative offset to next HBIN
0×0C	4	firstlink	First data block

C. CELL

The registry data in the HIVE is organized by CELLs. However the CELL storage space is not certain which are depended on the CELL data and types [3]. Each CELL contains a key, a value, a security description, a subkey-list or a value-list and the corresponding CELL which is named key CELL, value CELL, security description CELL, subkey-list CELL and value-list CELL.

The connection between HBINs and CELLs is shown as Fig. 1.

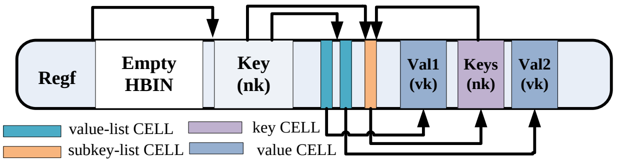


Fig. 1. Connection between HBINs and CELLs.

The above Fig. 1 shows that each registry key record ("nk") can be described as follows:

1) If it has any values, a pointer to a value-list. The value-list in turn points to a number of value records ("vk").
2) If it has any subkeys, a pointer to a subkey-list. The subkey-list in turn points to a number of subkey records which are of course key records ("nk");
3) Each subkey record has a pointer that points back to its parent key record.

V. WINDOWS ACCOUNT PASSWORD ENCRYPTION

Microsoft Windows operating system mainly used one-way hash algorithm to encrypt account password, and the LM hash and NTLM hash encryption are the mostly used to integrate single sign-on mechanism in the Microsoft systems [5]. The LM hash is used to encryption logon account in Windows XP, Windows 2000 and Windows 2003. What's the encryption process is:

1) Password converted to upper case;
2) Password is null-padded or truncated to 14 bytes;
3) Password is split into two halves of 7 bytes each;
4) Two DES keys are created, one from each 7 byte half:
   - convert each half to a bit stream;
   - Insert a zero bit after every 7 bits.
5) Each DES key is used to encrypt a preset ASCII string (KGS!@#$%), resulting in two 8-byte ciphertext values;
6) Concatenate the two 8-byte ciphertext values as the LM hash.

LM stored passwords have a few distinct disadvantages:

1) Passwords are not case sensitive;
2) Password are split into 7 chars and hashed separately, making brute force trivial;
3) Passwords are limited to a maximum of 14 characters in length.

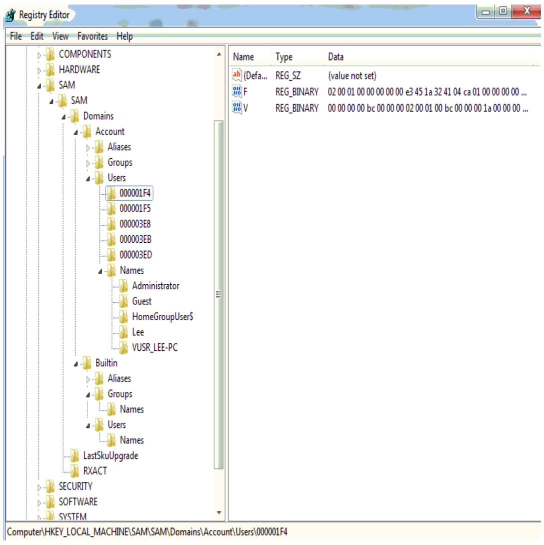
To strengthen the security of the account password, Microsoft add a new encryption method in early systems which named NTLM. NT LAN Manager (NTLM) is a challenge-response protocol that used throughout Microsoft's systems as an integrated single sign-on mechanism. Meanwhile Windows NT-based operating systems up through and including Windows Server™ 2003 store two password hashes for keep compatibility, the LAN Manager (LM) hash and the Windows NT hash. Starting in Windows Vista™, the capability to store both is there, but LM hash is turned off by default. The NT hash is a straight MD4 hash of the plaintext password. It supports all Unicode characters and passwords up to 256 characters long [5]-[7]. The NTLM response is calculated as follows:

1) The MD4 message-digest algorithm is applied to the Unicode mixed-case password. This results in a 16-byte value;
2) The 16-byte NTLM hash is null-padded to 21 bytes;
3) This value is split into three 7-byte thirds;
4) These values are used to create three DES keys (one from each 7-byte third);
5) Each of these keys is used to DES-encrypt the challenge from the Type 2 message (resulting in three 8-byte cipher text values);
6) These three cipher text values are concatenated to form a 24-byte value. This is the NTLM response.

VI. OBTAIN ACCOUNT INFORMATION AND CLEAR PASSWORD FROM SAM DATABASE

A. The Content of Project F and V

As has been stated before in this article, Security Account Manager (SAM) is a hierarchical database which is used to store user's account information. The SAM in the registry is organized as a tree and is analogous to a file system as shown in Fig. 2.



```
COMPONENTS
HARDWARE
SAM
  SAM
    Domains
      Account
        Aliases
        Groups
        Users
          000001F4
          000001F5
          000003E8
          000003EB
          000003ED
          Names
            Administrator
            Guest
            HomeGroupUser$
            Lee
            VUSR_LEE-PC
      Builtin
        Aliases
        Groups
          Names
        Users
          Names
    LastSkuUpgrade
    RXACT
SECURITY
SOFTWARE
SYSTEM
```

Name	Type	Data
(Defa...	REG_SZ	(value not set)
F	REG_BINARY	02 00 01 00 00 00 00 00 e3 45 1a 32 41 04 ca 01 00 00 00 00 ...
V	REG_BINARY	00 00 00 00 bc 00 00 00 02 00 01 00 bc 00 00 00 1a 00 00 00 ...

Computer\HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\000001F4

Fig. 2. The hierarchical tree of SAM.

In the entire SAM database, the main contents of the account are under the node of /Domain/Account/Users. Each account following two sub-items, F and V. Saved in the project F is the account registry records, such as the last login time, lockout time, the failed login count, total logins since creation and so on. Project V saves the basic information of the account, like user name, full name, contents, group ownership, password hash, etc. Table III and Table IV show the main contents of project F and V, respectively.

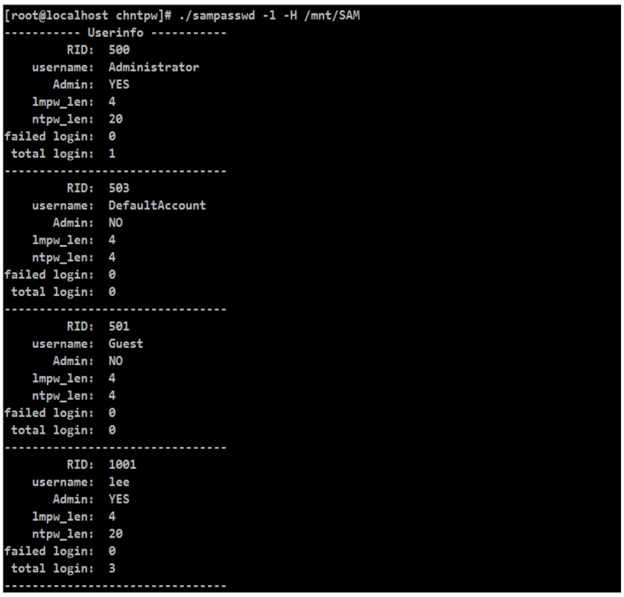
TABLE III: THE PROJECT F CONTENT

Offset	Size	Name	Notes
0x00	8	t_lockout	time of lockout
0x08	8	t_creation	time of account creation
0x10	8	t_login	time of last login
0x18	4	rid	RID
0x1C	2	ACB_bits	account type and status
0x1E	2	failedcnt	count of failed logins
0x20	2	logins	total logins since creation

TABLE IV: THE PROJECT V CONTENT

Offset	Size	Name	Notes
0x00	4	username_ofs	account offset
0x04	4	username_len	account length
0x08	4	fullname_ofs	full username
0x0C	4	fullname_len	full username length
0x10	4	comment_ofs	comment
0x14	4	comment_len	comment length
0x18	4	homedir_ofs	home directory
0x1C	4	homedir_len	home directory length
0x28	4	lmpw_ofs	LM hash offset
0x2C	4	lmpw_len	LM hash length
0x30	4	ntpw_ofs	NTLM hash offset
0x34	4	ntpw_len	NTLM hash length

B. Obtain Account Information



```
[root@localhost chntpw]# ./sampasswd -l -H /mnt/SAM
----------- Userinfo -----------
         RID:  500
    username:  Administrator
       Admin:  YES
    lmpw_len:  4
    ntpw_len:  20
failed login:  0
 total login:  1
-------------------------------
         RID:  503
    username:  DefaultAccount
       Admin:  NO
    lmpw_len:  4
    ntpw_len:  4
failed login:  0
 total login:  0
-------------------------------
         RID:  501
    username:  Guest
       Admin:  NO
    lmpw_len:  4
    ntpw_len:  4
failed login:  0
 total login:  0
-------------------------------
         RID:  1001
    username:  lee
       Admin:  YES
    lmpw_len:  4
    ntpw_len:  20
failed login:  0
 total login:  3
-------------------------------
```

Fig. 3. Obtain information from SAM.

To obtain the account information from SAM database, we first mount E01 disk image file use mount image pro and then mount the SAM database file in the virtual machine. Then, the account information can be obtained from the SAM database shows in Fig. 3.

C. Cracking Windows Passwords

There are a few ways to crack windows account password. The mostly used ways are brute-force attacks and dictionary attacks. Brute-force attacks is an application of brute-force search by generate all possible passwords and calculate their hash values and compare this hash value to the hash values that store in the system password database. Dictionary attack is based on trying all the strings in a pre-arranged list, typically derived from a list of words such as in a dictionary. Another effective cracking is known as rainbow tables algorithm which is a list of all possible plaintext permutations of encrypted passwords specific to a given hash algorithm. However, in this paper, we set the length of LM hash and NTLM hash as null that stored in the SAM database to clear the account password so that we can login the windows system without account passwords [1], [8], [9]. The data structure of project V likes:

```
struct user_V {
  int unknown1_1;
  int username_ofs;
  int username_len;
  int comment_ofs;
  int comment_len;
  int lmpw_ofs;
  int lmpw_len;
  int ntpw_ofs;
  int ntpw_len;
.......
};
```

In this data structure, through set lmpw_len=0 and ntpw_len=0 can clear Windows account password like Windows 7, Windows 8 and the latest operating system Windows 10.

VII. CONCLUSION

In this paper, we first analysis the structure of SAM and discusses the encryption algorithm used in Windows. Then, makes an experiment to show how to obtain the user account information from SAM database and crack the account password. By using the method what I mentioned above, we can crack almost all the Windows account passwords including Windows 7, Windows 8 and Windows 10 which is the latest operating system of Microsoft. However, due to the Windows closure, many data in the SAM database is still unknown what's the meaning it have. And deep research the Windows SAM and obtain more information will be the future work.

REFERENCES

[1] N. Peter, "The internal structure of the windows registry," Defence College of Management and Technology, Dept. of Informatics and Sensors, Cranfield University, 2009.

[2] N.-H. Petter. (2008). Offline NT password & registry editor. [Online]. Available: http://www.pogostick.net/~pnh/ntpasswd/

[3] J. Johansson. (2006). Security watch: The most misunderstood windows security setting of all time. [Online]. Available: https://technet.microsoft.com/en-us/magazine/2006.08.securitywatch.aspx

[4] C. K. Goel and G. Arya, "Hacking of passwords in windows environment," *International Journal of Computer Science & Communication Networks*, 2012.

[5] G. Eric. (2006). The NTLM authentication protocol and security support provider. [Online]. Available: http://davenport.sourceforge.net/ntlm.html

[6] T. D. Morgan. (2009). The windows NT registry file format version 0.4. [Online]. Available: http://sentinelchicken.com/data/TheWindowsNTRegistryFileFormat.pdf

[7] V. Jos. (1997). On NT password security. Open Solution Proviers. [Online]. Available: http://www.osp.nl/infobase/ntpass.html

[8] Remah. (2014). Deeper into the windows registry. [Online]. Available: http://www.techs-upportalert.com/content/deeper-windows-registry.htm

[9] B. Randhir, N. Kumar, and S. Sharma, *Analysis of Windows Authentication Protocols: NTLM and Kerberos*, 2014.

Jiang Du was born in 1969 of Chongqing, China and graduate from Southwest Jiaotong University in 1991. After graduation, he work for Chongqing University of Posts and Telecommunications and server as a lecturer in Telecom Engineering Department. In 1995, he studied for computer master's degree in Inha University and got the master's degree in 1997. In 2010, he was promoted to full professor and major field include information security, computer network and embedded systems.

In 2001, he won the second prize of military science and technology progress. In 2009, he won the first award of Chongqing science and technology progress. In 2010, he obtained the second prize of national science and technology progress.

At present, Prof. Jiang was the senior member of China Computer Institute and the committee member of Computer Security Committee.

Jiwei Li was born in 1990 of Yunnan province. And now is a master student of Chongqing University of Posts and Telecommunications. The search field is information security.