Q&A with Mr Thistle

asked by Thistle (pseudonym)
answered by Arkadiusz Bulski
recorded on 2015-04-10

What control will a user have over wiping of files? Wiping of files is not practical? You mean manual wiping?

There are two different functions, regular deletion and permanent deletion. One is reversible and other is highly restricted. Please refer to answer to next question.

Practicality is meant here as both performance and assurance. Wiping in general is a synonym to permanent removal but in this context it means a specific implementation, through overriding of file content. Historically, this is how it was done. There is at least one major deficiency, performance is unsatisfactory. Overriding a 4GB file for example, even at hard-disks maximum 120MB/s, still takes 34.1 seconds. And to be really sure, you should do that 35 times (Gutmann method).

Will there be an option for non-permanent wiping in case a user accidentally wipes a file? What safety measures will be there to prevent accidental complete wiping of content? Or is that a risk users have to take?

There are two distinct functions. Regular deletion (here called *deletion*) is an action that can be taken by non-privileged user. Rogue processes would be able to take this action without user interaction. Therefore this kind of action is inspect-able and undo-able. Browsing history would reveal any deletion and allow for recovery. Permanent deletion (here called *wiping*) is a different action that requires root privileges. Rogue processes would not be able to take this action. This kind of action is also inspect-able, revision history would reveal that wiping has taken place but file content would not be accessible anymore.

History of changes to files means that all versions of the file remain stored, or at least a history that can be viewed, isn't that impractical in some cases of confidential files? An option to not save a file history?

History of changes is a list of snapshots, states saved at some points in time, ordered chronologically. History can be browsed and every snapshot can be inspected for details but also every snapshot can be restored back. Confidentiality is not compromised because browsing past versions of files requires same level of access as browsing current version. Anyone having access to past history would have access to current file, anyway. When user deletes a file, it will be recoverable as long as it is browsable in history. When user permanently deletes a file (different than regularly), it will not be recoverable even if history mentions that such file existed in the past. Versioning can also be disabled.

Deleted files are permanently gone, how would that be done? In comparison to saving file history...

Technically there two ways of ensuring data is permanently gone, either through overriding data itself or overriding encryption keys that were used to encrypt said data.

Second approach is much better since keys occupy only few bytes and overriding few bytes takes almost no time. Versioning is completely independent.

Legal questions, may use of the program encounter difficulties with existing laws in some countries?

Depending on your country of residence, you may be:

- forbidden from using cryptographic products in general
- required to get license or send notification before importing (Russia)
- required to disclose cryptographic keys to authorities in advance (Russia)
- asked to decrypt your laptop contents (crossing US border)
- asked if you have any other undisclosed encrypted partitions (crossing US border)
- subpoenaed to produce keys or decrypted data itself
- jailed for long time or until your produce encryption keys (US and UK)

Lesson to learn here is that established law can put you in a position where technical solutions do not give you an easy and legal way out. Consider crossing US border with child pornography on your laptop (it was a real case). Officer asks you to mount all partitions and then asks if you have any hidden partitions on your laptop. Note that lying to a federal agent is a criminal offense in US. If you mount them all, jail, if you lie, possible jail, if you deny, something something jail. Plausible deniability feature may let you lie out of it but it will not make it any more legal.