



Security in IoT Ecosystem

Module 7

Smart Socket Pentest
Part III

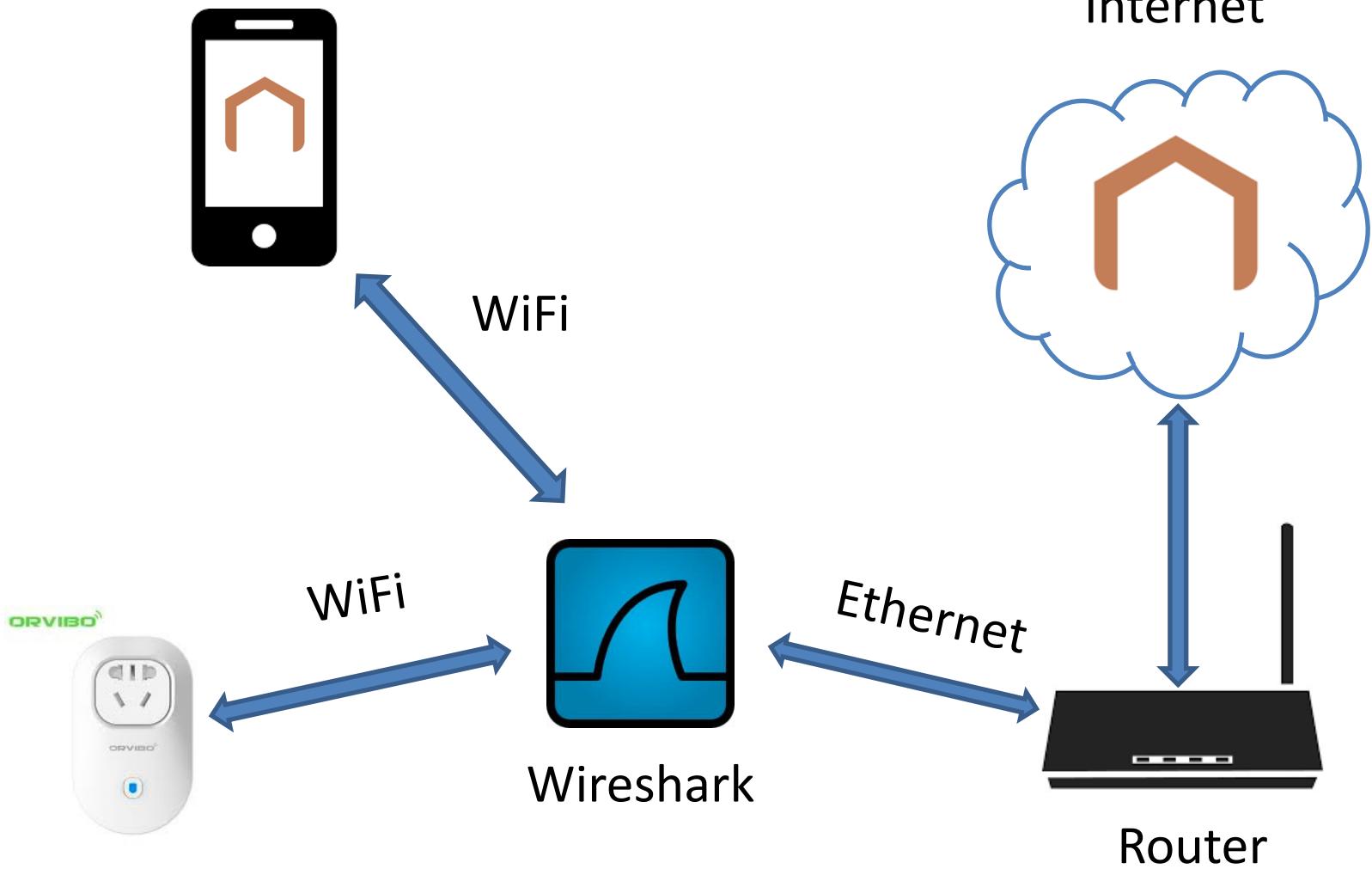
Prof.: Joaquín Recas



Smart Socket Initial Setup

- 1.** Initial Setup
- 2.** Capture Traffic
- 3.** Traffic analysis
- 4.** Apk Analysis

Study communications:





Information we know

- IP numbers:
 - Orvibo server, Raspberry Pi, Smartphone & Smartsocket
- There are messages with payload between the Smartplug and the Orvibo server
 - Encrypted content!



Next steps

- Can we decrypt the messages?
 - We need method and encryption key
- Where can we find the key?
 - Inside the device
 - On the Orvibo server
 - **In the HomeMate App**

JADX

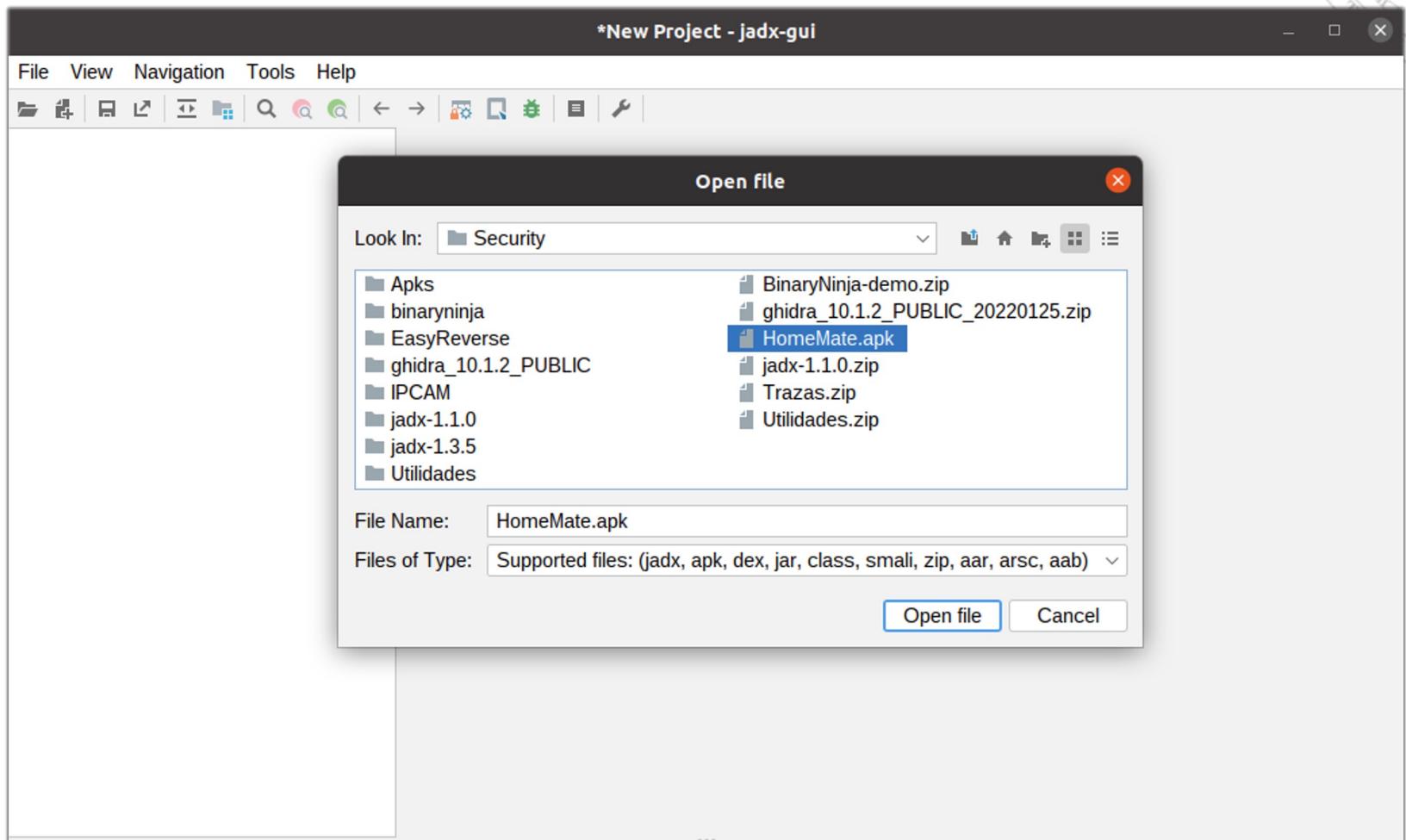


- Dex ([Dalvik Executable](#)) to Java decompiler
 - Command line and GUI tools for produce Java source code from Android **Dex** and **Apk** files
- Main features:
 - Decompile Dalvik bytecode to java classes from **APK**, **dex**, **aar** and **zip** files
 - Decode *AndroidManifest.xml* and other resources from *resources.arsc*
 - Deobfuscator included
- **jadx-gui** features:
 - View **decompiled code** with highlighted syntax
 - Jump to declaration
 - Find usage
 - Full text search

<https://github.com/skylot/jadx>



jadx-gui





jadx-gui: HomeMate

*HomeMate - jadx-gui

File View Navigation Tools Help

HomeMate.apk

Source code

- android
 - arch
 - core.internal
 - FastSafeIterableMap

```

package android.arch.core.internal;

@android.support.annotation.RestrictTo({android.support.annotation.RestrictTo.Scope.LIBRARY_GROUP})
public class FastSafeIterableMap {
    private java.util.HashMap<K, SafeIterableMap$Entry<K, V>> mHashMap;
    /* loaded from: classes.dex */
    public FastSafeIterableMap() {
        r1 = this;
        r1.<init>();
        java.util.HashMap<K, android.arch.core.internal.SafeIterableMap$Entry<K, V>> r0 = r1.mHashMap;
        r0.<init>();
        r1.mHashMap = r0;
        return r1;
    }

    @Override // android.arch.core.internal.SafeIterableMap
    protected android.util.ObjectIterator<V> iterator() {
        r1 = this;
        java.util.HashMap<K, android.arch.core.internal.SafeIterableMap$Entry<K, V>> r0 = r1.mHashMap;
        java.lang.Object r0 = r0.get(r2);
        android.arch.core.internal.SafeIterableMap$Entry r0 = (android.arch.core.internal.SafeIterableMap.Entry)
        return r0;
    }

    @Override // android.arch.core.internal.SafeIterableMap
    public V putIfAbsent(@android.support.annotation.NonNull K r4, @android.support.annotation.NonNull V r5) {
        r3 = this;
        android.arch.core.internal.SafeIterableMap$Entry r0 = r3.get(r4);
        if (r0 == 0) goto L9
        V r1 = r0.mValue
        L8:
        return r1
    L9:
}

```

Issues: 1 errors

Code Simple Fallback Split view

Too much information!!

What are we looking for??



jadx-gui: Search

The screenshot shows the jadx-gui interface for analyzing the HomeMate.apk application. A search dialog is open, displaying the results of a search for the word "import". The search options include "Case insensitive" checked, "Regex" unchecked, and "Active tab only" unchecked. The search results pane shows zero results found. In the bottom right, a blue callout box contains the text "It will take some time...". The bottom status bar indicates that the application is "Decompiling..." at 23% completion, with 0 errors and 201 warnings.

*HomeMate - jadx-gui

File View Navigation Tools Help

Source code

Search for text: import

Search definitions of:

Class Method Field Code Resource Comments

Search options:

Case insensitive Regex Active tab only

Node Code

<- > Showing results 0 to 0 of 0

Keep open Decompling: Open Cancel

Issues: 0 errors 201 warnings

Decompiling... 23%

Code Small Simple Fallback Split view

otation.RestrictTo.Scope.LIBRARY_GROUP})

.core.internal.SafeIterableMap<K, V> {

.SafeIterableMap.Entry<K, V>> mHashMap = new java.util.H

try<K, V> get(K r2) {

.SafeIterableMap\$Entry<K, V>> r0 = r1.mHashMap

y r0 = (android.arch.core.internal.SafeIterableMap.Entry

L8: r3 = this;

android.arch.core.internal.SafeIterableMap\$Entry r0 = r3.get(r4)

if (r0 == 0) goto L9

V r1 = r0.mValue

L9: return r1

L9:



jadx-gui: Search

The screenshot shows the jadx-gui interface. On the left, there's a tree view of an APK file named 'HomeMate.apk' with various source code packages like 'Source code', 'android', 'arch', and 'core'. A search dialog is open in the center, titled 'Text search: import', with the search term 'import' entered. Below the search bar are 'Search definitions of:' checkboxes (Class, Method, Field, Resource, Comments) and 'Search options:' checkboxes (Case insensitive, Regex, Active tab only). The 'Case insensitive' checkbox is checked. A message box in the center says 'Jadx is running low on memory. If you want all classes to be indexed, increase VM RAM.' On the right, there's a code editor window showing Java-like pseudocode. At the bottom, there are tabs for 'Code', 'Smali', 'Simple', 'Fallback', and 'Split view', with 'Code' selected. The status bar at the bottom shows 'Issues: 68 errors, 3661 warnings', 'Code', 'Smali', 'Simple', 'Fallback', and 'Split view' buttons, and 'JADX memory usage: 0.94 GB of 2.69 GB'.

Increase VM RAM to 6GB:

- Turn off
- Select the VM
- Go to settings-> System
- Increase base memory



jadx-gui: Search

A screenshot of the jadx-gui application interface. The main window shows the file structure of an APK file named "HomeMate.apk". The "Source code" section is expanded, displaying various Java packages and classes. A search dialog box is overlaid on the interface, containing fields for "Search for text:", "Search definitions of:" (with "Code" checked), "Search options:" (with "Case insensitive" checked), and a "Node" list. At the bottom of the search dialog are buttons for navigation and a checkbox for "Keep open". The status bar at the bottom of the application shows "Issues: 70 errors 3844 warnings" and "JAD MEMORY USAGE: 1.01 GB of 3.97 GB".

Possible searches:

- Password
- Encryption methods
 - Encrypt/Decrypt
 - AES
- On / Off sequence
- Any ideas?



jadx-gui : Password

*HomeMate - jadx-gui

File View Navigation Tools Help

Source code

Search for text: Password

Search definitions of: Method Field Code Resource Comments

Search options: Case insensitive Regex Active tab only

Node

```
m com.orvibo.homemate.view.custom.inputpassword.GridPasswordView.setPa...
m com.videogo.camera.ShareCameraItem.setPassword(String) void
m com.orvibo.hOMEMATE.core.ProcessPayload.modifyPassword(int, long)
m com.orvibo.homemate.api.UserApi.resetPassword(String, BaseResultLis...
m com.danale.video.sdk.platform.entity.Session.resetPassword(int, String)
m com.orvibo.homemate.model.ResetPassword.onEventMainThread(ResetPass...
m com.orvibo.homemate.view.custom.inputpassword.PasswordView.getPa...
m com.orvibo.homemate.view.custom.inputpassword.GridPasswordView.setPa...
m org.apache.http.auth.NTCredentials.getPassword() String
m com.danale.video.sdk.platform.entity.Session.resetPassword(int, String)
m com.orvibo.hOMEMATE.bo.CameraInfo.setPassword(String) void
m okhttp3.HttpUrl.setPassword() String
m com.videogo.util.LocalInfo.getPassword() String
m com.danale.video.sdk.platform.result.ModifyPasswordResult.ModifyPa...
m org.apache.http.auth.UsernamePasswordCredentials.getUsername()
m com.orvibo.homemate.model.ResetPassword.onResetPasswordResult(l...
m org.apache.commons.httpclient.HttpURL.setRawPassword(char[])
m com.orvibo.homemate.view.custom.inputpassword.GridPasswordView.setPa...
m com.orvibo.homemate.view.custom.inputpassword.PasswordView.setPa...
```

Code

```
void setPasswordVisibility(boolean)
void setPassword(String)
void modifyPassword(int, long, JSONObject)
void resetPassword(String, BaseResultListener)
boolean forgetPassword(int, String, String, PlatformResultHandler)
void onEventMainThread(ResetPasswordEvent)
String getPassword()
boolean getPasswordVisibility()
String getPassword()
boolean forgetPassword(int, String, PlatformResultHandler)
void setPassword(String)
String getPassword()
String getPassword()
void ModifyPasswordResult(int)
void UsernamePasswordCredentials(String, String)
void onResetPasswordResult(long, int)
void setRawPassword(char[])
void clearPassword()
void setPasswordType(PasswordType)
```

<- > Showing results 1 to 100 of 195

Keep open

Open Cancel

Issues: 70 errors 3844 warnings Code Small Simple Fallback Split view JADY memory usage: 1.14 GB of 3.97 GB



jadx-gui: AES

*HomeMate - jadx-gui

File View Navigation Tools Help

HomeMate.apk AESCrypt x

Text search: aes

Search for text: aes

Search definitions of: Class Method Field Code Resource Comments

Search options: Case insensitive Regex Active tab only

Node	Code
m com.ali.auth.third.core.storage.aes.AESCrypt.AESCrypt() void	void AESCrypt()
m com.ali.auth.third.ui.support BaseActivityResultHandler.onTaeSDKActivity	void onTaeSDKActivity(int, int, Intent, BaseWebViewActivity, Map<C
m com.ali.auth.third.login.handler.LoginActivityResultHandler.onTae	void onTaeSDKActivity(int, int, Intent, BaseWebViewActivity, Map<C
f com.orbyo.homenet.ap.ApConstant.ENCTKIPAES String	String ENCTKIPAES
f com.alibaba.wireless.security.open.staticdataencrypt.IStaticDataE	int OPEN_ENUM_CIPHER_AES256
f okhttp3.CipherSuite.TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 CipherS	CipherSuite TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
f okhttp3.CipherSuite.TLS_DHE_RSA_WITH_AES_256_CBC_SHA CipherSuite	CipherSuite TLS_DHE_RSA_WITH_AES_256_CBC_SHA
f com.ali.auth.third.core.storage.aes.AESCrypt.AES_MODE String	String AES_MODE
f okhttp3.CipherSuite.TLS_DHE_DSS_WITH_AES_256_CBC_SHA256 CipherS	CipherSuite TLS_DHE_DSS_WITH_AES_256_CBC_SHA256
f okhttp3.CipherSuite.TLS_DH_anon_WITH_AES_256_CBC_SHA CipherSuite	CipherSuite TLS_DH_anon_WITH_AES_256_CBC_SHA
f com.alibaba.sdk.android.oss.model.ObjectMetadata.AES_256_SERVER_S	String AES_256_SERVER_SIDE_ENCRYPTION
f com.danale.video.jni.DtmfAudioCodec.WIFI_ENCTYPE_WPA2_AES int	int WIFI_ENCTYPE_WPA2_AES
f okhttp3.CipherSuite.TLS_ECDH_RSA_WITH_AES_256_CBC_SHA CipherSuite	CipherSuite TLS_ECDH_RSA_WITH_AES_256_CBC_SHA
f com.alibaba.wireless.security.open.staticdataencrypt.IStaticDataE	int OPEN_ENUM_CIPHER_AES192
f okhttp3.CipherSuite.TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA CipherSu	CipherSuite TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
f com.videogo.exception.ErrorCode.ERROR_CAS_AES_DECRYPT_FAILED int	int ERROR_CAS_AES_DECRYPT_FAILED
f okhttp3.CipherSuite.TLS_PSK_WITH_AES_128_CBC_SHA CipherSuite	CipherSuite TLS_PSK_WITH_AES_128_CBC_SHA
f com.alibaba.wireless.security.open.staticdataencrypt.IStaticDataE	int OPEN_ENUM_CIPHER_AES128
f okhttp3.CipherSuite.TLS_DH_anon_WITH_AES_256_GCM_SHA384 CipherS	CipherSuite TLS_DH_anon_WITH_AES_256_GCM_SHA384

< > Showing results 1 to 100 of 510

Keep open

Issues: 70 errors 3844 warnings Code Simple Fallback Split view Open Cancel

JADY memory usage: 1.07 GB of 3.97 GB



com.orvibo.homemate.ap.ApConstant

*HomeMate - jadx-gui

File View Navigation Tools Help

Issues: 70 errors 3844 warnings Code Smali Simple Fallback Split view

JAD memory usage: 1.05 GB of 3.97 GB

ApConstant

```

1 package com.orvibo.
2
3 /* loaded from: class in /data/app/com.orvibo.homemate-1.apk */
4 public class ApConstant {
5     public static final String AUTH_OPEN = "OPEN";
6     public static final String AUTH_SHARED = "SHARED";
7     public static final String AUTH_WPA2PSK = "WPA2PSK";
8     public static final String AUTH_WPAPSK = "WPAPSK";
9     public static final String AUTH_WPAPSKWPA2PSK = "WPAPSKWPA2PSK";
10    public static final String BATTERY_VALUE = "batteryValue";
11    public static final String CMD = "cmd";
12    public static final int CMD_GET_DEVICE = 79;
13    public static final int CMD_RECEIVE_MEASURE_DATA = 143;
14    public static final int CMD_REMAIN_TIME = 158;
15    public static final int CMD_REQUEST_MEASURE = 160;
16    public static final int CMD_SCAN_WIFI = 80;
17    public static final int CMD_SET_WIFI = 81;
18    public static final String CMD_TYPE = "cmdType";
19    public static final String CO_CONCENTRATION = "coConcentration";
20    public static final String DEVICE_NAME = "deviceName";
21    public static final String ENC = "enc";
22    public static final String ENC_AES = "AES";
23    public static final String ENC_NONE = "NONE";
24    public static final String ENC_TKIP = "TKIP";
25    public static final String ENC_TKIPAES = "TKIPAES";
26    public static final String ENC_WEP = "WEP";
27    public static final String ENTITYFY = "EntityWifi";
28    public static final String ENTITY_DEVICE = "entityDevice";
29    public static final String ENTITY_WIFI = "entityWifi";
30    public static final String HARDWARE_VERSION = "hardwareVersion".
31
32
33
34

```

Tons of useful information!!

Code for Initial pairing



com.orvibo.homemate.ap.ApConstant

Encrypt/Decrypt byte arrays

File View Navigation Tools Help

HomeMate.apk

Source code

- android
- butterknife
- c.keeu.homematesecurity
- cn.colourlife.oauthlogin
- com
- cz.msebera
- de.greenrobot.event
- homemate.orvibo.com.securitylibrary
- BuildConfig
- SecurityAes
- io.card.payment
- javax.jmdns
- kotlin
- mtopsdk
- net.sourceforge.pinyin4j
- no.nordicsemi.android.support.v18.scanner
- okhttp3
- okio
- org
- pl

Resources

APK signature

Summary

*HomeM... SecurityAes BuildCo...

```

package homemate.orvibo.com.securitylibrary;

/* loaded from: classes3.dex */
8 public class SecurityAes {
    private static native String[] createPassword(byte[] bArr);

    private static native byte[] createSecurityKey(byte[] bArr);

    private static native byte[] decryptByte(byte[] bArr, int i, boolean z, String str);

    private static native byte[] decryptByteKey(byte[] bArr, int i, byte[] bArr2);

    private static native byte[] encryptByte(byte[] bArr, int i, boolean z, String str);

    private static native byte[] encryptByteKey(byte[] bArr, int i, byte[] bArr2);

    private static native boolean nativeIsPk(String str);

    static {
        System.loadLibrary("HomeMate_Security");
    }

    public static byte[] encrypt(byte[] data, String key, boolean isPk) {
        if (data == null || data.length == 0) {
            return null;
        }
        if (key == null) {
            key = "";
        }
        return encryptByte(data, data.length, isPk, key);
    }

    public static byte[] decrypt(byte[] data, String key, boolean isPk) {
        if (data == null || data.length == 0) {
    
```

Issues: 70 errors 3844 warnings

Code Smali Simple Fallback Split view

JADX memory usage: 1.12 GB of 3.97 GB



com.orvibo.homemate.ap.ApConstant

Sourcue code is not available!!

```

private static byte[] encryptByte(byte[] data, String key, boolean isPk) {
    if (data == null || data.length == 0) {
        return null;
    }
    if (key == null) {
        key = "";
    }
    return encryptByte(data, data.length, isPk, key);
}

public static byte[] decryptByte(byte[] data, String key, boolean isPk) {
    if (data == null || data.length == 0) {
        return null;
    }
    if (key == null) {
        key = "";
    }
    return decryptByte(data, data.length, isPk, key);
}

public static byte[] encryptKey(byte[] data, byte[] key) {
    if (data == null || data.length == 0) {
        return null;
    }
    return encryptByteKey(data, data.length, key);
}

```

Issues: 70 errors 3844 warnings

Code Smali Simple Fallback Split view

JADX memory usage: 1.14 GB of 3.97 GB



Looking for decryptByte

```
● iot@ubuntu: ~/Desktop/HomeMate/homemate
File Edit View Search Terminal Help
iot@ubuntu:~/Desktop/HomeMate/homemate$ rgrep decryptByte
Binary file lib/armeabi-v7a/libHomeMate_Security.so matches
Binary file lib/armeabi-v7a/libweibosdkcore.so matches
Binary file lib/arm64-v8a/libHomeMate_Security.so matches
Binary file lib/arm64-v8a/libweibosdkcore.so matches
Binary file classes4.dex matches
iot@ubuntu:~/Desktop/HomeMate/homemate$ █
```

We find it in a binary 😭



Binary Ninja

- Interactive disassembler, decompiler, and binary analysis platform for reverse engineers, malware analysts, vulnerability researchers, and software developers that runs on Windows, macOS, Linux.

Disassemble

Disassemble executables and libraries from multiple formats, platforms, and architectures.

Decompile

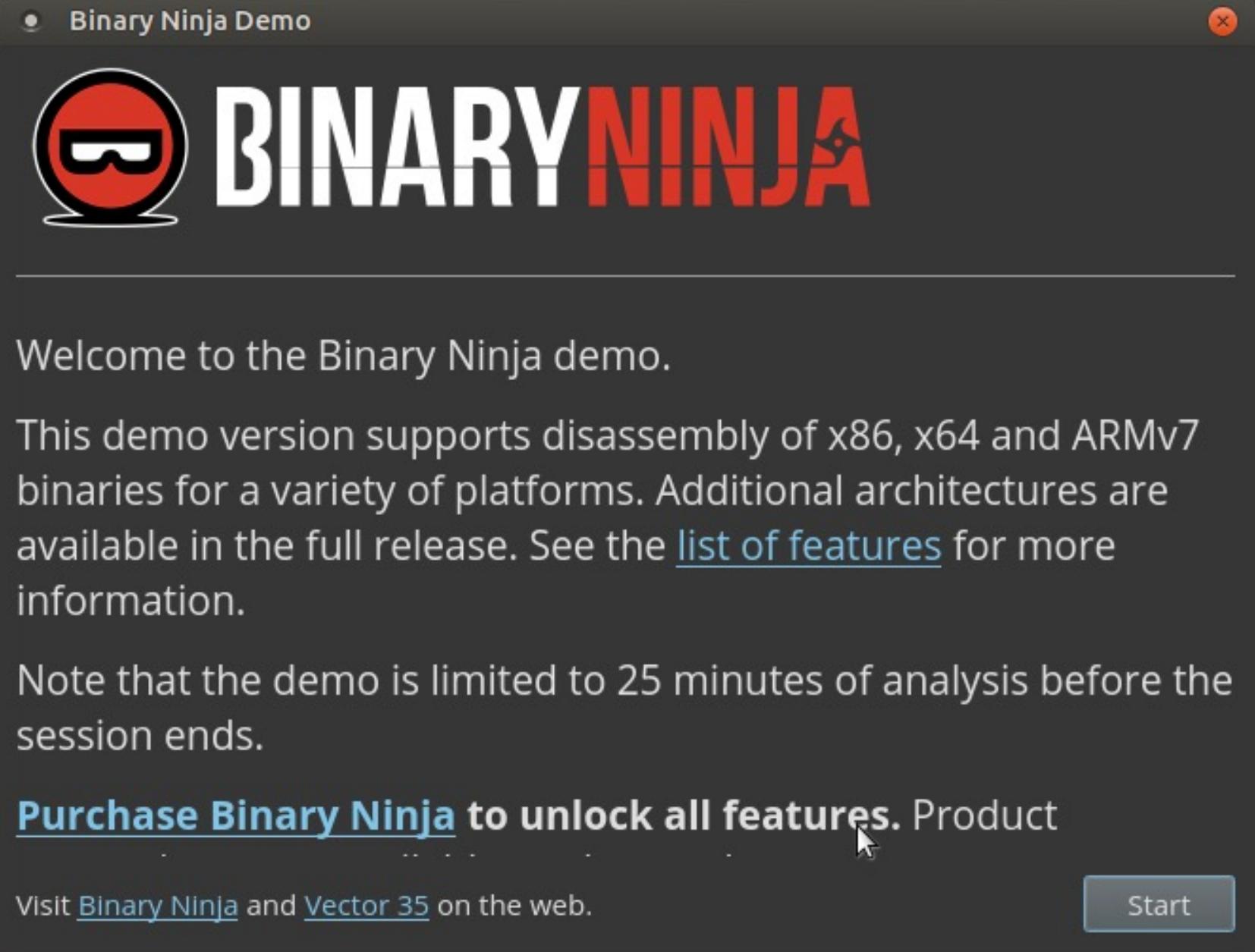
Decompile code to C or BNIL for any supported architecture - including your own

Analyze

Visualize control flow and navigate through cross-references interactively.

Annotate

Name variables and functions, apply types, create structures, and add comments.



The image shows a screenshot of the Binary Ninja demo application window. The title bar reads "Binary Ninja Demo". The main content area features the "BINARYNINJA" logo, which consists of the word "BINARY" in white and "NINJA" in red, with a small black icon of a ninja wearing sunglasses integrated into the letter "I". Below the logo is a red circular icon containing a white silhouette of a ninja wearing sunglasses. The text "Welcome to the Binary Ninja demo." is displayed, followed by a detailed description of the demo's capabilities and a link to the full release features. A note about the 25-minute analysis limit is also present. At the bottom, there is a call to action to purchase the full product, along with links to the Binary Ninja and Vector 35 websites, and a "Start" button.

Binary Ninja Demo

 **BINARYNINJA**

Welcome to the Binary Ninja demo.

This demo version supports disassembly of x86, x64 and ARMv7 binaries for a variety of platforms. Additional architectures are available in the full release. See the [list of features](#) for more information.

Note that the demo is limited to 25 minutes of analysis before the session ends.

[Purchase Binary Ninja to unlock all features.](#) Product

Visit [Binary Ninja](#) and [Vector 35](#) on the web.

[Start](#)

Binary Ninja: dedryptByte



libHomeMate_Security.so — Binary Ninja

File Edit View Tools Window Help

Cross References

Disassembly

```
int32_t
Java_homateap_orvibo_com_securitylibrary_SecurityAes
(int32_t* arg1, int32_t arg2,
int32_t arg3, int32_t arg4, int32_t arg5)
```

Tags

Bookmarks Tags Tag Types

Location Preview

Symbols

`__cxa_finalize`
`raise`
`sub_1bb8`
Java_homateap_orvibo_com_securitylibrary_SecurityAes_encryptByte
Java_homateap_orvibo_com_securitylibrary_SecurityAes_decryptByte
Java_homateap_orvibo_com_securitylibrary_SecurityAes_nativeIsPk
Java_homateap_orvibo_com_securitylibrary_SecurityAes_encryptByteKey
Java_homateap_orvibo_com_securitylibrary_SecurityAes_decryptByteKey
Java_homateap_orvibo_com_securitylibrary_SecurityAes_createSecurityKey
Java_homateap_orvibo_com_securitylibrary_SecurityAes_createPassword

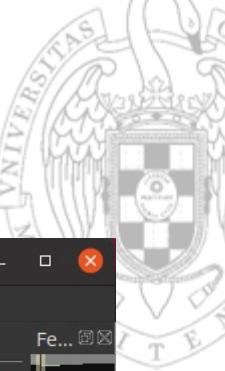
AesInit
AesDestroy
AesEncrypt
AesDecrypt
Cipher
InvCipher
AesEncryptEx
sub_2e94
AesDecryptEx

Java_homateap_orvibo_com...itylibrary_SecurityAes_decryptByteKey:

```
push {r4, r5, r6, r7, lr} {var_4} {__saved_r7} {__saved_r6} {__s...
add r7, sp, #0xc {__saved_r7}
sub sp, #0x24
push {r3} {var_3c}
pop {r4} {var_3c}
push {r2} {var_3c_1}
pop {r1} {var_3c_1}
push {r0} {var_3c_2}
pop {r5} {var_3c_2}
movs r0, #0x17
lsls r6, r0, #5
ldr r0, [r5]
ldr r3, [r0, r6]
movs r2, #
push {r5} {var_3c_3}
pop {r0} {var_3c_3}
str r1, [sp, #0x18] {var_20}
blx r3
str r0, [sp, #0x20] {var_18}
ldr r1, [sp, #0x38] {arg5}
cmp r1, #
str r1, [sp, #0x14] {var_24}
beq #0x1fec
```

Selection: 0x1f84 to 0x1f86 (0x2 bytes) ELF ▾ Graph ▾ Options ▾

Binary Ninja: dedryptByte



libHomeMate_Security.so — Binary Ninja

Cross References libHome...rity.so (ELF Graph)

```

int32_t Java_homateap_orvibo_com_securitylibrary_SecurityAes_decryptByteKey( Disassembly
    int32_t* arg1, int32_t arg2, int32_t arg3, int32_t arg4, int32_t arg5)
{
    movs    r2, #0
    push    {r5} {var_3c_3}
    pop     {r0} {var_3c_3}
    str     r1, [sp, #0x18] {var_20}
    blx    r3
    str     r0, [sp, #0x20] {var_18}
    ldr     r1, [sp, #0x38] {arg5}
    cmp     r1, #0
    str     r1, [sp, #0x14] {var_24}
    beq    #0x1fec
}

movs    r1, #1
push    {r4} {var_3c_10}
pop     {r0} {var_3c_10}
bl     #calloc
ldr     r1, [pc, #0x9c] {data_2094}
add     r1, pc {pkKey@GOT}
ldr     r1, [r1] {pkKey@GOT}
ldr     r6, [r1]
movs    r2, #0x10

movs    r0, #0xab
lsls    r0, r0, #2
ldr     r2, [r5]
ldr     r2, [r2, r0]
push    {r5} {var_3c_4}
pop     {r0} {var_3c_4}
str     r4, [sp, #0x1c] {var_1c_1}
push    {r1} {var_3c_5}
pop     {r4} {var_3c_5}
blx    r2
str     r0, [sp, #0x10] {var_28_1}
ldr     r0, [r5]
ldr     r3, [r0, r6]
movs    r2, #0
push    {r5} {var_3c_6}
pop     {r0} {var_3c_6}
push    {r4} {var_3c_7}
pop     {r1} {var_3c_7}

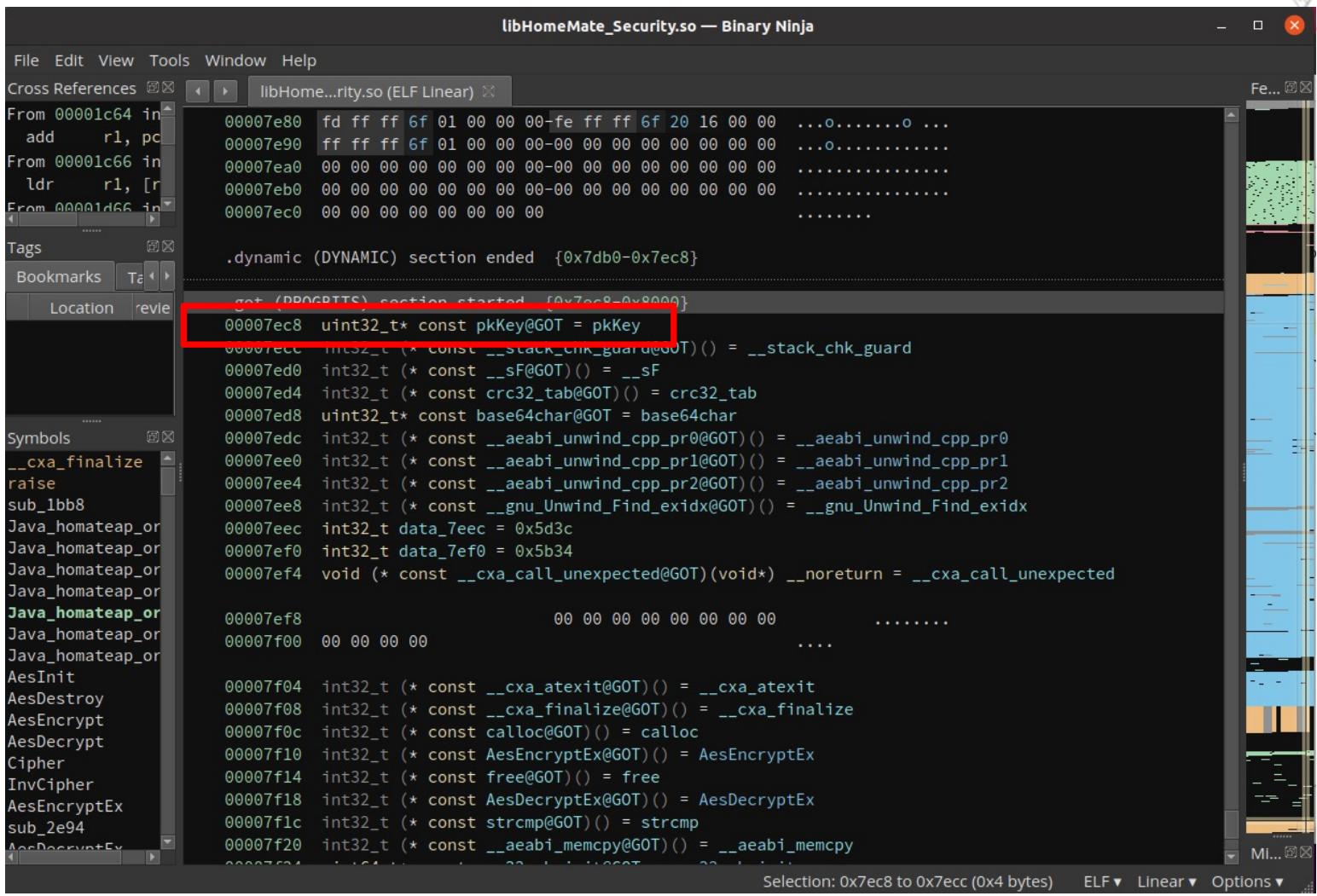
```

Symbols

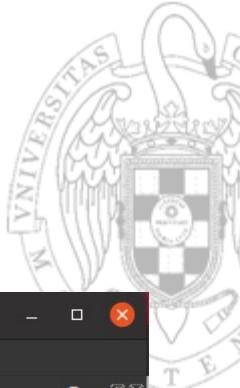
- __cxa_finalize
- raise
- sub_1bb8
- Java_homateap_or
- Java_homateap_or
- Java_homateap_or
- Java_homateap_or
- Java_homateap_or**
- Java_homateap_or
- Java_homateap_or
- AesInit
- AesDestroy
- AesEncrypt
- AesDecrypt
- Cipher
- InvCipher
- AesEncryptEx
- sub_2e94
- AesDecryptEx

Selection: 0x1f84 to 0x1f86 (0x2 bytes) ELF ▾ Graph ▾ Options ▾

Binary Ninja: pkKey



Binary Ninja: pkKey



libHomeMate_Security.so — Binary Ninja

File Edit View Tools Window Help

Cross References libHome...rity.so (ELF Linear)

Tags Bookmarks Location review

00007ffc int32_t (* const _Unwind_VRS_Pop@GOT)() = _Unwind_VRS_Pop

.got (PROGBITS) section ended {0x7ec8-0x8000}

.data (PROGBITS) section started {0x8000-0x800c}

00008000 data_8000:

00008000 00 00 00 00

....

00008004 uint32_t pkKey = 0x5d3c

00008008 uint32_t base64char = 0xdad0c

.data (PROGBITS) section ended {0x8000-0x800c}

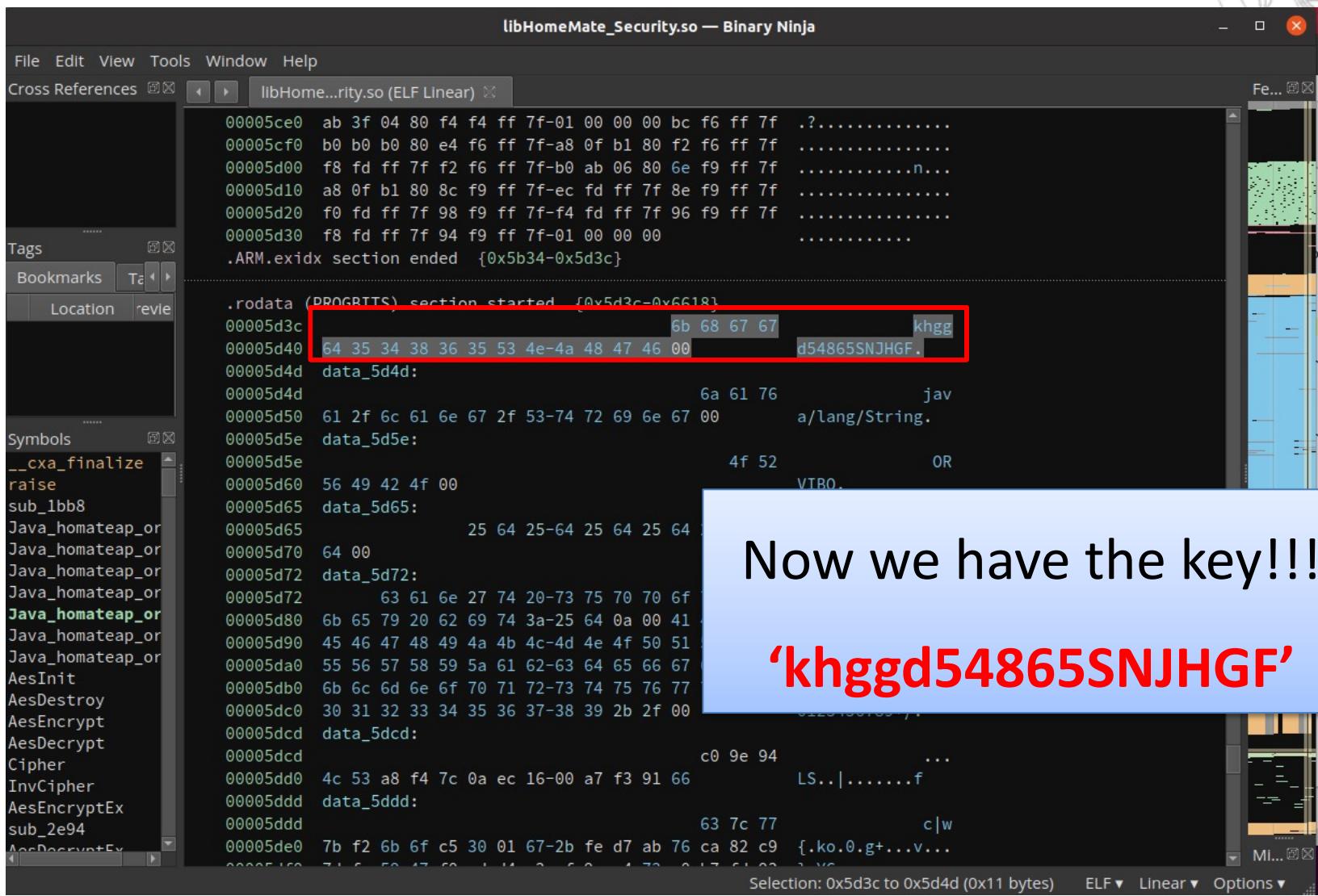
Symbols

--cxa_finalize
raise
sub_1bb8
Java_homateap_or
AesInit
AesDestroy
AesEncrypt
AesDecrypt
Cipher
InvCipher
AesEncryptEx
sub_2e94
AesDecryptEx

00008010 extern __aeabi_memclr
00008014 extern __aeabi_memclr4
00008018 extern __aeabi_memcpy
0000801c extern __aeabi_memset
00008020 extern __cxa_atexit
00008024 extern __cxa_begin_cleanup
00008028 extern void __cxa_call_unexpected(void*) __noreturn
0000802c extern __cxa_finalize
00008030 extern __cxa_type_match
00008034 extern __gnu_Unwind_Find_exidx
00008038 extern __sF
0000803c extern void __stack_chk_fail() __noreturn
00008040 extern __stack_chk_guard
00008044 extern void abort() __noreturn
00008048 extern calloc
0000804c extern fprintf
00008050 extern free
00008054 extern lrand48

Selection: 0x8004 to 0x8008 (0x4 bytes) ELF ▾ Linear ▾ Options ▾

Binary Ninja: pkKey



Now we have the key!!!

'khggd54865SNJHGF'

Binary Ninja: AES-ECB



... and the method: AES ECB

The screenshot shows the Binary Ninja interface for the file `libHomeMate_Security.so`. The assembly view displays the `AES_ECB_encrypt` function:

```
int32_t AES_ECB_encrypt(...)
```

```
push    {r4, r5, r6, r7, lr} {var_4} {__saved_r7} {__saved_r6} {__saved_r5} {__saved_r4}
sub     sp, #0x2c
movs   r4, #0
str    r1, [sp, #0x24] {var_1c}
str    r0, [sp, #8] {var_38}
push   {r0} {var_44}
pop    {r3} {var_44}
str    r4, [sp, #0x20] {var_20} {0x0}
```

The symbols pane shows several AES-related symbols, with `AES_ECB_encrypt` highlighted and enclosed in a red box:

- `AES_init_ctx`
- `AES_ECB_encrypt` (highlighted)
- `AES_ECB_decrypt`
- `base64_encode`
- `num_strchr`
- `base64_decode`
- `base64_get_encode_len`
- `base64_get_decode_len`
- `__aeabi_uidiv`
- `sub_4710`
- `__aeabi_uidivmod`
- `__divs13`
- `sub_47a4`
- `__aeabi_idivmod`
- `__aeabi_ldiv0`
- `sub_4860`
- `sub_4876`
- `sub_48e4`
- `sub_4914`

The assembly graph shows three distinct blocks of code connected by arrows:

- The first block contains the `AES_ECB_encrypt` assembly shown above.
- The second block contains the following assembly:

```
ldr    r0, [sp, #0x20] {var_20}
mvns r2, r0
movs r5, #4
str    r1, [sp, #0x28] {var_18_1}
push   {r1} {var_44_1}
pop    {r6} {var_44_1}
push   {r3} {var_44_2}
pop    {r7} {var_44_2}
```

- The third block contains the following assembly:

```
ldrb  r0, [r7]
ldrb  r1, [r6]
eors r1, r0
strb r1, [r6]
adds r5, r5, r2
adds r6, #1
adds r7, #1
cmp   r5, #0
```

At the bottom of the interface, the status bar shows: Selection: 0x4020 to 0x4022 (0x2 bytes) ELF▼ Graph▼ Options▼



Next steps

- Decrypt and understand the messages
 - Get the payload from the On/Off sequence
 - Use python to decrypt its content
 - Try to understand the logic
 - Take control of the device