"If you start seeing 10,000 messages come out of grandma's computer, it's probably not a sign that grandma is typing really fast and has had a whole bunch of coffee," Smith says. "It's probably a sign that her system has been taken over."

Creating a Safety Net for Computers

By Janelle Weaver

The rise of computer technology meant to make our lives easier comes with a cost: the ever-growing risk of security and privacy violations. Companies evaluate their customers' web browsing habits to target Internet ads, and "phishers" send fraudulent emails in an effort to procure credit card details from individuals who bank and shop online. Meanwhile, an application named Creepy allows users to track the locations of people based on geotagged photos uploaded to Twitter or Flickr.

Technology can even endanger someone's health, as demonstrated this August at the Black Hat Technical Security Conference. One of the keynote speakers showed that it's possible to remotely control glucose monitors and insulin pumps to alter doses of the hormone.

"Since I have both of these medical devices, I was quite interested in the hack," says Jonathan Smith, Olga and Alberico Pompa Professor of Engineering and Applied Science in the Department of Computer and Information Science. "Personally, I turn off the wireless interface on my insulin pump, so there's no way to attack me in that manner." Smith is not only thwarting hacks that could affect his health, he's also developing innovative strategies to prevent attacks that could sabotage personal computers and entire networks.

Bot Blockers

For a project funded by the Office of Naval Research, Smith collaborates with colleagues at Penn, Harvard and Princeton to shield networks against botnets – collections of computers controlled by a master for nefarious purposes. Botnets often originate from downloads of malicious software, such as spyware and adware.

In a common type of onslaught known as a denial-of-service attack, many computers send communication requests that collectively overwhelm a target computer. Not only can these barrages paralyze the machine and disable Internet sites, but they can also wreak havoc on financial activities and government services. "They create a lot of fear in the community because people worry that they'll lose their connectivity when they need it for something important," Smith says.

Smith and his team are devising ways to block downloads from websites that have infected machines in the past. Another tactic involves flagging abnormal

Dr. Jonathan Smith

activity. “If you start seeing 10,000 messages come out of grandma’s computer, it’s probably not a sign that grandma is typing really fast and has had a whole bunch of coffee,” Smith says. “It’s probably a sign that her system has been taken over.” By deflecting unusual Internet traffic coming from specific nodes, it’s possible to keep botnets at bay.

Better SAFE than Sorry

To build a next-generation computer capable of resisting attacks, Smith is collaborating with Benjamin Pierce, professor of Computer and Information Science, and André DeHon, associate professor of Electrical and Systems Engineering, along with scientists at Harvard and Northeastern University. They are working on the Semantically Aware Foundation Environment (SAFE) initiative led by BAE Systems and funded by the Defense Advanced Research Projects Agency (DARPA).

Smith’s task is to protect machines from being hijacked by decentralizing the operating system and enforcing access restrictions. For instance, someone approved to use the printer is prohibited from running irrelevant programs, changing files or memory settings, or controlling network devices. This undertaking requires an overhaul of computer hardware, operating systems and programming languages, which traditionally have not been designed with security in mind, Smith says.

In another large initiative that started last year, Smith is helping to develop a safer Internet called Nebula. This network will consist of secure paths that transmit information to data centers, such as nodes that provide medical advice. This approach could reduce healthcare costs and lead to earlier diagnoses by encouraging the sharing of medical data among physicians and by preventing excessive tests, Smith says. “We try to bash away at the security and privacy problems that get in the way of people feeling comfortable using the Net for all of the tasks in their lives.”

Thinking Like the Enemy

Sometimes the best defense comes from understanding the enemy. To figure out how to improve face recognition systems, Smith is testing which disguises work best. In one experiment, the accuracy of one of these systems dropped from almost perfect to as low as 15 percent when images of faces were obscured with mirrored sunglasses, a scarf or a dark nylon stocking.

These findings can also be used to foil face recognition systems and deter invasions of privacy, such as attempts to predict social security numbers from pictures of faces. This example highlights the need for precluding large-scale, 100 percent accurate face identification, Smith says. “Sometimes the good guys are using the cameras, and sometimes the bad guys are. I want to be on the side of the good guys.”