Student Seminar: Exploiting Two Factor Authentication of Android and IOS

Robin Solignac 235020

March 5, 2017

1 Introduction: The current 2 Factors Authentification

Two factor authentification (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 fllowing: after a succesful password authtification 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 beetween our personnal computers and smartphones. for this reason software manufacturer have sometime decided to implement syncronisation processes beetween the 2 devices in order to make transition and general use of the 2 smoother, bluring the line beetween the two.

3 exemple of such syncronisation who 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 remotly install an application on our phone if both are logged on the same google account. the only thing appering on the phone afterward is the application incon in the app tray and an notification saying "<app_name> as been succesfully installed"

Apple Continuity On recent version of Ios and macOs you can enable this setting to syncronise in clear, read and send your SMS from your mac.

Browser syncronisation Allmost all of today's most popular internet browser propose syncornization beetween theire mobile and desktop version logged under same user account. it will sync history, boommark and sometime currently open tabs

2.2 MitB: Man in the browser attack

MitB is a type of attack who assume that the attacker has an entier control and view on the PC browser of the victim. Like a man in the

middle attack, the attaker 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 acces to these data before they encrypted (or after they are decryted) And has also modify browser related setting like bookmark and current open tabs URLs. In short powerfull man in the browser attack can remotelly perform the same actions has someone getting physical acces to the browser

there are different way to do a MitB attack, using malware infecting the whole system, by API hooking or via malicious plugin. 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 autorization 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 autorization (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 Continity 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 authentification can be very easily bypassed on 2FA by an MitB attack.

4 Discutions

4.1 Android

4.2 Ios

5 Conclusion