# Student Seminar: Exploiting Two Factor Authentication of Android and IOS

Robin Solignac 235020

February 22, 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 it can be the solution.

## 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

But it's not the only fact of having a phone or a phonenumber who is used in pratice to authenticate but the fact that services can send message to it and that that user can get it without using the main (maybe compromised) communivcation channel. This is called an out of band channel.

Modern 2FA work by: 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 anywhere computing

## 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

## 3.2 Ios

# 4 Discutions

# 5 conclusion

# References