Embedding spy secrets in the hard drive fragments

April 26 2011, by Katie Gatto

(PhysOrg.com) -- A new way to hide your secrets has been created, which is good news for both the spies and the generally duplicitous regular people of the world. This new system, instead of relying on traditional methods of hiding data such as encryption to scramble the text, hides information in an entirely different way. The newest thing in covert operations it to manipulate the location of data fragments. Essentially, the data is still being scrambled, but it is in an entirely different way.

The system uses a 160-gigabyte portable hard drive to hide a 20-megabyte message. The system then scrambles the data in order to hide the text and create a message that is very hard to find, unless you happen to know how to find it, that is. This method is, in some ways, preferable to the idea of encryption. It is not that encryption is, or is not, inherently less secure, it is just that encrypted file kind of gives itself away. It makes it obvious that someone is trying to hide what is in the files. This system does not have any kind of a dead giveaway.

That is where the fine art of steganography, or hiding information in plain sight comes into play. A more traditional version of steganography involves added extra to the pixels in digital images that when properly decoded will reveal a message, but like all information smuggling techniques once it is discovered, it cannot be used anymore. This new system may last a bit longer because it depends not on adding new data to a hard drive, but by looking at whether or not the files are arranged sequentially. The end result looks like common usage over time, with the

adding and deleting of files.

The researchers, who hailed from the University of Southern California in Los Angeles and the National University of Science and Technology in Islamabad, Pakistan, have published a paper on this new data embedding method in the *Computers & Security* journal.

More information: Designing a cluster-based covert channel to evade disk investigation and forensics, *Computers & Security*, Volume 30, Issue 1, January 2011, Pages 35-49, doi:10.1016/j.cose.2010.10.005

Abstract

Data confidentiality on a computer can be achieved using encryption. However, encryption is ineffective under a forensic investigation mainly because the presence of encrypted data on a disk can be easily detected and disk owners can subsequently be forced (by law or other means) to release decryption keys. To evade forensic investigation, intelligent information hiding techniques that support plausible deniability have been proposed as an alternative to encryption; plausible deniability allows an evader to hide data in a manner such that he/she can deny the very existence of the data. In this paper, we present a new, plausible deniability approach to store sensitive information on a cluster-based filesystem. Under the proposed approach, a covert channel is used to encode the sensitive information by modifying the fragmentation patterns in the cluster distribution of an existing file. As opposed to existing schemes, the proposed covert channel does not require storage of any additional information on the filesystem. Moreover, the channel provides two-fold plausible deniability so that an investigator without the key cannot prove the presence of hidden information. We derive the theoretical capacity of the covert channel and show that a capacity of up to 24 bits/cluster can be achieved on a half-empty disk. The proposed data hiding and recovery algorithms are implemented on FAT32 based disk drives and we show that the disk (read/write) access time of the

algorithms is quite low as compared to the contemporary approaches. We also present statistics about the incidence of file fragmentation on actual file systems from 52 disk drives belonging to a diverse set of users. Based on these statistics, we present guidelines for selecting good cover files. Finally, we show that even if an investigator gets suspicious, he/she will incur an unreasonably high O(m2) complexity to reveal an m bit hidden message.

via Newscientist and Register