PHYS.ORG

Cybersecurity experts begin investigation on self-adapting computer network that defends itself against hackers

May 10 2012

(Phys.org) -- In the online struggle for network security, Kansas State University cybersecurity experts are adding an ally to the security force: the computer network itself.

Scott DeLoach, professor of computing and information sciences, and Xinming "Simon" Ou, associate professor of computing and information sciences, are researching the feasibility of building a computer network that could protect itself against online attackers by automatically changing its setup and configuration.

DeLoach and Ou were recently awarded a five-year grant of more than $1 million from the Air Force Office of Scientific Research to fund the study "Understanding and quantifying the impact of moving target defenses on computer networks." The study, which began in April, will be the first to document whether this type of adaptive cybersecurity, called moving-target defense, can be effective. If it can work, researchers will determine if the benefits of creating a moving-target defense system outweigh the overhead and resources needed to build it.

Helping Ou and DeLoach in their investigation and research are Kansas State University students Rui Zhuang and Su Zhang, both doctoral candidates in computing and information sciences from China, and Alexandru Bardas, doctoral student in computing and information sciences from Romania.

As the study progresses the computer scientists will develop a set of analytical models to determine the effectiveness of a moving-target defense system. They will also create a proof-of-concept system as a way to experiment with the idea in a concrete setting.

"It's important to investigate any scientific evidence that shows that this approach does work so it can be fully researched and developed," DeLoach said. He started collaborating with Ou to apply intelligent adaptive techniques to cybersecurity several years ago after a conversation at a university open house.

The term moving-target defense -- a subarea of adaptive security in the cybersecurity field -- was first coined around 2008, although similar concepts have been proposed and studied since the early 2000s. The idea behind moving-target defense in the context of computer networks is to create a computer network that is no longer static in its configuration. Instead, as a way to thwart cyber attackers, the network automatically and periodically randomizes its configuration through various methods -- such as changing the addresses of software applications on the network; switching between instances of the applications; and changing the location of critical system data.

Ou and DeLoach said the key is to make the network appear to an attacker that it is changing chaotically while to an authorized user the system operates normally.

"If you have a Web server, pretty much anybody in the world can figure out where you are and what software you're running," DeLoach said. "If they know that, they can figure out what vulnerabilities you have. In a typical scenario, attackers scan your system and find out everything they can about your server configuration and what security holes it has. Then they select the best time for them to attack and exploit those security holes in order to do the most damage. This could change that."

Creating a computer network that could automatically detect and defend itself against cyber attacks would substantially increase the security of online data for universities, government departments, corporations and businesses -- all of which have been the targets of large-scale cyber attacks.

In February 2011 it was discovered that the Nasdaq Stock Market's computer network had been infiltrated by hackers. Although federal investigators concluded that it was unlikely the hackers stole any information, the network's security had been left vulnerable for more than a year while the hackers visited it numerous times.

According to Ou, creating a moving-target defense system would shift the power imbalance that currently resides with hackers -- who need only find a single security hole to exploit -- back to the network administrators -- who would have a system that frequently removes whatever security privileges attackers may gain with a new clean slate. "This is a game-changing idea in cybersecurity," Ou said. "People feel that we are currently losing against online attackers. In order to fundamentally change the cybersecurity landscape and reduce that high risk we need some big, fundamental changes to the way computers and networks are constructed and organized."

Provided by Kansas State University

Citation: Cybersecurity experts begin investigation on self-adapting computer network that defends itself against hackers (2012, May 10) retrieved 27 April 2024 from https://phys.org/news/2012-05-cybersecurity-experts-self-adapting-network-defends.html