Toward a modular defense against hackers

April 11 2012

Tan, who directs the Security of Software Lab, has studied software security for more than a decade.

(Phys.org) -- The FBI's top cyber security officer gave a grim assessment last week of the nation's ability to defend itself from hackers.

America's economy, infrastructure and national security are at risk, Shawn Henry told The Wall Street Journal, unless major changes are made in technology and in the way computer and software networks are protected.

Henry's comments, which were echoed by cybersecurity experts, came as no surprise to Gang Tan, assistant professor of computer science and engineering.

From online buying and vote-counting to air-traffic control and electrical

power transmission, says Tan, software is indispensable to everyday life. But as software increases in complexity (lines of code), connectivity (almost all software is now online) and extensivity (plug-ins and other extensions make it easy to download programs), it becomes more vulnerable to hackers.

Tan has studied software security for more than a decade. With funding from the National Science Foundation (NSF), the National Security Agency and the U.S. Department of Defense, he has developed automated techniques to scan for errors in large software systems.

Recently, Tan received a five-year CAREER Award from NSF to study and develop a type of modular software that is less vulnerable to system-wide attacks by hackers. The award is one of the most coveted honors for young faculty members.

"Like a political separation of powers"

In his new project, Tan is attempting to apply to software systems the principle of least privilege, a technique used widely in computer security.

"The principle of least privilege is like the separation of powers in a political system," says Tan, who directs Lehigh's Security of Software, or SOS, Lab.

"Instead of structuring software as a monolithic system, we break software into multiple modules. Each module works as a separate protection domain. It needs only a very small privilege [access to data and administrative authority] to do its job.

"When software is monolithic, an entire system can be disabled or destroyed by one vulnerability and one lone hacker. When software is

broken into smaller modules with individual boundaries, if any one subsystem is taken out, the rest of the system will still function."

Researchers have made progress in privilege separation in software environments, says Tan, but challenges remain with operating system portability, high runtime overhead, architectural flexibility and compositional reasoning.

Tan proposes a three-part framework to facilitate the adoption of privilege separation. To isolate domains and monitor the flow of information between them, he will develop a "virtualization layer" using binary rewriting, optimization and verification. A binary-level tool will split an application into modules of least privilege, and a compositional reasoning mechanism will let developers assess an application's end-to-end information security.

"This is a divide-and-conquer approach with individual tasks for each module," he says. "It realizes the principle of least principle at the binary code level. It can be source language-independent, working for Java as well as C.

"These new tools and methodologies will make the principle of least principle easier to apply to big software systems. By monitoring information flow at the binary instead of the source-language level, it will be easier to check the security properties of individual modules, prevent malicious information flow between modules and allow only benign information flow."

Tan plans to test the effectiveness of his framework on real-world applications, including web browsers and Java Virtual Machines.

Provided by Lehigh University