

With Android 2.3, users will have not only a slew of new features (I can't wait!), but also a fix to a security issue present in the previous versions of Android: TapJacking. TapJacking occurs when a malicious application displays a fake user interface that you can interact with, but actually secretly passes interaction events, such as finger taps, to a hidden user interface behind it. Using this technique, a devious developer could potentially trick a user into making purchases, clicking on ads, installing applications, or even wiping all of the data from the phone. All around, TapJacking is not good!

In previous versions of Android, an attacker was able to display the fake user interface by creating a customized notification (called a Toast) to obscure the real interface. Fortunately, thanks to the Android Security Team and the diligent work of the Lookout Mobile Security team (love these guys!), the Android 2.3 SDK has added the ability for developers to prevent interaction events when they are obscured by another view. It's important to remember that the new security features require developers to explicitly set them to protect users from TapJacking - it is not automatic.