

Secret Messages Come in .Wavs

Declan McCullagh

(Reprinted From Wired Magazine)

FAIRFAX, Virginia -- Neil Johnson has a job that's nothing if not unusual: He investigates how to uncover concealed messages embedded in sound and video files.

A researcher at Virginia's George Mason University, Johnson is one of a small but growing number of digital detectives working in the field of computer steganalysis -- the science of detecting hidden communications.

"I analyze stego tools," said the 32-year-old security specialist who is the associate director of GMU's Center for Secure Information Systems. "I try to find out what can be detected or disabled. I see what their limitations are."

The tools he's talking about include programs such as Steghide, which can embed a message in .bmp, .wav and .au files; and Hide and Seek, which works with .gif images.

Most computer-based steganography tools have one thing in common: They conceal information in digitized information -- typically audio, video or still image files -- in a way that prevents a casual observer from learning that anything unusual is taking place.

The surprising news, according to Johnson and other researchers: Current stego programs don't work well at all. Nearly all leave behind fingerprints that tip off a careful observer that something unusual is going on.

Johnson's work on steganalysis may seem obscure, but it has important law enforcement and military applications. The National Security Agency and police agencies have underwritten his research -- his center's graduate program at GMU is even certified by the NSA.

The Pentagon funds related research at other institutions, and the Naval Research Laboratory is helping to organize the fourth annual Information Hiding Workshop in Pittsburgh from April 25 to 27.

Earlier this month, news reports said U.S. officials were worried that operatives of accused terrorist Osama bin Laden now use steganographic applications to pass messages through sports chat rooms, sexually explicit bulletin boards and other sites. That complicates the NSA's mission of "sigint," or signals intelligence, which relies on intercepting communications traffic.

A close cousin of steganography that's had an uptick in interest recently is watermarking, particularly for copyright purposes. Some publishers and broadcasters, worried that digital works are too easy to copy, are turning to encrypted copyright marks and serial numbers injected into the electronic versions of books, audio and video.

The practice of steganography has a distinguished history: The Greek historian Herodotus describes how one of his countrymen sent a secret message warning of an invasion by scrawling it on the wood underneath a wax tablet. To casual observers, the tablet appeared blank.

Secret Messages Come in .Wavs

Declan McCullagh

(Reprinted From Wired Magazine)

In World War II, both Axis and Allied spies used invisible inks such as milk, fruit juice and urine, which darken when heated. They also used tiny punctures above key words in documents that formed messages when combined.

Steganography differs from encryption, though in practice they're often combined. Unlike stego, which aims for undetectability, encryption relies on ciphers or codes to keep a message private after it has been detected.

Gary Gordon, vice president of cyber-forensics technology at WetStone Technologies, based in Freeville, New York, said that his firm has made progress in creating a tool to detect steganography.

"The goal is to develop a blind steganography detection prototype," Gordon said. "What we've done is gone out, using Web spiders, and downloaded pictures from the Web and run the tool against them."

Steganography, Gordon said, primarily turns up on hacker sites. But he and his associates also found instances of steganography on heavily traveled commercial sites such as Amazon and eBay.

Nearly any kind of file can be used by steganographers. One program, called snow, hides a message by adding extra whitespace at the end of each line of a text file or e-mail message.

Perhaps the strangest example of steganography is a program called Spam Mimic, based on a set of rules called a mimic engine by *Disappearing Cryptography* author Peter Wayner. It encodes your message into -- no kidding -- what looks just like your typical, delete-me-now spam message.

Gordon said his lab has had the most luck detecting stego when messages are hidden in JPEG images. "Steganography is not necessarily a negative thing," Gordon says. "It can be used for defense information and warfare purposes."

WetStone's "Steganography Detection and Recovery Toolkit" is being developed for the Air Force Research Laboratory in Rome, New York. The project overview, according to the company, is "to develop a set of statistical tests capable of detecting secret messages in computer files and electronic transmissions, as well as attempting to identify the underlying steganographic method. An important part of the research is the development of blind steganography detection methods for algorithms."

Gordon said the effort arose from a study the Air Force commissioned from WetStone on forensic information warfare in 1998. The company was asked to identify technologies that the Air Force needed to guard against and it highlighted steganography as one of them.

In addition to the NSA and the eavesdrop establishment, military installations, government agencies, and private employers could be affected by steganography. An employee or contractor could send sensitive information via e-mail that, if hidden, would not arouse suspicion.

Law enforcement agencies, on the other hand, seem most worried about steganography's effects on forensic examinations, such as when a computer is seized as evidence and examined by police. A

Secret Messages Come in .Wavs

Declan McCullagh

(Reprinted From Wired Magazine)

suspect successfully using steganography could embed incriminating evidence in something innocuous -- a digital family photo album, for instance -- and escape detection.

George Mason University's Johnson is building a stego-detector, a program he says examines hard drives "like a virus scanner" and identifies the electronic fingerprints sometimes left by steganographic applications.

"Different authors have different ways to hide information to make it less perceptible," Johnson says. "The author may come up with ideas that nobody else is using. That tool may have a special signature. Once that signature is detected, it can be tied to a tool."

Johnson says that in one recent case his techniques helped police to nab a suspect who raised suspicions after repeatedly e-mailing innocuous photographs to addresses that appeared to be of family members -- but he never received any replies. "I identified the stego signature that law enforcement used to catch the guy," Johnson says.

He says the Steganos program is one of the least detectable and provides "the most pleasing results."

Johnson admitted the NSA funded his early research, and said the spy agency brought him to its Fort Meade headquarters for an intensive question-and-answer session with many other government agencies represented. But he refuses to reveal who is funding his current project, except to say it is a law enforcement agency.

He also refused to say how far along his stego-detector is in the development process. "I'm not releasing that information." However, he did say that "it's vanilla enough to be compiled and adapted to run on almost anything."

The CIA declined to comment, and the FBI and NSA did not return phone calls.

First-generation stego programs typically embedded information in the least significant bits that represented the pixels of an image. But images, especially compressed ones, often have predictable patterns that are disrupted when an image is inserted.

The ability of an observer to detect steganography typically increases as the message grows longer. But embedding a one-bit message -- a yes or a no -- in a 1 MB MP3 file would be all but impossible to detect.

"The more stegotext we give the (observer), the better he may be able to estimate the statistics of the underlying coartext, and so the smaller the rate at which Alice will be able to tweak bits safely," write researchers Ross Anderson and Fabien Petitcolas in a 1998 paper.

They say: "Given a coartext in which any ciphertext at all can be embedded, then there will usually be a certain rate at which its bits can be tweaked without (anyone) noticing."

Secret Messages Come in .Wavs

Declan McCullagh

(Reprinted From Wired Magazine)

Anderson, a reader in security engineering at Cambridge University, dismisses most commonly used stego products as providing inadequate security.

"There are about three or four generations of stego software," Anderson says. "The stuff you can download is first generation and easily defeated."

He said that "uncompressed audio and video give you a lot of bandwidth. For covertness reasons, you'd probably want to hide your traffic in traffic that's very common."

His recommendation? A Windows program called MP3Stego, designed by a former student with whom Anderson has co-authored papers.

Another paper, by Cambridge researchers, described the design of a steganographic file system for Linux. It allows users to "plausibly deny" the number of files stored on a hard drive.

"There are tradeoffs between reliability and message size and robustness," Anderson says. "There's also a tradeoff between bandwidth and detectability.... The tradeoffs between bandwidth, robustness and detectability are beginning to be understood. They're not completely understood. That's one of the edges of research. "