Hide files within files for better data security

May 9 2011

Steganography is a form of security through obscurity in which information is hidden within an unusual medium. An artist might paint a coded message into a portrait, for instance, or an author embed words in the text. A traditional paper watermark is a well-known example of steganography in action. At first glance, there would appear to be nothing unusual about the work, but a recipient aware of the presence of the hidden message would be able to extract it easily. In the computer age, steganography has become more of a science than an art.

Those intent on hiding information from prying eyes can embed data in the many different file types that are ostensibly music files (mp3), images (jpeg), video (mpeg4) or word-processing documents. Unfortunately, there is a limit to how much hidden data can be embedded in such files without it becoming apparent that something is hidden because the file size increases beyond what one might expect to see for a common music or video file, for instance. A five minute music file in mp3 format and the widespread sampling rate of 128 kilobits per second, for instance, is expected to be about 5 megabytes in size. Much bigger and suspicions would be aroused as to the true nature of the file, examination with widely available mp3-tagging software would reveal something amiss with the file's contents. The same could be said for almost all other file types.

However, one group of files that vary enormously in size and are usually rather difficult to examine in detail because they comprise of compiled computer code are executable, or exe, files. These files tend to contain lots of what might be described as "junk data" of their own as well as

internal programmer notes and identifiers, redundant sections of code and infuriatingly in some senses coding "bloat". All of this adds up to large and essentially random file sizes for exe files. As such, it might be possible to embed and hide large amounts of data in encoded form in an exe file without disrupting the file's ability to be executed, or run, as a program but crucially without anyone discovering that the exe file has a dual function.

Computer scientists Rajesh Kumar Tiwari of the GLNA Institute of Technology, in Mathura and G. Sahoo of the Birla Institute of Technology, in Mesra, Ranchi, India, have developed just such an algorithm for embedding hidden data in an executable file. They provide details in the *International Journal of Internet Technology and Secured Transactions*. The algorithm has been built into a program with graphical user interface that would take a conventional exe file and the data to be hidden as input and merge the two producing a viable exe file with a hidden payload. The technology could be used on smart phones, tablet PCs, portable media players and any other information device on which a user might wish to hide data.

More information: "A novel steganographic methodology for high capacity data hiding in executable files" in Int. J. Internet Technology and Secured Transactions, 2011, 3, 210-222
DOI:10.1504/IJITST.2011.039779

Abstract
The prevalence of multimedia data in our digital world exposes a new opportunity for communication using steganographic mediums and new steganographic cover mediums for data hiding are constantly being proposed from classical image file, mp3, mp4, text, html and executable files. Most of the previous works on executable file were consequently done at the source code or compilation level and stores only a small amount of secret data. In this work, we present and analyse a novel

methodology that illustrates how we can store a large amount of secret data in executable files. For implementing our proposed methodologies we use Microsoft platform for the illustration purpose only.

Provided by Inderscience Publishers