New project ensures 'what you see is what you send'

February 25 2014

Imagine a user who intends to send $2 to a friend through PayPal. Embedded malware in the user's laptop, however, converts the $2 transaction into a $2,000 transfer to the account of the malware author instead.

Researchers at Georgia Tech have created a prototype software, Gyrus, that takes extra steps to prevent malware from sending spam emails and instant messages, and blocking unauthorized commands such as money transfers.

Current protection programs might recognize the original user's intent to send email, transfer money or engage in other transactions, but cannot verify the specifics such as email contents or amount of money. Without context, it is impossible to properly verify the user's full intent, regardless of whether the software is protecting a financial transfer, an industrial control system or a wide range of other user-driven applications.

"Gyrus is a transparent layer on top of the window of an application. The user experience with the application will be exactly the same as when Gyrus is not installed or activated. Of course, if Gyrus detects that user-intended data has been tampered with, it will block the traffic and also notify the user," explained Wenke Lee, director of the Georgia Tech Information Security Center (GTISC).

The Georgia Tech research is based on the observation that for most text-

based applications, the user's intent will be displayed entirely on screen, as text, and the user will make modifications if what is on screen is not what he or she wants. Users help Gyrus do its job by establishing pre-defined rules that help the software determine whether commands—authorized or not—fit with established user intentions. In the researchers' words, Gyrus implements a "What You See Is What You Send" (WYSIWYS) policy.

"The idea of defining correct behavior of an application by capturing user intent is not entirely new, but previous attempts in this space use an overly simplistic model of the user's behavior," said Yeongjin Jang, the Georgia Tech Ph.D. student who led the study.

"For example, they might infer a user's intent based on a single mouse click without capturing any associated context so the attackers can easily disguise attacks as a benign behavior," Jang added. "Instead, Gyrus captures richer semantics including both user actions and text contents, along with applications semantics, to make the system send only user-intended network traffic. Gyrus indirectly but correctly determines user intent from the screen that is displayed to the user. "

There are two key components to Gyrus' approach. First, it captures the user's intent and interactions with an application. Second, it verifies that the resulting output can be mapped back to the user's intention. As a result, the application ensures accurate transactions even in the presence of malware.

More information: www.cc.gatech.edu/~yjang37/papers/gyrus.pdf

Provided by Georgia Institute of Technology