With A Little Help From Your Friends: A New Way To Block Spam

May 18 2005

Friends can help friends block spam -- or at least their computers can. So says a University of Florida computer engineer who has pioneered a new approach to zapping the junk e-mail that slows productivity and poses an increasing security threat to computer users worldwide.
With colleagues at the University of California-Los Angeles, Oscar Boykin, a UF assistant professor of electrical and computer engineering, has simulated a system that taps a user's "social network" of friends and colleagues to root out spam. Current antispam software blocks incoming spam by matching keywords or images with previously identified spam. A computer outfitted with the proposed system would first check incoming messages with its own anti-spam software -- then, if no match were found, automatically check it against the software on the "trusted" computers among a user's circle of regular contacts.

"Your software would classify the message when it could, but when it couldn't, it would query your 'network of trust,' in effect asking 'do you know if this message is spam or not?'" Boykin said.

Boykin and Vwani Roychowdhury, an electrical engineering professor at UCLA, have co-authored two articles related to the proposal in recent months. The first appeared in April in the journal Computer, published by the Institute of Electrical and Electronics Engineers. The second, also co-authored by UCLA doctoral student Joseph Kong and available now at www.arxiv.org, is slated for presentation at the Second Conference on Email and Anti-Spam at Stanford University this summer.

Spam constitutes more than two-thirds of all e-mail, accounting for billions of messages daily. An increasingly annoying and expensive time-waster, spam has also become more threatening in recent years with the advent of “phishing” -- when criminals use false e-mail to dupe people into revealing personal financial data. Such crimes accounted for $2.4 billion in fraud affecting nearly 2 million people in 2003-04, according to a 2004 survey by the research firm Gartner Inc.

Boykin said he got the idea for the social approach from an insight that his e-mail records contain consistent patterns that can distinguish friends and colleagues from spammers. For example, unlike spammers, normal users usually e-mail one or maybe several people, not hundreds or thousands, and they typically receive e-mails in reply. “There is a very striking difference in the parts of the e-mail network that were associated with spam versus those that were just normal communication,” he said.

He and Roychowdhury realized that software could be developed that takes a page from peer-to-peer networks to exploit these already established networks of friends and acquaintances. Unlike client-server models, in which a central computer serves a community of users, peer-to-peer networks link users directly with one another. Instead of sharing music -- perhaps the most well-known peer-to-peer activity -- the proposed software would silently share information with its “friends” on the network.

“Rather than searching for music, your software would send queries across the network in search of other trusted computers that have already identified a message as spam,” he said.

He and Roychowdhury created mathematical models and a computer simulation of the system. They found that the more users the system included, the more spam e-mail it could detect. Boykin said that points

to the system's main challenge: To be effective, it would have to be widely used, which would require extensive marketing and high public confidence. Developing the software to make the system a reality, on the other hand, is not a difficult challenge, Boykin said.

Bill Yerazunis, a senior research scientist at Mitsubishi Electronics Research Laboratories in Cambridge, Mass., and an expert on spam, said the UF/UCLA research is "well-founded" and that there is a "good chance" the system would work well.

He said a potential shortcoming is that sharing information about incoming e-mail might present a security problem.

"You have to trust your circle of friends' computers to see your incoming mail stream but not compromise the possibly highly personal e-mail you get," he said.

Source: UF