Researchers of cybersecurity in Chinese University of Hong Kong (CUHK) have discovered bug in the OAuth 2.0 protocol, which allows hackers to log in to a billion Android app accounts at once and steal Facebook and other social media data. The OAuth 2.0 is a single sign-in protocol that serves users to sign in to a third party service by using their Facebook and other social media accounts without creating a new username for the service. Around 600 well-known apps on Google Play China and Google Play US were analyzed, out of which 182 were found to be using the single sign-in option with Google, Facebook and Sina Weibo.

Originally, the protocol was intended to be used for websites. This is why application developers were not able to apply it similarly for Android app security and had a hard time implementing it appropriately to 41% of the analyzed apps, which included those of hotel booking, VoIP call, banking, shopping, music, video, etc.

Suppose you open an app and it gives you an option to sign in with your Facebook ID instead of making a new ID. The server at Facebook gives you a token for access. This is where many app developers failed to put a check on the information being sent by the social media account for its correctness. These apps would hence log in immediately even if the user information sent by social media apps did not match with those of the user signing in to the Android app. According to the researchers, hackers could easily bypass Android app security here with the help of a Man in the Middle Attack. If the hacker gets to know your social media email address and your name, they can download the same app and use MiTM attack for replacing your profile with theirs. In case of an app that includes transactions, like shopping or banking app, the attacker can easily pay through your credit card, transfer money into their account or carry out any other transactions.

According to the researchers, it is also the responsibility of identification providers Google, Facebook and Sina Weibo to give clear Android app security guidelines to third party app developers, to which social media service providers have agreed.