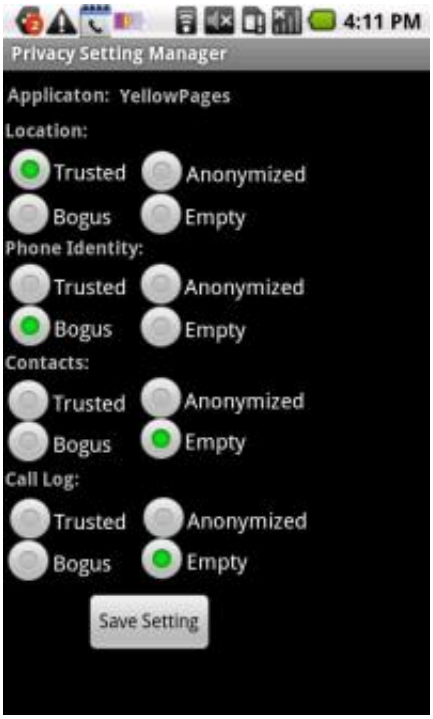
Researchers create privacy mode to help secure Android smartphones

April 13 2011



The new security tool works by creating a privacy setting manager that allows users to customize the level of information each smartphone application can access. Credit: Xuxian Jiang, North Carolina State University

Researchers at North Carolina State University have developed software that helps Android smartphone users prevent their personal information from being stolen by hackers.

"There are a lot of concerns about potential leaks of personal

information from smartphones," says Dr. Xuxian Jiang, an assistant professor of computer science at NC State and co-author of a paper describing the research. "We have developed software that creates a privacy mode for Android systems, giving users flexible control over what personal information is available to various applications." The privacy software is called Taming Information-Stealing Smartphone Applications (TISSA).

TISSA works by creating a privacy setting manager that allows users to customize the level of information each smartphone application can access. Those settings can be adjusted any time that the relevant applications are being run – not just when the applications are installed.

The TISSA prototype includes four possible privacy settings for each application. These settings are Trusted, Anonymized, Bogus and Empty. If an application is listed as Trusted, TISSA does not impose additional information access restrictions. If the user selects Anonymized, TISSA provides the application with generalized information that allows the application to run, without providing access to detailed personal information. The Bogus setting provides an application with fake results when it requests personal information. The Empty setting responds to information requests by saying the relevant information does not exist or is unavailable.

Jiang says TISSA could be easily modified to incorporate additional settings that would allow more fine-grained control of access to personal information. "These settings may be further specialized for different types of information, such as your contact list or your location," Jiang says. "The settings can also be specialized for different applications."

For example, a user may install a weather application that requires location data in order to provide the user with the local weather forecast. Rather than telling the application exactly where the user is, TISSA

could be programmed to give the application generalized location data – such as a random location within a 10-mile radius of the user. This would allow the weather application to provide the local weather forecast information, but would ensure that the application couldn't be used to track the user's movements.

The researchers are currently exploring how to make this software available to Android users. "The software modification is relatively minor," Jiang says, "and could be incorporated through an over-the-air update."

More information: The paper, "Taming Information-Stealing Smartphone Applications (on Android)," was co-authored by Jiang; Yajin Zhou, a Ph.D. student at NC State; Dr. Vincent Freeh, an associate professor of computer science at NC State; and Dr. Xinwen Zhang of Huawei America Research Center. The paper will be presented in June at the 4th International Conference on Trust and Trustworthy Computing, in Pittsburgh, Pa.

Provided by North Carolina State University