

White Paper
Five-Year Strategic Plan (FYSP)
for
Federal Networking and Information Technology Research & Development Program

The FYSP must include enhanced countermeasures for insider threat detection and mitigation as a priority.

Awareness of information value has literally exploded in recent years. It is widely-known there is a large and growing international black market for personally identifiable information to facilitate identity theft. Evidence of this can be found in the near daily announcements of information loss or theft that has reached epidemic proportions.

Technology vendors have responded to the seemingly endless stream of information loss disclosures by providing Data Loss Prevention (DLP) tools in an effort to stem the hemorrhaging of information from enterprise networks.

However, these first generation DLP tools were designed to detect accidental loss of information through carelessness or negligence on the part of insiders with authorized access to the information—they were not designed with malicious users in mind.

The increasing value of information coupled with continuing deployments of DLP tools will, in effect, drive nefarious insiders to find and use more technically sophisticated ways to steal information.

One way insiders can steal information is through the use of digital steganography. By using any of the more than 1,000 steganography applications available as freeware or shareware on the Internet, insiders can steal sensitive information with no risk of detection. There is no risk of detection because neither the current generation of DLP tools nor any other current generation network security appliance can detect the use of digital steganography by insiders.

In addition to insider theft of sensitive information, steganography applications can also be used to steal intellectual property. In his remarks at the inauguration of the National Intellectual Property Rights Coordination Center, DHS Secretary Chertoff said “Our national assets and our productive resources in many ways are concentrated in our intellectual property.”¹

Accordingly, protecting intellectual property from loss or theft is an Economic, National, and Homeland Security imperative.

Steganography is also being used by criminals to conceal evidence of criminal activity such as distribution of child pornography and drug trafficking, for example, and is being used by terrorists for covert communication.

In terms of importance, the Federal Plan for Cyber Security and Information Assurance Research and Development² stated that steganographic technologies “... pose a potential threat to U.S. national

¹ Remarks by Homeland Security Secretary Michael Chertoff at the Inauguration of the National Intellectual Property Rights Coordination Center, July 10, 2008, http://www.dhs.gov/xnews/releases/pr_1215736423265.shtm

² Federal Plan for Cyber Security and Information Assurance Research and Development, Report by the Interagency Working Group on Cyber Security and Information Assurance, National Science and Technology Council, April 2006, http://www.nitrd.gov/pubs/csia/csia_federal_plan.pdf

The opinions and positions in the white papers and comments posted on this web site are those of the submitters only and do not necessarily represent those of the Federal government, the NITRD program and its participating agencies, or the National Coordination Office.

security.” and that “The threat posed by steganography has been documented in numerous intelligence reports.”

In terms of capability gaps, the Plan states that “Resources to evaluate, integrate, and deploy the numerous basic research advances are limited and should be enhanced.”

The role for the NITRD Program is to prioritize the expansion of research on existing analytical detection capabilities highly enough to be competitive for funding. The role for the commercial sector is to transition the expanded research results into state-of-the-art digital forensics tools for use by examiners in federal, state, and local law enforcement agencies; the intelligence community; and the private sector and state-of-the-art network security tools for real-time detection of insider use of steganography.

Research into advanced steganography countermeasures is inherently a multi-agency effort because every agency has sensitive information that could be stolen by insiders using steganography. Accordingly all agencies would benefit from enhanced countermeasures to detect insider use of steganography.

A key strategic goal would be to establish a national repository of steganography applications, fingerprints, and signatures that could be used to develop world-class steganalysis tools.

A key challenge will be to provide resources sufficient to establish and maintain the repository and perform the technical research on every steganography application in the repository in order to discover the digital signature of the application, if one exists, and the corresponding algorithm to extract information hidden with the application that can then be integrated into automated steganalysis tools.

The impact of prioritizing research on steganography applications and subsequent development of world-class steganalysis tools will be the detection of attempts to use steganography to steal sensitive information, to include intellectual property, along with detection of attempts to use steganography to conceal evidence of criminal activity that would have otherwise gone undetected.

Improved steganalysis tools will enhance efforts to combat cyber crime and will enhance National and Homeland Security by improving insider threat detection and mitigation capability.