From Zero to App-Hero

Static and dynamic Android application reverse engineering

About myself

Bjoern Kerler

- Reverse Engineer and Cryptoanalyst
- Likes to break software and hardware :)

- Twitter: https://twitter.com/viperbjk
- Github: https://github.com/bkerler

Topics of this marvellous presentation

1. Introduction to static Android application reversing
   Level: Bad-Ass – Lone Ranger

2. Reversing using dynamic application Android reversing (debugging and hooking/injection)
   Level: Couch-Potato - I like watching

Introduction to static application reversing

Mar. 2019

Your Con

What do we need ?

1. Disassembler
   IDA Pro, Hopper, Radare2, Capstone,…

2. Decompiler
   JEB, Jad-Gui, APKTool,…

3. Debugger
   JDB, ADB, Android Studio, IDA Pro, …

Location of an android application

- Free apps are stored as base.apk in /data/apps/[Your Appname]

- Some paid apps are encrypted as .asec encrypted ext4 container, containing the apk (see AppsOnSD.sks for aes key)

- Appname is based on java namespace

Structure of an android application

APKs are ZIP-Files:

- AndroidManifest.xml
- Classes[Nr].dex
- Lib folder for native libraries
- Res folder for resources (language, strings, values, certificates, etc.)

Get code from binaries

- Classes[Nr].dex:
  DEX=Dalvik Executable, can be converted to Java Smali Format
  Has main application code, sometimes multidex

- Native libraries:
  Folder for each platform (x86, arm, ..)
  Dynamic libraries as .so (mainly custom support stuff such as crypto)

Typical way of reversing

- Classes[Nr].dex:
  JEB (Expensive), JAD-X (Free), Bytecode-Viewer (Free), IDA Pro (Expensive/Bytecode)

- Native libraries:
  IDA Pro (Expensive), JEB (Expensive), Hopper (Fair), Radare2/Capstone (Free)

Our target for today

https://play.google.com/store/apps/details?id=it.ideasolutions.kyms&hl=en

Categories Home Top Charts New Releases

KYMS - Keep your media safe

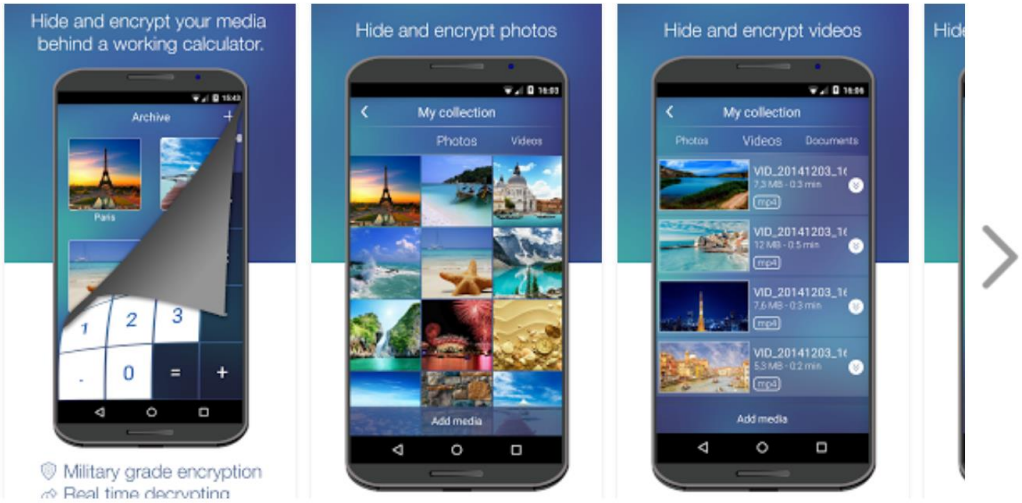
IdeaSolutions S.r.l. Video Players & Editors ★★★★☆ 12,439

USK: All ages

Contains ads · Offers in-app purchases

This app is compatible with all of your devices.

Add to Wishlist Install



Kyms looks like a working and stylish calculator App but it hides an inviolable vault in which to hide and encrypt all your multimedia and text files with military grade security (AES Encryption).

https://play.google.com/store/apps/details?id=it.ideasolutions.kyms&hl=en

Categories Home Top Charts New Releases

KYMS - Keep your media safe

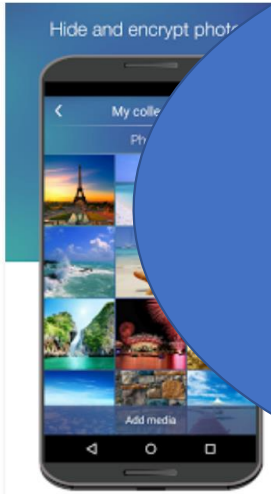
IdeaSolutions S.r.l. Video Players & Editors ★★★★☆ 12,439

USK: All ages

Contains ads · Offers in-app purchases

This app is compatible with all of your devices.

Add to Wishlist Install



Yeah, “military“ sounds frightening secure ☺

Kyms looks like a working and stylish calculator App but it hides an inviolable vault in which to hide and encrypt all your multimedia and text files with military grade security (AES Encryption).

Mar. 2019

Your Con

Lets download it

Options of downloading apks

- Test device, rooted :
  Install from play store, grab base.apk from /data/app/it.ideasolutions.kyms-1

- Use Racoon (Java) or gplaycli (python)

- Get apk by googling from serious apk download site

Options of downloading apks

- Test device, rooted :
  Install from play sto from
  /data/app/it.idea

- Use Racoon (Java)

Only if you are in desperate need of additional free malware/rootkits or „protective“ modifications ☺

- ~~Get apk by googling from serious apk download site~~

Raccoon

Datei Markt Gerät Ansicht Hilfe

KYMS - Keep your media safe

IdeaSolutions S.r.l.

12,7 MiB | 21.09.2017
4,29 | 12439
Kostenlos | Über 1.000.000 Downloads

Kyms sieht aus wie ein funktionierender und stylischer Taschenrechner, versteckt aber einen unüberwindbaren Safe, in dem Du alle deine Multimediadateien und txt Dokumente verstecken und nach Militärstandard (AES) verschlüsseln kannst.

*** Schneller Internet Browser mit Multi-tab. Automatischer Download! ***

Kyms ist die einzige App im Store, die in Echtzeit verschlüsselt, ohne Wartezeit! Wenn Du zum Beispiel auf ein Video drückst, startet es unmittelbar und die Verschlüsselung wird im Hintergrund weitergeführt.

Mit Kyms kannst du verstecken und schützen:
- Fotos
- Videos:ALLE WERDEN IN ECHTZEIT VERSCHLÜSSELT WÄREND DU SIE ANSCHAUST!!

Über | Berechtigungen | Screenshots

Download

pname:it.ideasolutions.kyms

KYMS - Keep your ...
IdeaSolutions S.r.l.

Main app!!

Native library spotted in apk !!

Gruppen | Berechtigungen | Inh

- it.ideasolutions.kyms-20.apk
  - AndroidManifest.xml
  - META-INF
  - assets
  - build-data.properties
  - classes.dex
  - fabric
  - jsr305_annotations
  - lib
    - armeabi-v7a
    - armeabi
      - libkyms-jni.so
    - x86
  - protobuf.meta
  - res
  - resources.arsc
  - values

Entpacken

Umbenennen

Löschen

Transfer

Kyms sieht aus wie ein
versteckt aber einen un
Multimediadateien und
Militärstandard (AES)

*** Schneller Internet
***

Kyms ist die einzige Ap
Wartezeit! Wenn Du zu
unmittelbar und die Ver

Mit Kyms kannst du ve
- Fotos
- Videos:ALLE WERDE
DU SIE ANSCHAUST!

Über | Berechtigung

Lets install it on emulator to see how it works

What do we know

- Having a look at the some files and the main database, they do look encrypted. App page said “aes” is used.

- User can enter pin and password, or just password instead

- Calculator needs pin (enter pin and press enter), asks for password, then shows secret main area

Crafting our attack plan

- Searching for any “aes” or “encrypt” debug string
- As database is encrypted, normally sqlcipher or direct aes encryption is being used
- AES Key is either a) derived via KDF (PBKDF-SHA1/SHA256 or scrypt) or b) custom crypto

Lets go using JEB

Mar. 2019

Your Con

JEB 2.3 - C:\Emulator\it.ideasolutions.kyms-20.apk

Datei Bearbeiten Navigation Aktion Native Debu

Project... Byteco...

Obfuscation is being used.
Class names and functions are replaced by a, aa, aaa, b, bb and so on

- a
  - a
    - a
      - a
      - a
- android
- b
  - a
    - a
      - a
- c
  - a
    - a
      - a
      - b
- com
  - a
    - a
    - b
  - android
    - vending
      - billing
  - b
    - a
      - a
        - a
        - b
        - c
        - d
        - e
        - f
        - g
        - h

Filter: type "Enter" to validate

```
.class public final a$b
.super Object

.annotation system EnclosingClass
    value = a
.end annotation

.annotation system InnerClass
    accessFlags = 0x19
    name = "b"
.end annotation

.field public static final bottomsheet_default_sheet_width:I = 0x7F0B0013

.class public final a$a
.super Object

.annotation system EnclosingClass
```

Description | Hex Dump | Disassembly | Zeichenketten

Logger | Console

```
Basisverzeichnis: C:\Decompiler\jeb2.4_floating
Programmverzeichnis: C:\Decompiler\jeb2.4_floating\bin
System: Windows 10 10.0 (amd64) de_DE
Java: Oracle Corporation 1.8.0_141
Plugin loaded: class com.pnf.plugin.oat.OATPlugin
Plugin loaded: class com.pnf.plugin.pdf.PdfPlugin
Suche nach Update…
Dei der Update-Suche ist ein Fehler aufgetreten
Creating a new project (primary file: C:\Emulator\it.ideasolutions.kyms-20.apk)
Adding artifact to project: C:\Emulator\it.ideasolutions.kyms-20.apk
```

coord: (0,0,0) | addr: La/a/a$a; | loc: ?

Available decompilers: dex, arm, mips

Mar. 2019

JEB 2.3 - C:\Emulator\it.ideasolutions.kyms-20.apk

Datei Bearbeiten Navigation Aktion Native Debugger Fenster Hilfe

Project... | Byteco...

- a
  - a
    - a
      - a
      - a
- android
- b
- c
- com
- d
- e
- it
  - ideasolutions
    - a
      - a
      - b
    - browser
    - kyms
      - a
      - app
      - b
      - calculator
      - crypto
      - data
      - gallery
      - ui
      - util
      - a
- javax
- net
  - sqlcipher
    - database

Filter: type "Enter" to validate

Bytecode/Disassembly | java<Unbound>

```
.class public final a$a
.super Object

.annotation system EnclosingClass
    value = a
.end annotation

.annotation system
    accessFl
    na
```

Ahhhh spotted crypto in it.ideasolutions.kyms. Obviously not fully obfuscated ☺

```
    ublic final a$a
    uper Object

.annotation system EnclosingClass
```

Description | Hex Dump | Disassembly | Zeichenketten

Logger | Console

```
Basisverzeichnis: C:\Decompiler\jeb2.4_floating
Programmverzeichnis: C:\Decompiler\jeb2.4_floating\bin
System: Windows 10 10.0 (amd64) de_DE
Java: Oracle Corporation 1.8.0_141
Plugin loaded: class com.pnf.plugin.oat.OATPlugin
Plugin loaded: class com.pnf.plugin.pdf.PdfPlugin
Suche nach Update…
Dei der Update-Suche ist ein Fehler aufgetreten
Creating a new project (primary file: C:\Emulator\it.ideasolutions.kyms-20.apk)
Adding artifact to project: C:\Emulator\it.ideasolutions.kyms-20.apk
```

null (11 items) | Available decompilers: dex, arm, mips

Looks like file decryption

☺

JEB 2.3

DecryptInputStream/Source

```
ions.kyms.crypto;

tion;
eam;

putStream extends InputStream {

b;
Object c;

DecryptInputStream(byte[] arg3, String arg4) {
    super();
    this.c = new Object();
    this.a = DecryptInputStream.nativeConstructor(arg3, arg4);

ic void close() {
    ject v1 = this.c;
    onitor_enter(v1);
    (!this.b) {
        DecryptInputStream.nativeClose(this.a);
        this.b = true;
    }

    __monitor_exit(v1);
    return;
label_11:
    __monitor_exit(v1);
}
catch(Throwable v0) {
    goto label_11;
```

Description | Source

- a
- app
- b
- calculator
- crypto
  - CryptoSession
  - CryptoUtils
  - DecryptInputStream
    - <init>
    - a
    - b
    - c
    - close
    - nativeClose
    - nativeConstructor
    - nativeRead
    - nativeReset
    - nativeSkip
    - read
    - read
    - reset
    - skip
  - a
- data

Filter: type "Enter" to validate

Logger | Console

```
Programmverzeichnis: C:\Decompiler\jeb2.4_floating\bin
System: Windows 10 10.0 (amd64) de_DE
Java: Oracle Corporation 1.8.0_141
Plugin loaded: class com.pnf.plugin.oat.OATPlugin
Plugin loaded: class com.pnf.plugin.pdf.PdfPlugin
Suche nach Update…
Dei der Update-Suche ist ein Fehler aufgetreten
Creating a new project (primary file: C:\Emulator\it.ideasolutions.kyms-20.apk)
Adding artifact to project: C:\Emulator\it.ideasolutions.kyms-20.apk
Decompiling at Lit/ideasolutions/kyms/crypto/DecryptInputStream;->close()V+22h
```

coord: (0,21,0) | addr: Lit/i...tream;->close()V+12h | loc: ? | Available decompilers: dex, arm, mips

What the ..... Empty function ?!?!?

☹

DecryptInputStream/Source

```
_exit(v1);

exit(v1);

le v0) {
bel_11;

row v0;

e static native void nativeClose(long arg0) {

private static native long nativeConstructor(byte[] arg0, String arg1) {
}

private static native int nativeRead(long arg0, byte[] arg1, int arg2, int arg3) {
}

private static native void nativeReset(long arg0) {
}

private static native long nativeSkip(long arg0, long arg1) {
}

public int read() {
    return 0;
}

public int read(byte[] arg3, int arg4, int arg5) {
```

Description | Source

- kyms
  - a
  - app
  - b
  - calculator
  - crypto
    - CryptoSession
    - CryptoUtils
    - DecryptInputStream
      - <init>
      - a
      - b
      - c
      - close
      - nativeClose
      - nativeConstructor
      - nativeRead
      - nativeReset
      - nativeSkip
      - read
      - read
      - reset
      - skip
    - a
  - data

Filter: type "Enter" to validate

Logger | Console

```
Programmverzeichnis: C:\Decompiler\jeb2.4_floating\bin
System: Windows 10 10.0 (amd64) de_DE
Java: Oracle Corporation 1.8.0_141
Plugin loaded: class com.pnf.plugin.oat.OATPlugin
Plugin loaded: class com.pnf.plugin.pdf.PdfPlugin
Suche nach Update…
Dei der Update-Suche ist ein Fehler aufgetreten
Creating a new project (primary file: C:\Emulator\it.ideasolutions.kyms-20.apk)
Adding artifact to project: C:\Emulator\it.ideasolutions.kyms-20.apk
Decompiling at Lit/ideasolutions/kyms/crypto/DecryptInputStream;->close()V+22h
```

coord: (0,40,31) | addr: Lit/i...BLjava/lang/String;)J | loc: ? | Available decompilers: dex, arm, mips | D...t

That could be an overloaded or an exported native function, which is loaded dynamically, in this case by using a dynamic library from the lib folder ☺

DecryptInputStream/Source

```
_exit(v1);

xit(v1);

e v0) {
l_11;

v0;

te static native void nativeClose(long arg0) {

private static native long nativeConstructor(byte[] arg0, String arg1) {
}

private static native int nativeRead(long arg0, byte[] arg1, int arg2, int arg3) {
}

private static native void nativeReset(long arg0) {
}

private static native long nativeSkip(long arg0, long arg1) {
}

public int read() {
    return 0;
}

public int read(byte[] arg3, int arg4, int arg5) {
```

Description | Source

- a
- app
- b
- calculator
- crypto
  - CryptoSession
  - CryptoUtils
  - DecryptInputStream
    - <init>
    - a
    - b
    - c
    - close
    - nativeClose
    - nativeConstructor
    - nativeRead
    - nativeReset
    - nativeSkip
    - read
    - read
    - reset
    - skip
  - a
- data

Filter: type "Enter" to validate

Logger | Console

```
Programmverzeichnis: C:\Decompiler\jeb2.4_floating\bin
System: Windows 10 10.0 (amd64) de_DE
Java: Oracle Corporation 1.8.0_141
Plugin loaded: class com.pnf.plugin.oat.OATPlugin
Plugin loaded: class com.pnf.plugin.pdf.PdfPlugin
Suche nach Update…
Dei der Update-Suche ist ein Fehler aufgetreten
Creating a new project (primary file: C:\Emulator\it.ideasolutions.kyms-20.apk)
Adding artifact to project: C:\Emulator\it.ideasolutions.kyms-20.apk
Decompiling at Lit/ideasolutions/kyms/crypto/DecryptInputStream;->close()V+22h
```

coord: (0,40,31) | addr: Lit/i...BLjava/lang/String;)J | loc: ? | Available decompilers: dex, arm, mips | D...t

JEB 2.3 - C:\Emulator\it.ideasolutions.kyms-20.apk

Datei Bearbeiten Navigation Aktion Native Debugger Fenster Hilfe

Project Explorer | Bytecode/Hierarchy

- it
  - ideasolutions
    - a
      - a
      - b
    - browser
    - kyms
- javax
- net
  - sqlcipher
    - database
    - AbstractCursor
    - AbstractWindowedCursor
    - BuildConfig
    - BulkCursorNative
    - BulkCursorProxy
    - BulkCursorToCursorAdaptor
    - CrossProcessCursorWrapper
    - Cursor
    - CursorIndexOutOfBoundsException
    - CursorWindow
    - CursorWrapper
    - DatabaseErrorHandler
    - DatabaseUtils
    - DefaultDatabaseErrorHandler
    - IBulkCursor
    - IContentObserver
    - MatrixCursor
    - R
    - SQLException
    - StaleDataException
- org
  - apache
  - iavia

Filter: type "Enter" to validate

As expected, we spotted as well net.sqlcipher which is being used for database encryption ☺

```
.method publi
        .registers 5
00000000  iget-object        v0, p0, f$4->c:f
00000004  iget-object        v1, p0, f$4->a:ContentFrameLayout
00000008  iget-boolean       v2, p0, f$4->b:Z
0000000C  invoke-static      f->a(f, ContentFrameLayout, Z)V, v0, v1, v2
00000012  return-void
.end method

.class f$a
.super Object

.implements AbsListView$OnScrollListener

.annotation system EnclosingClass
    value = f
.end annotation

.annotation system InnerClass
```

Description | Hex Dump | Disassembly | Zeichenketten

Logger | Console

```
Programmverzeichnis: C:\Decompiler\jeb2.4_floating\bin
System: Windows 10 10.0 (amd64) de_DE
Java: Oracle Corporation 1.8.0_141
Plugin loaded: class com.pnf.plugin.oat.OATPlugin
Plugin loaded: class com.pnf.plugin.pdf.PdfPlugin
Suche nach Update…
Dei der Update-Suche ist ein Fehler aufgetreten
Creating a new project (primary file: C:\Emulator\it.ideasolutions.kyms-20.apk)
Adding artifact to project: C:\Emulator\it.ideasolutions.kyms-20.apk
Decompiling at Lit/ideasolutions/kyms/crypto/DecryptInputStream;->close()V+22h
```

coord: (77615,3,40) | addr: ...tions/kyms/app/f$a; | loc: ? | Available decompilers: dex, arm, mips | D...t

SQLCipher has three traditional ways of inputting a dbpassword :

1. Via „PRAGMA KEY“ sqlite command
2. Via Class Constructor and/or OpenorCreateDatabase function

JEB 2.3 - C:\Emulator\it.ideasolutions.kyms-20.apk

Datei Bearbeiten Navigation Aktion Native Debugger Fenster Hilfe

Project Explorer | Bytecode/Hierarchy

- it
  - ideasolutions
    - a
      - a
      - b
    - browser
    - kyms
- javax
- net
  - sqlcipher
    - database
    - AbstractCursor
    - AbstractWindowedCursor
    - BuildConfig
    - BulkCursorNative
    - BulkCursorProxy
    - BulkCursorToCursorAdaptor
    - CrossProcessCursorWrapper
    - Cursor
    - CursorIndexOutOfBoundsException
    - CursorWindow
    - CursorWrapper
    - DatabaseErrorHandler
    - DatabaseUtils
    - DefaultDatabaseErrorHandler
    - IBulkCursor
    - IContentObserver
    - MatrixCursor
    - R
    - SQLException
    - StaleDataException
- org
  - apache
  - iavia

Filter: type "Enter" to validate

```
.method publi
        .registers 5
00000000  iget-object        v0, p0, f$4->c:f
00000004  iget-object        v1, p0, f$4->a:ContentFrameLayout
00000008  iget-boolean       v2, p0, f$4->b:Z
0000000C  invoke-static      f->a(f, ContentFrameLayout, Z)V, v0, v1, v2
00000012  return-void
.end method

.class f$a
.super Object

.implements AbsListView$OnScrollListener

.annotation system EnclosingClass
    value = f
.end annotation

.annotation system InnerClass
```

Description | Hex Dump | Disassembly | Zeichenketten

Logger | Console

```
Programmverzeichnis: C:\Decompiler\jeb2.4_floating\bin
System: Windows 10 10.0 (amd64) de_DE
Java: Oracle Corporation 1.8.0_141
Plugin loaded: class com.pnf.plugin.oat.OATPlugin
Plugin loaded: class com.pnf.plugin.pdf.PdfPlugin
Suche nach Update…
Dei der Update-Suche ist ein Fehler aufgetreten
Creating a new project (primary file: C:\Emulator\it.ideasolutions.kyms-20.apk)
Adding artifact to project: C:\Emulator\it.ideasolutions.kyms-20.apk
Decompiling at Lit/ideasolutions/kyms/crypto/DecryptInputStream;->close()V+22h
```

coord: (77615,3,40) | addr: ...tions/kyms/app/f$a; | loc: ? | Available decompilers: dex, arm, mips | D...t

JEB 2.3 - C:\Emulator\it.ideasolutions.kyms-20.apk

Datei Bearbeiten Navigation Aktion Native Debugger Fenster Hilfe

Project Explorer | Bytecode/Hierarchy

```
    }

    throw v0;
}

protected void a(String arg3) {
    if(this.c == null) {
        this.c = new it.ideasolutions.kyms.data.f(this.b).getWritableDatabase(arg3);
        this.s();
        h.a(this.b).a();
    }
}

private static int a(List
```

3. Via getWritableDatabase(dbpassword) or getReadableDatabase(dbpassword) function

So dbpassword=arg3 in this case

coord: (0,134,0) | addr: Lit/ideasolu...deasolutions/kyms/data/ad;)V | loc: ? | Available decompilers: dex, arm, mips | Default Layout | 730,1M

JEB 2.3 - C:\Emulator\it.ideasolutions.kyms-20.apk

Datei Bearbeiten Navigation Aktion Native Debugger Fenster Hilfe

Querverweise

Index	Adresse	Label	Komm
0	Lit/ideasolutions/kyms/data/SettingsManager;->a(Ljava/lang/String;Ljava/lang/String;Ljava/lang/String;)V+20h		
1	Lit/ideasolutions/kyms/data/sqldatabase_handler$1;->run()V+32h		
2	Lit/ideasolutions/kyms/data/sqldatabase_handler$6;->run()V+14h		

OK Abbrechen

Tracing back function a (with getWritableDatabase), we see only three functions are calling it

SettingsManager does look way too interesting ☺

```
b).getWritableDatabase(arg3);
ad[] arg13) {
```

```
Creating a new project (primary
Adding artifact to project: C:\Emulator\it.ideasolutions.kyms-20.apk
Decompiling at Lit/ideasolutions/kyms/crypto/DecryptInputStream;->close()V+22h
Decompiling at Lnet/sqlcipher/database/SQLiteDatabase;->openDatabase(Ljava/lang/String;[CLnet/sqlcipher/database/SQLite
Decompiling at Lit/ideasolutions/kyms/app/al;-><clinit>()V+4h
Decompiling at Lit/ideasolutions/kyms/data/SettingsManager;->d(Ljava/lang/String;)V+Eh
```

Available decompilers: dex, arm, mips

Default Layout 895,2M

```java
public void a(String arg3, String arg4, String arg5) {
    if(arg4 != null) {
        this.g(arg3);
    }
    else {
        arg4 = arg3;
    }

    this.a(arg5);
    sqldatabase_handler.a().a(this.b(arg4));
}
```

Sqldatabase_handler.a().a(dbpassword)

So this.b(arg4) must be our dbpassword

Ok, pointing to our beloved native library … argh !

```
                v0 = 0;
                break;
            }
        }

        return v0;
    }

    public String b(String arg2) {
        return SettingsManager.nativeGenerateKey(arg2);
    }

    public void b(a arg2) {
        this.w.remove(arg2);
    }

    public void b(b arg2) {
```

JEB 2.3 - C:\Emulator\it.ideasolutions.kyms-20.apk

Datei Bearbeiten Navigation Aktion Native Debugger Fenster Hilfe

Project Explorer | Bytecode/Hierarchy

a, aa, ab, ac, ad, ae, af, ag, ah, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, w, x, y

Filter: type "Enter" to validate

Byte... | Decr... | SQLi... | c/So... | v/So... | h/So... | d/So... | al/S... | am/... | ao/S... | Setti...

```
                v0 = 0x7F0C0110;
                break;
            }
        }

        return v0;
    }

    public long d() {
        return this.o.getLong(SettingsManager.k, 0);
    }

    public void d(String arg2) {
        this.a(arg2);
        SettingsManager.nativeChangeKeyPassword(this.e());
        this.g(null);
    }

    private static int e(int
        int v0 = 0x7F0C010A;
        switch(arg1) {
            case 1: {
                v0
```

Descriptio

Logger

```
Plugin load
Plugin loade
Suche nach Up
Dei der Update-
Creating a new pro
Adding artifact to p
Decompiling at Lit/ideas
Decompiling at Lnet/sqlciphe
Decompiling at Lit/ideasolutions/
Decompiling at Lit/ideasolutions/kyms/
```

Searching for strings „Pin“ and „Password“, we find this one, which is also used for sqlcipher init. And yes, it‘s also pointing to native library !

This.e() points to the entered user password, so user password is being used by native library function to generate our db password !

coord: (0,298,34) | addr: Lit/ideasol...;->d(Ljava/lang/String;)V+Eh | loc: ? | Available decompilers: dex, arm, mips | Default Layout | 643,1M

Lets get dirty

…

Native libraries

Opening up libkyms-jni.so in IDA Pro, we immediately see „EVP_Cipher“, which means OpenSSL is most probably used.

IDA - libkyms-jni.so C:\Emulator\libkyms-jni.so

File Edit Jump Search View Debugger Options Windows Help

Library function | Data | Regular function | Unexplored | Instruction | External symbol

Functions window

Function name

- EVP_CIPHER_CTX_key_length
- EVP_CIPHER_CTX_new
- EVP_CIPHER_CTX_nid
- EVP_CIPHER_CTX_num
- EVP_CIPHER_CTX_original_iv
- EVP_CIPHER_CTX_rand_key
- EVP_CIPHER_CTX_reset
- EVP_CIPHER_CTX_set_app_data
- EVP_CIPHER_CTX_set_cipher_data
- EVP_CIPHER_CTX_set_flags
- EVP_CIPHER_CTX_set_key_length
- EVP_CIPHER_CTX_set_num
- EVP_CIPHER_CTX_set_padding
- EVP_CIPHER_CTX_test_flags
- EVP_CIPHER_asn1_to_param
- EVP_CIPHER_block_size
- EVP_CIPHER_flags
- EVP_CIPHER_get_asn1_iv
- EVP_CIPHER_impl_ctx_size
- EVP_CIPHER_iv_length
- EVP_CIPHER_key_length
- EVP_CIPHER_nid
- EVP_CIPHER_param_to_asn1
- EVP_CIPHER_set_asn1_iv
- EVP_CIPHER_type
- EVP_Cipher
- EVP_CipherFinal
- EVP_CipherFinal_ex
- EVP_CipherInit
- EVP_CipherInit_ex
- EVP_CipherUpdate
- EVP_DecryptFinal
- EVP_DecryptInit
- EVP_DecryptInit_ex
- EVP_Digest
- EVP_DigestFinal
- EVP_DigestFinal_ex
- EVP_DigestInit
- EVP_DigestInit_ex
- EVP_DigestSignFinal

Line 14 of 6558

IDA View-A

```
.plt:00032904 ; Inp
.plt:00032904 ; Inp
.plt:00032904 ; Inp
.plt:00032904
.plt:00032904 ; ---
.plt:00032904
.plt:00032904
.plt:00032904 ; Needed Libra
.plt:00032904 ; Needed Library
.plt:00032904 ; Shared Name 'libkym
.plt:00032904 ;
.plt:00032904 ; Options     : EF_ARM_SOFT_FLOAT
.plt:00032904 ; EABI version: 5
.plt:00032904 ;
.plt:00032904
.plt:00032904 ; Processor       : ARM
.plt:00032904 ; ARM architecture: ARMv7
.plt:00032904 ; Target assembler: Generic assembler for ARM
.plt:00032904 ; Byte sex        : Little endian
.plt:00032904
.plt:00032904 ; ==========================================================================
.plt:00032904
.plt:00032904 ; Segment type: Pure code
.plt:00032904                 AREA .plt, CODE
.plt:00032904                 ; ORG 0x32904
.plt:00032904                 CODE32
.plt:00032904                 STR             LR, [SP,#-4]!
.plt:00032908                 LDR             LR, =(_GLOBAL_OFFSET_TABLE_ - 0x32914)
.plt:0003290C                 ADD             LR, PC, LR ; _GLOBAL_OFFSET_TABLE_
.plt:00032910                 LDR             PC, [LR,#8]!
.plt:00032910 ; ---------------------------------------------------------------------------
.plt:00032914 off_32914       DCD _GLOBAL_OFFSET_TABLE_ - 0x32914
.plt:00032914                                         ; DATA XREF: .plt:00032908↑r
.plt:00032918 ; [0000000C BYTES: COLLAPSED FUNCTION __cxa_atexit. PRESS CTRL-NUMPAD+ TO EXPAND]
.plt:00032924 ; [0000000C BYTES: COLLAPSED FUNCTION __cxa_finalize. PRESS CTRL-NUMPAD+ TO EXPAND]
.plt:00032930 ; [0000000C BYTES: COLLAPSED FUNCTION __android_log_print. PRESS CTRL-NUMPAD+ TO EXPAND]
.plt:0003293C ; [0000000C BYTES: COLLAPSED FUNCTION operator new(uint). PRESS CTRL-NUMPAD+ TO EXPAND]
.plt:00032948 ; [0000000C BYTES: COLLAPSED FUNCTION operator delete(void *). PRESS CTRL-NUMPAD+ TO EXPAND]
```

00032904 00032904: .plt:00032904 (Synchronized with Hex View-1)

Output window

```
Propagating type information...
Function argument information has been propagated
```

Searching for “nativeGenerateKey“ in the function list however returns nothing ?!?

IDA - libkyms-jni.so C:\Emulator\libkyms-jni.so

File Edit Jump Search View Debugger Options Windows Help

Library function | Data | Regular function | Unexplored | Instruction | External symbol

Functions window

Function name

- EVP_CIPHER_CTX_key_length
- EVP_CIPHER_CTX_new
- EVP_CIPHER_CTX_nid
- EVP_CIPHER_CTX_num
- EVP_CIPHER_CTX_original_iv
- EVP_CIPHER_CTX_rand_key
- EVP_CIPHER_CTX_reset
- EVP_CIPHER_CTX_set_app_data
- EVP_CIPHER_CTX_set_cipher_data
- EVP_CIPHER_CTX_set_flags
- EVP_CIPHER_CTX_set_key_length
- EVP_CIPHER_CTX_set_num
- EVP_CIPHER_CTX_set_padding
- EVP_CIPHER_CTX_test_flags
- EVP_CIPHER_asn1_to_param
- EVP_CIPHER_block_size
- EVP_CIPHER_flags
- EVP_CIPHER_get_asn1_iv
- EVP_CIPHER_impl_ctx_size
- EVP_CIPHER_iv_length
- EVP_CIPHER_key_length
- EVP_CIPHER_nid
- EVP_CIPHER_param_to_asn1
- EVP_CIPHER_set_asn1_iv
- EVP_CIPHER_type
- EVP_Cipher
- EVP_CipherFinal
- EVP_CipherFinal_ex
- EVP_CipherInit
- EVP_CipherInit_ex
- EVP_CipherUpdate
- EVP_DecryptFinal
- EVP_DecryptInit
- EVP_DecryptInit_ex
- EVP_Digest
- EVP_DigestFinal
- EVP_DigestFinal_ex
- EVP_DigestInit
- EVP_DigestInit_ex
- EVP_DigestSignFinal

Line 14 of 6558

IDA View-A

```
.plt:00032904 ; Inp
.plt:00032904 ; Inp
.plt:00032904 ; Inp
.plt:00032904
.plt:00032904 ; ---
.plt:00032904 ; Needed Lib
.plt:00032904 ; Needed Libra
.plt:00032904 ; Needed Library
.plt:00032904 ; Shared Name 'libkym
.plt:00032904 ;
.plt:00032904 ; Options     : EF_ARM_SOFT_FLOAT
.plt:00032904 ; EABI version: 5
.plt:00032904 ;
.plt:00032904
.plt:00032904 ; Processor       : ARM
.plt:00032904 ; ARM architecture: ARMv7
.plt:00032904 ; Target assembler: Generic assembler for ARM
.plt:00032904 ; Byte sex        : Little endian
.plt:00032904
.plt:00032904 ; ==========================================================================
.plt:00032904
.plt:00032904 ; Segment type: Pure code
.plt:00032904                 AREA .plt, CODE
.plt:00032904                 ; ORG 0x32904
.plt:00032904                 CODE32
.plt:00032904                 STR             LR, [SP,#-4]!
.plt:00032908                 LDR             LR, =(_GLOBAL_OFFSET_TABLE_ - 0x32914)
.plt:0003290C                 ADD             LR, PC, LR ; _GLOBAL_OFFSET_TABLE_
.plt:00032910                 LDR             PC, [LR,#8]!
.plt:00032910 ; ---------------------------------------------------------------------------
.plt:00032914 off_32914       DCD _GLOBAL_OFFSET_TABLE_ - 0x32914
.plt:00032914                                         ; DATA XREF: .plt:00032908↑r
.plt:00032918 ; [0000000C BYTES: COLLAPSED FUNCTION __cxa_atexit. PRESS CTRL-NUMPAD+ TO EXPAND]
.plt:00032924 ; [0000000C BYTES: COLLAPSED FUNCTION __cxa_finalize. PRESS CTRL-NUMPAD+ TO EXPAND]
.plt:00032930 ; [0000000C BYTES: COLLAPSED FUNCTION __android_log_print. PRESS CTRL-NUMPAD+ TO EXPAND]
.plt:0003293C ; [0000000C BYTES: COLLAPSED FUNCTION operator new(uint). PRESS CTRL-NUMPAD+ TO EXPAND]
.plt:00032948 ; [0000000C BYTES: COLLAPSED FUNCTION operator delete(void *). PRESS CTRL-NUMPAD+ TO EXPAND]
```

00032904 00032904: .plt:00032904 (Synchronized with Hex View-1)

Output window

```
Propagating type information...
Function argument information has been propagated
```

Searching for „nativeGenerateKey“ also returns no hit on the exports list ?!?

sqlcipher::CursorWindow::putNull(uint,uint)	000C7C36
sqlcipher::CursorWindow::read_field_slot(int,int,sqlcipher::fie...	000C7A70
sqlcipher::CursorWindow::~CursorWindow()	000C788
sqlcipher::compile(_JNIEnv *,_jobject *,sqlite3 *,_jstring *)	000C4
sqlcipher::dbopen(_JNIEnv *,_jobject *,_jstring *,int)	000C
sqlcipher::get_window_from_object(_JNIEnv *,_jobject *)	00
sqlcipher::native_key(_JNIEnv *,_jobject *,_jbyteArray *)	C4E3C
sqlcipher::native_key_mutf8(_JNIEnv *,_jobject *,_jcharArray *)	000C4F34
sqlcipher::native_rawExecSQL(_JNIEnv *,_jobject *,_jstring *)	000C5018
sqlcipher::native_rekey(_JNIEnv *,_jobject *,_jbyteArray *)	000C4EB8
sqlcipher::native_status(_JNIEnv *,_jobject *,int,uchar)	000C4DC8
sqlcipher::register_android_database_CursorWindow(_JNIEn...	000C653C
sqlcipher::register_android_database_SQLiteCompiledSql(_J...	000C4C70
sqlcipher::register_android_database_SQLiteDatabase(_JNIE...	000C52CC
sqlcipher::register_android_database_SQLiteProgram(_JNIEn...	000C5940
sqlcipher::register_android_database_SQLiteQuery(_JNIEnv *)	000C5DB4

Searching for the string „nativeGenerateKey“ we find a java native call nativeGenerateKey(String) :?

IDA View-A | Occurrences of binary: "nativeGenerate | H | Structures | Enums | Imports

```
.rodata:0014E960 aLandroidCont_1 DCB "(Landroid/ ent/Context;)V",0
.rodata:0014E960                                         ; DATA XREF: .data:0017F0E0↓o
.rodata:0014E97D aNativehaskey   DCB "nativeHasKey",0    ; DATA XREF: .data:0017F0E8↓o
.rodata:0014E98A aZ_0            DCB "()Z",0             ; DATA XREF: .data:0017F0EC↓o
.rodata:0014E98A                                         ; .data:0018009C↓o
.rodata:0014E98E aNativegenerate DCB "nativeGenerateKey",0 ; DATA XREF: .data:0017F0F4↓o
.rodata:0014E9A0 aLjavaLangStr_0 DCB "(Ljava/lang/String;)Ljava/lang/String;",0
.rodata:0014E9A0                                         ; DATA XREF: .data:0017F0F8↓o
.rodata:0014E9A0                                         ; .data:0017F104↓o
.rodata:0014E9C7 aNativeauthenti DCB "nativeAuthenticate",0 ; DATA XREF: .data:0017F100↓o
.rodata:0014E9DA aNativeclearkey DCB "nativeClearKey",0  ; DATA XREF: .data:0017F10C↓o
.rodata:0014E9E9 aV              DCB "()V",0             ; DATA XREF: .data:0017F110↓o
.rodata:0014E9E9                                         ; .data:0017FEC8↓o ...
.rodata:0014E9ED aNativechangeke DCB "nativeChangeKeyPassword",0
.rodata:0014E9ED                                         ; DATA XREF: .data:0017F118↓o
```

Getting the reference for the string, we see a function pointer table …. So sub_39E30 must be nativeGenerateKey ☺

```
.data:0017F0E8    DCD aNativehaskey        ; "nativeHasKey"
.data:0017F0EC    DCD aZ_0                 ; "()Z"
.data:0017F0F0    DCD sub_39C34+1
.data:0017F0F4    DCD aNativegenerate      ; "nativeGenerateKey"
.data:0017F0F8    DCD aLjavaLangStr_0      ; "(Ljava/lang/String;)Ljava/lang/String;"
.data:0017F0FC    DCD sub_39E30+1
.data:0017F100    DCD aNativeauthenti      ; "nativeAuthenticate"
.data:0017F104    DCD aLjavaLangStr_0      ; "(Ljava/lang/String;)Ljava/lang/String;"
.data:0017F108    DCD sub_39F58+1
.data:0017F10C    DCD aNativeclearkey      ; "nativeClearKey"
.data:0017F110    DCD aV                   ; "()V"
.data:0017F114    DCD sub_3A228+1
```

Disassembly is best for details, but we prefer decompiling this time instead ☺

IDA View-A | Occurrences of binary: "nativeGenerate | Hex View-1

```
                                nativeGenerateKey

                                var_70= -0x70
                                var_68= -0x68
                                var_64= -0x64
                                var_40= -0x40
                                var_30= -0x30
                                var_20= -0x20
                                var_10= -0x10

F0 B5                           PUSH            {R4-R7,LR}
03 AF                           ADD             R7, SP, #0xC
99 B0                           SUB             SP, SP, #0x64
04 B4                           PUSH            {R2}
20 BC                           POP             {R5}
04 00                           MOVS            R4, R0
2F 48                           LDR             R0, =(__stack_chk_guard_ptr - 0x39E42)
78 44                           ADD             R0, PC ; __stack_chk_guard_ptr
00 68                           LDR             R0, [R0] ; __stack_chk_guard
00 68                           LDR             R0, [R0]
18 90                           STR             R0, [SP,#0x70+var_10]
14 A8                           ADD             R0, SP, #0x70+var_20
10 21                           MOVS            R1, #0x10
F8 F7 02 EE                     BLX             j_RAND_bytes
01 28                           CMP             R0, #1
3F D1                           BNE             loc_39ED2
```

```
10 A8                           ADD             R0, SP, #0x70+var_30
10 21                           MOVS            R1, #0x10
F8 F7 FC ED                     BLX             j_RAND_bytes
01 28                           CMP             R0, #1
3B D1                           BNE             loc_39ED6
```

```
0C A8                           ADD             R0, SP, #0x70+var_40
10 21                           MOVS            R1, #0x10
F8 F7 F6 ED                     BLX             j_RAND_bytes
01 28                           CMP             R0, #1
37 D1                           BNE             loc_39EDA
```

```
int __fastcall nativeGenerateKey(int a1, int a2, int a3)
{
  int v3; // r5@1
  int v4; // r4@1
  int v5; // r1@4
  int result; // r0@4
  const char *v7; // r1@8
  char v8; // [sp+10h] [bp-64h]@7
  char v9; // [sp+34h] [bp-40h]@3
  char v10; // [sp+44h] [bp-30h]@2
  char v11; // [sp+54h] [bp-20h]@1

  v3 = a3;
  v4 = a1;
  if ( j_RAND_bytes(&v11, 16) != 1 )
  {
    v7 = "key RAND_bytes error";
LABEL_11:
    throwEx(v4, v7);
    return 0;
  }
  if ( j_RAND_bytes(&v10, 16) != 1 )
  {
    v7 = "salt RAND_bytes error";
    goto LABEL_11;
  }
  if ( j_RAND_bytes(&v9, 16) != 1 )
  {
    v7 = "iv RAND_bytes error";
    goto LABEL_11;
  }
  v5 = sub_3A4E8(v4, &v9, &v10, v3, (int)&v11);
  result = 0;
  if ( v5 == 1 )
  {
    pthread_mutex_lock((pthread_mutex_t *)&unk_182D8C);
    if ( !dword_182D90 )
      dword_182D90 = operator new[](0x10u);
    _aeabi_memcpy();
    pthread_mutex_unlock((pthread_mutex_t *)&unk_182D8C);
    tohex((unsigned __int8 *)&v11, 16, &v8);
```

So, we got a random key (16 bytes)=v11, salt (16 bytes)=v10 and iv (16 bytes)=v9 generated that needs to be stored somewhere …
And a func sub_3a4E8 that does something with it
☺

```
int __fastcall sub_3A4E8(int a1, void *iv, void *salt, int a4, int a5)
{
  void *v5; // r4@1
  int v6; // r5@1
  signed int v7; // r6@1
  void *v8; // r6@2
  int v9; // r0@2
  int v10; // r4@4
  int v11; // r4@5
  FILE *v12; // r4@6
  FILE *v13; // r4@7
  int keysize; // ST20_4@8
  int v15; // r1@8
  int v16; // r5@8
  int v17; // r4@9
  int v18; // r1@9
  void (__fastcall *v19)(int, int, const char *); // r3@9
  const char *v20; // r2@9
  int v21; // r0@10
  int result; // r0@17
  int v23; // [sp+8h] [bp-5Ch]@3
  void *v24; // [sp+10h] [bp-54h]@2
  int v25; // [sp+18h] [bp-4Ch]@2
  const void *ptr; // [sp+1Ch] [bp-48h]@1
  int v27; // [sp+20h] [bp-44h]@2
  char v28[32]; // [sp+24h] [bp-40h]@3
  char v29; // [sp+44h] [bp-20h]@1
  int v30; // [sp+54h] [bp-10h]@17

  v5 = iv;
  v6 = a1;
  ptr = salt;
  v7 = 0;
  if ( PKCS5_PBKDF2_HMAC_0((int *)a1, a4, (int)salt, (int)&v29) != 1 )
    goto LABEL_17;
  v25 = v6;
  v27 = 0;
  v8 = (void *)j_EVP_CIPHER_CTX_new();
  v9 = j_EVP_aes_128_cbc();
  v24 = v5;
```

Func sub_3a4E8 uses pbkcs5_pbkdf2_hmac .. and result of that function is being used to decrypt the key using aes_128_cbc

☺

```
signed int __fastcall PKCS5_PBKDF2_HMAC_0(int *a1, int a2, int a3, int a4)
{
  int v4; // ST20_4@1
  int *v5; // r4@1
  const char *v6; // r6@1
  int v7; // r5@1
  int v8; // r0@1
  int v9; // r0@1
  int v10; // r1@1
  signed int result; // r0@2
  int v12; // r0@3
  int v13; // [sp+14h] [bp-1Ch]@1

  v4 = a3;
  v5 = a1;
  v13 = a2;
  v6 = (const char *)(*(int (__fastcall **)(int *))(*a1 + 676))(a
  v7 = strlen(v6);
  v8 = j_EVP_sha1();
  v9 = j_PKCS5_PBKDF2_HMAC((int)v6, v7, v4, 16, 10000, v8);
  v10 = *v5;
  if ( v9 == 1 )
  {
    (*(void (__fastcall **)(int *, int, const char *))(v10 + 680))(v5, v13, v6);
    result = 1;
  }
  else
  {
    v12 = (*(int (__fastcall **)(int *, const char *))(v10 + 24))(v5, "java/security/InvalidKeyException");
    (*(void (__fastcall **)(int *, int, const char *))(*v5 + 56))(v5, v12, "PKCS5_PBKDF2_HMAC error");
    result = 0;
  }
  return result;
}
```

Having a closer look at PKCS5_PBKDF2_HMAC function, let's google if they used openssl ☺

PKCS5_PBKDF2_HMAC, PKCS5_PBKDF2_HMAC_SHA1 - password based derivation routines with salt and iteration count

SYNOPSIS

```
#include <openssl/evp.h>

int PKCS5_PBKDF2_HMAC(const char *pass, int passlen,
                      const unsigned char *salt, int saltlen, int iter,
                      const EVP_MD *digest,
                      int keylen, unsigned char *out);
```

```
v8 = j_EVP_sha1();
v9 = j_PKCS5_PBKDF2_HMAC((int)v6, v7, v4, 16, 10000, v8);
v10 = *v5;
if ( v9 == 1 )
{
  (*(void (__fastcall **)(int *, int, const char *))(v10 + 680))(v
  result = 1;
}
else
{
  v12 = (*(int (__fastcall **)(int *, const char *))(v10 + 24
  (*(void (__fastcall **)(int *, int, const char *))(*v5 + 56
  result = 0;
}
return result;
}
```

Googling the PKCS5_PBKDF2_HMAC function, we immediately see that :

Saltlen=16
Iterations=10000
Algo=SHA1

☺

IDA... | Pseud... | Occurrences of binary: "nativeG... | Hex... | Str... | En... | Im... | Ex...

```
32  salt_1 = salt;
33  v7 = 0;
34  if ( PKCS5_PBKDF2_HMAC_0((int *)a1, a4, (int)salt, (int)&v29) != 1 )
35    goto LABEL_17;
36  v25 = v6;
37  v27 = 0;
38  v8 = (void *)j_EVP_CIPHER_CTX_new();
39  v9 = j_EVP_aes_128_cbc();
40  iv_1 = v5;
41  if ( j_EVP_CipherInit_ex(v8, v9) )
42  {
43    if ( j_EVP_CipherUpdate(v8, encryptedkey, &v27, a5, 16,
44    {
45      v10 = v27;
46      if ( j_EVP_CipherUpdate(v8, &encryptedkey[v27], &v27
47      {
48        v11 = j_EVP_CipherFinal_ex(v8, &encryptedkey[v27 +
49        j_EVP_CIPHER_CTX_free(v8);
50        if ( v11 )
51        {
52          filehandle = fopen((const char *)dword_182D98,
53          if ( filehandle )
54          {
55            v7 = 1;
56            fputc(1, filehandle);
57            fwrite(salt_1, 1u, 0x10u, filehandle);
58            fwrite(iv_1, 1u, 0x10u, filehandle);
59            fwrite(encryptedkey, 1u, 0x20u, filehandle);
60            fclose(filehandle);
61            v13 = fopen((const char *)dword_182D98, (const char
62            if ( v13 )
63            {
64              keysize = getFileSize();
65              v16 = v15;
```

Ok. So what we know so far :
A password is being used to derive an aes_key using PBKDF2_SHA1(Generated Salt[16],Iterations=10000) and then encrypts a random key (encryptedkey) using aes_cbc_128bit with a random iv.

But where are the encryptedkey, generated salt, generated iv being stored to ?
☺

IDA... | Pseud... | Occurrences of binary: "nativeG... | Hex... | Str... | En... | Im... | Ex...

```
32  salt_1 = salt;
33  v7 = 0;
34  if ( PKCS5_PBKDF2_HMAC_0((int *)a1, a4, (int)salt, (int)&v29) != 1 )
35    goto LABEL_17;
36  v25 = v6;
37  v27 = 0;
38  v8 = (void *)j_EVP_CIPHER_CTX_new();
39  v9 = j_EVP_aes_128_cbc();
40  iv_1 = v5;
41  if ( j_EVP_CipherInit_ex(v8, v9) )
42  {
43    if ( j_EVP_CipherUpdate(v8, encryptedkey, &v27, a5, 16,
44    {
45      v10 = v27;
46      if ( j_EVP_CipherUpdate(v8, &encryptedkey[v27], &v27
47      {
48        v11 = j_EVP_CipherFinal_ex(v8, &encryptedkey[v27
49        j_EVP_CIPHER_CTX_free(v8);
50        if ( v11 )
51        {
52          filehandle = fopen((const char *)dword_182D98,
53          if ( filehandle )
54          {
55            v7 = 1;
56            fputc(1, filehandle);
57            fwrite(salt_1, 1u, 0x10u, filehandle);
58            fwrite(iv_1, 1u, 0x10u, filehandle);
59            fwrite(encryptedkey, 1u, 0x20u, filehandle);
60            fclose(filehandle);
61            v13 = fopen((const char *)dword_182D98, (const char
62            if ( v13 )
63            {
64              keysize = getFileSize();
65              v16 = v15;
```

Yay, a file is being written with
char_1
salt[0x10]
iv[0x10]
encryptedkey[0x20]

File size of 0x41 in total. And there is only one file that fits : “main.key“ in the application “files“ subfolder
☺

So we need a bruteforcer “to go”

```python
import hashlib
import binascii
from Crypto.Cipher import AES
import struct
import sys

def pkcs7Verify(data,i):
    dlen=len(data)
    val = int(data[-1])
    if val > i:
        return b''
    h=int(data[-val])
    if (val!=h):
        return b''
    v = dlen - val
    return data[:v]

def main(argv):
    z=0
    for password in sys.stdin:
        if (password == ""):
            break
        password=str(password).replace('\n','')
        key=b''
        iv=b''
        data=b''
        version=b''

        with open('main.key','rb') as fr:
            version=fr.read(1)
            salt=fr.read(0x10)
            iv=fr.read(0x10)
            key=fr.read(0x20)

        aeskey = hashlib.pbkdf2_hmac('sha1',bytes(password,'utf8'),bytes(salt),10000,0x10)
        decryptor = AES.new(aeskey, AES.MODE_CBC, iv)
        dbkey = decryptor.decrypt(key)
        dbkey = pkcs7Verify(dbkey,32)
        if len(dbkey)>0:
            print ('SQLCipher key found:'+str(binascii.hexlify(dbkey))+'\nPassword found:'+str(password)+'\n')
            break
        z+=1
        if ((z%100)==0):
            print('Current password: '+str(password))
            z=1
```

In Python, just PoC. Way faster if Pyopencl and multithreading would be used ☺

To conclude

- Static reverse engineering is really time consuming and brain damaging.
- Obfuscation and encryption can make reading code really tough.
- Sometimes you have both Java and Native worlds to cope with.
- But it will give you a very deep insight.

Dynamic application reversing

Or: This is how we do if want to spend more time on beer and friends ☺

Mar. 2019

Your Con

What do we need ?

1. Emulator or Test device
   Emulator:x86, Test device:ARM

2. Debugger
   JDB, ADB, Android Studio, IDA Pro, …

or:

2. Injection Framework
   FRIDA.RE, XPosed

Wait what ?

Debugger:

Lets you step through each instruction while the app is running.

Injection Framework:

Take over functions by hooking into dynamically

Injection ?

It‘s like playing pirates. Jump on the boat, enter the boat, get the gold.

“FRIDA.re” needs two languages for that :

- Python for the User interactions
- Javascript (Duktape) for injections

Lets see some injection examples ☺

Injection on java functions

```
Java.perform(function() {
  var SQLHelper = Java.use("net.sqlcipher.database.SQLiteOpenHelper");

  if (SQLHelper.getWritableDatabase) {
    console.log("We got getWritableDatabase");
    SQLHelper.getWritableDatabase.overload.implementation = function(password) {
      console.log(password);
      return this.getWritableDatabase.overload.apply(this, arguments);
    }
  }
```

Injection on native functions

```
setImmediate(function() {
    Java.perform(function() {
        var sqlite3_key = Module.findExportByName("libsqlcipher_android.so","sqlite3_key");
        if (sqlite3_key)
        {
            Interceptor.attach(sqlite3_key, {
                onEnter: function (args)
                {
                    console.log("We got SQLCipher key");
                    var len=args[2];
                    var pw=Memory.readUtf8String(args[1],parseInt(len));
                    console.log(pw);
                },

                onLeave: function(ret)
                {
                }
            });
        }
    });
});
```

Easy mate, easy ….

To automate things, I initially modified "Appmon" http://dpnishant.github.io/appmon :

1. Start the target app, make sure adb works
2. Run appmon script on the app :

   "python appmon.py –a it.ideasolutions.kyms –p android –s scripts\Android –c"
3. Do your app-stuff
4. Run 127.0.0.1:5000 to see the results
5. Enjoy your spare time !

Easy mate, easy ….

After some months of deep research on native and java functions, backtracing callers and performance, I completely rewrote a new tool:

“Appmonitor“ …. to be released soon.

AppMonitor (c) B.Kerler 2019

Menu

Hook

Selection

- Bluetooth
- Clipboard
- Crypto
  - Cipher
  - Hash
  - Keystore
  - OpenSSL
  - PBKDF
  - PBKDF2
- Database
- FileSystem
- FlagSecure
- IPC
- Network
- Process
- Runtime
- SQLCipher
- SQLiteDatabase
- Syscall
- WebView

Un/Select all

Monitor

	Idx	Function	Caller	Data
4	3	WebView:android.webkit.WebView.evaluateJavascript	java.lang.Thread.getStackTrace(Thread.java:...	Script:(window.AFMA_ReceiveMessage || function() {})('onDefaultPositionReceived',{"x":20,"y":341,"widt...
5	4	WebView:android.webkit.WebView.evaluateJavascript	java.lang.Thread.getStackTrace(Thread.java:...	Script:(window.AFMA_ReceiveMessage || function() {})('onAdVisibilityChanged',{"isVisible":"1"});;
6	5	WebView:android.webkit.WebView.evaluateJavascript	java.lang.Thread.getStackTrace(Thread.java:...	Script:(window.AFMA_ReceiveMessage || function() {})('onScreenInfoChanged',{"width":360,"height":640...
7	6	WebView:android.webkit.WebView.evaluateJavascript	java.lang.Thread.getStackTrace(Thread.java:...	Script:(window.AFMA_ReceiveMessage || function() {})('onDefaultPositionReceived',{"x":20,"y":341,"widt...
8	7	WebView:android.webkit.WebView.evaluateJavascript	java.lang.Thread.getStackTrace(Thread.java:...	Script:(window.AFMA_ReceiveMessage || function() {})('onAdVisibilityChanged',{"isVisible":"1"});;
9	8	fopen:libkyms-jni.so.fopen		Options:Filename:/data/user/0/it.ideasolutions.kyms/files/main.key;Mode:rb;;
10	9	fread:libkyms-jni.so.fread		Data:Size:41;Data:01eda89889b5d69e3e26d9c120b66daadc0cb4d8879150f8cbb3cbb1e0572316b63c09...
11	10	EVP_sha1:base.odex.EVP_sha1	{'address': '0xd900b62f', 'name': '0x3a62f', '...	SHA1:Init;
12	11	PKCS5_PBKDF2_HMAC:base.odex.PKCS5_PBKDF2_HMAC	{'address': '0xcbf8508f', 'name': None, 'mod...	Arguments:Password:70617373776f7264;Salt:eda89889b5d69e3e26d9c120b66daadc;Iter:10000;Len:16;
13	12	EVP_CipherInit_ex:base.odex.EVP_CipherInit_ex	{'address': '0xffc3677c', 'name': None, 'mod...	InitOptions:Algo:419;Name:AES-128-CBC;Key:27c741b53724bd5ec6f4b7809b575299;Iv:0cb4d8879150f...
14	13	EVP_CipherUpdate:base.odex.EVP_CipherUpdate	{'address': '0x1c', 'name': None, 'moduleNa...	Input [Size:20]:3c09d250eae4ff85b62b49f2b8277c7d79d7e0657b85143bd03318f1b3160e52;Output [Siz...
15	14	EVP_CipherFinal_ex:base.odex.EVP_CipherFinal_ex	{'address': '0xb', 'name': None, 'moduleNam...	Output [Size:3]:232a23;

Save process log

Select Process: it.ideasolutions.kyms

Run Monitor

Console

```
We got getReadableDatabase
We got SQLCipher
Hook: EVP_CipherInit_ex in: libkyms-jni.so at: 0xd9097554
Hook: EVP_CipherUpdate in: libkyms-jni.so at: 0xd9097220
Hook: EVP_CipherFinal_ex in: libkyms-jni.so at: 0xd909744c
Hook: EVP_sha1 in: libkyms-jni.so at: 0xd90984c0
Hook: PKCS5_PBKDF2_HMAC in: libkyms-jni.so at: 0xd90988e0
We hooked PKCS5_PBKDF2_HMAC in: libkyms-jni.so
We hooked fopen in: libkyms-jni.so
We hooked fwrite in: libkyms-jni.so
We hooked fread in: libkyms-jni.so
We hooked recv
We hooked send
```

Save console log

DEMO time !!!

On our target app ☺

Recommendations :

- Use hidden root (reverse shell), not su or magisk, a lot apps tend to detect these, same applies for emulators

- Grab a current android device, unlock it (not Huawei).

- For creating a ramdisk with hidden root, you may use: https://github.com/bkerler/android_universal

Recommendations :

- Use dwarf or frick !!!!!!
  https://github.com/iGio90/Dwarf

That’s it folks !

Thanks for listening