# How does steganography work and does it threaten enterprise data?

**NIST just released revision 4 of SP 800-53, which, among other things, covers the threat posed by steganography. How does steganography work, and what threat does it pose to enterprises?**

**Ask the Expert!**

Have questions about enterprise security? Send them via email today! (All questions are anonymous.)

Steganography is an ancient technique for hiding information in plain sight. It has been used throughout history as a covert means of communication. It is rumored that the ancient Greek would shave the head of a messenger and write a message on his bald head. Over time, his hair would grow in and hide the message. He would pass through enemy lines without anyone being aware that the valuable message was right in front of them. The messenger would get his head shaved again when he was ready to deliver the message to the intended recipient.

Luckily, the modern, technical equivalent does not require that you shave your head. Instead, covert information can be embedded into standard file types. One of the most common steganographic techniques is to embed a text file into an image file. Anyone viewing the image file would see no difference between the original file and the file with the message embedded into it. This is accomplished by storing the message using least significant bits in the data file.

The least-significant bits are those that are at the far right of a binary number. For instance, the decimal number 255 is represented in binary code as 11111111. The least significant bit is the last "1" at the far right of the number. If we change the "1"

to a "0" we would get 11111110, which represents 254. The hidden file can be stored using these bits throughout the file. These minor changes cannot be perceived by viewing the image file.

There are a number of steganography tools with which you can experiment. One of my favorites is an older open source tool called steghide. It can be downloaded for Windows and also exists in the default repositories for most Linux distributions. The tool can embed data into both image and audio files fairly simply using the command line syntax *steghide embed -cf image.jpg -ef message.txt*. It also supports encryption and compression of the embedded file.

The threat to enterprises should be clear based on the capabilities of steganography. An employee could easily attach a seemingly generic image file to an email that actually contains an embedded document full of company secrets within its code. The image file could slip through security controls, such as data loss prevention systems, and be delivered to a competitor's email inbox.

The potential for the loss of intellectual property and confidential information through steganography is great. The tools are easy to use and the modified files are hard to detect. NIST has elevated the risk of network exfiltration through steganography by adding guidance to the NIST Special Publication 800-53 standard, which includes strict protocol adherence, deep packet inspection and other data loss prevention techniques. Detecting steganography can be complex, but at least no one needs to shave their head.

## More News and Tutorials

*This was first published in August 2013*

To add a Comment, please create a user name.