

# Avalanche Disclosure

Story about static analysis of 15k mobile Apps



# Who am I?

- Work hard on defense
- Have fun in offensive
- Break things

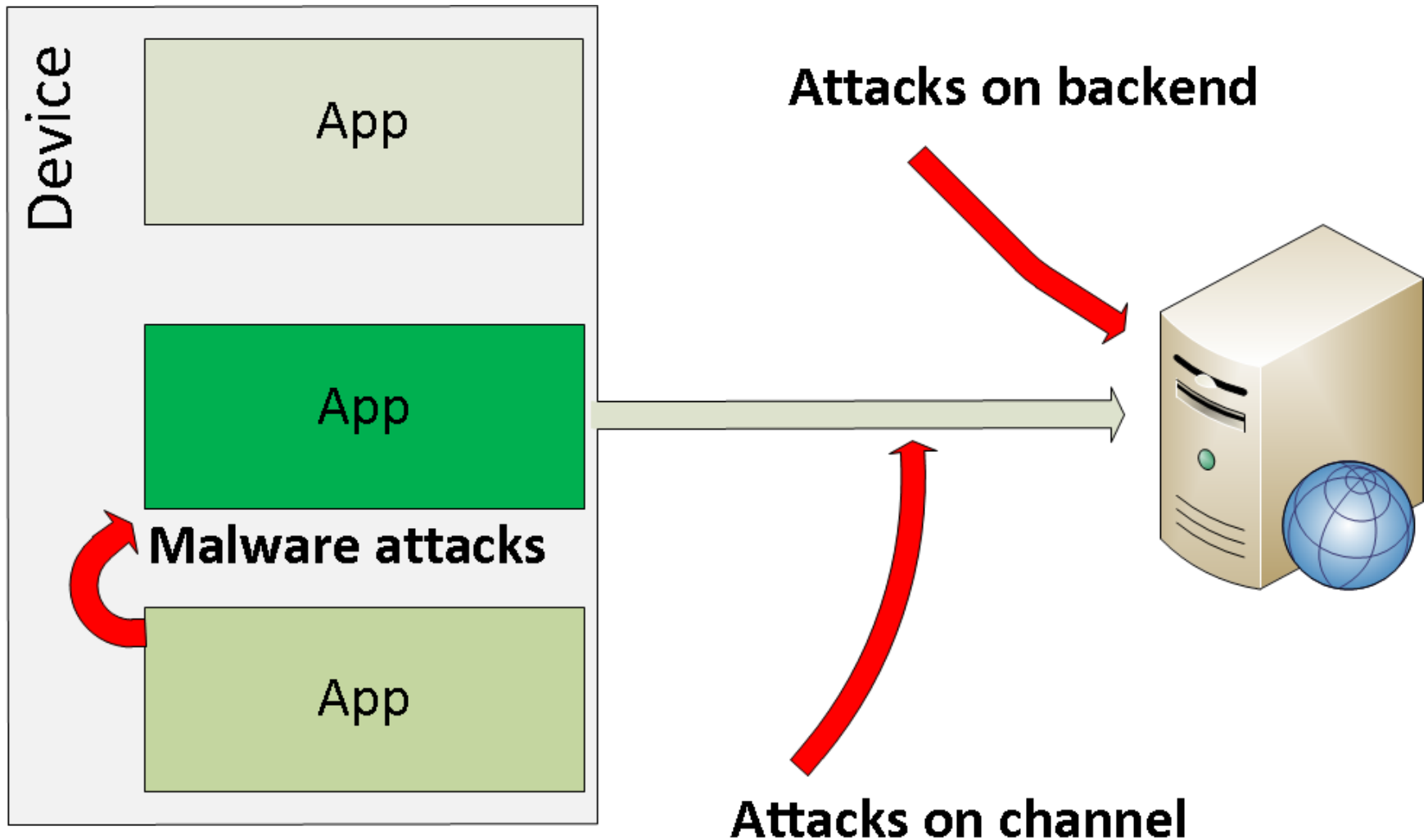
Alexey Troshichev  
@pl0lq  
pl0lq@hackapp.com

# What's wrong with an App ?

- ✓ Insecure transfer
- ✓ Injections
- ✓ Insecure storage
- ✓ Architecture flaws

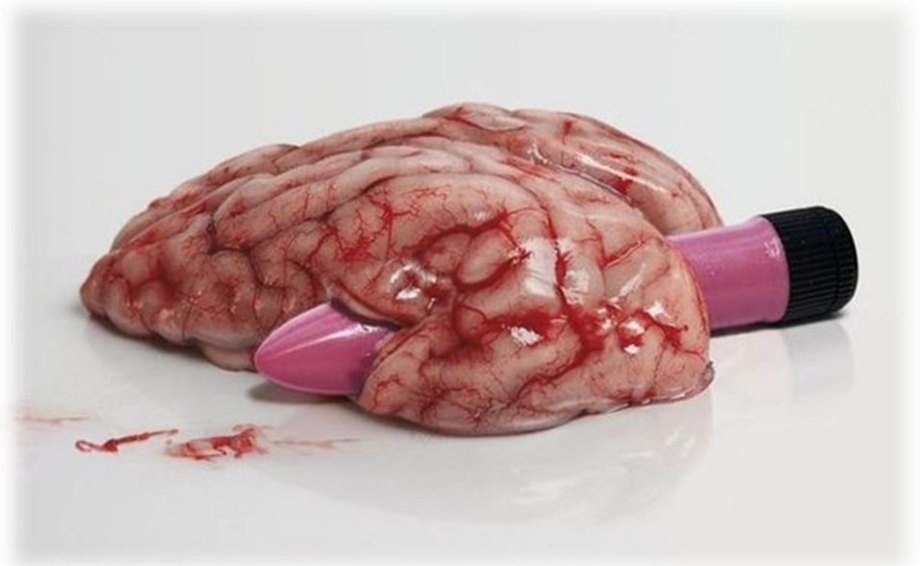
*Mobile OWASP for bla-bla-bla ...*

# Common Attacks



# On-device analysis ?

- ✓ Unlock Device
- ✓ Remove DRM
- ✓ Setup research environment
- ✓ Dynamic analysis
- ✓ Time & Brains



App is dangerous for user, but  
what's about vendor ?

Why should we waste time attacking  
one user, when we can just break into  
backend to get them all ?

Why always just binary file?

# What App can tell us?

- ✓ Testing environment disclosure
- ✓ Third party services authentication data
- ✓ Built-in accounts
- ✓ Something you can't even imagine =)



# Why it's interesting?

- ✓ Installation is not important
- ✓ Finally, we are just searching strings...
- ✓ ...and it could be automated =)





# Let's build a Grinder !

# AWK, STRINGS, GREP ?

- ✓ Not suitable for binary containers
- ✓ Too many garbage



# “Typical” Application

## Mobile APP



**Multimedia**  
(pics,audio)



**GUI Resources**

**DRM**



**Executable**



**Containers**  
(xml,plist,sqlite)

# Actual Application



**Multimedia**  
(pics,audio)



**GUI Resources**

???

**DRM**



**Executable**



**Containers**  
(xml,plist,sqlite)

# Steps

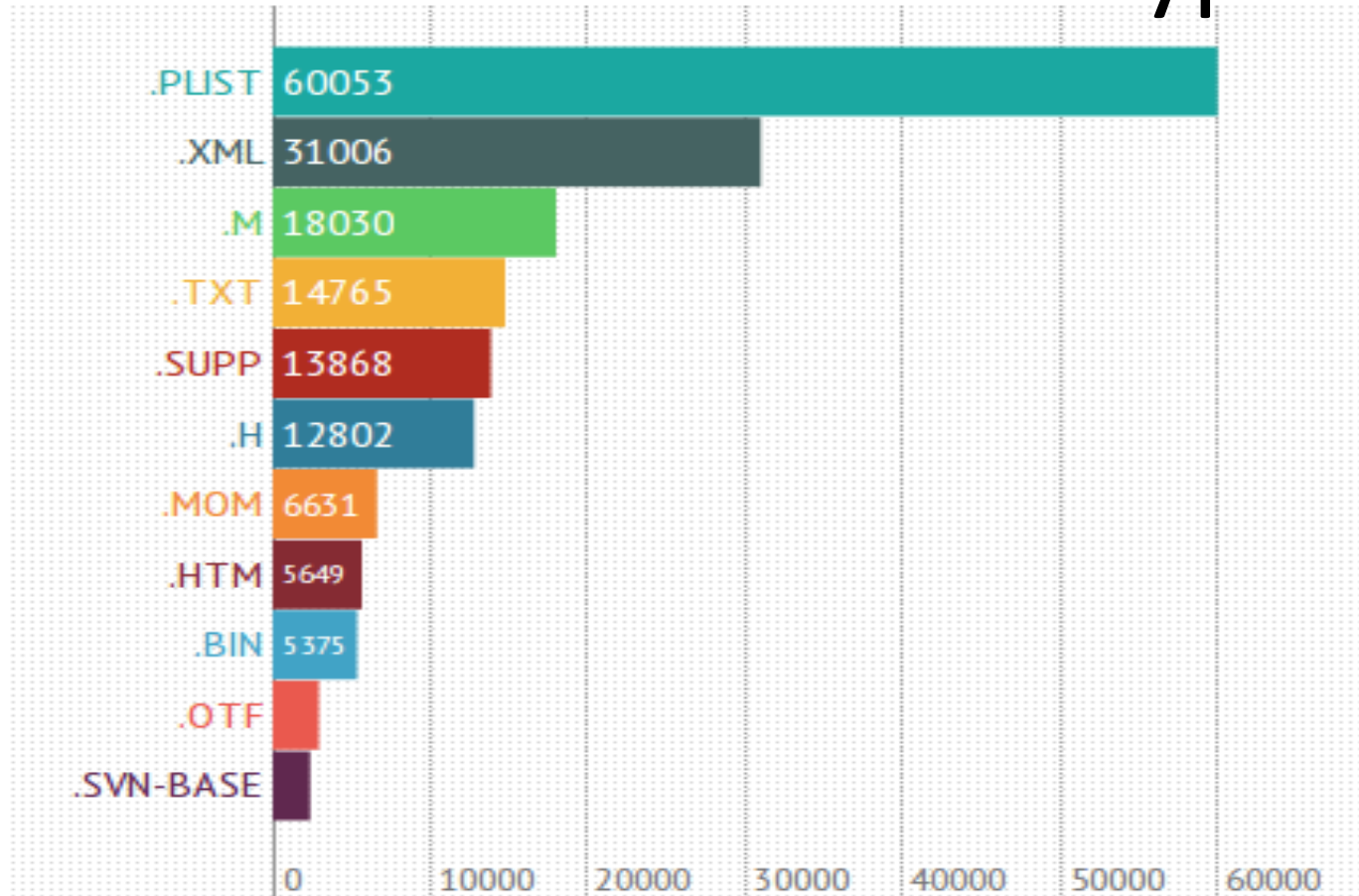
- ✓ Containers recursive traversal
- ✓ “Unusual” files search
- ✓ Selective GREP
- ✓ Structure validation

Let's take ~15k iOS Apps  
from iTunes Finance section...

...I like Finance

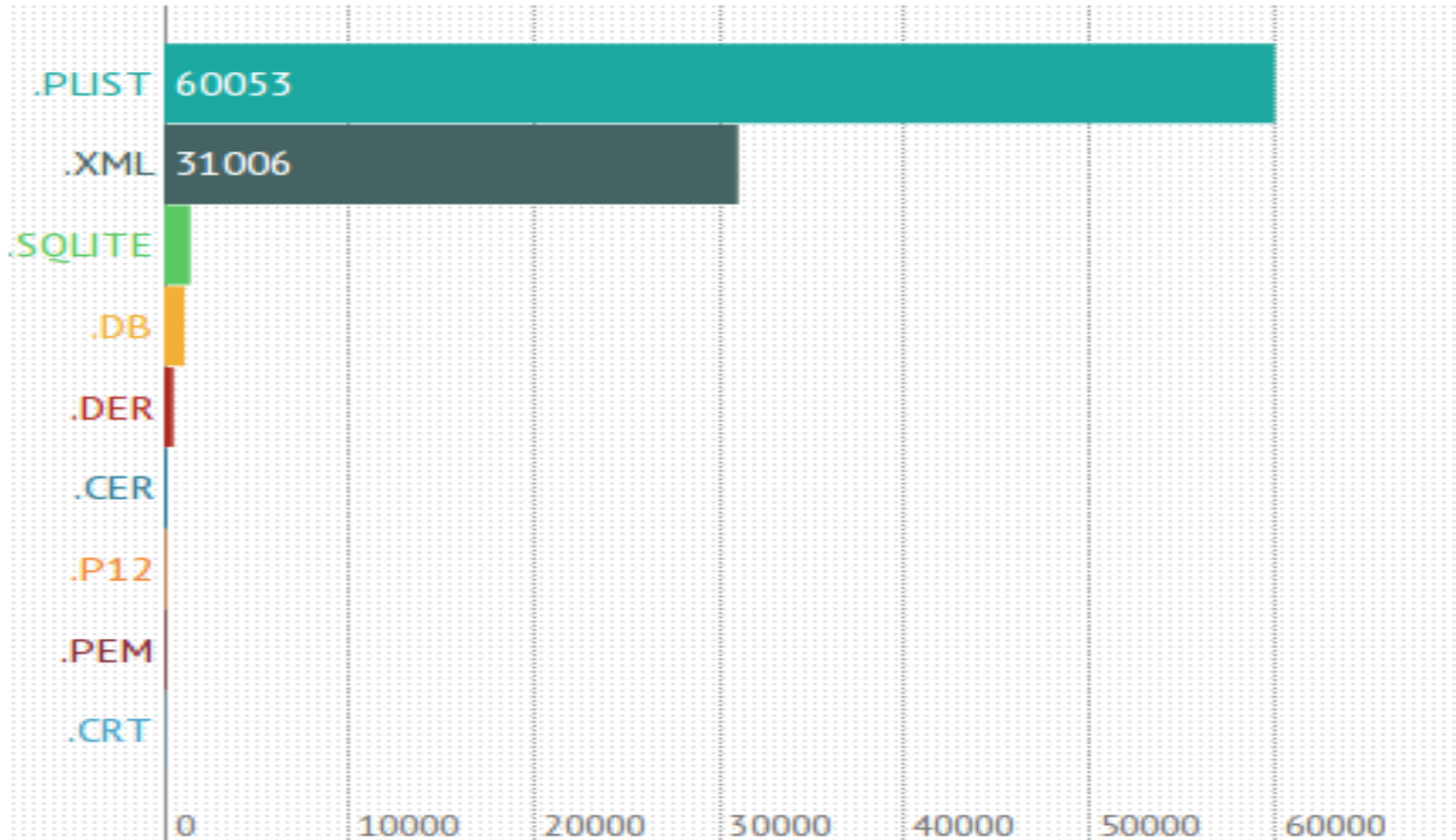
# What's inside ?

## 224061 files of 1396 types



# Low hanging fruits

94452 files = 42% of whole





# Shared authentication

# “Secure” communication

```
<key>SOAP_URL_test</key>  
<string>https://iphone:[REDACTED]@test.together.sk/fw/soap/calculator?ws=1</string>  
<key>URL_IMAGE_PRODUCTION</key>  
<string>https://www.top-pojisteni.cz/public/img/companies/</string>  
<key>SOAP_URL_MYFOLDER_test</key>  
<string>https://iphone:[REDACTED]@test.together.sk/fw/soap/myfolder?ws=1</string>  
<key>SOAP_username_production</key>
```

```
<key>CustomContentAPI-Stage</key>  
<string>https://saveology:[REDACTED]@staging.saveology.com/api/mobile/v3/Redis.get</string>  
<key>GetAccountAPI-Stage</key>  
<string>https://saveology:[REDACTED]@staging.saveology.com/api/mobile/v1/user</string>  
<key>DealOfDayAPI</key>  
<string>https://www.saveology.com/api/mobile/v2/deal-of-the-day</string>
```

# Third party services

share\_twitter\_secret:VfIR7csxGLP0FiD6KWDLUxyDrhug7trYi3PLTdXQ8g0  
twitter\_token\_secret:CPofIjw3MnVOo03puZglDScsYS4DZ9Lj5FnVUwsRc  
twitter\_token\_secret:36S8891OJNa4FcbQEahb7h0AJafG7ggI3uKXccHUjQ  
twitterconsumersecret:pwUS9XsYveUpi6Ne6O6susfb7zYj40Usy6IrsBUPE  
twitter\_client\_secret:NUzaObtcDyubO7ORI9rRkZ2UbFB0WP2dmY3FONnz3s  
twitter\_client\_secret:BqEPkR1g6BOXjW3v0yB6j22EKXt34u2M9brhmOXJO  
detwitter\_oauth\_token\_secret:qHLCXtPIZDuFSQWn9VGW0PT4uHxQpttHb2AbJgYFvM  
detwitter\_oauth\_token\_authorized:1183833127-lnSV1JJJaJn1iUb4EoLtoc8xBSjRd6cnO3c3sJ73  
detwitter\_oauth\_token:1183833127-lnSV1JJJaJn1iUb4EoLtoc8xBSjRd6cnO3c3sJ73  
twitter\_secret\_token:a8OdTlrtcQALu3bGLJPFV6WxBxytey2tJdm2D13hY  
twitter\_secret:7i41Neu6PkXfSb3jHLbTxSHBzDf2XqvcWqU99O9feaU  
twitter\_access\_token:15442828-aIcPiDj8D2jdkdf1ZdACIKyMMTv4KPC2jZ8ROyg

http://planopawnshop: [REDACTED]d32@twitter.com/

# Third party services

urbanairship\_app\_master\_secret:zeN4\_2\_pSNGp1tGVgHyBaA  
urbanairship\_app\_master\_secret:yyIjQ2y7QIawrLylf8mOBQ  
urbanairship\_app\_master\_secret:yWC9YRFrQ\_CKRn4EE49kaA  
urbanairship\_app\_master\_secret:yusUEaygR2uUBseIBHcWqA  
urbanairship\_app\_master\_secret:xxz2gDKLRI-FbXvBVX\_oYw  
urbanairship\_app\_master\_secret:WKSonIEeSImK5R8bIOqXow  
urbanairship\_app\_master\_secret:vZidXLJbSGak7boCWlbS9A  
urbanairship\_app\_master\_secret:WEluWOBRxuckgGSEGXBpQ  
urbanairship\_app\_master\_secret:sCSUGJ5sSk-BUWi6ZunAnq

You should never have to include the master secret in client code — that's used for authenticating to actually send push, which means that if someone was able to get that key from your package they could actually send pushes to your users. We use the com.0x82.urbanairship module to help us manage registration, location services, etc — I haven't implemented UA without it in a while, but would highly

```
<key>BingMapsKey</key>  
<string>AiI8ZfnTy5qeVjP5VhQx41ToJPk60UNJ5z[REDACTED]oqKi</string>  
<key>DTCompiler</key>
```

# Access to user data

AWS-secret:eyH0aw7IW7wdL8z2eSyK/A8q7rIF7uEMVpvQkbwC

```
cache/  
cache/123.jpeg  
cache/2361c1e2fe2c53523c6e3d0d20607543f4ce6a71zafa91.mp4  
cache/he_office_professional_plus_2013_x86_x64_dvd_1149745.iso  
cache/he_windows_7_ultimate_with_sp1_x64_dvd_u_677312.iso  
cache/he_windows_8_x64_dvd_915421.iso
```

```
sr/313B781E-B3E9-43B9-913D-3F9F28F00E18-1752-000001852072EFEB/card.xml  
sr/313B781E-B3E9-43B9-913D-3F9F28F00E18-1752-000001852072EFEB/photo.jpeg  
sr/313B781E-B3E9-43B9-913D-3F9F28F00E18-1752-000001852072EFEB/thumb.jpeg  
sr/313D2C89-8D49-4EC7-806E-4DF03D2EAD0C-3126-000002F9564997C5/card.xml  
sr/313D2C89-8D49-4EC7-806E-4DF03D2EAD0C-3126-000002F9564997C5/photo.jpeg  
sr/313D2C89-8D49-4EC7-806E-4DF03D2EAD0C-3126-000002F9564997C5/thumb.jpeg
```

You “publish” your contacts and photos by installing the app...  
=(



# Not identified

- RSA private key:MIICeQIBADANBgkqhkiG9w6xmHVejkTokPs68ow==
- secret:164AC36F64FCC2D5
- secret:33728B17A93A4A92
- secret:4711429DAE3C6F7C
- secret:62ebd594bc903feeea5ee459715e08fa
- secret:6508E621E259AC4A
- secret:697E46CE13AA557B
- secret:76a863da0821f58ecb13e31cb761c573
- secret:a7df64e1d5a33a93c12b06fa0f8c6f47
- secret\_android:2859389F73072C90
- secret\_android:3D05E67E03216A9B
- secret\_android:66549A9BB401AF56
- secret\_android:678649CED531B8E8
- secret\_android:745A209380630940

(and more, and more, and more...)

**4%** Apps released  
with hardcoded credentials

# DEV Environment

orsapp/apn/client/subscriptionForm.php

## Push Notifications

Message:

Certificate:

Euribors - Development ▼

Subscription:

Any ▼

Test Devices Only: ☐

Submit to message queue

svn://mokah.siab01.com/  
https://test.freerange360.com/  
http://test.mmf.berlingskemedi.net  
http://test.informatel.com  
http://test.improveagency.com  
http://test.appswiz.com  
https://test.freerange360.  
https://dev.magtab.com:8888  
http://dev.touchpublisher.com  
http://dev.pressrun.com/  
http://dev.openstreetmap.de/  
http://dev.aleph-labs.com

(and more, and more... )



# Mad Stuff

# Shocking configs

```
#define URLQA2 @"https://wsstage.onlineaccounts.org/wescom/SMSGatewayBluepoint"
#define GUIDQA2 @"f332299e-a300-4588-8a7c-809bc2935f84"
#define DefaultSymAccQA2 @"800139"
#define cryptKeyA_QA2 @"dwcl4"
#define cryptKeyB_QA2 @"lumee"
#define cryptKeyC_QA2 @"s500gmGvzSmkBB0gD408Ra"
#define testLoginQA2 @"530187"
#define testPassQA2 @"wrg1999"
#define testPinQA2 @""
#define webServiceLoginQA2 @"wrgTester"
#define webServicePassQA2 @"wrgTester"
#define geezioUrlQA2 @""
```

SMS gateway

OpenVpn config

```
client
dev tun
remote-cert-tls server
remote 173.255.213.195
reneg-sec 43200
script-security 2
#up clientexec.sh
#down clientexec.sh
comp-lzo no
persist-key
persist-tun
tun-mtu 1500
mssfix 1300
verb 3
cipher AES-256-CBC
<key>
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBCcwggSj
7elvztpIVkRjYEGzz2n9rXG87DtYnVklPH5dXKWM
KaGaWka+EmPcvOm747/QFvHTknOn1KNq9f8+CN3
```

# Unpredictable

```
<?php
$host = "mysql01";
$username="cq001ec4";
$password="db_tI8MLaT9";
$db="cq001ec4_cqwebsite";

$dsn = "mysql:host=$host;dbname=$db
```

```
<?php
// Turn off all error reporting
//error_reporting(0);

if($_SERVER['SERVER_NAME']=="localhost"
    $db_ip = 'localhost';
    $db_user = 'root';
    $db_pass = '';
    $db_name = 'fincurve';
} else {
    $db_ip = 'db379990573.db.1and1.
    $db_user = 'dbo379990573';
    $db_pass = 'monkey76';
    $db_name = 'db379990573';
}

/* Connect to Database */
```

# Developers Certificates

P12 containers, most are encrypted, but..

```
Issuer: C=US, O=Apple Inc., OU=Apple Worldwide Developer Relati
Validity
    Not Before: Mar 19 10:56:31 2013 GMT
    Not After : Mar 19 10:56:31 2014 GMT
Subject: UID=7F7WVHURH4, CN=iPhone Distribution: Assurland.com,
Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (2048 bit)
        Modulus (2048 bit):
            00:a6:1c:66:89:d4:97:90:65:29:a6:db:f9:68:75:
```

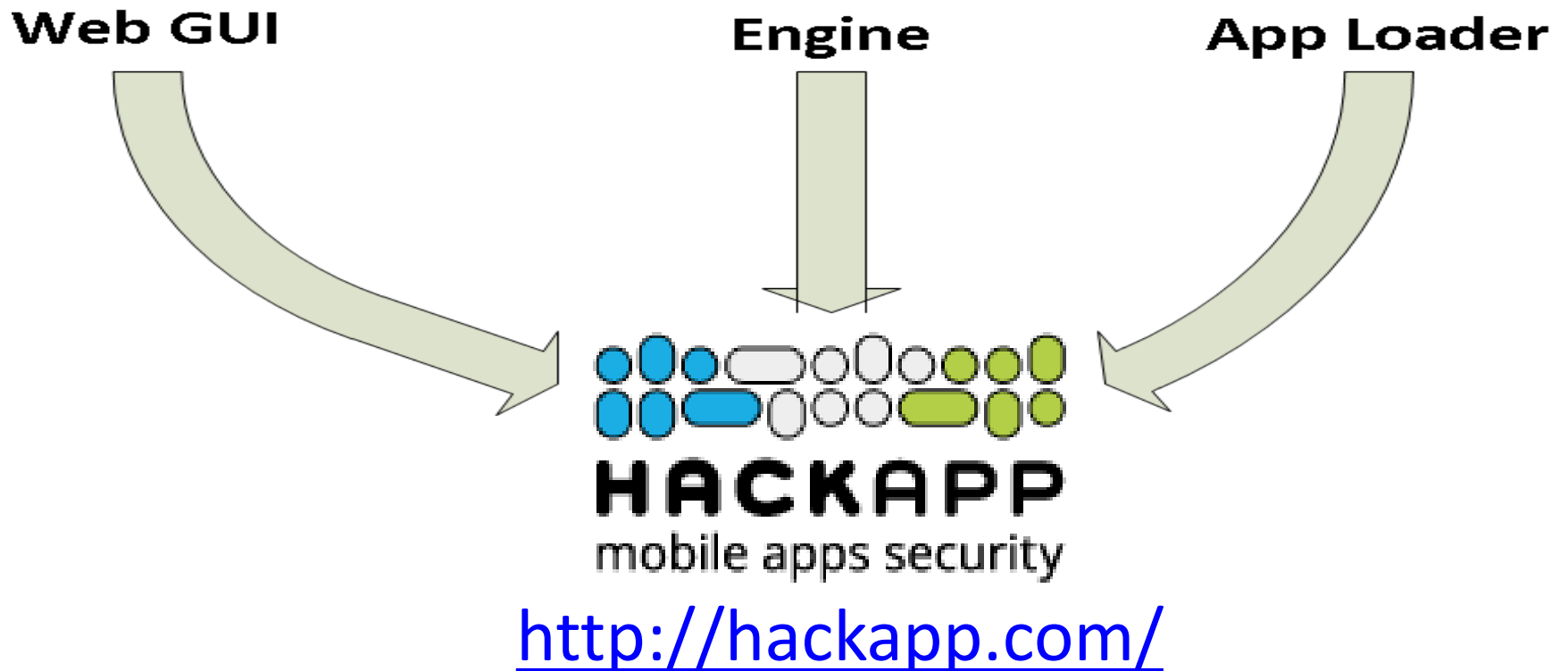
```
Private-Key: (2048 bit)
modulus:
    00:a6:1c:66:89:d4:97:90:65:29:a6:db:f9:68:75:
    a5:f9:05:fa:23:01:82:27:f8:93:15:19:67:32:46:
```



# HAVE NO TIME TO EXPLAIN

```
com.9188.lottorybundelid.ipa_d9817b095b8217fc881f5a98443f03c8.pem:-----BEGIN RSA PRIVATE KEY-----
com.finexlondon.FinCURVE.ipa_00e3eeacaa24eafba663a5d272c5a9ec.pem:-----BEGIN RSA PRIVATE KEY-----
com.finexlondon.FinCURVE.ipa_faef8505449bd5bac40700065775a29c.pem:-----BEGIN RSA PRIVATE KEY-----
com.hybridpaytech.hybridpin-3.0.ipa_0944acdfabce787e9ebaf565300b7da6.pem:-----BEGIN RSA PRIVATE KEY-----
com.jpmorgan.access.ipa_e850cc34d1a44fcf1c0d702330544b63.pem:-----BEGIN RSA PRIVATE KEY-----
com.jpmorgan.access.ipa_e850cc34d1a44fcf1c0d702330544b63.pem:-----BEGIN RSA PRIVATE KEY-----
com.pluribussystems.pokketipad.ipa_2f9008e6329d43ef2013d49a20d52045.pem:-----BEGIN RSA PRIVATE KEY-----
com.pluribussystems.pokketipad.ipa_a95b21b5945e08b8dd4c38deefdbe3c7.pem:-----BEGIN RSA PRIVATE KEY-----
com.pluribussystems.pokketipad.ipa_b191047ad222b18add7497202b2f04b8.pem:-----BEGIN RSA PRIVATE KEY-----
com.pluribussystems.pokketipad.ipa_e6134f7b63a2f9834b28abbb9ad7003a.pem:-----BEGIN RSA PRIVATE KEY-----
com.pluribussystems.pokketiphone.ipa_2f9008e6329d43ef2013d49a20d52045.pem:-----BEGIN RSA PRIVATE KEY-----
com.pluribussystems.pokketiphone.ipa_a95b21b5945e08b8dd4c38deefdbe3c7.pem:-----BEGIN RSA PRIVATE KEY-----
com.pluribussystems.pokketiphone.ipa_b191047ad222b18add7497202b2f04b8.pem:-----BEGIN RSA PRIVATE KEY-----
com.pluribussystems.pokketiphone.ipa_e6134f7b63a2f9834b28abbb9ad7003a.pem:-----BEGIN RSA PRIVATE KEY-----
com.santander.mobilebank.ipa_8186ad3f28f15b38b9fd23415d863e64.pem:-----BEGIN RSA PRIVATE KEY-----
com.santander.mobilebank.ipa_e33e923aab4b35a9ce979acbe22b63cc.pem:-----BEGIN RSA PRIVATE KEY-----
com.sdge.sdge.ipa_7697f83feca6f59d988846d9ad594f85.pem:-----BEGIN RSA PRIVATE KEY-----
com.sdge.sdge.ipa_9a574ad668ca18656e51808f99a7435a.pem:-----BEGIN RSA PRIVATE KEY-----
com.vanguard.eyehdlite.ipa_720cfee1288113c89f14330f105e1d23.pem:-----BEGIN RSA PRIVATE KEY-----
com.vanguard.eyehdlite.ipa_77993b4d93a77c161ac9b188b5e999ee.pem:-----BEGIN RSA PRIVATE KEY-----
no.bnbank.mobilbank.ipa_c9e877acb35cff8c0382890b197e381f.pem:-----BEGIN RSA PRIVATE KEY-----
no.bnbank.mobilbank.ipa_e33e923aab4b35a9ce979acbe22b63cc.pem:-----BEGIN RSA PRIVATE KEY-----
no.bnbank.tabletbank.ipa_c9e877acb35cff8c0382890b197e381f.pem:-----BEGIN RSA PRIVATE KEY-----
no.bnbank.tabletbank.ipa_e33e923aab4b35a9ce979acbe22b63cc.pem:-----BEGIN RSA PRIVATE KEY-----
no.dinbank.sbank.ipa_c9e877acb35cff8c0382890b197e381f.pem:-----BEGIN RSA PRIVATE KEY-----
no.dinbank.sbank.ipa_e33e923aab4b35a9ce979acbe22b63cc.pem:-----BEGIN RSA PRIVATE KEY-----
no.gjensidige.brettbank.ipa_6894665fe30cb9de73fd4e9884a9fa00.pem:-----BEGIN RSA PRIVATE KEY-----
```

# Is there an App for that?











# Dashboard

dashboard

Hide empty

+ Add app

| Application (bugs)                                                                                        | Source                        | Last status         | Status                                                                                          | Actions                |
|-----------------------------------------------------------------------------------------------------------|-------------------------------|---------------------|-------------------------------------------------------------------------------------------------|------------------------|
|  Trader <span>3</span>      | App Store <a href="#">URL</a> | 2013-10-29 21:54:54 |  Completed   | <a href="#">Delete</a> |
|  BARXdirect <span>20</span> | App Store <a href="#">URL</a> | 2013-10-29 21:54:33 |  Completed   | <a href="#">Delete</a> |
|  1035681 <span>20</span>    | App Store <a href="#">URL</a> | 2013-10-29 21:54:24 |  Completed   | <a href="#">Delete</a> |
|  wozhongla <span>2</span> | App Store <a href="#">URL</a> | 2013-10-29 21:53:51 |  Completed | <a href="#">Delete</a> |

# Report

## analysis results



com.rcm1.dclistings

[Share](#)[Download in ZIP](#)

### Info

critical

Saved secrets in app bundle

2

### Resources

info

URLs Found

2

### Files

info

Files are under MIT license

1

### Issues

3



# Details

bug details ◀ ▶ critical

## Synopsis

Saved secrets in app bundle

## Description

Affected files:

- [RCM1 Mobile RCM1 Mobile Marketplace.app/Info.plist](#)
- [RCM1 Mobile RCM1 Mobile Marketplace.app/RCM1 Mobile Marketplace-Info.plist](#)

Plain text authentication secrets seems to be saved in app bundle

BingMapsKey:Ail8ZfnTy5qeVjP5VhQx41ToJpK6OUNJ5z7DJ17ealtNw007DXEdyTg9KByboqKi

## Solution

Do not store any authentication secrets in your app. Keep in mind, that your app is available for everyone on the net.

# Questions ?



|          |                                                        |
|----------|--------------------------------------------------------|
| URL:     | <a href="http://hackapp.com/">http://hackapp.com/</a>  |
| Twitter: | @hackapp                                               |
| Mail:    | <a href="mailto:info@hackapp.com">info@hackapp.com</a> |