Student Seminar: Exploiting Two Factor Authentication of Android and IOS

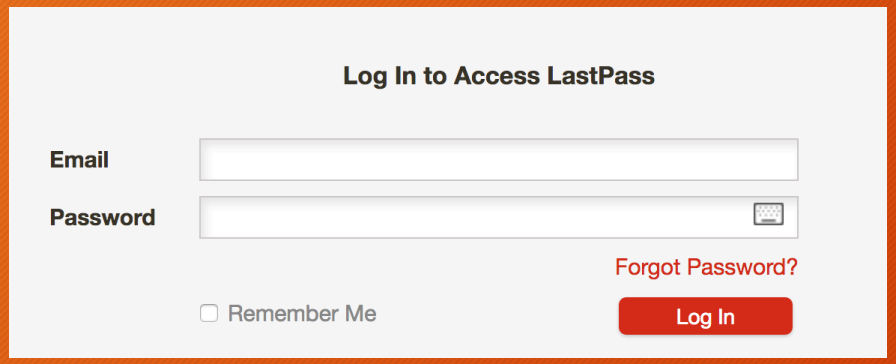
Robin Solignac

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

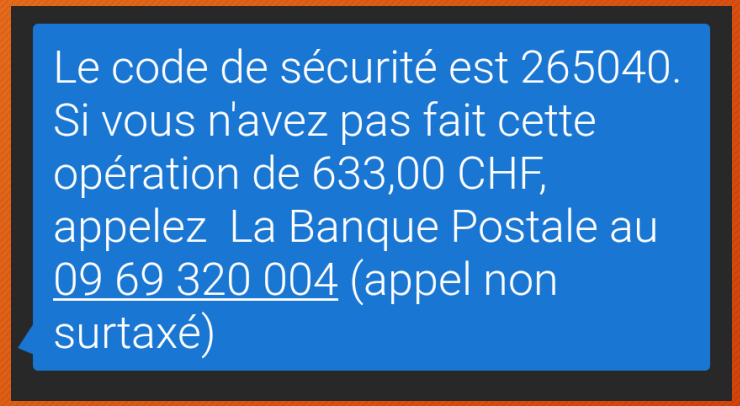
1. Presentation of 2FA model
The choice of smartphones

- 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

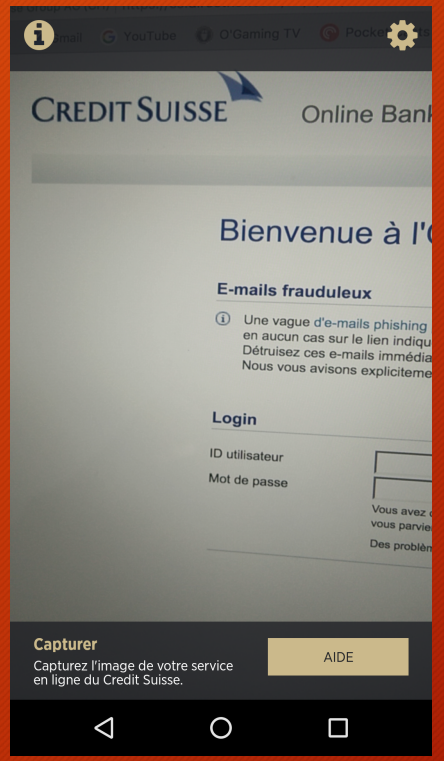
- Implement by Google, Microsoft, Amazon, Twitch, Twitter, Visa, Lastpass, …

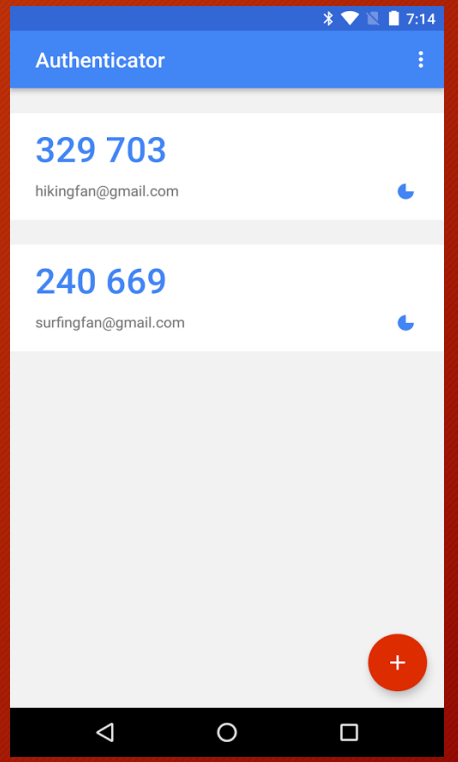
1. Presentation of 2FA model
Smartphone 2FA implementation

- SMS One Time Password (OTP)



- Dedicated application
  - Can rely on OTP or not





1. Presentation of 2FA model
SMS 2FA scheme

- User try to authenticate on PC with password
- If succeeds, service send SMS containing OTP to user's phone
- User enter OTP on PC
- If correct, user successfully authenticate

2. Key concepts

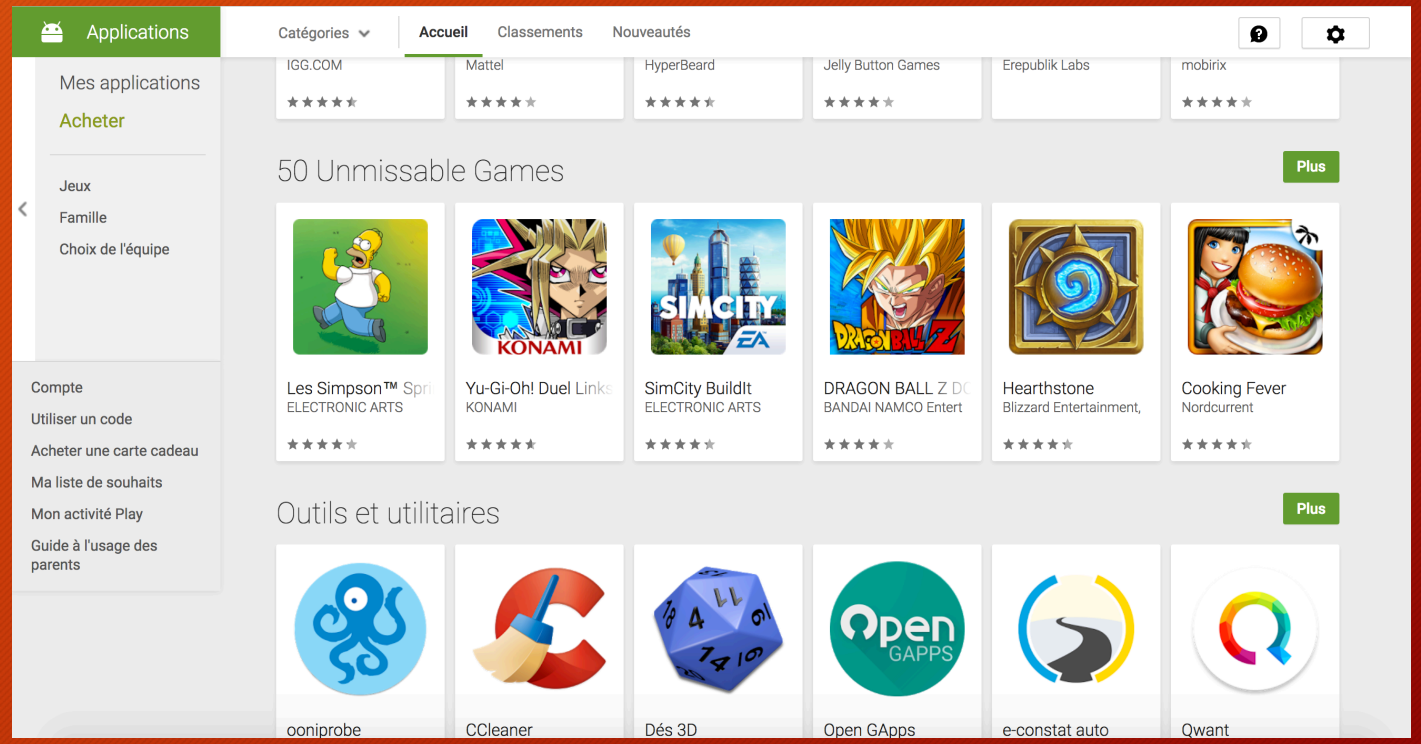
2. Key concepts
Synchronization

- 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

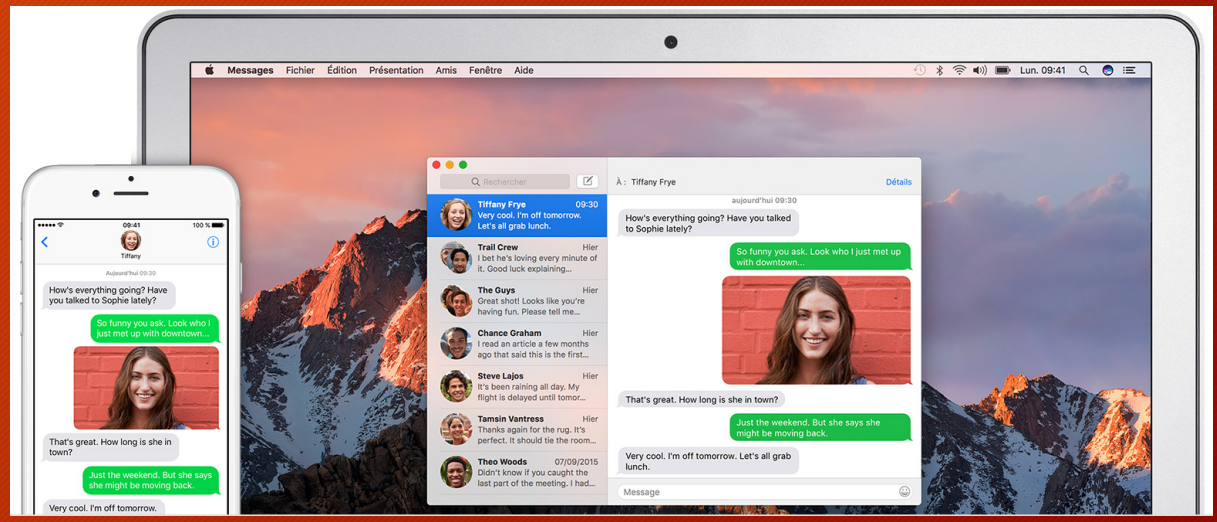
- Possibility to install, from the browser, applications on the phone
- Need to be logged under the same Google account
- Authorization also confirmed from the browser



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

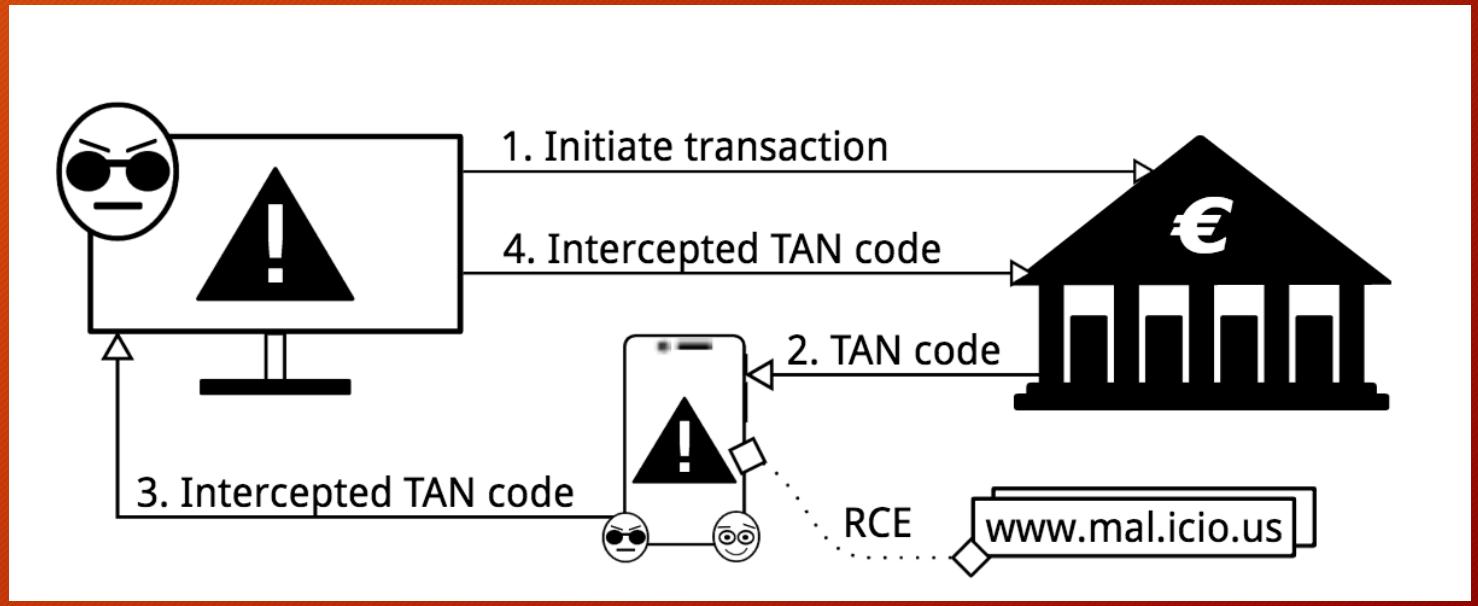
3. 2FA Attacks
The model

- 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
- Goal: steal the SMS

3. 2FA Attacks Android

- Form MitB hijack Google session
- Remotely Install SMS stealing app from playstore
- App will forward OTP or TAN to attacker

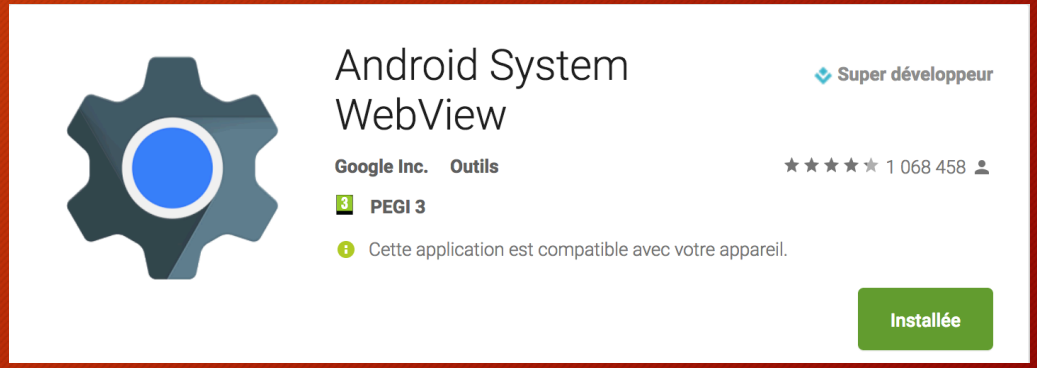
- 2 difficulties:
  - Bypass Google Bouncer
  - Activate the App



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.
- Example: execute malicious code remotely via web-view



3. 2FA Attacks
Android | App activation

- Apps can’t be triggered by an external event (i.e. SMS) until being opened for the 1st time
- Need to trick user into opening it

- Solution 1: clickbait title
  - Make user want to click on the notification

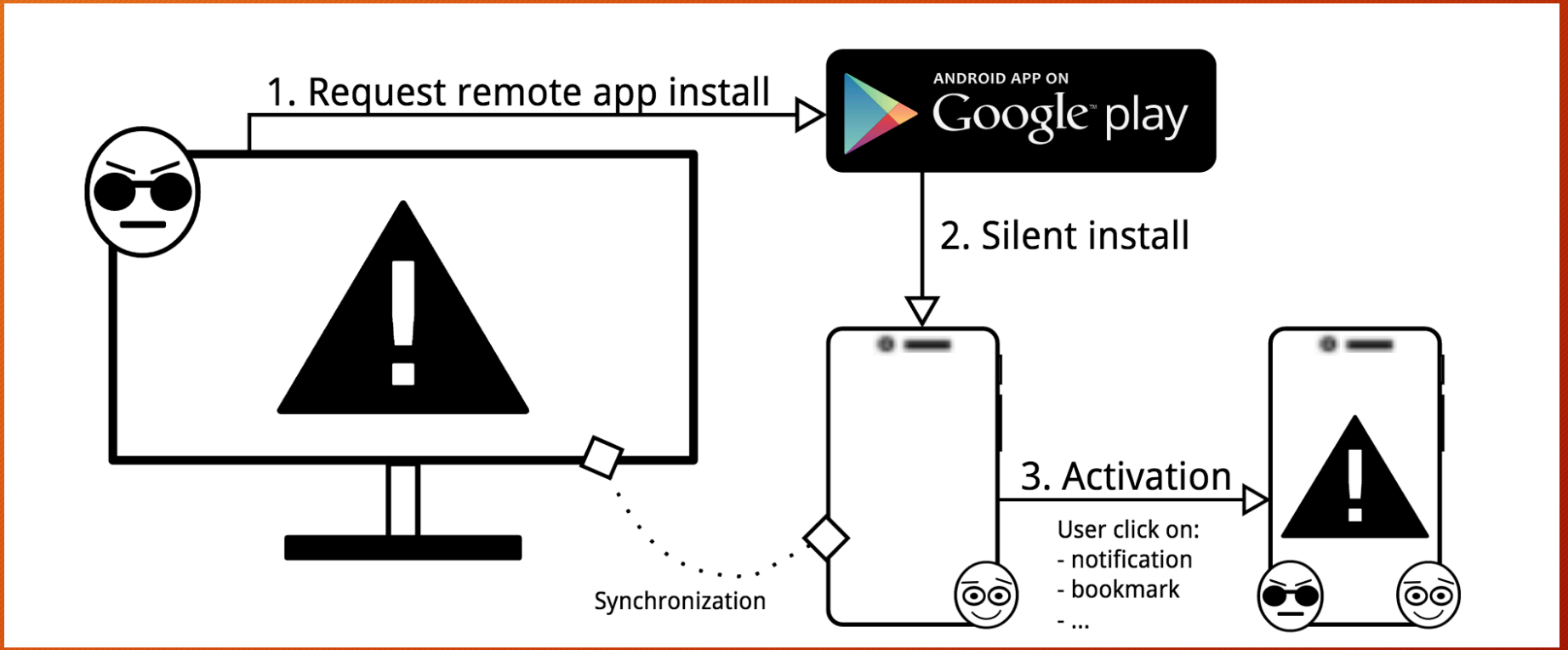
3. 2FA Attacks
Android | App activation

- Solution 2: Browser redirection activation
  - Webpages can trigger opening of apps (i.e. Twitter)
  - Modify all history, bookmarks and tabs to links who will trigger the app
  - This is consider as a valid first opening
  - Malicious app can then redirect to the original link

- After activation:
  - rewrite all links back to normal
  - Hide the app

http:\\mal.icio.us\proxy.php?url=<original_url>

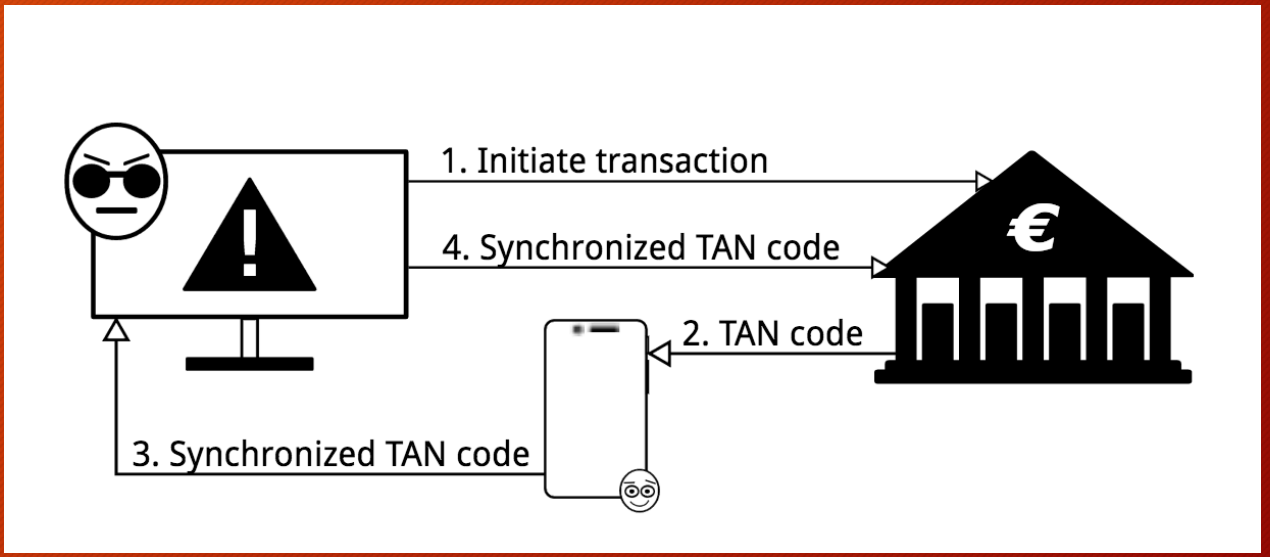
3. 2FA Attacks
Android | Setup Summary



3. 2FA Attacks iOS

- Since 2015 App can’t read SMS and notification

- But if Continuity is activated:
  - All SMS are automatically send to the mac
  - Readable in clear by the browser



4. Discussion

Particularity, feasibility and solutions

4. Discussion
An attack on assumption

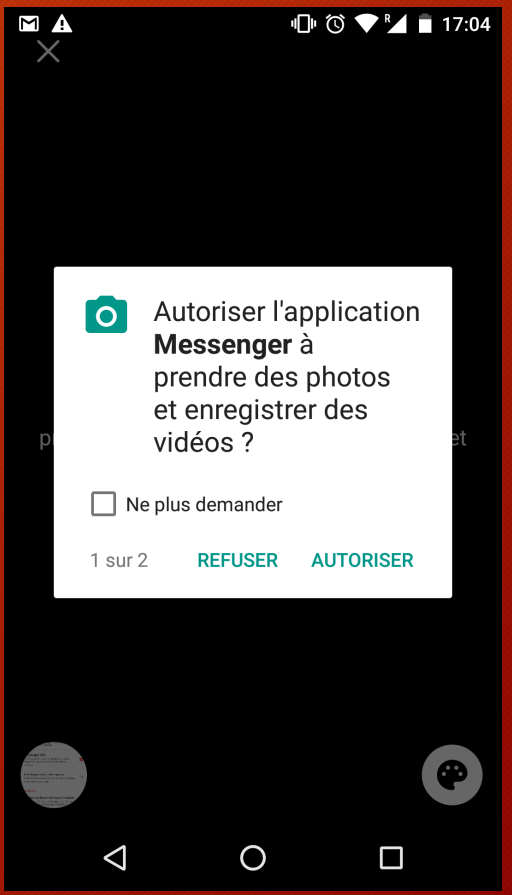
- After initial MitB infection, No use of bug or exploit, Only features offered by Google and Apple
- Hearth of the problem:
  - Sync features reduce the air-gap
  - 2FA assume the Air-Gap exist while designing the scheme
  - Result: System unsecure by flawed assumption
- Hard to fix:
  - Either Modify (reduce) offered sync features
  - Or find New model on new set of assumption

4. Discussion
Android | Feasibility

- Highly feasible:
  - Google account extremely likely to exist & used on both devices
  - Google chrome very likely to be used on smartphone
  - Result: attack very likely to be possible & successful

4. Discussion
Android | Solutions

- Already exist:
  - New authorization scheme since Marshmallow (October 2015)
  - Authorization confirmed at runtime by clicking on smartphone screen
  - Impossible to authorize remotely or from webpages
- Problem:
  - App compiled for older version still used old scheme
  - Can be done purposely will still running on newer version
  - Likely to be not be possible in the future.
- So attack still valid today but not in the (near ?) future



4. Discussion
iOS | Feasibility

- Need more prerequisite than android attack
  - Need to be a Mac
  - Off by default
  - Need to be on the same LAN
- But If the first condition is fulfil, two others are very likely.

- Reduce scalability more than feasibility

4. Discussion
iOS | Solution

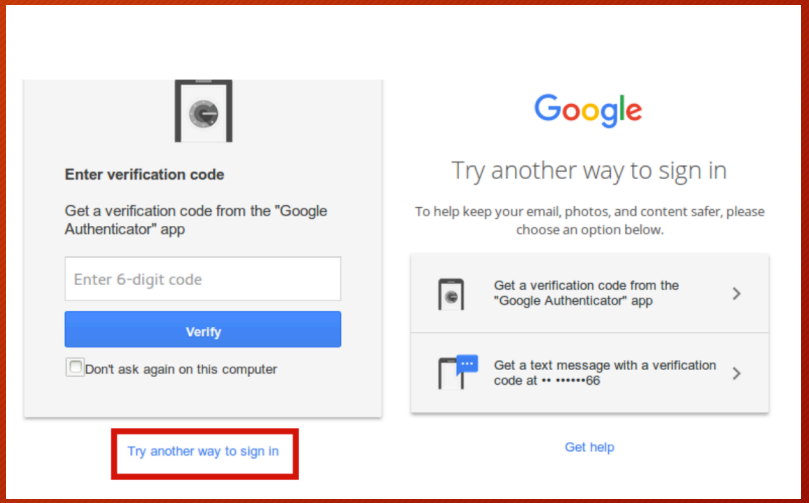
- On Apple side: Sync only messages from number in contact list

- Relative small impact on user experience
- Seems to defeat the attack

4. Discussion
Other 2FA on smartphone

- Most of services also propose dedicated app for 2FA
- Sandboxing: App can’t access each other data
- Theoretically defeat attacks

- Problem: Most of services also propose SMS 2FA as backup solution
- So attacks still work by asking to use backup solution



5. Conclusion

5. Conclusion

- Souls of 2FA on smartphones: Air gap between smartphone and PC
- Not true anymore for all channels used by smartphone
- 2FA implementation must choose wisely: Must be sure use channel is really out of band
- SMS doesn’t seems to be anymore on iOS and Android

Images used

- 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
- Konoth et al. paper : http://fc16.ifca.ai/preproceedings/24_Konoth.pdf
- Personal screenshots