encrypted file system(NTFS) recovery--EFS

翻译

ouailuo143 于 2011-07-16 20:15:14 发布 1444 收藏
分类专栏： 操作系统 文章标签： file system microsoft encryption permissions application


操作系统 专栏收录该内容
5 篇文章 0 订阅
订阅专栏

introduction

this article updates the quick writeup that started in the temp directory of this domain detailing how to import users encrypted file system (efs) keys from an old offline profile into a new system in order to gain authorized access to previously inaccessible encrypted data.

note well that this method is for advanced users. there are some programs/services out there that maybe better suited for you.

01.	elcomsoft offer a program called advanced efs data recovery (aefsdr) that works in 2k/xp. price 99usd (~61ukp) - demo available.
02.	microsoft have a recovery program (reccerts.exe) only available via payed support - cost unknown, but some prices are listed: uk: here & usa: here.
03.	passware offer a program called efskey that works similarly to aefsdr, though noteably slower in decryption. price 95usd (~58ukp) - demo available.

an interesting coincidence:
windows 2k was released 31/03/2000 first introducing efs
windows xp was released 25/10/2001 some efs updates added
my 1st post on efs recovery 09/02/2003
elcomsoft releases aefsdr 25/02/2003
microsoft makes known reccerts.exe 28/02/2003
passware release efs key beta 06/2003

this method is free and is the last stop before expensive specialist recovery, like file encryption key (fek) matching and recovering old magnetic disk layers.

recently added!!
one & two unfinished 1024*768 images giving a brief overview.

the error and keys

efs filenames are coloured green, by default in xp - else check advanced properties. on attempting to open such a file, a blank document is created and an error message like this displayed:

notepad: cannot open the c:\documents and settings\foo\my documents\report.txt file. make sure a disk is in the drive you specified.
or - wordpad: access to c:\docume~1\foo\mydocu~1\report.txt was denied.

or - windows picture and fax viewer: no preview available

this is a decryption mismatch - if this error is displayed for all users listed in the properties -> advanced -> details dialog and the recovery agents, an incorrect or absent encryption keys was attempted. this mayof been caused by a number of events - the most common being a reinstall.

it is highly recommended when first using efs that you export your public and private keys to another storage medium (cipher /?) - these keys are randomly generated at creation, similar installs will not create similar keys. strangely there is no prompt when first using efs, and thus many people are unaware of the risk or forget. it is also advisable to create a recovery agent, though some users may decide not to for security reasons.

if you have following folders and their contents from the orginal install of 2k or xp - you can recover you efs data. knowledge of your password is also required for this amount of data.

c:\documents and settings\foo\application data\microsoft\crypto\
- private keys

c:\documents and settings\foo\application data\microsoft\protect\
- locks your current password to your private keys

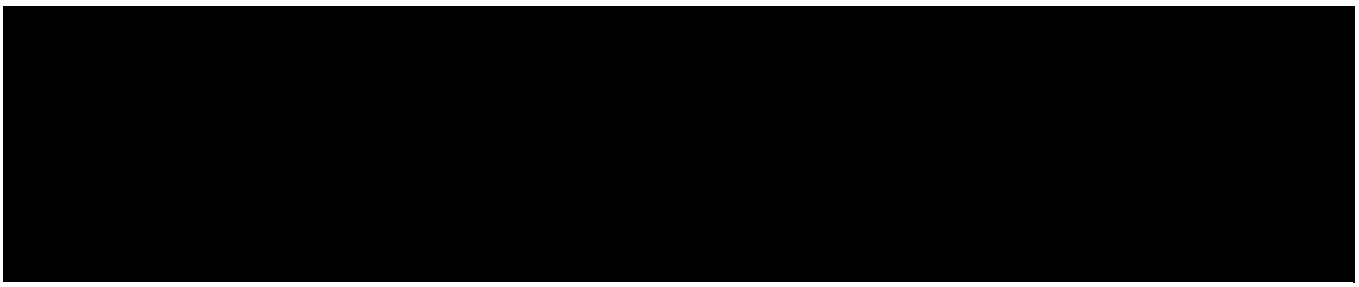
c:\documents and settings\foo\application data\microsoft\systemcertificates\
- public keys (not essential to be the orginal as another valid key can be madeup)

this data maybe on an unbootable system, a backup, roaming profile or currently on the system, either in the file system or in the free space. if you have these files skip this remaining section.

there are a number of ways of reinstalling, here are some:

01.	low level format of the disk,oem xp cd bootup, format and install	specialist recovery required
02.	oem xp cd bootup, format and install	if keys have not been overwriten - good, else 1
03.	oem xp cd bootup, install over top of orginal windows directory (press l)	good
04.	retail restore cd - a colourfull front end of ghost	if keys have not been overwriten - good, else 1

if method 03 - your orginal profile are most likely still in the c:\documents and settings\ folder.



orginal folders	current folders
all users	all users.windows
default user	default user.windows
foo	foo.%machinename%
localservice	localservice.nt authority
networkservice	networkservice.nt authority

if method 02 or 04, there is a chance that the reinstall has not overwritten the orginal efs keys. most formats only wipe the file structure and since all file are copied and the pagefile is created before profile creation and encryption keys even further on, it is possible that on reinstall the orginal encryption keys have not been overwritten and are still on the disk somewhere. it is possible to search the volume for this key data and if present, recover it - if you are serious about attemping this, power down the machine as soon as possible, because as reinstall uptime increases the chances of this key data being overwritten also increases.

recovery with the orginal profile in the file system

you can do this procedure on the current install, however the more cautious may want to use a second test install. backup all changes if you use the current.

you will need a user account of the same user and machine number as the orginal. check this orginal folder name: c:\documents and settings\%username%\application data\microsoft\crypto\rsa\s-1-5-21-1078081533-1606980848-854245398-1003

machine is: 1078081533-1606980848-854245398
useracc is: 1003

converted into hex the machine sid is: fd374240 f094c85f 16c0ea32
(convert each block into hex and reverse bytes for each section) useracc is: 3eb

goto: hklm\sam\sam\domains\account\users\%usernumbers%

check if a user account is already present of the orginal account number. if there is, check the username (\v) logon and create a profile and change the password to the one from the orginal machine. if there is not a user account of the same number, create one that is, you may want to modify hklm\sam\sam\domains\account\f offset 48 to the required number before you create. add the user to the admin group.

goto: hklm\sam\sam\domains\builtin\aliases\00000220\c and modify the machine sid prefixing your orginal user number. (towards the end)

goto: hklm\sam\sam\domains\account\v and modify the machine sid at the end to your orginal number.

goto: hklm\software\microsoft\windows nt\currentversion\profilelist\ select key called your machine number suffixed by your user number, export, modify the key to the orginal machine/user number and import.

copy the orginal three folders into:
c:\documents and settings\%username%\application data\microsoft\

restart - login using the orginal password. access to your files should be possible. decrypt.

NOTE: this method is slightly brief and advanced. I have not written up a newer version of this article yet, which will include a simpler step by step. In the meantime if you get stuck, try following this procedure instead:

first set the orginal sid. probably easier if you run newsid than editing hex values in the registry, download here: http://www.sysinternals.com/ntw2k/source/newsid.shtml make sure that you are using a test install or backedup setup or specifically not using efs since on changing the sid you will not have access to your currently encrypted files. set the new sid to be the one in your old profile directory eg: c:\documents and settings\%username%\application data\microsoft\crypto\rsa\s-1-5-21-1078081533-1606980848-854245398-1003 -> newsid would be s-1-5-21-1078081533-1606980848-854245398 - after this is done, reboot if not automatic. ignore any further reference to the sid in the article since this is now correct.

encrypt a test file, then browse to c:\documents and settings\%username%\application data\microsoft\crypto\rsa\ - is the number on the end of the sid eg 1003 the same as the previous number? if it is the same, skip this next part.

if not, check the other accounts on the computer else you either need to create a user that does have the same user or modify your existing user to have the orginal number - probably easier if you create new user. user numbers increment, since they are linked with security, no two users must ever have the same number, if the orginal usernumber is higher than the current one, create some new accounts, logon, encrypt a test file and check the number untill you have a correct user number. if orginal number is lower than the current one you will need to reset the usernumber counter, run regedit -> default registry permissions deny access to hklm\sam\sam\... select the hkey_local_machine\security\ key and right-click(if xp/2003srv) or use regedt32 and do security -> permissions(if 2k) check the allow full control while selecting the admistrators group -> advanced -> check reset permissions on all child objects and enable propagation of inhertitable permissions -> ok/yes/ok. since the sam hive is setup as a link folder with sam, you should now be able to access hklm\sam\sam\domains\account\ - double click the f value, at offset 0048 there is 4 bytes that state the next created usernumber, make a note of this, so you can restore later. you need to convert the orginal usernumber into hex. run calc -> view: scientific -> type in the user number eg, 1003 and then change the base (top left) from dec to hex. the number should now read 3eb, now what is really means is 00,00,03,eb reverse these byte so it reads: eb,03,00,00 this is the new value to enter in at offset 48. after editing you will need to restart the machine. now when you create a new user it should have the correct number. remember to reset the counter back to what it was before.

once you have a user, with the correct user number and the machine has the correct sid number, copy the old folders from c:\documents and settings\%username%\application data\microsoft\ into the current users folders. set the users password to the one that was used before and try to access the files. check ntfs permissions also if denied.

CHECK!! - updates soon
note if you are restoring a 2k efs access and still get errors, it is possible that the locking file was not updated on a password change - since efs on 2k(only) relies primarily on the syskey (major weakness if syskey is stored locally) you may have to import the orginal syskey - details of this are listed on the ntsecurity page or email me for a more step-by-step process.

recovery with the orginal profile not in the file system

it is _highly_ recommended to mount the disk containing the volume with the orginal install on as slave on a second machine as your recovery activities may overwrite the key data. - if you are using a laptop, get a 2.5" to 3.5" ide cable. avoid all data writes to the orginal volume.

you will need a decent hex editor (winhex recommended) and filemon from sysinternals or equivalent.

first some key pieces of information need to be optained from the encrypted files themselves. you can either jump on the ntfs to the efs header or (recommended) use ntbackup to backup one of the encrypted files you cannot access. open the backup with a hex editor and scroll down untill you see something like this.

green = the machine sid and usernumber in hex
fd374240 f094c85f 16c0ea32 eb030000 -> reverse
404237fd 5fc894f0 32eac016 000003eb -> convert to decimal
1078081533-1606980848-854245398-1003 -> prefix with s-1-5-21- for full sid/userno.

red = the public key thumbprint
79B73C0C5A501E06B9EC0A6EF4A3B8CB23BF84E9 - this is the filename of the public key

blue = the private key guid - this section maynot be present if other users have been added.

now to search the orginal volume for the data of the two critical files - the private key and the locking file.

within the private key the guid(blue) is stored, the difference between the efs header is that it is stored in ascii, not unicode. if the private key guid was not present in the efs header you can search for "cryptoapi private key" in unicode, some results maynot be the correct ones, but this will be obvious on sight. the private key should look some thing like this. recover and name "privatekey" for now.

note well - if you do not find this private key, this method will not work and specialist methods must be used.

---

blue = private key guid - mentioned before
cyan = the locking file name and also mentioned within.
9f7479dc ea80 924a b41f 6392c4e3b72d -> some reversing
dc79749f-80ea-4a92-b41f-6392c4e3b72d

do a search for this string in unicode. the locking file should look something like this. recover and name as pictured in cyan in ascii.

note well again - if you do not find this locking file, this method will not work and specialist methods must be used.

---

cyan = the locking file name - mentioned before
yellow = a hex string required for the credhist file
dc42a7eeac5b104481336024113992ff - as is.

if you have just successfully recovered these two pieces of data, things are looking very good!! no further data needs to be recovered from the orginal install.

create a file called credhist so it looks like this:

---

yellow = as is, taken from the locking file - mentioned before

create a file called preferred so it looks like this:

---

on the second installation that you are running, encypyt a file so that you create a set of efs keys. copy out the public key from c:\documents and settings\foo\application data\microsoft\systemcertificates\my\certificates\ and rename to the public key thumbprint mentioned in the efs header - mentioned before. open in the hex editor and update the following sections.

---

blue = private key guid - mentioned before
red = public key thumbprint - mentioned before

follow the method "recovery with the orginal profile in the file system" detailed in the previous section and place the files into their correct locations. reboot.

c:\documents and settings\foo\application data\microsoft\

\crypto\rsa\s-1-5-21-1078081533-1606980848-854245398-1003\privatekey
\protect\credhist
\protect\s-1-5-21-1078081533-1606980848-854245398-1003\ (2files)
dc42a7eeac5b104481336024113992ff
preferred
\systemcertificates\my\certificates\79b73c0c5a501e06b9ec0a6ef4a3b8cb23bf84e9

the privatekey needs the correct name, this is determined from the private key guid by some unknown hashing process, however filemon can record the system request and thus the correct file name can be resolved. run filemon and simply select one of the encrypted files, stop filemon and apply a highlighting filter of "file not found" scroll up untill you see highlight entry by the process lsass. you should see the complete folder name request with the correct file name - something like this: bb1c31a261eed4c09b0a92ad011aae21_904f931f-4993-4059-ab65-e3961044d535 - you can ignore the second half, it is merely the machine guid querried from the registry - hklm\software\microsoft\cryptography\machineguid - you can just used the resolved hash followed by an underscore - bb1c31a261eed4c09b0a92ad011aae21_

now try accessing the encrypted file - it should all matchup. decrypt.

recovery with no information at all - specialist methods.

even if the key data has been overwritten it can still be recovered, unsure of companies and price, but this page details the technique - interesting to read, aside from efs.

the other way is matching the fek - if you scroll backup to the efs header image you will notice there is a section of size 128bytes, after username@machinename - within this block are the keys for decrypting the data, plus probably some user verifying entries. without the correct efs key this cannot be decrypted. although the encryption process appears to work on a 512 bytes basis, it really encrypts/decrypts in 8 bytes blocks. many popular file formats have standard headers of 8bytes and more, thus for these files, the plain text is already know, and thus can be matched against all fek keys for the correct key, once found the key can be applied to the remaining file. the first step in this process would be to determine the key format from a working system and then apply the correct encryption algorithm to the encrypted data. the time taken to get a match would vary greatly on the hardware and algorithm used and since the fek is different for each file, it could take along time to decrypt all the files - though not impossible...

in closing - backup your efs keys properly!!