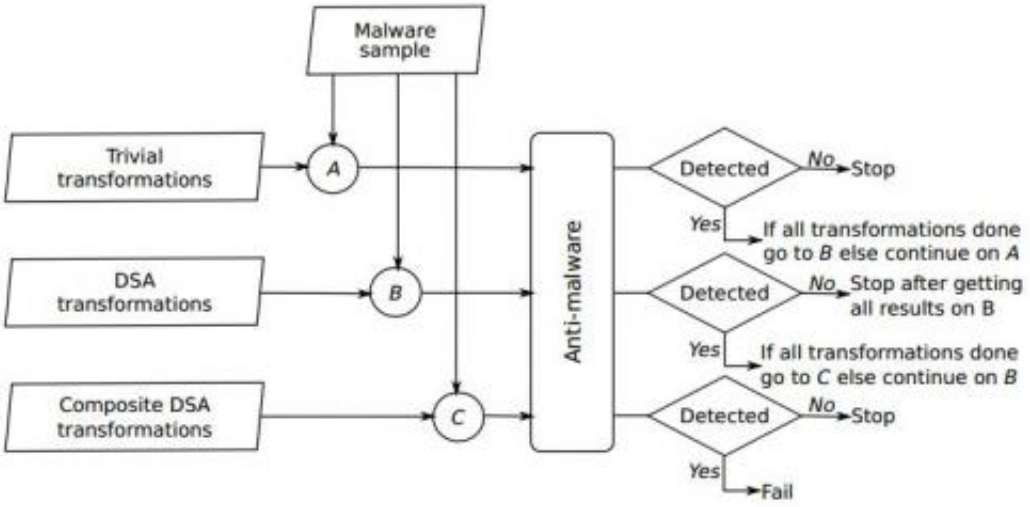
Android antiviral products easily evaded, study says

May 30 2013



Evaluating anti-malware. Credit: Yan Chen

Think your antivirus product is keeping your Android safe? Think again. Northwestern University researchers, working with partners from North Carolina State University, tested 10 of the most popular antiviral products for Android and found each could be easily circumnavigated by even the most simple obfuscation techniques.

"The results are quite surprising," said Yan Chen, associate professor of electrical engineering and computer science at Northwestern's McCormick School of Engineering and Applied Science. "Many of these products are blind to even trivial transformation attacks not involving

code-level changes—operations a teenager could perform."

The researchers began by testing six known viruses on the fully functional versions of 10 antiviral products.

Using a tool they developed called DroidChameleon, the researchers then applied common techniques—such as simple switches in a virus's binary code or file name, or running a command on the virus to repackage or reassemble it—to transform the viruses into slightly altered but equally damaging versions. Dozens of transformed viruses were then tested on the antiviral products, often slipping through the software unnoticed.

All of the antiviral products could be evaded, the researchers found, though their susceptibility to the transformed attacks varied.

The products' shortcomings are due to their use of overly simple content-based signatures, special patterns the products use to screen for viruses, the researchers said. Instead, the researchers suggested, the products should use a more sophisticated static analysis to accurately seek out transformed attacks. Only one of the 10 tested tools currently utilizes a static analysis system.

The researchers chose to study Android products because it is the most commonly used operating system in the United States and worldwide, and because its open platform enabled the researchers to easily conduct analyses. They emphasized, however, that other operating systems are not necessarily more protected from virus attacks.

Antiviral products are improving. Last year, 45 percent of signatures could be evaded with trivial transformations. This year, the number has dropped to 16 percent.

"Still, these products are not as robust and effective as they must be to stop malware writers," Chen said. "This is a cat-and-mouse game."

More information: A paper about the research, "Evaluating Android Anti-Malware Against Transformation Attacks," was presented earlier this month at the 8th ACM Symposium on Information, Computer and Communications Security (ASIACCS 2013).

Provided by Northwestern University