Technology

Peer-to-peer under fire

Never mind copyright – security's now the big P2P network issue

Joseph Wilson

Henry Waxman has his hands full . As chairman of the U.S. House of Representatives committee on oversight and government reform, he is the man leading investigations into everything from the Abu Ghraib prison abuses to the government's response to Hurricane Katrina.

On July 24, the committee heard testimony from technology experts as part of a new investigation into the evils of peer-to-peer (P2P) networks.

P2P networks like BitTorrent or Kazaa allow users to download large files bit by bit from others on the network who have the files they want.

Instead of focusing on oft-repeated claims of copyright infringement, this new investigation zooms in on the security risks P2P networks pose when people share files they don't mean to.

I caught up with Safwat Fahmy, CEO of SafeMedia Corp., mere hours after he talked to the committee.

"Contaminated P2P networks represent a huge security risk," says Fahmy, whose company has recently released what he calls a P2P Disaggregator (P2PD), an application that "destroys contaminated P2P networks. A contaminated network is one that has pirated or illegal files... and is so spread out that there is no ownership over input and output," he says.

Fahmy's P2PD technology works at the level of the modem or router provided by the Internet service provider (ISP), keeping people from posting illegally copied files on contaminated networks like LimeWire or Kazaa.

I bring up the fact that our telephone conversation is taking place on Skype, a P2P application that allows people to talk over the Web. He assures me that the technology only filters out illegal content.

Instead of arguing about the economic damage file sharing does to the media industry, our conversation focuses on a strongly worded section of a SafeMedia press release stating that file sharing creates an overwhelming security risk for users as well as national security.

"It's a huge problem," says Fahmy. "At the House of Representatives hearing, there was a demonstration where people were able to pull documents off LimeWire detailing troop deployment in Iraq and clearly classified documents from a defence contractor."

One of the groups demonstrating the fallibility of P2P networks was Tiversa, a network security firm that boasts ex-Democratic presidential candidate General Wesley Clark as a board member.

Along with reps from the Center for Digital Strategies at Dartmouth College, Tiversa ran test searches that netted sensitive documents being shared without their owners' knowledge, such as photocopies of birth certificates and passports, credit card numbers, bank statements, tax returns, even a diagram of a Pentagon computer network including a list of passwords.

Such demonstrations naturally make governments and businesses really nervous. LimeWire creator Mark Gorton was at the hearing to assure naysayers that "LimeWire takes the problem of inadvertent file sharing seriously."

He must have been uncomfortable in the hot seat, though, as many of the sensitive files found during Tiversa's test were found on the LimeWire network.

So who's to blame? The tendency when it comes to new technologies is to blame the technology itself as being "dangerous," "threatening" or even "contaminated." However, reps at the hearing also spoke of the ignorance of P2P users and their inability to manage their files properly.

Many users dump all their files into one folder and unintentionally share sensitive files alongside their MP3s. Furthermore, the programs themselves often dupe users into sharing folders they aren't aware of, or use wizards to find folders on users' computers that contain media files.

A recent report by the U.S. Federal Trade Commission, however, summarizes the blame game perfectly: "Peer-to-peer file sharing is a neutral technology.... Its risks result largely from how individuals use the technology rather than being inherent in the technology itself. "

It will be interesting to see how P2P networks fare in upcoming months.