REVERSE ENGINEERING

Instrumenting the native layer of mobile apps

Giovanni (iGio90) Rocca
Vincenzo (rEDSAMK) Greco

ABOUT US

And everything following is our own opinion,
our methodologies,
our skills,
our passion
which is not related to what we do to in our company

- 7 years of cooking school. Not graduated.
- No technical backgrounds, didn't had the chance to attempt any trainings.

Growth with

- Open sourcing knowledge
- Passion
- Patience
- Google
- Community projects

Open sourcing

- Documentations
- Tutorials
- PDF
- Videos
- Keynotes

HackInBo® Spring 2018 Edition 10ª EDIZIONE

My Journey

2016

* First MITM and approach to reverse engineering

* Maintainer - together with other guys - of the java API implementation for Pokémon Go (https://github.com/Grover-c13/PokeGOAPI-Java)

* Creator of **PokéMesh**

My Journey

2017–18

Break any attempt to protect **Supercell** games from a 3rd party client re-implementation

- Encryption logic
- Protocol structure
- Frida detection
- Arxan
    - CRC / Anti-Tamper jump (Thanks frida <3)
    - Single byte change on obfuscated blocks (Thanks unicorn / GDB <3)
    - Strings encryption logic

:[*fun, challenge*] => [*improvements, sharing knowledge*]

My Journey

2017–18

Bandai NAMCO - **Dragon Ball Z Dokkan Battle**

Tencent - **Arena of Valor**

Tencent - **PUBG Mobile**

Netmarble - **Lineage2**

Ludia - **Jurassic World Alive**

- Encryption logic
- Protocol structure
- Protections
- Whatever

:[*fun, challenge*]

Reverse Engineering

WHAT'S YOUR GOAL?

HiB?

- We can't speak about what we love to do with our girlfriends / parents
- Someone believes we do cool stuffs
- We play fair
- It's about dedication
- Spreading open sourcing and sharing knowledge
- Get in touch with awesome people that give us hints and suggestions

Environment

- **A decompiler** (IDA, Hopper, Binary Ninja, Radare...)
- **Dynamic instrumentation**
  Frida (https://www.frida.re)
- **Debugging**
  GDB (https://developer.android.com/ndk/downloads/index.html)
  Gef (https://github.com/hugsy/gef)
- **Emulation**
  Unicorn (https://github.com/unicorn-engine/unicorn)
  uDdbg (https://github.com/iGio90/uDdbg)

- **OnePlus 5T - Android 8 (Rooted)**
  Frida
  GDB
- **Lenovo P2 - Android 7 (Rooted)**
  Frida
  GDB
- **iPhone 6s - iOS11 (Jailbroken)**
  Frida
  LLDB

…Environment

- Coffee
- A bunker somewhere in the desert, shipped with strong silent weapons that will burn any bees flying around

Stickers on the wall:

- Random DOES NOT exists
- Use always the fastest way... ALWAYS... (don't waste time)

To complete the env...

...on Android

1) Download the APK of the target
2) Unzip to access the content

- APK files can be eventually grabbed from /data/app/target_package_name/

Additional resources

* **apktool** := to extract resources
https://ibotpeaches.github.io/Apktool/

* **dex2jar** := to convert the APK into a jar := plain java sources
https://github.com/pxb1988/dex2jar

To complete the env...

...on iOS

1) Dump the decrypted IPA

https://github.com/AloneMonkey/frida-ios-dump

2) Unzip to access the content

Logical approach

1) Understanding the source of network requests and data serialization
* hooking low level functions
* backtracing

2) Are you trying to prevent instrumentation?

3) Build a proxy server

4) Understanding encryptions / hash logic

5) Understanding the structure of the protocol buffers (from raw bytes)
* through static analysis or by reverse engineering

6) Build your client

7) Make your life easier for the next session (improve)

8) Repeat

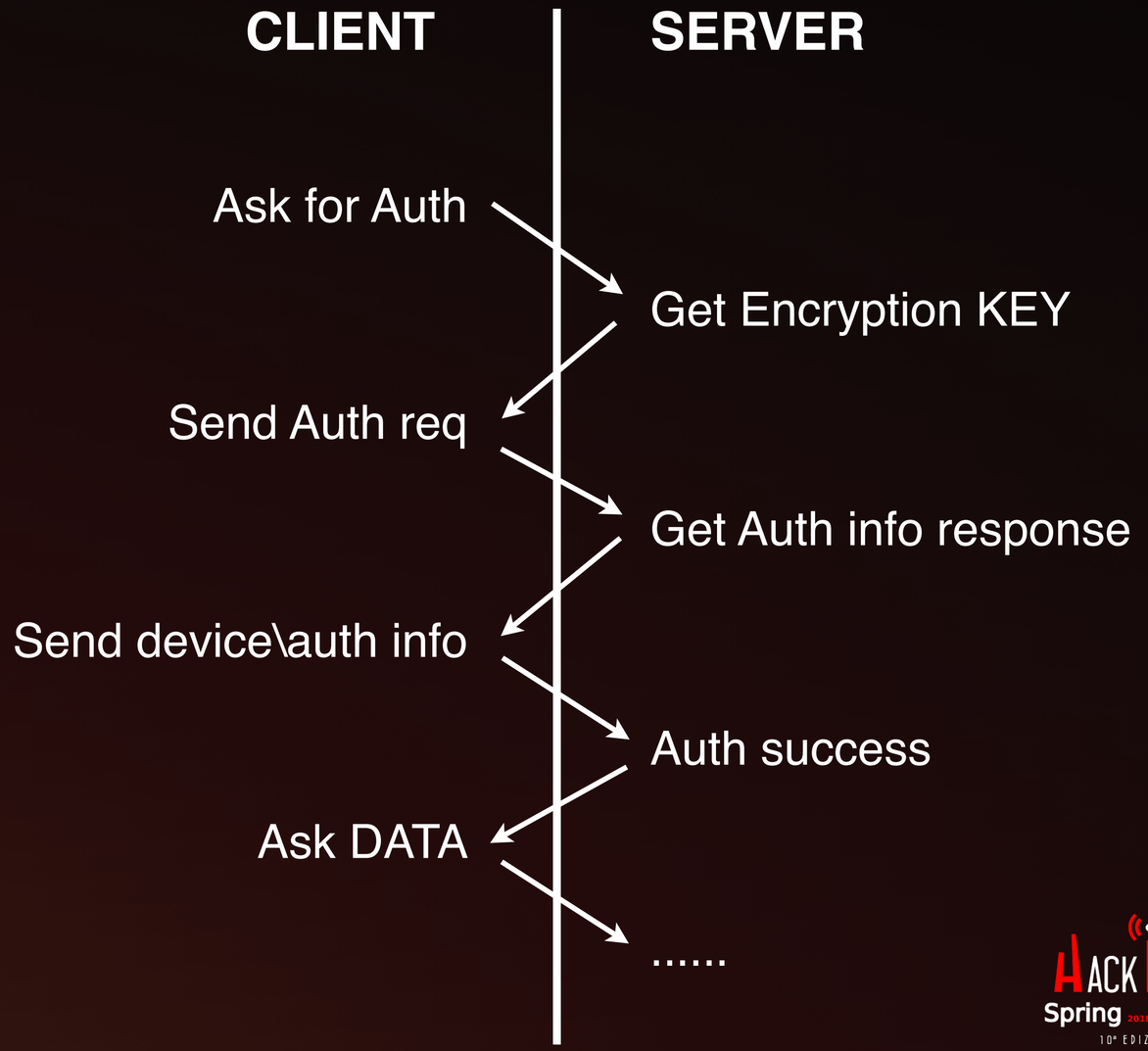
Table of content

- Reading network requests
- Bypassing protections
- Tips & Tricks
- Build an own implementation of general purpose functions
- Navigating through obfuscation
- Data serialization
- Creating phisical cracks using the same approach

DEMO

Communication example


```
▼ object {2}
  ▼ headers {9}
      magic : 13158
      head_version : 8
      body_version : 8
      command : 16403
      is_response : ☐ false
      sequence : 112
      head_len : 22
      body_len : 32
      compressed : ☐ false
  ▼ body_decoded {2}
    ▼ data_head {4}
        command_id : 1302
        magic : 1323
        rsp_seq : 341
        req_seq : 35
      data_body : 005ad7482b0000000000747366346706
```

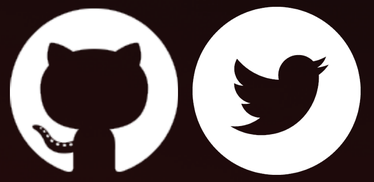



HACK IN BO Spring 2018 Edition 10ª EDIZIONE

THANKS!

Get in touch!


/iGio90


/rEDSAMK


SecRet - https://discord.gg/hTVhy3V

Giovanni (iGio90) Rocca
Vincenzo (rEDSAMK) Greco

OVERWOLF

SecRet

HACK IN BO®
Spring 2018 Edition
10ª EDIZIONE