Dynamic detection system could protect smartphones from malicious content

February 23 2016

Credit: Peter Griffin/Public Domain

The danger of acquiring a computer virus or spyware used to come with the risk of visiting the dark, sketchy corners of the Internet. But now trusted and harmless smartphone apps like MyFitnessPal and Candy Crush carry their own risks.

"Even reputable apps can lead users to websites hosting malicious

content," said Yan Chen, professor of computer science at the Northwestern University McCormick School of Engineering. "No matter what app you use, you are not immune to malicious ads."

Most people are accustomed to the ads they encounter when interacting with apps on mobile devices. Some pop up between stages in games while others sit quietly in the sidebars. Mostly harmless, ads are a source of income for developers who often offer their apps for free. But as more and more people own smartphones, the number of malicious ads hidden in apps is growing—tripling in just the past year.

In order to curb attacks from hidden malicious ads, Chen and his team are working to better understand where these ads originate and how they operate. This research has resulted in a dynamic system for Android that detects malicious ads as well as locates and identifies the parties that intentionally or unintentionally allowed them to reach the end user.

Last year, Chen's team used its system to test about one million apps in two months. It found that while the percentage of malicious ads is actually quite small (0.1 percent), the absolute number is still large considering that 2 billion people own smartphones worldwide. Ads that ask the user to download a program are the most dangerous, containing malicious software about 50 percent of the time.

Ad networks could potentially use Chen's system to prevent malicious ads from sneaking into the ad exchange. Ad networks buy space in the app through developers, and then advertisers bid for that space to display their ads. Ad networks use sophisticated algorithms for targeting and inventory management, but there are no tools available to check the safety of each ad.

"It's very hard for the ad networks," Chen said. "They get millions of ads from different sources. Even if they had the resources to check each ad,

those ads could change."

The team will present their research, findings, and detection system on Monday, Feb. 22, 2016 at the 2016 Network and Distributed System Security Symposium in San Diego, California.

Chen's work culminated from the exploration of the little-studied interface between mobile apps and the Web. Many in-app advertisements take advantage of this interface: when users click on the advertisement within the app, they are led to an outside web page that hosts malicious content. Whether it is an offer to download fake anti-virus software or fake media players or claim free gifts, the content can take many forms to trick the user into downloading software that gathers sensitive information, sends unauthorized and often charged messages, or displays unwanted ads.

When Chen's detection software runs, it electronically clicks the ads within apps and follows a chain of links to the final landing page. It then downloads that page's code and completes an analysis to determine whether or not it's malicious. It also uses machine-learning techniques to track the evolving behaviors of malware as it attempts to elude detection.

Currently, Chen's team is testing ten-times more ads with the intention of building a more efficient system. He said their goal is to diagnose and detect malicious ads even faster. As people put more and more private information into their phones, attackers are motivated to pump more malicious ads into the market. Chen wants to give ad networks and users the tools to be ready.

"Attackers follow the money," Chen said. "More people are putting their credit card and banking information into their phones for mobile payment options. The smartphone has become a treasure for attackers, so they are investing heavily in compromising them. That means we will

see more and more malicious ads and malware."

Provided by Northwestern University