Team develops a simple defense for complex smartphone malware (w/ video)

February 28 2013, by Kevin Storr

(Phys.org)—University of Alabama at Birmingham (UAB) researchers have developed simple but effective techniques to prevent sophisticated malware from secretly attacking smartphones. The Tap-Wave-Rub (TWR) methods – tapping, waving a hand over or rubbing the phone's proximity sensor – are being presented at the 6th Association for Computing Machinery Conference on Security and Privacy in Wireless and Mobile Networks (WiSec'13) April 17-19, 2013, in Hungary, Budapest.

The designers say the TWR system will turn the phone's weakest security component, the user, into its strongest defender.

"The most fundamental weakness in mobile device security is that the security decision process is dependent on the user," says Nitesh Saxena, Ph.D., the director of the Security and Privacy In Emerging computing and networking Systems (SPIES) lab and assistant professor of computer and information sciences at UAB. "For instance, when installing an Android app, the user is prompted whether or not the application should have permissions to access a given service on the phone. The user may be in a rush or distracted, or maybe it is the user's kid who has the phone. Whatever the case may be, it is a well-known problem that people do not look at these warnings; they just click 'yes.'"

It is this weakness of the human user that malicious entities exploit. For example, a malware writer whose goal is to make hidden phone calls or texts to premium rate numbers may hide a malicious code within a simple tic-tac-toe app. When prompted at the time of installing this game app, pressing "yes" would allow the game to make phone calls.

Attackers create a phone or text number that charges large sums of money for use. The malware then triggers a program that asks your mobile device to call or text that number. Such malware is already prevalent, and researchers and practitioners anticipate this and other forms of malware to become one of the greatest threats affecting millions of smartphone users in the near future.

Accepting terms on computers and smartphones is habitual repetition, and hackers with mal intent know this; they can leverage a user's vulnerability to, among other things, make a harmless-looking game dangerous.

TWR works by using the proximity sensor that comes standard in most smartphones. These sensors, for example, save power by turning the screen off when a phone is near the user's ear.

TWR methods help verify the user's desire to voice dial or message, or access any other resource on the phone, by requiring the user to tap, wave their hand over or rub the sensor before actions are executed. By means of a TWR gesture, the device basically captures the user's intent to perform an action. In the absence of this gesture, when a malicious app attempts to dial a phone number, the device will simply block it. The strength of this malware defense lies in its simplicity and broad applicability to different forms of constantly evolving malware.

Saxena's team carefully chose tapping, waving and rubbing because they are the least likely movements to be replicated accidentally. In other words, the device will be less likely to confuse any of those motions during daily activities such as walking, dropping the phone or playing a video game.

"We purposely designed the TWR program to not involve yes/no and to force people to stop for a moment and think about whether or not the action requested by the phone is what they really would like their mobile device to perform," Saxena said.

There is a disclaimer.

"Any mechanism may not guarantee 100 percent safety, as there is always a little chance of error," Saxena said. "You must also pay attention to what you are downloading and what permissions are granted at the time of installation to fully protect yourself."

UAB graduate student Babins Shrestha, a researcher in the SPIES Lab who coauthored the article, will present the paper at WiSec'13.

"There are anti-virus applications available for mobile devices but, unlike our method, they are ineffective, eat up your phone's resources and cannot keep up with new strains of malware," Shrestha said.

UAB undergraduate student Justin Harrison has also been involved with the project, integrating the TWR gestures with the voice dialing service. The project team, which is funded by the National Science Foundation and includes researchers from University of Michigan-Dearborn, also developed an implicit gesture mechanism—"phone tapping"—explicitly geared for protecting near field communication (NFC) transactions. These usually require the user to tap their phone with a payment terminal or another phone. This gesture is detected using the phone's accelerometer, which is also standard on all smartphones.

More information: www.sigsac.org/wisec/WiSec2013/

Provided by University of Alabama at Birmingham

Citation: Team develops a simple defense for complex smartphone malware (w/ video) (2013, February 28) retrieved 24 April 2024 from https://phys.org/news/2013-02-team-simple-defense-complex-smartphone.html