Science & Technology

Computer, Heal Thyself

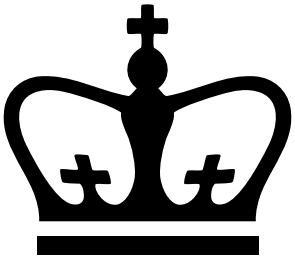
Winter 2006-07

When software vendors discover that their product is susceptible to worms or viruses, they develop a fix, or patch, that customers then must laboriously test to make sure it won't disrupt their computers. The entire process can take months. In the meantime, systems administrators face a tough choice: Shut down the vulnerable software or keep it running despite the possibility of disaster.

Angelos Keromytis, an associate professor of computer science, wants to provide a third option. He's developing technology that enables a computer network to spot a security breach automatically and then create, test, and implement a temporary fix. This could be done in less than a minute, with no human involvement. The system uses a honeypot, a computer set up specifically to lure worms, viruses, and hackers. When the honeypot detects a security breach, it steers the intruder to an isolated part of the network to be analyzed. There, a computer tests potential changes to the source code of the software targeted by the worm, until it finds a solution that won't disrupt the application.

This fall, Keromytis received a $1.3 million grant from the National Science Foundation and the National Security Agency to fine-tune his technology. It's already licensed to Revive Systems, a start-up Keromytis founded with entrepreneurs Loren Burnett and Bob Stratton last winter. The company raised $2.5 million this year and plans to market its product initially to large server centers and hosting centers. The company isn't ready yet to announce a release date.

"We're not going to be able to deal with every type of conceivable bug," says Keromytis, whose research team includes computer science professors Salvatore Stolfo and Gail Kaiser. "But we should be able to head off 90 to 95 percent of security breaches, which will save people an incredible amount of money and frustration."



Guide to school abbreviations