New technology to help users combat mobile malware attacks

27 March 2015, by Katherine Shonesy

University of Alabama at Birmingham researchers have developed simple but effective techniques to prevent sophisticated malware from secretly attacking smartphones. This new malware defense is being presented at the IEEE International Conference on Pervasive Computing and Communications, or PerCom, today in St. Louis.

As mobile phones increase in functionality, they are becoming increasingly ubiquitous in everyday life. At the same time, these devices also are becoming easy targets for malicious activities.

One of the primary reasons for such malware explosion is user willingness to download applications from untrusted sources that may host apps with hidden malicious codes. Once installed on a smartphone, such malware can exploit it in various ways.

For example, it can access the smartphone's resources to learn sensitive information about the user, secretly use the camera to spy on the user, make premium-rate phone calls without the user's knowledge, or use a Near Field Communication, or NFC, reader to scan for physical credit cards within its vicinity.

Such malware already is prevalent, and researchers and practitioners anticipate that this and other forms of malware will become one of the greatest threats affecting millions of smartphone users in the near future.

"The most fundamental weakness in mobile device security is that the security decision process is dependent on the user," said Nitesh Saxena, Ph.D., the director of the Security and Privacy In Emerging computing and networking Systems (SPIES) Lab and an associate professor of computer and information sciences in the College of Arts and Sciences at UAB. "For instance, when installing an Android app, the user is prompted to choose 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.'"

Current operating systems provide inadequate security against these malware attacks, putting the burden of prevention upon the user. The current anti-virus systems are ineffective against such constantly evolving malware. UAB pursued research to find a mechanism that would defend against mobile malware that can exploit critical and sensitive mobile device services, especially focusing on the phone's calling service, camera and NFC.

This study from researchers within the UAB College of Arts and Sciences Department of Computer and Information Sciences and Center for Information Assurance and Joint Forensics Research explains how natural hand gestures associated with three

primary smartphone services—calling, snapping and tapping—can be detected and have the ability to withstand attacks using motion, position and ambient sensors available on most smartphones as well as machine learning classifiers.

If a human user attempts to access a service, the gesture would be present and access will be allowed. In contrast, if the malware program makes an access request, the gesture will be missing and access will be blocked.

To demonstrate the effectiveness of this approach, researchers collected data from multiple phone models and multiple users in real-life or near real-life scenarios, simulating benign settings and adversarial scenarios.

The results showed that the three gestures can be detected with a high overall accuracy and can be distinguished from one another and from other benign or malicious activities to create a viable malware defense.

"In this method, something as simple as a human gesture can solve a very complex problem," Saxena said. "It turns the phone's weakest security component—the user—into its strongest defender."

The research team believes that, in the future, transparent gestures associated with other smartphone services, such as sending SMS or email, also can be integrated with this system. The researchers also aim to commercialize this technology in the near future.

Provided by University of Alabama at Birmingham