Experts identify easy way to improve smartphone security

October 29 2014, by Bobbie Mixon

Study participants were asked to select one of two apps. One app displayed risk information, and another app displayed safety information. Risk and safety information were presented as filled ovals similar to the one to five stars used to present consumer ratings. Credit: Christopher S. Gates, Purdue University

What information is beaming from your mobile phone over various computer networks this very second without you being aware of it?

Experts say your contact lists, email messages, surfed webpages, browsing histories, usage patterns, online purchase records and even password protected accounts may all be sharing data with intrusive and sometimes malicious applications, and you may have given permission.

"Smartphones and tablets used by today's consumers include many kinds of sensitive information," says Ninghui Li, a professor of Computer Science at Purdue University in Indiana.

The apps downloaded to them can potentially track a user's locations, monitor his or her phone calls and even monitor the messages a user sends and receives—including authentication messages used by online banking and other sites, he says, explaining why unsecured digital data are such a big issue.

Li, along with Robert Proctor and Luo Si, also professors at Purdue, lead a National Science Foundation (NSF)-funded project "User-Centric Risk Communication and Control on Mobile Devices," that investigates computer security. The work pays special attention to user control of security features in mobile systems.

Li, Proctor and Si believe they may have a simple solution for users, who unknowingly allow voluntary access to their personal data.

Most users pay little attention

"Although strong security measures are in place for most mobile systems," they write in a recent report inthe journal IEEE Transactions on Dependable and Secure Computing, "the area where these systems often fail is the reliance on the user to make decisions that impact the security of a device."

Most users pay little attention, say the researchers, to unwanted access to

their personal information. Instead, they have become habituated to ignore security warnings and tend to consent to all app permissions.

"If users do not understand the warnings or their consequences, they will not consider them," says Proctor, a Distinguished Professor of psychological sciences at Purdue.

"If users do not associate violations of the warnings with bad consequences of their actions, they will likely ignore them," adds Jing Chen, a psychology Ph.D. student who works on the project.

In addition, there are other influences that contribute to users ignoring security warnings. In the case of Android app permissions, of which there are more than 200, many do not make sense to the average user or at best require time and considerable mental effort to comprehend.

"Permissions are not the only factor in users' decisions," says Si, an associate professor of Computer Science at Purdue, who also led research on a paper with Li that analyzed app reviews.

"Users also look at average ratings, number of downloads and user comments," Si says. "In our studies, we found that there exist correlations between the quality of an app and the average rating from users, as well as the ratio of negative comments about security and privacy."

"This is a classic example of the links between humans and technology," says Heng Xu, program director in the Secure and Trustworthy Cyberspace program in NSF's Social, Behavioral and Economic Sciences Directorate. "The Android smartphones studied by this group of scientists reveals the great need to understand human perception as it relates to their own privacy and security."

"The complexity of modern access control mechanisms in smartphones can confuse even security experts," says Jeremy Epstein, lead program director for the Secure and Trustworthy Cyberspace program in NSF's Directorate for Computer and Information Science and Engineering, which funded the research.

"Safeguards and protection mechanisms that protect privacy and personal security must be usable by all smartphone users, to avoid the syndrome of just clicking 'yes' to get the job done. The SaTC program encourages research like Dr. Li's and colleagues that helps address security usability challenges."

Numbers speak to the amount of unsecured personal data

According to Google, the current developer of the Android operating system, more than 400 million Android devices were activated in 2012. As of July 2013, users had downloaded more than 50 billion apps from Google Play, Android's official app store.

The numbers speak to the amount of unsecured personal data now available for offsite storage and use by third parties.

In an effort to make it easier for users to understand what information an app can access, the online Google Play store arranged app permissions into categories available for review before an app is purchased.

One category, "Contacts/Calendar," warns that when users are faced with giving permission for this group, the app may use the device's contacts and/or calendar information to "read your contacts, modify your contacts, read your calendar events plus confidential information, add or modify calendar events and send email to guests without owners'

knowledge."

Another category, "Cellular data settings" warns the app "can use settings that control your mobile data connection and potentially the data you receive."

Smartphone security researchers identify these requests as "dangerous permissions," because they come with associated risks. Furthermore, Li and colleagues argue that nearly all apps make permission requests with such risks.

Including a risk score has "significant positive effects"

The researchers believe, however, that assigning a risk score to each app and displaying a summary of that information may slow down unwarranted access to personal information by making the risk more transparent and by giving incentive to developers to use less personal information.

Li and his team conducted several experiments that employed a risk score strategy. They found including a risk score had "significant positive effects" for those selecting apps to install on a user's Android smartphone. They also reported that risk scores could lead to more user curiosity about security-related information thereby reducing how often security warnings are disregarded.

Experiments asked participants to select between two apps presented to them in three ways: with risk summary information not displayed, with risk summary information displayed as text and/or with risk summary information displayed as a series of filled ovals similar to the one to five stars used to present consumer ratings.

In a first experiment, the researchers verified that the presence of risk-summary text could influence participants' decisions as to whether to install an app. Participants chose the app identified as less-risky 77 percent of the time.

In another experiment, the researchers focused on how risk information is communicated to the consumer. They wanted to know whether users would be more responsive to "risk information" or "safety information." Li and colleagues tested the question using a number of filled circles—for half of the participants, they framed the filled circles to mean more risk. For the other half, they framed the filled circles to mean less risk or more security.

The researchers compared the response times for the two different ways of communicating risk. They found consumer decisions to install the app were faster when information was presented in the safety condition, indicating people have a natural tendency to react to safety information over risk information.

The outcome suggests it may be better to present permission warnings as safety information rather than the more common risk assessments.

"This result is surprising in one sense because security warnings typically are conveyed as risks," says Li. "However, in another sense it is not too surprising because the positive framing of safety is more compatible with other aspects of selecting a desirable app."

"When technologists design and implement security mechanisms for systems used by the mass population, they should not design for other technologists," Li says. "Instead, they need to understand what can be comprehended and effectively used by the mass population."

More information: "Effective Risk Communication for Android

Apps," *IEEE Transactions on Dependable and Secure Computing*, 16 December 2013 DOI: 10.1109/TDSC.2013.58