Packages - Feature Request #2282

Add cryptsetup emergency self destruction

2019-04-13 05:49 PM - Anonymous

Status:	open	**% Done:**	0%
Priority:	bug		
Assignee:			
Category:			

Description

There must be emergency self destruction in cryptsetup so if user is forced to say passphrase, they can use self destruction passphrase to make decryption impossible.
https://www.kali.org/tutorials/emergency-self-destruction-luks-kali/ for patches.

History

#1 - 2019-04-13 06:01 PM - Anonymous

Current repository: https://git.kali.org/gitweb/?p=packages/cryptsetup.git;a=summary

#2 - 2019-04-13 06:28 PM - Anonymous

Tried to build using upstream and kali/master branches, there is no luksAddNuke.

#3 - 2019-04-13 06:41 PM - bill-auger

this seems like a feature request better proposed to the upstream - have you asked them?

https://gitlab.com/cryptsetup/cryptsetup/

#4 - 2019-04-13 06:50 PM - freemor

Interesting idea.. but legally likely to get you into more trouble then out of it.

In most jurisdictions;

- destruction of evidence is illegal
- lying to the cops/etc is illegal

In some jurisdictions you can be legally compelled to provide passwords (as in the right one) giving them the wrong one and then not being able to provide a correct one could land you in serious trouble.

I'm not saying any of these are reasons for us not to provide it. But people need to be aware that this is probably gonna get you in more trouble.

Also a lot of authorities are smart enough these days to shoulder surf and grab your device once you unlock it and only then announce their presence.

#5 - 2019-04-14 12:45 PM - Anonymous

IIRC, this feature was rejected by upstream.
Sometimes, illegal rubber-hose cryptoanalysis may be used.

#6 - 2019-04-14 12:49 PM - Anonymous

Update: it was. https://gitlab.com/cryptsetup/cryptsetup/raw/master/FAQ (5.21)

#7 - 2019-04-14 12:51 PM - Anonymous

Also, the user could lie about password being forgotten and try to guess, providing nuke password.

#8 - 2019-04-15 12:22 AM - freemor

REad through the Upstreams reasoning and pasting it below to save people the scrolling and to preserve it for this issue if the link goes dead at some future date. Their reasoning is strong, and in line with some of what I said above. I feel that this is probably best left as something a motivated user can compile and install them selves (against all the below reasoning). If they really want it.

From the Upstream link above:

```
* 5.21 Why is there no "Nuke-Option"?
```

A "Nuke-Option" or "Kill-switch" is a password that when entered upon unlocking instead wipes the header and all passwords. So when somebody forces you to enter your password, you can destroy the data instead.

While this sounds attractive at first glance, it does not make sense once a real security analysis is done. One problem is that you have to have some kind of HSM (Hardware Security Module) in order to implement it securely. In the movies, a HSM starts to smoke and melt once the Nuke-Option has been activated. In reality, it just wipes some battery-backed RAM cells. A proper HSM costs something like 20'000...100'000 EUR/USD and there a Nuke-Option may make some sense. BTW, a chipcard or a TPM is not a HSM, although some vendors are promoting that myth.

Now, a proper HSMs will have a wipe option but not a Nuke-Option, i.e. you can explicitly wipe the HSM, but by a different process than unlocking it takes. Why is that? Simple: If somebody can force you to reveal passwords, then they can also do bad things to you if you do not or if you enter a nuke password instead. Think locking you up for a few years for "destroying evidence" or for far longer and without trial for being a "terrorist suspect". No HSM maker will want to expose its customers to that risk.

Now think of the typical LUKS application scenario, i.e. disk encryption. Usually the ones forcing you to hand over your password will have access to the disk as well, and, if they have any real suspicion, they will mirror your disk before entering anything supplied by you. This neatly negates any Nuke-Option. If they have no suspicion (just harassing people that cross some border for example), the Nuke-Option would work, but see above about likely negative consequences and remember that a Nuke-Option may not work reliably on SSD and hybrid drives anyways.

Hence my advice is to never take data that you do not want to reveal into any such situation in the first place. There is no need to transfer data on physical carriers today. The Internet makes it quite possible to transfer data between arbitrary places and modern encryption makes it secure. If you do it right, nobody will even be able to identify source or destination. (How to do that is out of scope of this document. It does require advanced skills in this age of pervasive surveillance.)

Hence, LUKS has not kill option because it would do much more harm than good.

Still, if you have a good use-case (i.e. non-abstract real-world situation) where a Nuke-Option would actually be beneficial, please let me know.