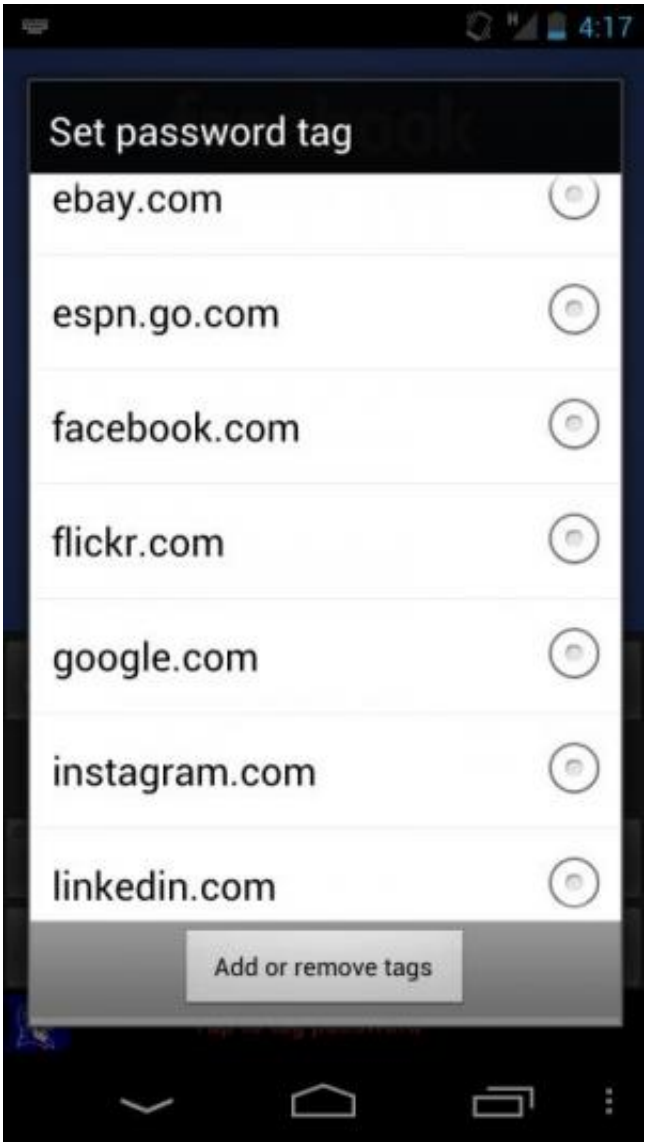
Feature stops apps from stealing phone users' passwords

June 27 2013



This screenshot of an Android phone shows the selection phone users have when logging into apps with ScreenPass. Credit: Landon Cox, Duke.

Imagine downloading a NetFlix app to your phone so that you can watch movies on the go. You would expect the app to request your account's username and password the first time it runs. Most apps do.

But, not all apps are what they appear to be. They can steal log-in and password information. In 2011, researchers at North Carolina State University discovered a convincing imitation of the real Netflix app that forwarded users' login details to an untrusted server. And, in June, the security firm F-Secure discovered a malicious, fake version of the popular game "Bad Piggies" in the Google Play Store.

Attacks like these are rare, said Duke computer scientist Landon Cox, but, "we will likely see more of them in the future." To protect users against the threat of malicious apps, Cox and his team have built ScreenPass. ScreenPass adds new features to an Android phone's operating system to prevent malicious apps from stealing a user's passwords.

"Passwords are a critical glue between mobile apps and remote cloud services," Cox said. "The problem right now is that users have no idea what happens to the passwords they give to their apps."

This is where ScreenPass comes in. It provides a special-purpose software keyboard for users to securely enter sensitive text such as passwords. An area below the keyboard allows users to tell ScreenPass where they want their text sent, such as Google, Facebook, or Twitter. ScreenPass then tracks a users' password data as the app runs and notifies the user if an app tries to send a password to the wrong place.

ScreenPass guarantees that users always input passwords through the secure keyboard. It does this by using computer vision to periodically

scan the screen for untrusted keyboards.

"If a malicious app can trick a user into inputting their password through a fake keyboard, then there is no way to guarantee that an app's password is sent only to the right servers," Cox said. If ScreenPass detects an untrusted keyboard, then an app may be trying to "spoof" the secure keyboard in order to steal the user's password.

Cox and his team presented ScreenPass at the MobiSys 2013 conference in Taipei on June 27.

In trials on a prototype phone, ScreenPass detected attack keyboards that tried to avoid detection by changing the font, color, and blurriness of letters on the keys. "The only attack keyboard that ScreenPass could not detect was a keyboard with a flowery background that blended in with the keyboard letters," Cox said.

He and his team also installed ScreenPass on the phones of 18 volunteers for three weeks to test how user-friendly it was. Users reported no additional burden at having to tell ScreenPass where their passwords should be sent.

Finally, testing ScreenPass on 27 apps from the Android Marketplace, the team found three apps sent passwords over the network in plaintext, four stored passwords in the local file system without encryption, and three apps sent passwords from different domains to a third-party server owned by the app developer. Cox would not provide the names of the apps, but said ScreenPass also easily detected the fake Netflix app.

Cox's team plans to make ScreenPass publicly available to continue to improve smartphone password security.

More information: "ScreenPass: Secure Password Entry on

Touchscreen Devices." Liu, D. et. al. MobiSys 2013. June 27, 2013.

Provided by Duke University