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

Device

App

Malware attacks

App

Attacks on backend

Attacks on channel
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)

DRM

Executable

GUI Resources

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

#ZeroNights2013  hackapp.com
Shared authentication
“Secure” communication
Third party services

share_twitter_secret:VflR7csxGLP0FiD6KWDLUxyDrhug7trYi3PLTdXQ8g0
twitter_token_secret:CPofiJw3MnVO03puZglDScsYS4DZ9Lj5FnVUwsRc
twitter_token_secret:36S88910JNa4FcbQElahb7h0AJafG7ggI3uKXccHUjQ
twitterconsumersecret:pwUS9XsYveUpi6Ne6O6susfb7zYj40Usy6IrsBUPE
twitter_client_secret:NUzaObtcDyubO7ORI9rRkZ2UbFB0WP2dmY3FONnz3s
twitter_client_secret:BqEPkR1g6BOXjW3v0yB6j22EKXt34u2M9brhmOXJ0
detwitter_oauth_token_secret:qHLCXtPIZDuFSQWhn9VGW0PT4uHxQpttHb2AbJgYFvm

detwitter_oauth_tokenauthorized:1183833127-lnSV1JJaJn1iUb4Eoltoc8xBSjRd6cnO3c3sJ73

detwitter_oauth_token:1183833127-lnSV1JJaJn1iUb4Eoltoc8xBSjRd6cnO3c3sJ73

twitter_secret_token:a8OdTIrtcQALu3bGLJPFV6WxBxytey2tJdm2D13hY
twitter_secret:7i41Neu6PkJFsB3jHLbTxDHBzDf2XqvcWqU9909feaU
twitter_access_token:15442828-a1 sharksJ8D2jkdf1ZdACIKyMMTv4KPC2yZ8ROyg

http://planopawnshop:******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:WKSonieiEeSImK5R8bI0qXow
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...
Access to user data

AWS-secret:eyH0aw7Iw7wdL8z2eSyK/A8q7rI/F7uEMVpvQkbwC

You “publish” your contacts and photos by installing the app... =(
Not identified

- RSA private key:MIICeQIBADANBgkqhkiG9w6xmHVejkTokPs68ow==
- secret:164AC36F64FCC2D5
- secret:33728B17A93A4A92
- secret:4711429DAE3C6F7C
- secret:62ebd594bc903feeeea5ee459715e08fa
- 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

svn://mokah.siab01.com/
https://test.freerange360.com/
http://test.mmf.berlingskemedia.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

SMS gateway

OpenVpn config
Unpredictable

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

// 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.land100.com";
    $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):

Private-Key: (2048 bit)
modulus:
HAVE NO TIME TO EXPLAIN
Is there an App for that?

Web GUI

Engine

App Loader

http://hackapp.com/

#ZeroNights2013
## Dashboard

<table>
<thead>
<tr>
<th>Application (bugs)</th>
<th>Source</th>
<th>Last status</th>
<th>Status</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trader</td>
<td>App Store <a href="#">URL</a></td>
<td>2013-10-29 21:54:54</td>
<td>✔ Completed</td>
<td>Delete</td>
</tr>
<tr>
<td>BARXdirect</td>
<td>App Store <a href="#">URL</a></td>
<td>2013-10-29 21:54:33</td>
<td>✔ Completed</td>
<td>Delete</td>
</tr>
<tr>
<td>1035681</td>
<td>App Store <a href="#">URL</a></td>
<td>2013-10-29 21:54:24</td>
<td>✔ Completed</td>
<td>Delete</td>
</tr>
<tr>
<td>wozhongla</td>
<td>App Store <a href="#">URL</a></td>
<td>2013-10-29 21:53:51</td>
<td>✔ Completed</td>
<td>Delete</td>
</tr>
</tbody>
</table>
###_analysis results

**com.rcm1.dclistsings**

<table>
<thead>
<tr>
<th>Category</th>
<th>Type</th>
<th>Description</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Info</strong></td>
<td>critical</td>
<td>Saved secrets in app bundle</td>
<td>2</td>
</tr>
<tr>
<td><strong>Resources</strong></td>
<td>info</td>
<td>URLs Found</td>
<td>2</td>
</tr>
<tr>
<td><strong>Files</strong></td>
<td>info</td>
<td>Files are under MIT license</td>
<td>1</td>
</tr>
<tr>
<td><strong>Issues</strong></td>
<td></td>
<td></td>
<td>3</td>
</tr>
</tbody>
</table>
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:Ail8ZfnTy5qeVjP5VhQx41TojPk6OUNj5z7Dj17ealtNw007DXEdyTg9KByoqKi

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: http://hackapp.com/
Twitter: @hackapp
Mail: info@hackapp.com