Setting up a decoy network may help deflect a hacker's hits

September 9 2016, by Matt Swayne

Instead of trying to stop these hackers' scans, researchers set up a detector to monitor incoming web traffic to determine when hackers are scanning the network. Image: © iStock Photo Vladimir Timofeev, Pennsylvania State University

Computer networks may never float like a butterfly, but Penn State

information scientists suggest that creating nimble networks that can sense jabs from hackers could help deflect the stinging blows of those attacks.

"Because of the static nature of a computer network, the attacker has a time advantage," said Dinghao Wu, assistant professor of information sciences and technology. "Hackers can spend a month, two months, six months or more just studying the network and finding vulnerabilities. When they return to use that information to attack, the network typically has not changed and those vulnerabilities are still there, too."

The researchers, who release their findings at the Information Security Conference held in Honolulu today (Sept. 8), created a computer defense system that senses possible malicious probes of the network and then redirects that attack to a virtual network that offers little information about the real network.

Typically, the first step a hacker takes when attacking a network is a probe to gain information about the system—for example, what software types and versions, operating systems and hardware the network is running. Instead of trying to stop these hackers' scans, researchers set up a detector to monitor incoming web traffic to determine when hackers are scanning the network.

"We can't realistically stop all scanning activities, but we can usually tell when a malicious scan is happening," said Wu. "If it's a large-scale scan, it is usually malicious."

Once a malicious scan is detected, the researchers use a network device—called a reflector—to redirect that traffic to a decoy, or shadow network, according to Li Wang, a doctoral candidate in information sciences and technology, who worked with Wu. The shadow network is isolated and invisible from the real network, but can mimic the structure

of a physical network to fool the hackers into believing they are receiving information about an actual network.

"A typical strategy would be to create a shadow network environment that has the same look as the protection domain," said Wang. "It can have the same number of nodes, network topology and configurations to fool the hacker. These shadow networks can be created to simulate complex network structures."

The system, which is a type of defense known in the computer industry as a moving target defense, also gives network administrators the option to more easily change parts of the shadow network's virtual system, making it even more difficult for hackers to assess the success of their scans.

Because the reflector can act as a regular network device when no malicious attacks are present, there should be little effect on the real network's performance and functionality, according to Wu.

The researchers created a prototype for the system and tested it on a simulated network that runs on a computer—a virtual local area network. This allowed them to simulate both the attack and defense without using an actual network. The prototype was able to sense the incoming scan and deflect it to a shadow network.

According to the researchers, the information that was gathered from the attack scan only produced information from the shadow network.

Wu said the next step is to deploy the system in an actual network.

The Penn State Fund for Innovation, National Science Foundation and the Office of Naval Research supported this work.

Provided by Pennsylvania State University

Citation: Setting up a decoy network may help deflect a hacker's hits (2016, September 9) retrieved 30 January 2023 from https://techxplore.com/news/2016-09-decoy-network-deflect-hacker.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.