

Student Seminar: Exploiting Two Factor Authentication of Android and IOS

Robin Solignac 235020

February 26, 2017

Abstract

Applications which can be used in different platforms now use two factor authentication (2FA) to allow users to conveniently switch from one platform to another. For example, when a user tries to login his gmail, it is not enough to enter correct password (first factor), it is also necessary to enter a PIN which is received by an SMS (second factor). The aim of this project explaining the attacks against 2FA in IOS and Android devices and what can be the solutions.

1 Introduction: The current 2 Factors Authentication

Two factor authentication (2FA) is a combinaison of 2 acces control requirement in order to make it more robust to attacker. to authenticate yourself to an online service you both need to provide something you know (your password) and something you have. A large majority of people in todays world has phone and a large share of them are smart, one of the most most used “something you have” is a phone or a smartphone

More than that, it’s the fact that the service can through this phone send you a message who will not transit on your (maybe compromised) PC who is used. your smartphone is an out of band channel.

the current 2FA scheme is the flowing: after a succesful password authentication it send a One- Time Passwords (OTP) to the smartphone of the user most of the time via SMS but also sometime via a dedicated app.

2 Key concepts

2.1 Syncornisation

Our use of informatic is mostly divided between our personal computers and smartphones. For this reason software manufacturers have sometimes decided to implement synchronisation processes between the 2 devices in order to make transition and general use of the 2 smoother, blurring the line between the two.

3 examples of such synchronisation which will be used in our attack are the following:

Google play remote install It's possible from a PC via the Google Play website to remotely install an application on our phone if both are logged on the same Google account. The only thing appearing on the phone afterward is the application icon in the app tray and a notification saying "<app_name> has been successfully installed"

Apple Continuity On recent versions of iOS and macOS you can enable this setting to synchronise in clear, read and send your SMS from your Mac.

Browser synchronisation Almost all of today's most popular internet browsers propose synchronization between their mobile and desktop versions logged under the same user account. It will sync history, bookmark and sometimes currently open tabs

2.2 MitB: Man in the browser attack

MitB is a type of attack which assumes that the attacker has an entire control and view on the PC browser of the victim. Like a man in the middle attack, the attacker can see all data exchanged by the browser and server and can modify them (on the fly). It also can send and receive data in the name of the user. But unlike the former it has access to these data before they are encrypted (or after they are decrypted) and has also modified browser-related settings like bookmark and current open tabs URLs. In short, a powerful man in the browser attack can remotely perform the same actions as someone getting physical access to the browser

There are different ways to do a MitB attack, using malware infecting the whole system, by API hooking or via malicious plugins. TO COMPLETE ?

3 2FA Attack on

3.1 Android

The principle to the attack is to, via a MitB, install from the web play-store an application from with authorization to read SMS (autorisation confirmed from the browser too). Then when an SMS is received it is forward to the attacker, thus bypassing F2A. In order to succed the attacker need to pass two defense setup by Google.

Bypassing Google boncer llzezeffe

Activate the app When installed, an Android app can't be triggered by external event (such as RECEIVE_SMS) until it has been explicitly open for the first time. So we need to trick the user to open the app from the phone. The first way is to give a clickbait title to the app so that the user will be tempted to open it when he sees the installation notification. The second is to trigger its opening from the mobile browser by cliking a link

3.2 Ios

Since 2015 Ios has forbid the application to read all notificatino or SMS without explicit authorization (or they will be rejected from entering the appstore). Since then, the previous attack does not work.

However if the infected browser is on a Mac and Continuity is activated on the Iphone. the browser can still has acces to to SMS in clear on the mac as soon as both are on the same LAN, which is likely to eventually occurs as they belong to the same person.

So under these pretty likely to appers conditons, the 2FA authentication can be very easily bypassed on 2FA by an MitB attack.

4 Discussions

4.1 Android

4.2 Ios

5 Conclusion