DEFCON

History of the worst Android app ever: mAadhaar

AppSec Village - Defcon 27 - Sunday August 11, 2019

Elliot Alderson

@fs0c131y

Whoami

- French security researcher
- Focused on mobile apps, especially messaging apps
- Sometimes, I find cool stuff
- The India government hate me

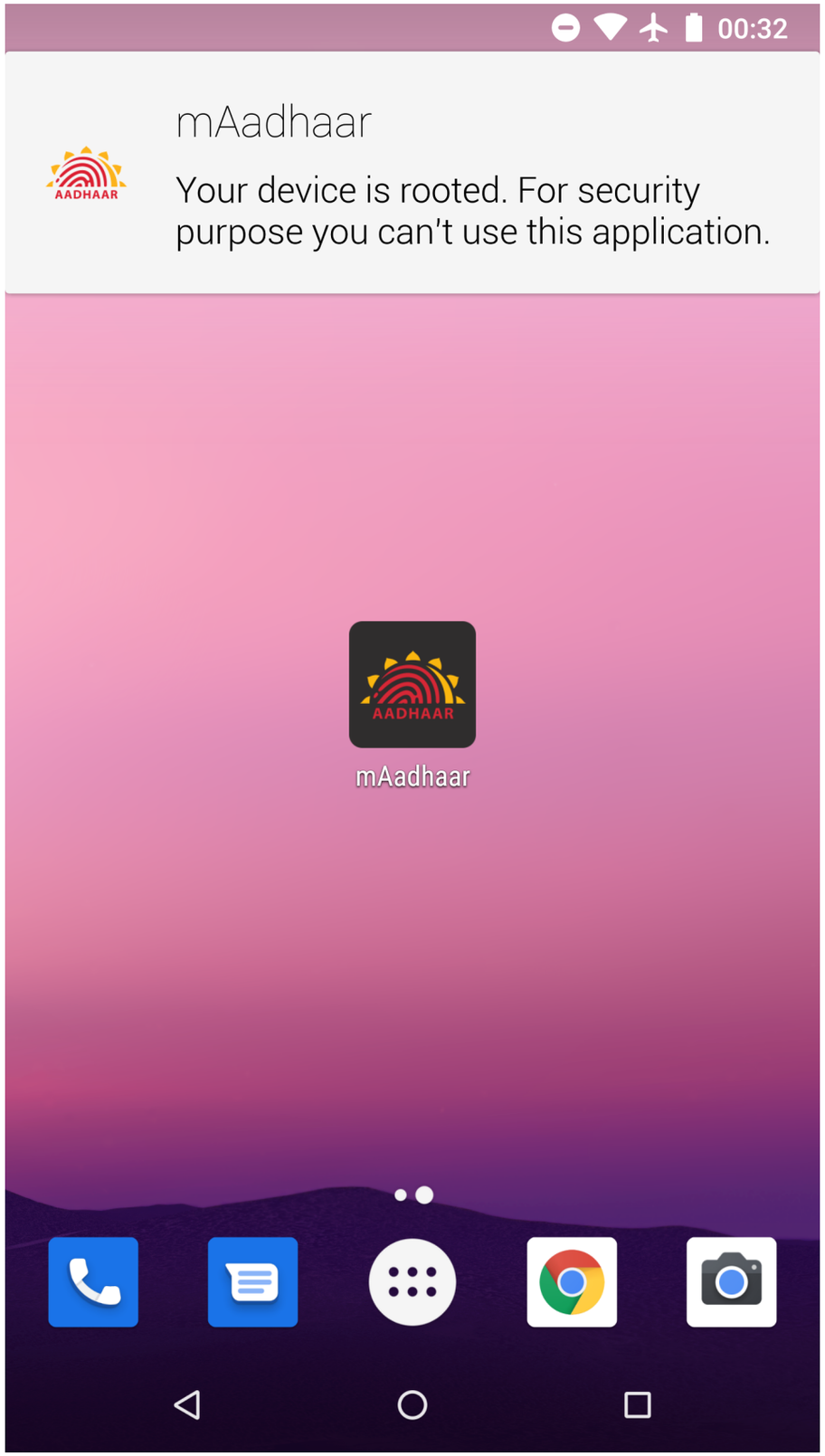
What is Aadhaar?

- Introduced in 2012 by the Indian government
- 12-digit unique identity number based on biometric and demographic data
- Biggest identification program of the world
- Tense subject in India
- Mandatory for many formalities: hospital admission, open a phone line, …

What is mAadhaar?

Elliot Alderson
@fs0c131y

Root Detection



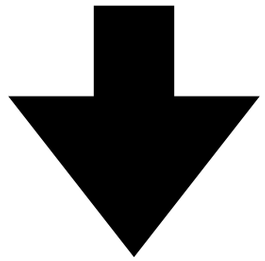
Elliot Alderson
@fs0c131y

SplashScreenActivity.java

```
} else if (new b( context: this).a()) {
    string = "Your device is rooted. For security purpose you can't use this application.";
```

SplashScreenActivity.java

```
} else if (new b( context: this).a()) {
    string = "Your device is rooted. For security purpose you can't use this application.";
```

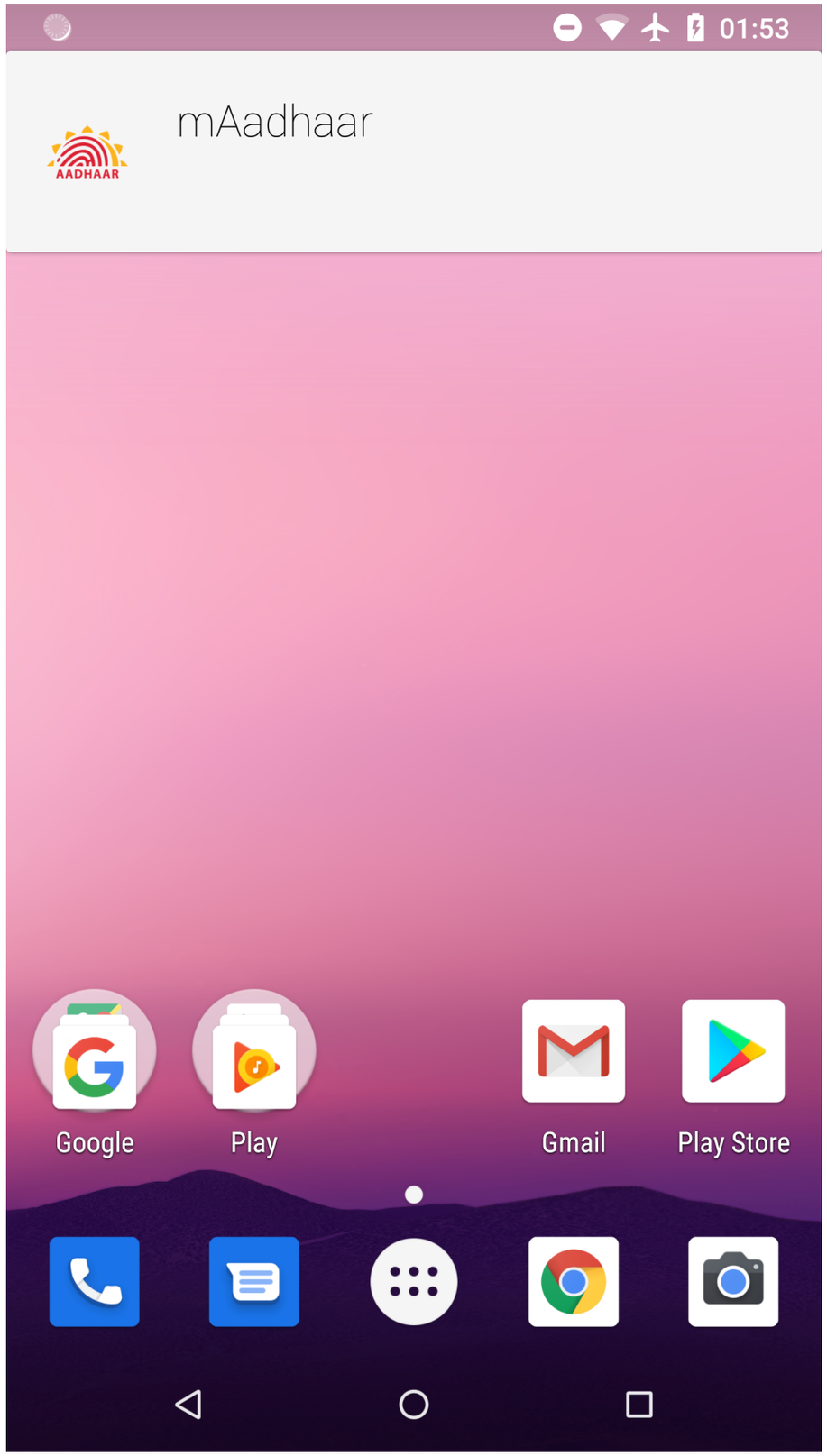


```
package com.scottyab.rootbeer;

import ...

public class b {

    private final Context f1167a;
    private boolean b = true;

    public b(Context context) {
        this.f1167a = context;
    }
```

Frida function to bypass the root detection

```
function bypassRootDetection() {

    // com.scottyab.rootbeer.b.a()
    var b = Java.use('com.scottyab.rootbeer.b');
    b.a.overload().implementation = function () {
        return false;
    }
}
```

Tampering Detection



Elliot Alderson
@fs0c131y

DEFCON

SplashScreenActivity.java

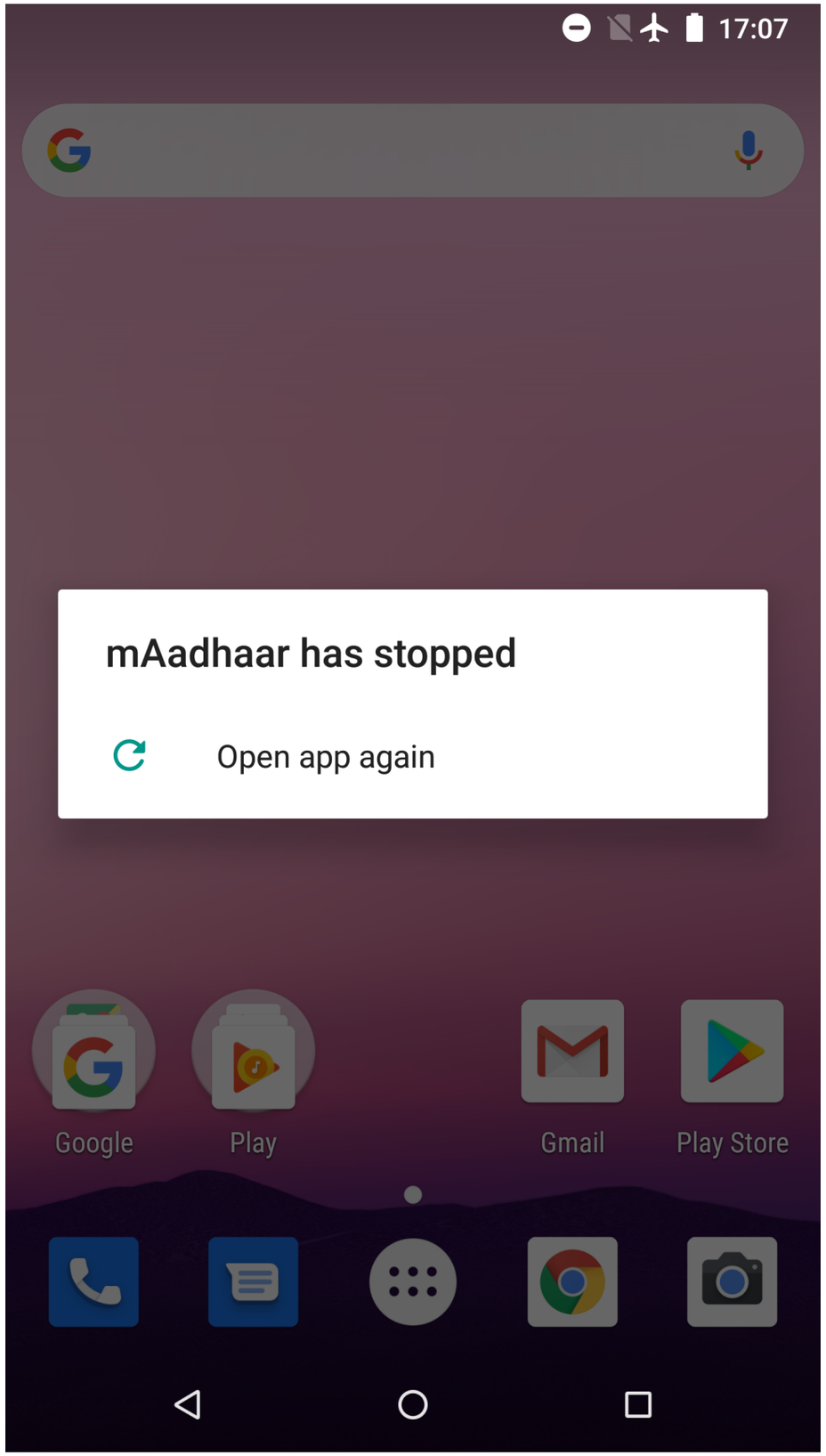
```
if (!(f.checkSignature( context: this) && f.checkPackageName( context: this))) {
    string = "";
```

Elliot Alderson
@fs0c131y

Frida function to bypass the tampering detection

```
function bypassAntiRepackage() {

    // public static boolean b(Context arg4)
    var f = Java.use('in.gov.uidai.mAadhaarPlus.b.f');
    f.a.overload('android.content.Context').implementation = function (context) {
        return true;
    }
    f.b.overload('android.content.Context').implementation = function (context) {
        return true;
    }
}
```

Debug Flag Detection


17:07
mAadhaar has stopped
Open app again
Google
Play
Gmail
Play Store

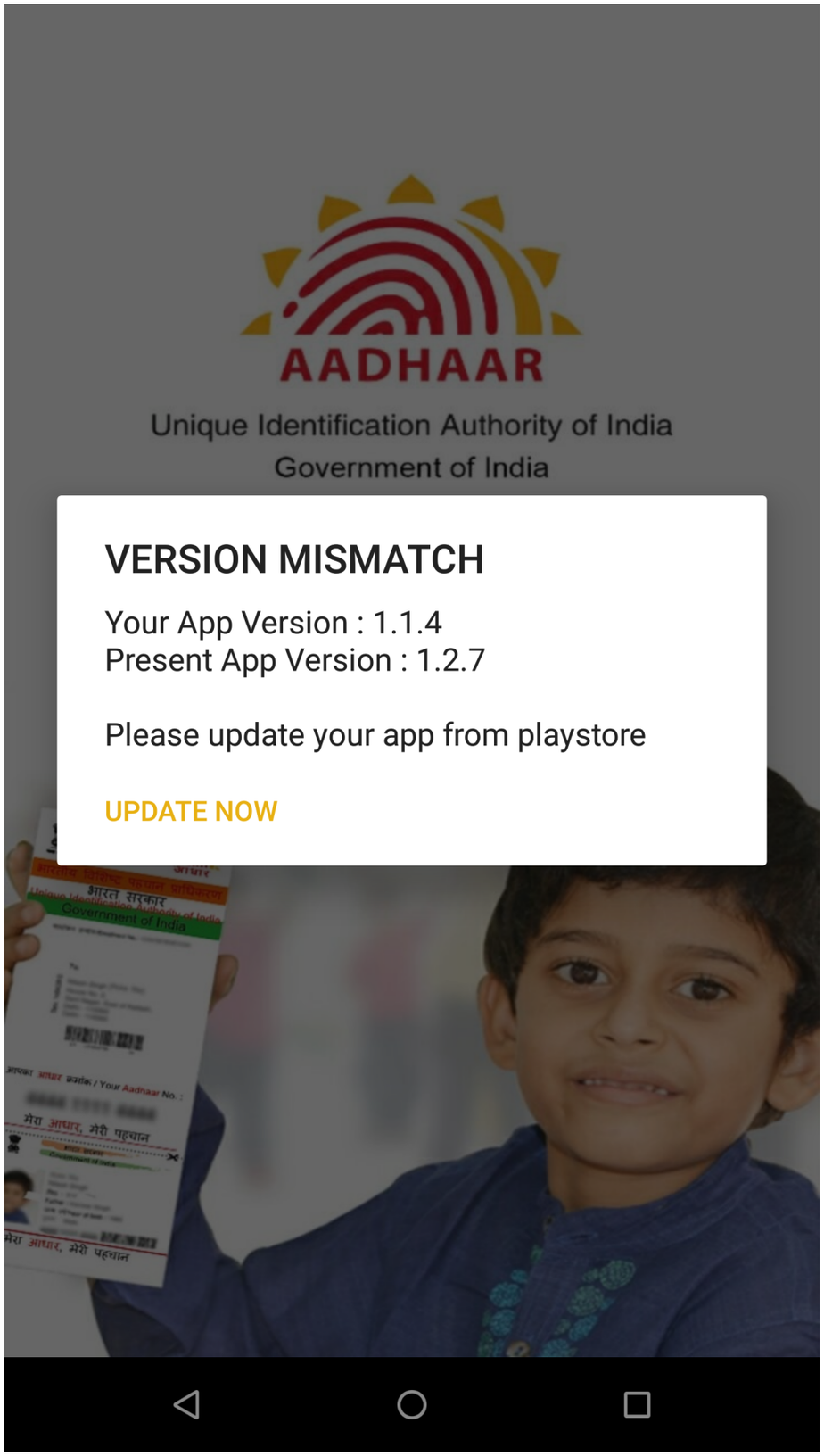
in.gov.uidai.mAadhaarPlus.j.c

```
public static String a(String str) {
    StackTraceElement stackTraceElement = Thread.currentThread().getStackTrace()[4];
    return "[" + stackTraceElement.getFileName().replace( target: ".java",  replacement: "") +
            stackTraceElement.getMethodName() + "::" + "]" + str;
}

public static void a(String str, String str2) {
    if (BaseApplication.b) {
        Log.e(str, a(str2));
    }
}
```

Frida function to bypass the debug flag detection

```
function bypassAntiDebug() {

    // public static String a(String arg5)
    var c = Java.use('in.gov.uidai.mAadhaarPlus.j.c');
    c.a.overload('java.lang.String').implementation = function (arg5) {
        console.log('[+] START antidebug');
        console.log('arg6 = ' + arg5);
        console.log('[+] END antidebug');

        return "OK";
    }

}
```

App Version Check


AADHAAR
Unique Identification Authority of India
Government of India
VERSION MISMATCH
Your App Version : 1.1.4
Present App Version : 1.2.7
Please update your app from playstore
UPDATE NOW

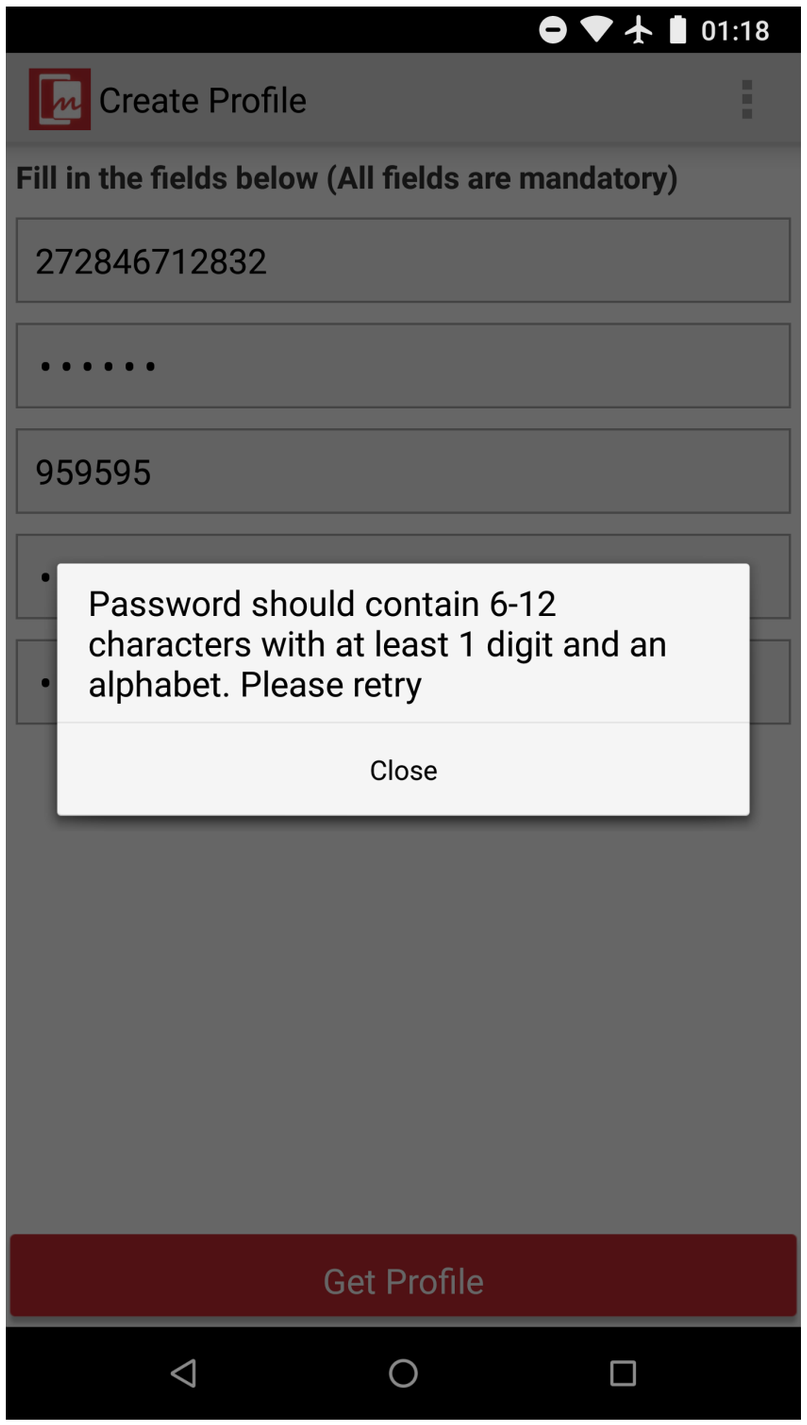
SplashScreenActivity.java

```
} else if (!j.c(str, str2)) {
    android.support.v7.app.c b2 = new android.support.v7.app.c.a(
            new ContextThemeWrapper( base: SplashScreenActivity.this,  themeResId: 2131821049)).b();
    b2.setTitle("VERSION MISMATCH");
    String sb = "Your App Version : " + str2 +
            "\nPresent App Version : " + str +
            "\n\nPlease update your app from playstore  ";
```

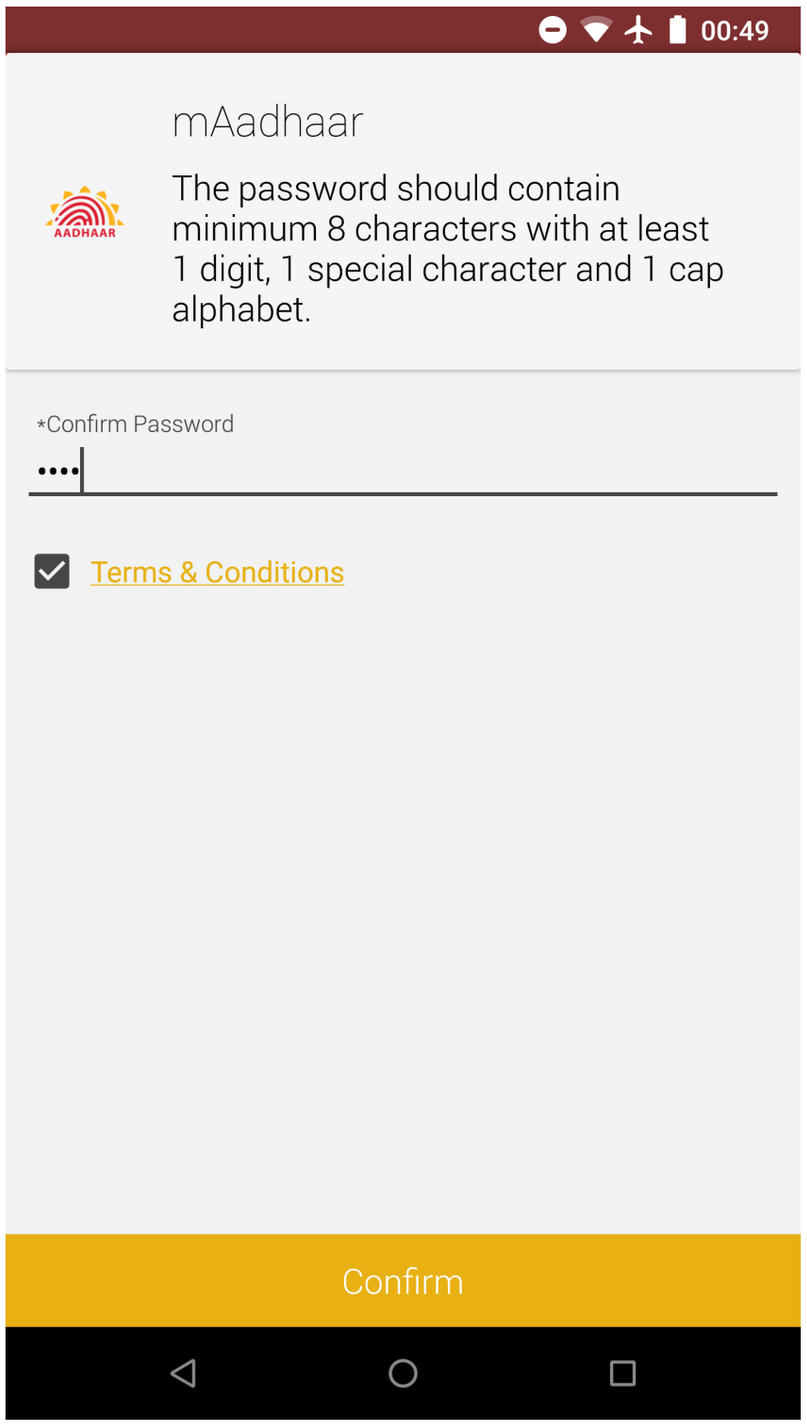
Frida function to bypass the app version check

```
function bypassVersionCheck() {

    // in.gov.uidai.mAadhaarPlus.j.i.c(String arg8, String arg9)
    var i = Java.use('in.gov.uidai.mAadhaarPlus.j.i');
    i.c.overload('java.lang.String', 'java.lang.String').implementation = function (arg8, arg9) {
        return true;
    }

}
```

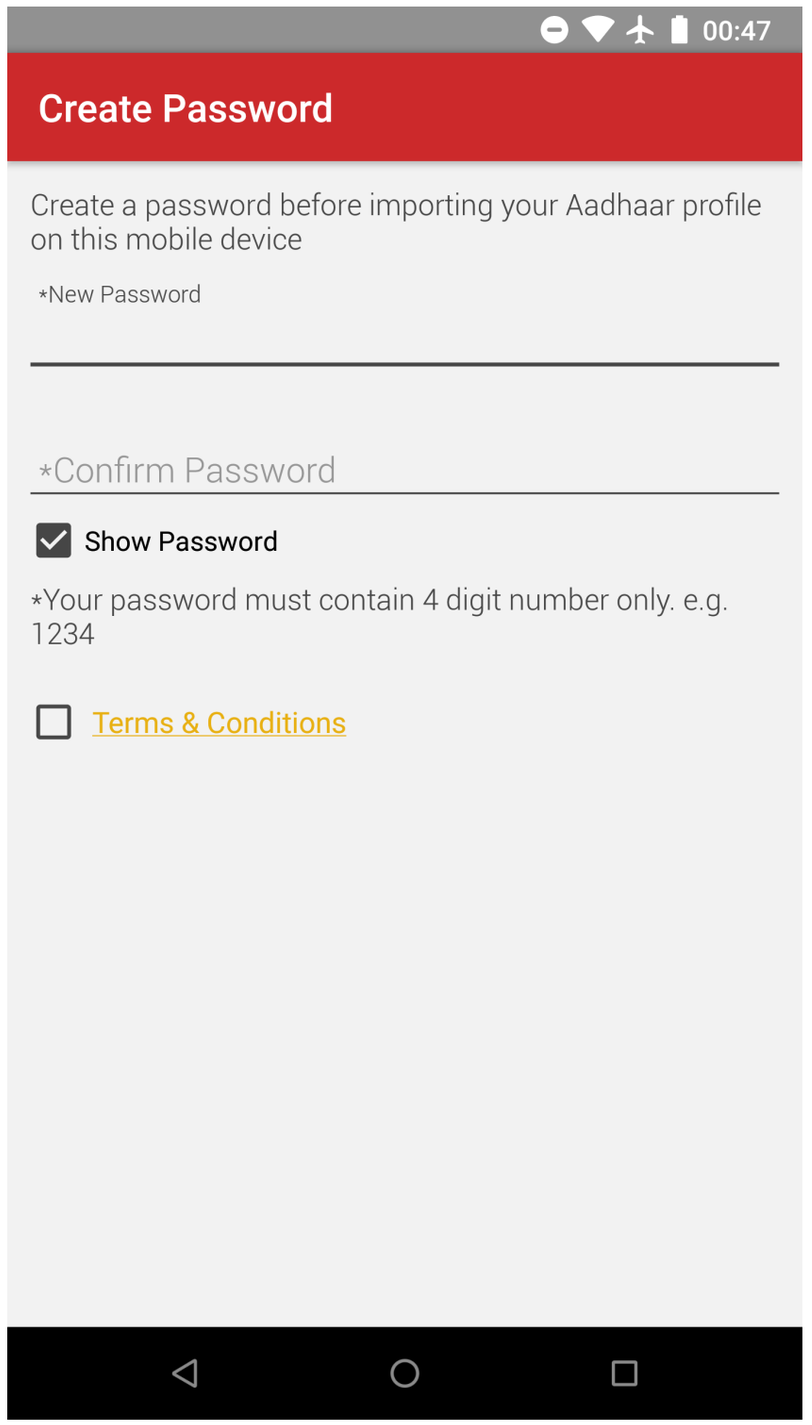
User Password



Bumble Bee



V1.1.0



V1.2.7

Elliot Alderson
@fs0c131y

DEFCON

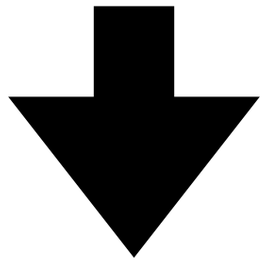
Database Password

in.gov.uidai.mAadhaarPlus.util.i in v1.1.0

```
public static String generateDBPassword() {
    Random random = new Random();
    random.setSeed(123456789);
    String encodeBase64 = encodeBase64( str: "db_password_123" + random.nextInt( n: 10));
    Log.d(TAG,  msg: "Password: " + encodeBase64);
    return encodeBase64;
}
```

in.gov.uidai.mAadhaarPlus.util.i in v1.1.0

```
public static String generateDBPassword() {
    Random random = new Random();
    random.setSeed(123456789);
    String encodeBase64 = encodeBase64( str: "db_password_123" + random.nextInt( n: 10));
    Log.d(TAG,  msg: "Password: " + encodeBase64);
    return encodeBase64;
}
```



db_password_1235

in.gov.uidai.mAadhaarPlus.j.c in v1.2.7

```
public static String c() {
    if (VERSION.SDK_INT < 26)
        return Secure.getString(BaseApplication.a().getContentResolver(), name: "android_id");

    if (ActivityCompat.checkSelfPermission(BaseApplication.a(), str: "android.permission.READ_PHONE_STATE") == 0)
        return ((TelephonyManager) BaseApplication.a().getSystemService(TELEPHONY_SERVICE)).getImei();

    return null;
}
```


Elliot Alderson

@fs0c131y

Best Practices by @TeamZetetic

- Take a passphrase from the user and mix it with a device id
- A significant part of the key material is a secret coming directly from the user when the application runs
- Hardcoding a key in application code is not suitable for any secure implementation
- Developers: When you are using a lib, a tool or a SDK RTFM!

Debug Features

in.gov.uidai.mAadhaarPlus.b.f in v1.1.0

```
public static void writeLog(String str) {
    boolean z = true;
    try {
        if (isLogger) {
            String str2 = Environment.getExternalStorageDirectory().getPath() + "/mAadhaar";
            String str3 = str2 + "/Log_" + new SimpleDateFormat( pattern: "yyyyMMddHH").format(new Date()) + ".txt";
            String format = new SimpleDateFormat( pattern: "yyyy-MM-dd-HH-mm-ss").format(new Date());
            File file = new File(str2);
            if (!file.exists()) {
                file.mkdirs();
            }
```

Frida function to enable debug feature

```
// in.gov.uidai.mAadhaarPlus.b.f.writeLog(String arg6)
var f = Java.use('in.gov.uidai.mAadhaarPlus.b.f');
f.writeLog.overload('java.lang.String').implementation = function (arg6) {
    console.log('[+] START writeLog');
    f.isLogger.value = true;
    console.log('arg6 = ' + arg6);
    console.log('[+] END writeLog');
    f.writeLog.overload('java.lang.String').apply(this, arguments)
}
```

```
DSB0090:/sdcard/mAadhaar $ cat Log_2018011201.txt
2018-01-12-01-14-22
Request url: http://10.66.204.42:9050/uidclientintegrationserver/reqOTPMAdhaar
2018-01-12-01-14-22
Request method: 1
2018-01-12-01-14-22
Request body: <?xml version="1.0" encoding="UTF-8"?><ApiRequestMessage xmlns="http:/
ecurityParameters>VkVSU0lPTl8xLjG91m8saMdATnmlxl6b2CvpnT1kf88TlHoHAtadytHEujCCASIwD
Mk5eLO+TDnKpdUlJsIA6IzMKE7OY5H0RjA/1pCY3JHJvHsw9XSsz15ObvUEqk2BzwypKwH1Yp84E8toVKx/
OGOivJDFMknvxfgN6+/YL/8hrHxV9SWfgzIu0v2z/hTHNPVkrAtLCOYIRQoYl2S+yfqjtPzRNdsCAwEAAcb
9IgpdL5sHZb+oWBUNWU8/D+KQZ2aWO0uv3HGbX4fyLerRTlq2Pp+jRFZ/uJoAE1A+LcY9rTiOGB35ITfLKt
FsRaoW5hYwJmv8ij+xHSO0wvWQc+g4qxkCBi6mIpNtknNryHYnfhGc8emVTh2eLRWw1HDV4tfXLC+HPndGu
DAA2VjwOQfEN0c/iyTp+8nwutaS4TIA4m9tm6LILHkEhkOB0Y0LJPnrdJ+cvSg8Z3rcMR8WHQAOEYdn+e3B
JtF5jPkxUN3x63rMPCBb1sv8XsOYbmjhVn+4gvcniKMfJpuxYIBuuqOFd5j4xUQCe9ggU+YPfFMtmRScV1W
Fj01a02Qf89a9D6ooMA6yaJly8+pI4zVuljsmrWOskwwOh0ziHz5ea+p+R8i62DYZvNJPxMBufOY8rFJmrk
2DC/p3bPX66mzRzod3pidErSc=</securityParameters><data>VkVSU0lPTl8xLjG+L14j0tgdJcbpLP
g5ZKAqTWO47laF8KUDtfc6FRVIG1Tve5PYH5lNC5l0/W8iTH8+XRBwLKOWuxcY0T+c/gMRUH9wwzXsjDbL/
h1nnTJO7gCjs9+eSNw1kkoU8/EJCtHQILCoudIx3Ro5yePPp2xdYubiCeshqDroMsmFaswyOHVmEhjWbfxS
kHoHCOQiQSVdxvEUTRPXlFeTnYT91s4GrSMn2Up1xo3BeI9Izxm2Sg9azGiDZ60YgmZq7nbx8jAiAdQkRP1
gNsTz8TvKucf/4yphG8gfeDlWidIw2JqY4SooEoTSkvFhsYUQ/CDrjKQdR79vfWbZZRbmJYooHMC6ee1lOI
kPvQw/ngQj5G3Wp2dGJUaBRrNXJFlHs8C5UhOk1XtDrkylgTlLQDA6SMlVgaIIgiQ3YTKuWGV2QnwNU04v2
1/A5rxsuRYctL0hISGZEacGs4U2CkLRd/lIQoVgdrtiC/t4wsBZ66tDW8saiIg2R8cdObvTGzuLKEnNoDqn
9rrbdYT++XvA==</data></ApiRequestMessage>DSB0090:/sdcard/mAadhaar $
```

MITM

CVE-2019-14516

```
GET /faqs HTTP/1.1
Host: resident.uidai.gov.in
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Linux; Android 8.1.0; Nexus 6P Build/OPM6.171019.030.E1; wv)
Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
X-Requested-With: in.gov.uidai.mAadhaarPlus
Connection: close
```

```
GET / HTTP/1.1
Host: uidai.gov.in
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Linux; Android 8.1.0; Nexus 6P Build/OPM6.171019.030.E1; wv)
Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
X-Requested-With: in.gov.uidai.mAadhaarPlus
Connection: close
```

Elliot Alderson
@fs0c131y

Responsible Disclosure

Responsible Disclosure

- Disclose a vulnerability in India is extremely hard
- Disclose a vulnerability in a governmental program is even harder
- In the past, security researchers has been arrested or threatened by the police
- At this time, Aadhaar one of the hottest subject in India
- Despite all my effort, UIDAI never contacted me

Wrap up

- The first versions of the app were very insecure
- They started to consider security after I disclosed the issues
- In the latest version, they added a lot of check but very easy to bypass
- The disclosure process was and still is a mess

Thank you