UC SANTA BARBARA

THE Current

February 24, 2010

Andrea Estrada

Computer Security Group Addresses Internet Vulnerabilities

It's like something out of a Robert Ludlum novel: Cybercriminals bent on stealing confidential information hijack the computers of unsuspecting users around the world and infect them with malicious software. Unbeknownst to their owners, these computers form a network of zombie machines –– a botnet –– that volunteers whatever information the cybercriminals command it to find.

Recently, researchers in the Computer Security Group at UC Santa Barbara went on a virtual crime spree of their own and took control of Torpig, one of the largest and most notorious botnets in the world. Pretending to be hijackers, the researchers dived into what they call the "underground economy" and exposed Torpig's inner workings. In the process, they discovered that 180,000 Windows computers –– mainly in the United States and Europe –– were under the botnet's control. These computers were providing data on online bank accounts, credit and debit card accounts, and e-mail accounts. The researchers collaborated with the FBI and other law enforcement agencies, as well as with the banks and financial institutions involved, to notify the owners of the compromised accounts.

The botnet investigation, which is part of an ongoing grant from the National Science Foundation to study the workings of the underground economy, is only one of several projects the group has undertaken over the last several years in its quest to make the cyberworld a safer place. Others include the development of Web sites that examine the veracity of suspicious Web programs or Web pages, and a study of

electronic voting machines and their vulnerability to election-altering attacks.

Earlier this month, the group received a $6.2 million grant from the U.S. Army Research Office to lead a multi-campus, collaborative effort to develop a comprehensive security system that can defend against cyber attacks. Designed to determine whether and how an infiltration by hackers might affect the outcome of a particular military mission, the system will automatically identify attacks on the Internet, assess the degree of damage, identify possible responses, and predict future threats.

"It's called situational awareness," said Richard Kemmerer, professor of computer science. "Every kind of information you can think of –– including state secrets –– exists on a computer somewhere. Unless that computer is locked up with no connection to the outside world, there's a chance of that information getting compromised." Kemmerer is one of the UC Santa Barbara group's three core faculty members. The others include Giovanni Vigna, professor of computer science, and Christopher Kruegel, associate professor of computer science.

The new project calls on the group to advance current state-of-the-art cyber security in five key areas: devising sound yet practical techniques to automatically analyze network activity to obtain an up-to-date view of how the network is being used; developing comprehensive analysis techniques to automatically extract relationships in the network; creating a situational awareness framework that will identify targets of cyber attacks and estimate the impact of a successful attack; developing models of adversary behavior that will help predict the effects of future attacks; and establishing a visualization framework that will provide an easily understood view of the network's status, and to help learn about attacks while they are in process.

In addition to Kemmerer, Vigna, and Kruegel, the research team includes Tobias Höllerer, associate professor of computer science, and João Hespanha, professor and vice chair of electrical and computer engineering. The other universities involved in the project are UC Berkeley and Georgia Institute of Technology.

Two main characteristics make the Computer Security Group at UCSB uniquely qualified to lead projects that range from botnets to voting machines to national security.

"On the one hand, we're academics, so our approach to problems is based on the scientific method and theoretical modeling," explained Vigna. "But we also have the

skills and knowledge to be very practical and rooted in the real world. When we do research, it's very applied and we create tools the whole world can use. Other academics do proofs of concepts, but we go a step further and actually build programs that people can use to protect themselves."

"We want our ideas to be used in practice," said Kemmerer, who also holds UCSB's Computer Science Leadership Endowed Chair. "In order to do this, we build tools that implement the novel research ideas we come up with. Making these tools available free on the Internet allows other researchers to build on our work and to validate that it functions as advertised. In addition to providing tools to practitioners and other researchers, this is just good science."

Combining academic and real-world pursuits was not always the premise of the Computer Security Group. It began 28 years ago as the Reliable Software Group with Kemmerer at the helm. His research involved several different areas of system dependability. Security was one piece of the reliable software puzzle. When Vigna came to UCSB in 1997 as a postdoctoral researcher, he brought his experience as a network engineer –– and a hacker –– and he and Kemmerer began collaborating on new ideas.

"It was probably the result of a synergy between my more low-level approach and his theoretical perspective," Vigna said. When Kruegel joined the team, that synergy became even stronger. "We have a group that is very uniquely positioned with respect to the international scene," noted Vigna.

Kruegel, who had been a postdoctoral student at UCSB, left the university to join the faculty of the Technical University of Vienna. In 2005, he established the International Secure Systems Lab in Vienna, which also operates facilities at the Institute Eurécom on the French Riviera and at UCSB. He returned to the computer science department at UCSB in 2008.

Related Links

Computer Security Group

About UC Santa Barbara

The University of California, Santa Barbara is a leading research institution that also provides a comprehensive liberal arts learning experience. Our academic community

of faculty, students, and staff is characterized by a culture of interdisciplinary collaboration that is responsive to the needs of our multicultural and global society. All of this takes place within a living and learning environment like no other, as we draw inspiration from the beauty and resources of our extraordinary location at the edge of the Pacific Ocean.