Déni plausible (cryptologie)

Le **déni plausible** est la possibilité pour une personne soupçonnée d'utiliser un logiciel de chiffrement de nier de manière tout à fait plausible l'existence d'un fichier chiffré créé par ce logiciel.

Ainsi, dans le cadre de l'utilisation des logiciels FreeOTFE ou TrueCrypt, cela est possible car aucun élément du fichier chiffré « conteneur » ou « volume » créé par eux ne permet de le relier directement ou indirectement à ce logiciel. Ni le contenu du fichier, ni le nom et/ou l'extension du fichier, ni même la taille de ce volume n'ont de lien avec le logiciel de chiffrement.

1 Utilisation du déni plausible en cryptographie

En cryptographie, le déni de chiffrement peut être utilisé pour décrire les techniques de stéganographie, dans lesquelles l'existence d'un fichier chiffré peut être niée (ou réfutée) dans le sens où personne ne peut prouver qu'un message chiffré existe, par exemple dissimulé dans une image.

Quelques logiciels poussent le raisonnement plus loin, tels que MaruTukku (en), FreeOTFE et (dans une bien moindre mesure) TrueCrypt, dissimulant des volumes tout entiers.

Le propriétaire de données chiffrées peut révéler une ou plusieurs clefs (ou mot de passe) qui vont permettre de déchiffrer certaines informations, et ensuite nier (réfuter) que d'autres données chiffrées existent, un état qui ne peut pas être prouvé en l'absence de la connaissance de la clef (ou des clefs) ou du mot de passe (ou des mots de passe) nécessaire à la révélation éventuelle d'autres données chiffrées. L'existence de données cachées à l'intérieur d'autres données manifestement chiffrées est alors niable (réfutable) dans le sens où leur existence ne peut être prouvée. Les logiciels FreeOTFE et TrueCrypt (ainsi que l'obsolète Marutukku) permettent un tel fonctionnement, par l'utilisation d'un compartiment caché dans le volume chiffré (un seul possible pour TrueCrypt, une infinité pour FreeOTFE et Marutukku).

2 Voir aussi

- Stéganographie

3 Sources, contributeurs et licences du texte et de l'image

3.1 Texte

- **Déni plausible (cryptologie)** *Source :* https://fr.wikipedia.org/wiki/D%C3%A9ni_plausible_(cryptologie)?oldid=116250522 *Contributeurs :* Gh~frwiki, Trou, Toutoune25, Loveless, Gloran, Thijs !bot, Macassar, Van Rijn, Isaac Sanolnacov, AlleborgoBot, Okram, DumZiBoT, Luckas-bot, ArthurBot, LucienBOT, Thouny, Bugmenot1992, Caylane, Mjbmrbot, MerlIwBot, Metamorforme42, Addbot et Anonyme : 7

3.2 Images

- **Fichier:Crypto_key.png** *Source :* https://upload.wikimedia.org/wikipedia/commons/5/5b/Crypto_key.png *Licence :* LGPL *Contributeurs :* Transféré de fr.wikipedia à Commons. *Artiste d'origine :* Original téléversé par Dake sur Wikipedia français Later versions were uploaded by Croquant at fr.wikipedia.
- **Fichier:Nuvola_apps_kgpg.png** *Source :* https://upload.wikimedia.org/wikipedia/commons/a/a2/Nuvola_apps_kgpg.png *Licence :* LGPL *Contributeurs :* http://icon-king.com *Artiste d'origine :* David Vignoni / ICON KING
- **Fichier :_Nuvola_apps_password.png** *Source :* https://upload.wikimedia.org/wikipedia/commons/7/7c/Nuvola_apps_password.png *Licence :* LGPL *Contributeurs :* http://icon-king.com *Artiste d'origine :* David Vignoni / ICON KING

3.3 Licence du contenu

- Creative Commons Attribution-Share Alike 3.0