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

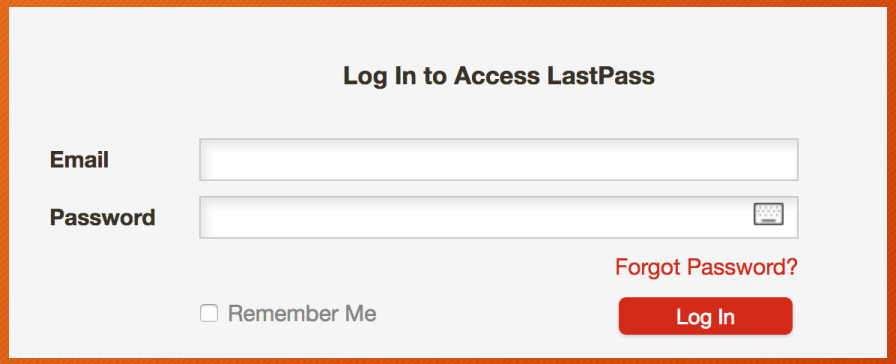
Robin Solignac

235020

# 1. Introduction: The 2 Factors Authentication Model

# 1. Presentation of 2FA model
# The concept

- Combination of 2 access control in order to authenticate
  - Something you know + Something you have




- Main goal: prevent authentication by third party in case of compromised password or main communication channel

# 1. Presentation of 2FA model
# The choice of smartphones

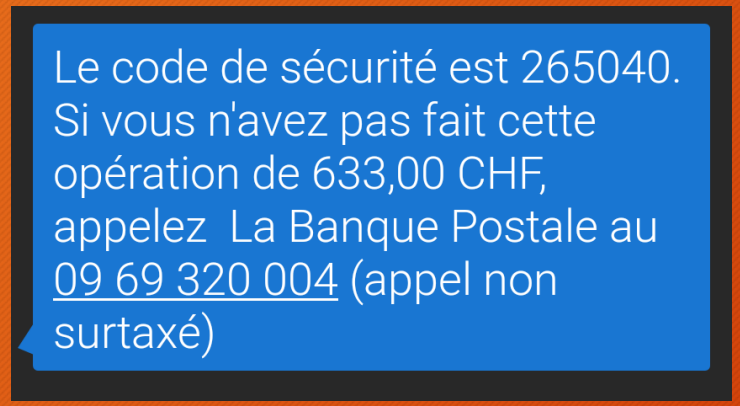
- Majority of online modern 2FA use (smart)phone as “something you have”
  - Convenient: Don’t require the user to carry yet another card or devices
  - Available: Large majority of user have one
  - Reachable & Out of band: services can send message to it without using the main communication channel

- Implement by Google, Microsoft, Amazon, Twitch, Twiter, Visa, …

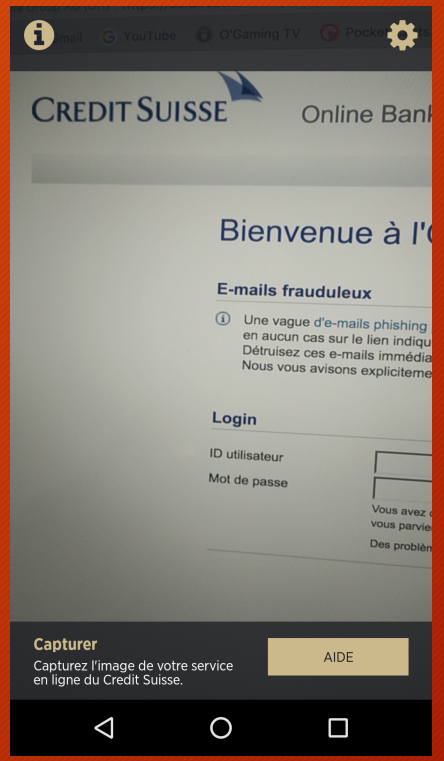
# Presentation of 2FA model
# 2FA one smartphone

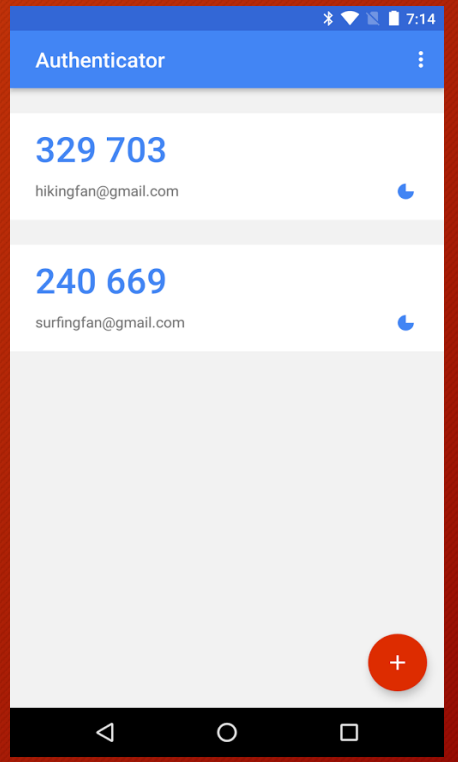
# 1. Presentation of 2FA model
# Smartphone 2FA implementation

- SMS One Time Password (OTP)




- Dedicated application
  - Can rely on OTP or not



# Presentation of 2FA model

# 2. Key concepts

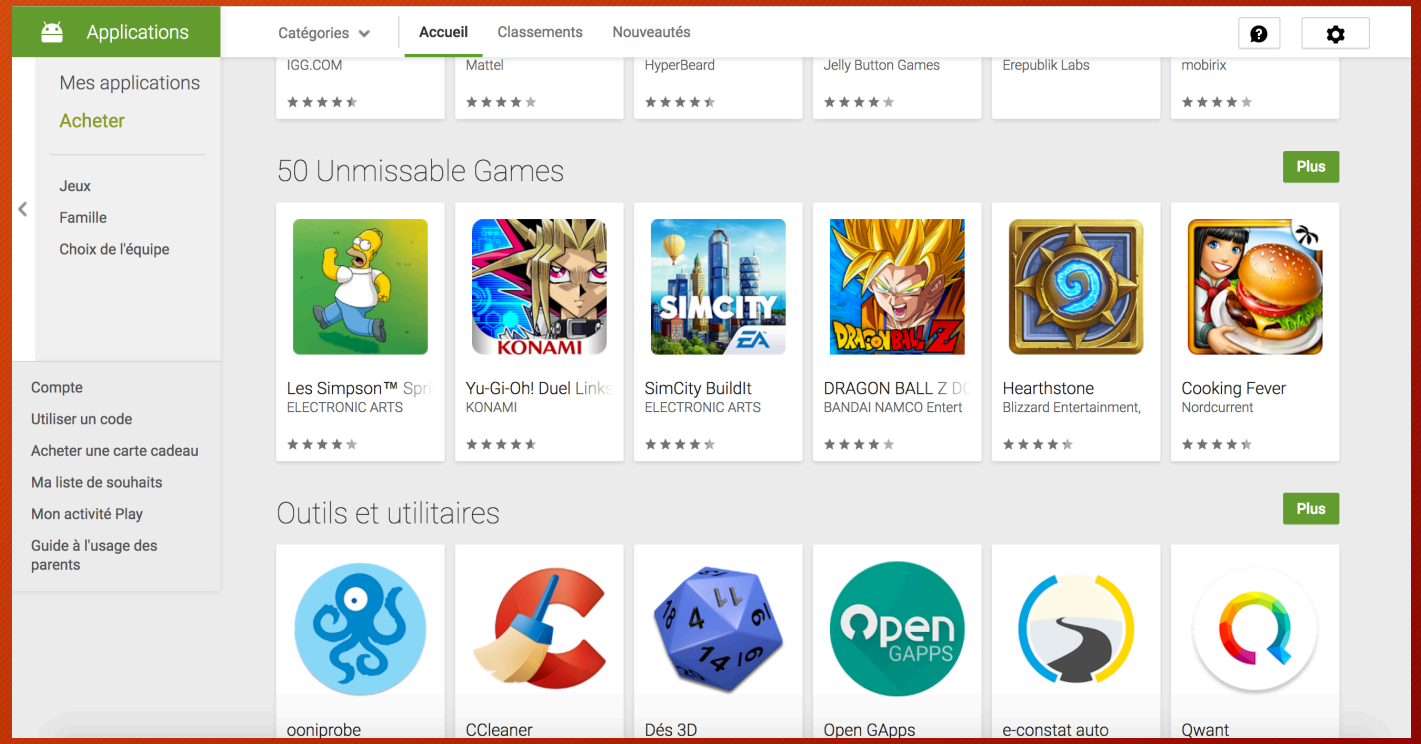
# 2. Key concepts
# Synchronization

- Actions performed one devices will have impact on the other
- Make use of the 2 smoother

- Purposely implements by developers
- Blur the line (Air-gap) between the two

# 2. Key concepts
# Synchronization: Google play store website

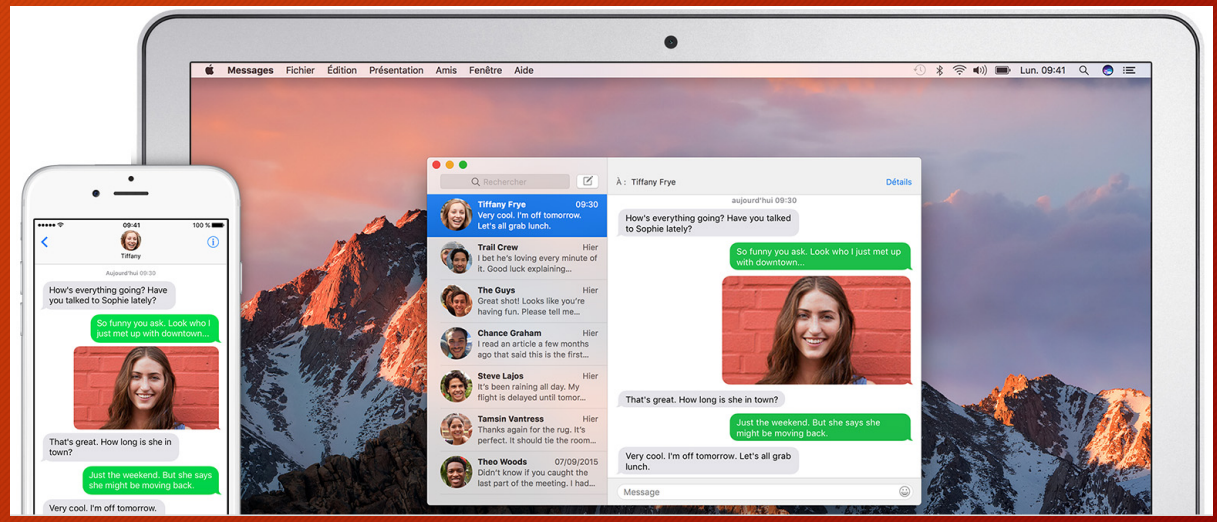
- Possibility to install, from the browser, applications on the phone
- Need to be logged under the same Google account
- Authorization confirmed from the browser too



# 2. Key concepts
# Synchronization: Apple Continuity

- If user posses an IPhone and a Mac, ability to send and read SMS and IMessages from the mac.

- Message stored in clear on the mac
- Off by default
- Need to be on the same LAN



# 2. Key concepts
# Synchronization: Browser Sync

- Synchronization of Bookmarks, history and open tabs between devices
- Available on majority of popular browser
- Sync if logged under the same user account

# 2. Key concepts
# MitB: Man in the browser attack

- Stronger Variant of Man in Middle attack. the attacker can do everything a browser can.
- Like man in the middle:
  - Read and modify all data exchanged
  - Send arbitrary data in the name of the user
- Unlike man in the middle:
  - Read and modify encrypted data before encryption & after decryption
  - Read and modify browser related information: settings, cookies, bookmarks, history.

# 3. 2FA Attacks

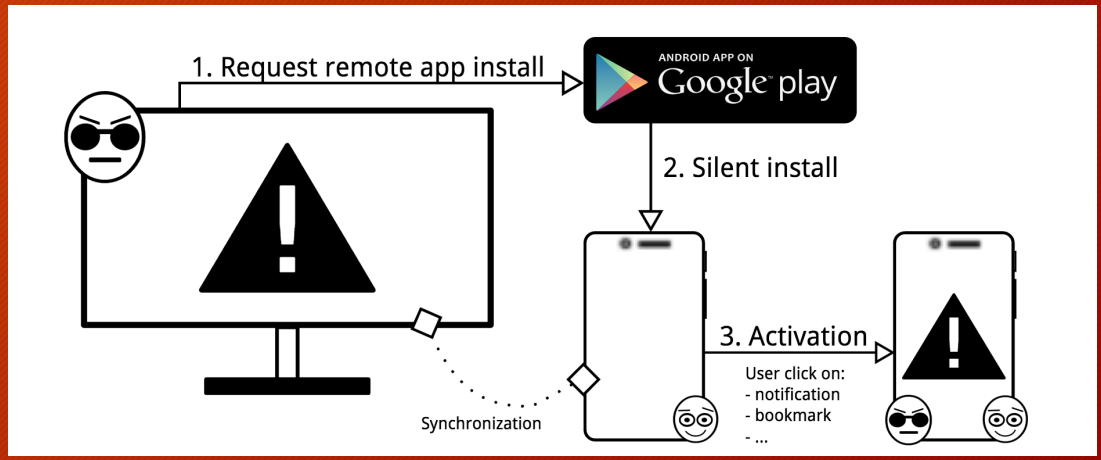
# 3. 2FA Attacks
# The model

- The PC is compromised (physically stolen, Malware, malicious plugin, …)
- MitB attack is performed
- Connection to the service is hijacked (via password or cookie)
- To complete authentication (or transaction) OTP\TAN is send via SMS to victim phone
- Phone is sane and run either on Android or Ios

# 3. 2FA Attacks
# Android

- Form MitB (here Chrome) hijack Google session
- Remotely Install SMS stealing app from playstore
- App will forward OTP and TAN to attacker

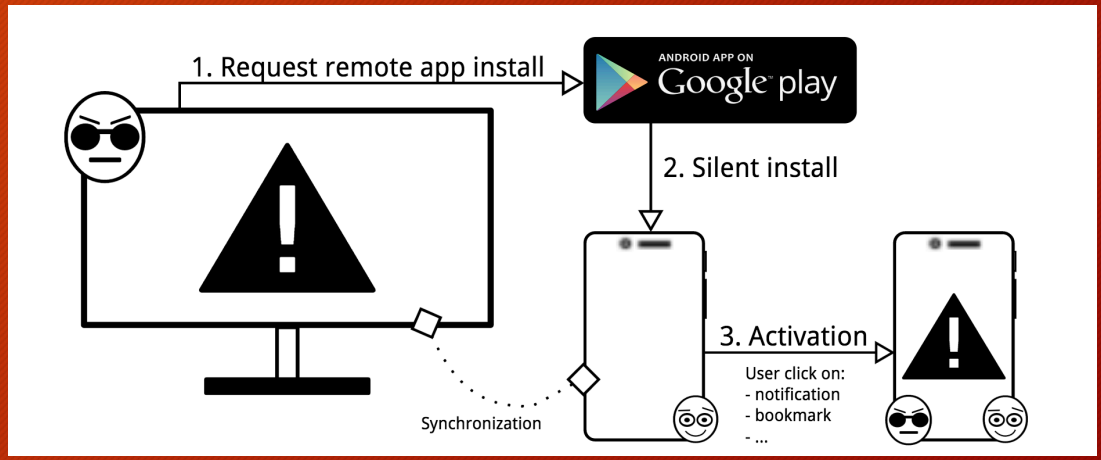
- 2 difficulties:
  - Bypass Google Bouncer
  - Activate the app



# 3. 2FA Attacks
# Android | Google Bouncer

- Automated malware analysis tool deployed on Playstore
- Analyses all uploaded apps
- Static and dynamic analysis

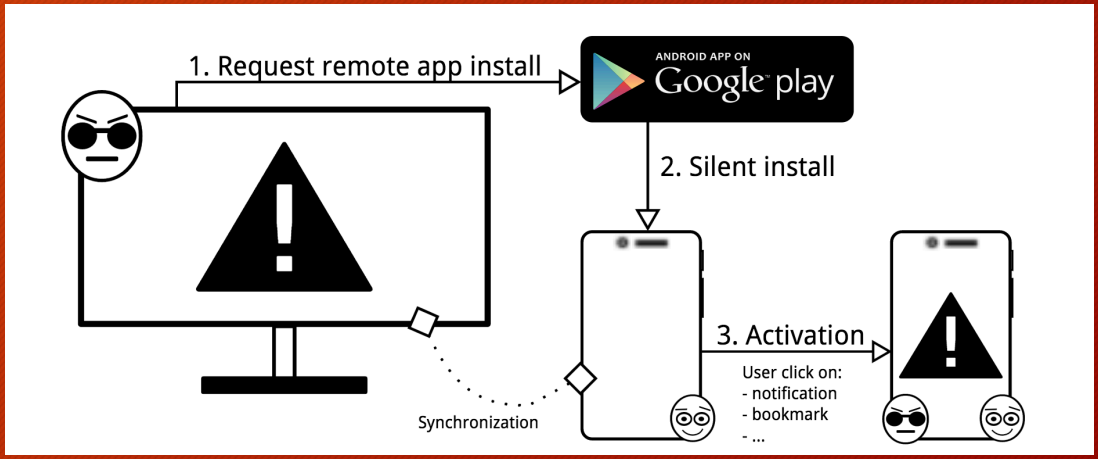
- Recent work show its easy to bypass.
- Exemple: execute malicious code remotly via web-view



# 3. 2FA Attacks
# Android | App activation

- t

- t



# 3. 2FA Attacks
## Ios

# 4. Discussion

# Presentation of 2FA model

# Presentation of 2FA model

# Presentation of 2FA model

# Presentation of 2FA model

# Images sources

- Epfl website: http://camipro.epfl.ch/paiement
- Google Authenticator presentation on playstore : https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2
- Apple website : https://support.apple.com/fr-ch/HT204681
- Personal screenshots