Mobile App Security - Overview

Author: Nghia Van Le - Sun* Cyber Security Research

Table of Content

1. Mindset: chmod 777 myApp

The developers are directly responsible for the application's security:

- No objective reasons:
  - Requires physical influence on the device:
    + Users lost their devices
    + The devices without password protection
    + ...

- Operating System protection:
  - iOS: Jailbreak devices
  - Android: Rooted devices

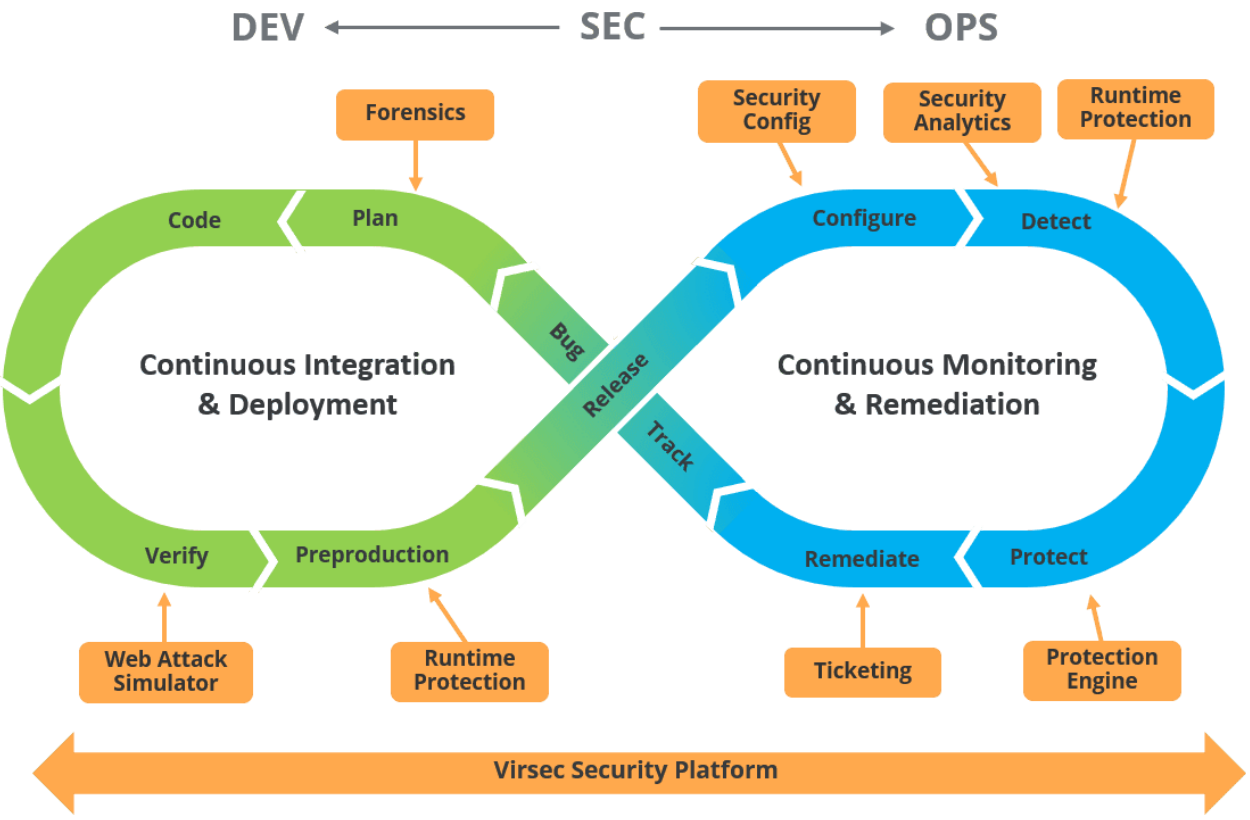
- Only subjective reason:
  - Is your code secure?

2. Requires

2.1 Secure SDLC & DevSecOps

- “Security wasn't originally an integral part of software development. It was an afterthought, performed at the network level by operation teams who had to compensate for poor software security!”

- “Nowadays, security must be baked inside software because compensating for vulnerabilities is often very difficult.”



2.2 Architecture, Design and Threat Modeling Requirements

- Architectural Information:
    - All app components are identified and known to be needed
    - All app components are defined with its function
    - All connected remote services has been defined and security has been addressed in a high-level architecture

- Security is addressed within all parts of the software development lifecycle

- Identifying Sensitive Data: Data in apps, personal data, card/payment information...

- Identifies potential threats and countermeasures

- All security controls have a centralized implementation (Principles of testing)

- Security controls are enforced on both the client side and remote endpoints (Injection Flaws)

- An explicit policy for how cryptographic keys (if any) are managed, and the lifecycle of cryptographic keys is enforced

- A mechanism for enforcing updates of the mobile app exists

- A responsible disclosure policy is in place and effectively applied

- The app should comply with privacy laws and regulations

3. Key Areas in Mobile Application Security

3.1 Local Data Storage

- What
    - What can I store?
    - What should I store?
    - and What am I allowed to store?

- How
    - No unintentionally leaked data: log files, cloud storage, backups, or the keyboard cache...
    - All sensitive data stored must be encrypted
    - No sensitive data is shared with third parties unless it is a necessary part of the architecture

- No store encryption key locally
- No store credentials/sensitive data outside sandbox
- ...

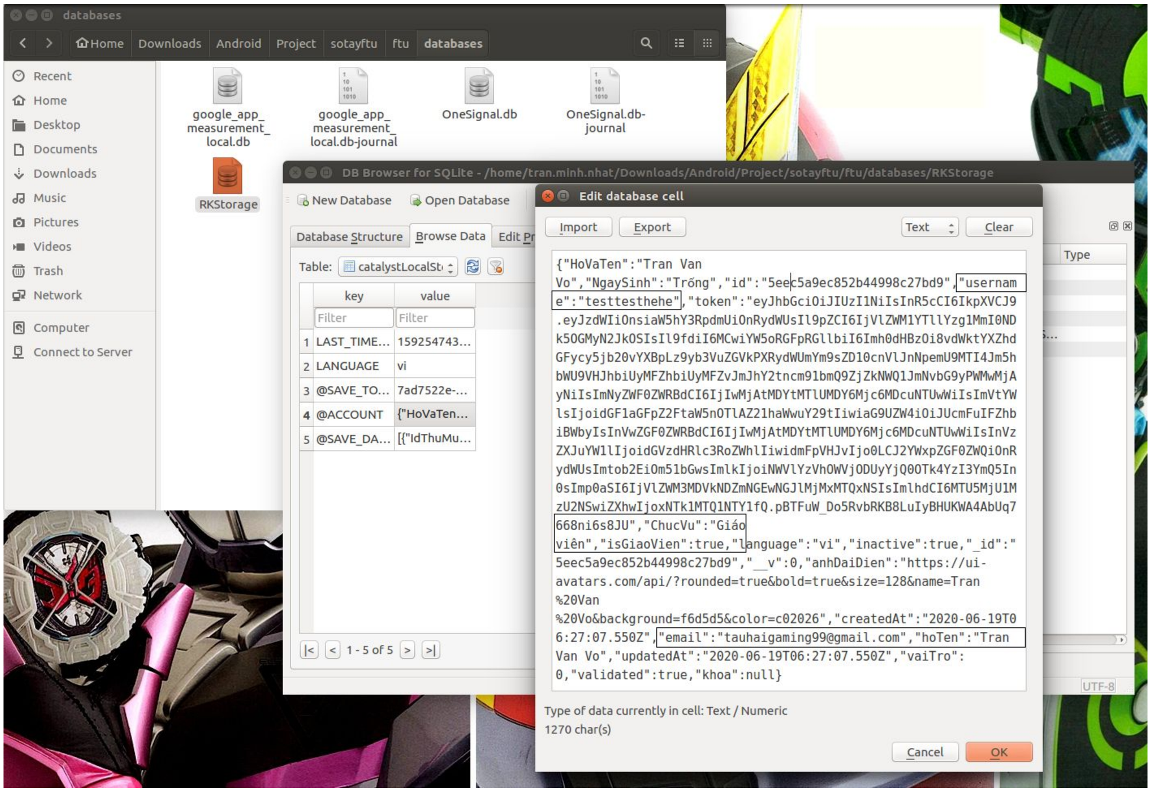


Table: catalystLocalSt

	key	value
1	LAST_TIME...	159254743...
2	LANGUAGE	vi
3	@SAVE_TO...	7ad7522e-...
4	@ACCOUNT	{"HoVaTen...
5	@SAVE_DA...	[{"IdThuMu...

```
{"HoVaTen":"Tran Van
Vo","NgaySinh":"Trống","id":"5eec5a9ec852b44998c27bd9","usernam
e":"testtesthehe","token":"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9
.eyJzdWIiOnsiaW5hY3RpdmUiOnRydWUsIl9pZCI6IjVlZWM1YTllYzg1MmI0ND
k5OGMyN2JkOSIsIl9fdiI6MCwiYW5oRGFpRGllbiI6Imh0dHBzOi8vdWktYXZhd
GFycy5jb20vYXBpLz9yb3VuZGVkPXRydWUmYm9sZD10cnVlJnNpemU9MTI4Jm5h
bWU9VHJhbiUyMFZhbiUyMFZvJmJhY2tncm91bmQ9ZjZkNWQ1JmNvbG9yPWMwMjA
yNiIsImNyZWF0ZWRBdCI6IjIwMjAtMDYtMTlUMDY6Mjc6MDcuNTUwWiIsImVtYW
lsIjoidGF1aGFpZ2FtaW5nOTlAZ21haWwuY29tIiwiaG9UZW4iOiJUcmFuIFZhb
iBWbyIsInVwZGF0ZWRBdCI6IjIwMjAtMDYtMTlUMDY6Mjc6MDcuNTUwWiIsInVz
ZXJuYW1lIjoidGVzdHRlc3RoZWhlIiwidmFpVHJvIjo0LCJ2YWxpZGF0ZWQiOnR
ydWUsImtob2EiOm51bGwsImlkIjoiNWVlYzVhOWVjODUyYjQ0OTk4YzI3YmQ5In
0sImp0aSI6IjVlZWM3MDVkNDZmNGEwNGJlMjMxMTQxNSIsImlhdCI6MTU5MjU1M
zU2NSwiZXhwIjoxNTk1MTQ1NTY1fQ.pBTFuW_Do5RvbRKB8LuIyBHUKWA4AbUq7
668ni6s8JU","ChucVu":"Giáo
viên","isGiaoVien":true,"language":"vi","inactive":true,"_id":"
5eec5a9ec852b44998c27bd9","__v":0,"anhDaiDien":"https://ui-
avatars.com/api/?rounded=true&bold=true&size=128&name=Tran
%20Van
%20Vo&background=f6d5d5&color=c02026","createdAt":"2020-06-19T0
6:27:07.550Z","email":"tauhaigaming99@gmail.com","hoTen":"Tran
Van Vo","updatedAt":"2020-06-19T06:27:07.550Z","vaiTro":
0,"validated":true,"khoa":null}
```

Type of data currently in cell: Text / Numeric

1270 char(s)

Example 3.1. Store credentials/sensitive data inside sandbox

3.2 Communication with Trusted Endpoints

- Identify trusted endpoints.
- Data is encrypted on the network using TLS & best practices.
- The app either uses its own certificate store, or pins the endpoint certificate or public key
- The app doesn't rely on a single insecure communication channel for critical operations

3.3 Authentication and Authorization

- Authentication: There's no one-size-fits-all approach to authentication
    - Verifying that Appropriate Authentication is in Place
    - Refer to industry best practices
    - Apply best practices for Passwords/Token (create/rotate/expired/timeout…)
    - Step-up authentication is required to enable/perform actions that deal with sensitive data or transactions

- Authorization
    - Know the advantages and disadvantages of different possible authorization frameworks and architectures
    - Authorization models should be defined and enforced at the remote endpoint

3.4 Interaction with the Mobile Platform

- The app only requests the minimum set of permissions necessary.
- All inputs from external sources and the user are validated and if necessary sanitized
- Does not export sensitive functionality via custom URL schemes.
- Prevents usage of custom third-party keyboards whenever sensitive data is entered
- Webview:

- JavaScript should be enabled only if necessary
- Configured to allow only the minimum set of protocol
- A WebView’s cache, storage, and loaded resources (JavaScript, etc.) should be cleared before the WebView is destroyed

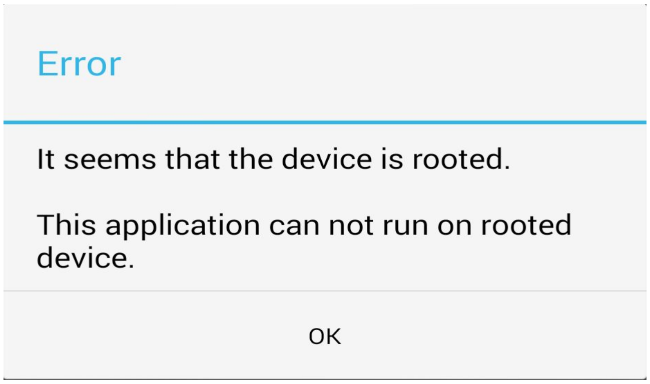
3.5 Code Quality and Exploit Mitigation

The checklist on Android and iOS is a bit different, but will follow the general requirements:

- Making Sure That the App is Properly Signed
- All third party components are identified and checked for known vulnerabilities
- Removing debugging Symbols, debugging code
- The app catches and handles possible exceptions
- Make sure that free security features are activated

3.6 Anti-Tampering and Anti-Reversing

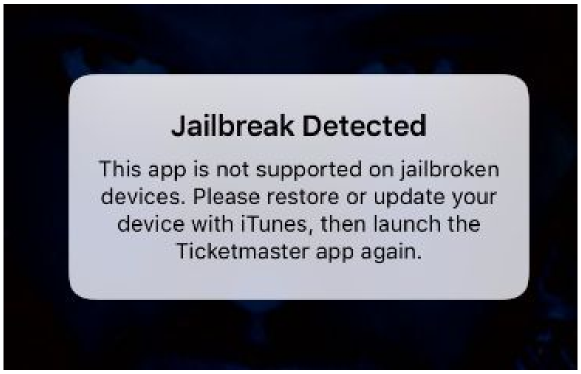
- Implement Root/Jailbreak Detection
- Implement Emulator Detection



Error

It seems that the device is rooted.

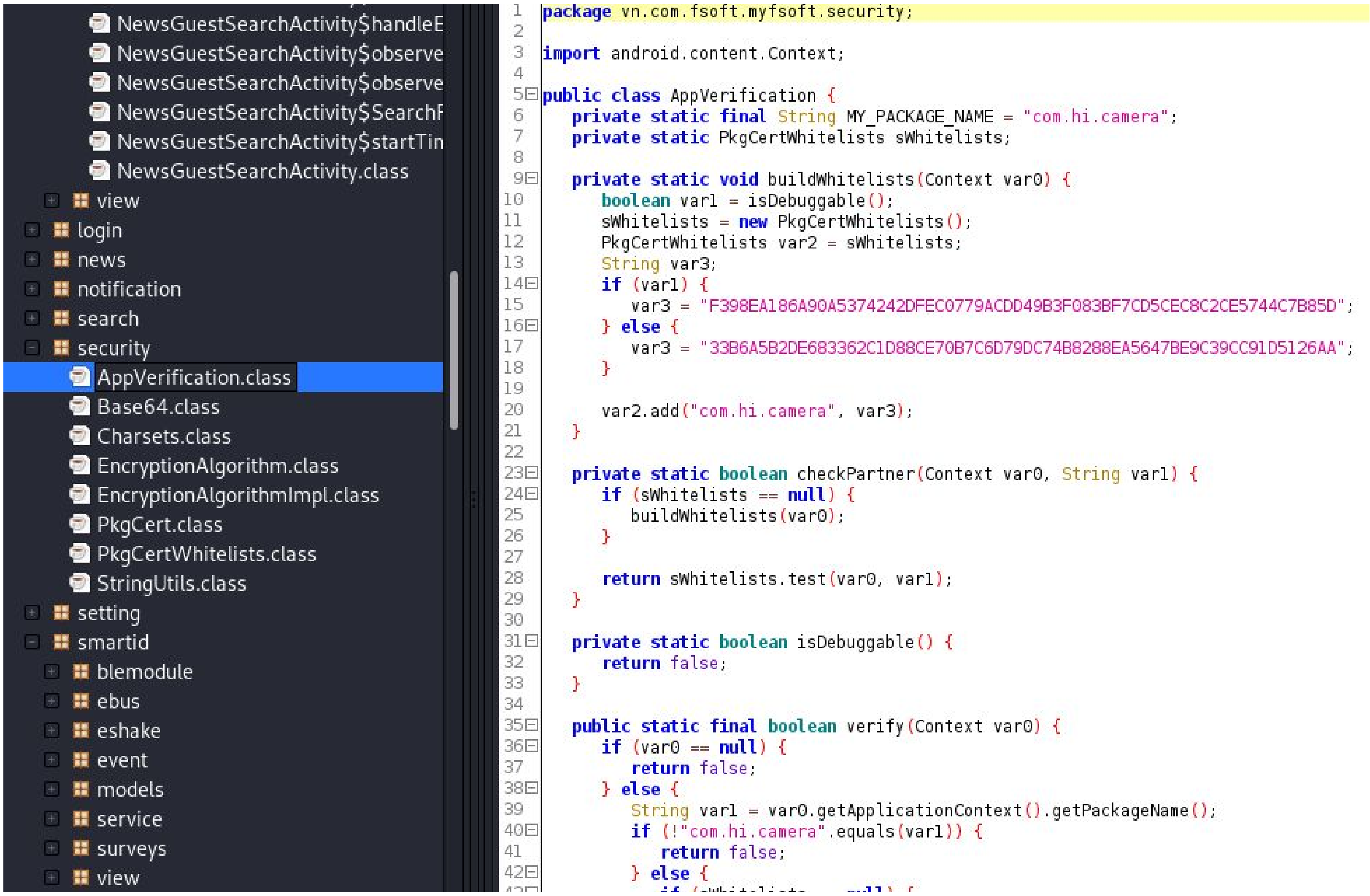
This application can not run on rooted device.



Jailbreak Detected

This app is not supported on jailbroken devices. Please restore or update your device with iTunes, then launch the Ticketmaster app again.

- Code Obfuscation


NewsGuestSearchActivity$handleE
NewsGuestSearchActivity$observe
NewsGuestSearchActivity$observe
NewsGuestSearchActivity$SearchF
NewsGuestSearchActivity$startTin
NewsGuestSearchActivity.class
view
login
news
notification
search
security
AppVerification.class
Base64.class
Charsets.class
EncryptionAlgorithm.class
EncryptionAlgorithmImpl.class
PkgCert.class
PkgCertWhitelists.class
StringUtils.class
setting
smartid
blemodule
ebus
eshake
event
models
service
surveys
view

```
package vn.com.fsoft.myfsoft.security;

import android.content.Context;

public class AppVerification {
   private static final String MY_PACKAGE_NAME = "com.hi.camera";
   private static PkgCertWhitelists sWhitelists;

   private static void buildWhitelists(Context var0) {
      boolean var1 = isDebuggable();
      sWhitelists = new PkgCertWhitelists();
      PkgCertWhitelists var2 = sWhitelists;
      String var3;
      if (var1) {
         var3 = "F398EA186A90A5374242DFEC0779ACDD49B3F083BF7CD5CEC8C2CE5744C7B85D";
      } else {
         var3 = "33B6A5B2DE683362C1D88CE70B7C6D79DC74B8288EA5647BE9C39CC91D5126AA";
      }

      var2.add("com.hi.camera", var3);
   }

   private static boolean checkPartner(Context var0, String var1) {
      if (sWhitelists == null) {
         buildWhitelists(var0);
      }

      return sWhitelists.test(var0, var1);
   }

   private static boolean isDebuggable() {
      return false;
   }

   public static final boolean verify(Context var0) {
      if (var0 == null) {
         return false;
      } else {
         String var1 = var0.getApplicationContext().getPackageName();
         if (!"com.hi.camera".equals(var1)) {
            return false;
         } else {
            if (sWhitelists == null) {
```

Example 3.6. Code Not Obfuscated

- Anti-Debugging Checks
- Application source code integrity checks
- File storage integrity checks
- Device Binding