Gray-hat hackers make security flaws public

BY TOM O'DONNELL
IEEE Ethics Committee

Somewhere between the good-guy consumer advocates (wearing white hats) and the bad-guy malicious hackers (in black) lie the so-called "gray-hat hackers." These are self-styled Robin Hoods who make it their business to expose security flaws in software in a very public way. The most well-known exemplars of the gray-hat hacking aesthetic form the collective, L0pht.

L0pht's eight members devote themselves to breaking into software systems and then posting detailed descriptions of the procedures they employed on their Web site. The descriptions may be used by the affected organizations (e.g., Microsoft) to repair the flaw. However, this method of publication makes the information equally available to "black-hat" hackers who may exploit it to capture banking transactions, passwords or credit card information for example. L0pht's approach to hacking has won them as many friends as enemies, with some of their friends coming from rather unexpected places.

During a recent U.S. Senate hearing in which L0pht members testified on the threat to national security that cyber-terrorists might pose, Senator Joseph Lieberman, Conn., USA, praised them saying, "You are performing an act of very good citizenship and...a valuable service to your country."

To be sure, exposing software loopholes to provide protection from cyber-terrorists is positive. But is it really necessary to outfit malicious hackers with the tools to wreak havoc during the window of time between L0pht's announcement of a security flaw and the implementation of any actions the affected organizations might take to safeguard themselves from the security breech? L0pht's members defend their policy not to contact vendors prior to exposing a flaw in their products. They claim that vendors tend to sweep tips from hackers under the rug in order to avoid negative publicity.

"We are all extremely ethical and moral but we are not white-hat hackers. We have our own moral and ethical standards," says Lopht.

While L0pht and other gray-hat hackers may have their own moral and ethical standards, they might take more into consideration the victims of black-hat hackers making use of their knowledge. It is not enough to take the attitude of one L0pht member, "We try to stay somewhat neutral — we're not on the vendor's side, we're not on the hacker's side. When we release the tools, they can be used for good or bad."

Facilitating malicious hacking, then washing your hands of the consequences is not responsible computing.