
jtsec
BEYOND IT SECURITY

ASCT

Android Security Configuration Tester

Introducción

- Android Security **Configuration** Tester
- Certificaciones ligeras
- Inspirado en certificaciones Common Criteria

7.6 CATEGORÍA: PROTECCIÓN DE EQUIPOS Y SERVICIOS

7.6.1. FAMILIA: DISPOSITIVOS MÓVILES

GALAXY Note 8 (SM-N950F)

Versión	Android 7.1.1 Kernel 4.4.13 Compilación NRD90M
Familia	Dispositivos móviles
Fabricante	Samsung Electronics
Clasificación	ENS ALTO
Fecha Inclusión	01/06/2018
Revisión de Validez	30/11/2020

Descripción

Galaxy Note 8 es un Smartphone Samsung con Sistema operativo Android. Destaca por su pantalla de 6,3''. En su interior cuenta con procesador de 10nm, almacenamiento interno de 64GB que puede extenderse hasta los 256GB a través de microSD, y RAM de 6GB. Todo ello protegido con su plataforma Samsung Knox, certificación IP68.

Observaciones

Procedimiento de empleo seguro: CCN-STIC 1601 Configuración Segura Samsung Galaxy S8/S8+

Certificaciones ligeras

- ✓ https://www.jtsec.es/es/entrada-blog/18/ccn-publica-la-metodologia-lince-para-evaluacion-de-productos-it

ASCT

- 1. Análisis de aplicaciones
- 2. Análisis del sistema de ficheros
- 3. Kernel Module Signing
- 4. Security-Enhanced Linux
- 5. Análisis de procesos
- 6. Comprobación del cifrado
- 7. Address Space Layout Randomization
- 8. Android Verified Boot

- 1. Aplicaciones instaladas

- 3. Protecciones de Linux

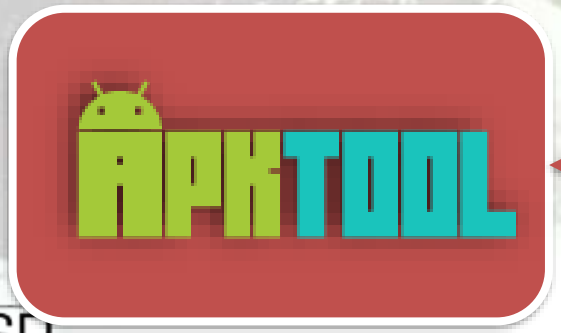
- 2. Sistema de ficheros

- 4. Estado del cifrado

- 6. Android Verified Boot

- 5. ASLR

Análisis de aplicaciones instaladas



```
#### SRC-IG-0100: Extracción de aplicaciones ####

Extrayendo aplicaciones del dispositivo
```

Análisis de aplicaciones instaladas

```
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
S: WARNING: Could not write to (/home/berbus/.local/share/apktool/framework), us
ing /tmp instead...
S: Please be aware this is a volatile directory and frameworks could go missing,
 please utilize --frame-path if the default storage directory is unavailable
I: Loading resource table from file: /tmp/1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
I: Using Apktool 2.3.4 on DefaultContainerService.apk
I: Loading resource table...
I: Decoding Shared Library (androidhwext), pkgId: 2
I: Decoding AndroidManifest.xml with resources...
S: WARNING: Could not write to (/home/berbus/.local/share/apktool/framework), us
ing /tmp instead...
S: Please be aware this is a volatile directory and frameworks could go missing,
 please utilize --frame-path if the default storage directory is unavailable
I: Loading resource table from file: /tmp/1.apk
```

Análisis de aplicaciones instaladas

- Estructura de ficheros de la aplicación

```
Amazon_Shopping_Global.apk          HwCamera.apk                        MyVodafone_CZ.apk
Amazon_Shopping_Global.apk.files    HwCamera.apk.files                  MyVodafone_CZ.apk.files
Apps_store_ZA.apk                   HWCardManager.apk                   MyVodafone_IT.apk
Apps_store_ZA.apk.files             HWCardManager.apk.files             MyVodafone_IT.apk.files
BackupRestoreConfirmation.apk       HwCompass.apk                       MyVodafone_RO.apk
BackupRestoreConfirmation.apk.files HwCompass.apk.files                 MyVodafone_RO.apk.files
BasicDreams.apk                     HwDeskClock.apk                     Newsstand.apk
BasicDreams.apk.files               HwDeskClock.apk.files               Newsstand.apk.files
Bluetooth.apk                       HwFileManager.apk                   NfcNci.apk
Bluetooth.apk.files                 HwFileManager.apk.files             NfcNci.apk.files
Books.apk                           HwFloatTasks.apk                    NoiseField.apk
Books.apk.files                     HwFloatTasks.apk.files              NoiseField.apk.files
Calculator.apk                      HwFMRadio.apk                       OMACP.apk
Calculator.apk.files                HwFMRadio.apk.files                 OMACP.apk.files
Calendar.apk                        HwIms.apk                           PacProcessor.apk
Calendar.apk.files                  HwIms.apk.files                     PacProcessor.apk.files
CalendarProvider.apk                HwInternetAudioService.apk          PartnerBookmarksProvider.apk
CalendarProvider.apk.files          HwInternetAudioService.apk.files    PartnerBookmarksProvider.apk.files
CaptivePortalLogin.apk              HwLauncher6.apk                     PhaseBeam.apk
CaptivePortalLogin.apk.files        HwLauncher6.apk.files               PhaseBeam.apk.files
CellBroadcastReceiver.apk           HwLogCollectService.apk             Phonesky.apk
CellBroadcastReceiver.apk.files     HwLogCollectService.apk.files       Phonesky.apk.files
CertInstaller.apk                   HwMediaCenter.apk                   Photos.apk
CertInstaller.apk.files             HwMediaCenter.apk.files             Photos.apk.files
```

Análisis de aplicaciones instaladas

- Contenido de las aplicaciones

```
apps [master] ⚡ tree GoogleFeedback.apk.files -L 1
GoogleFeedback.apk.files
├── AndroidManifest.xml
├── apktool.yml
├── original
├── res
└── smali
```

```
<?xml version="1.0" encoding="utf-8" standalone="no"?><manifest xmlns:android="http://schem
android" android:installLocation="auto" package="cn.wps.moffice_eng">
    <application android:allowBackup="false" android:debuggable="false" android:icon="@draw
id:label="@null" android:name="cn.wps.moffice.OfficeApp" android:sharedUserId="cn.wps.moffi
="@null">
        <activity android:excludeFromRecents="true" android:launchMode="singleTask" androi
ocumentmanager.PreStartActivity2" android:taskAffinity="cn.wps.moffice_eng.thirdparty" andr
            <intent-filter>
                <action android:name="android.intent.action.VIEW"/>
                <action android:name="android.intent.action.EDIT"/>
                <category android:name="android.intent.category.DEFAULT"/>
                <category android:name="android.intent.category.BROWSABLE"/>
                <data android:mimeType="text/plain"/>
                <data android:mimeType="application/msexcel"/>
```

Análisis de aplicaciones instaladas

```
#### SRC-IG-0101: Buscando sharedUserId ####

Buscando permisos del tipo sharedUserId
Match found in FusedLocat_AndroidManifest.xml
1:<?xml version="1.0" encoding="utf-8" standalone="no"?><manifest xmlns:android="http://schema
ndroid" android:sharedUserId="android.uid.system" coreApp="true" package="com.android.location.
sionCode="23" platformBuildVersionName="6.0-eng.jenkins.20161125.024427">
Match found in GmsCore.ap_AndroidManifest.xml
1:<?xml version="1.0" encoding="utf-8" standalone="no"?><manifest xmlns:android="http://schema
ndroid" android:sharedUserId="com.google.uid.shared" android:sharedUserLabel="@string/common_ap
ogle.android.gms" platformBuildVersionCode="23" platformBuildVersionName="6.0-2166767">
Match found in GoogleBack_AndroidManifest.xml
1:<?xml version="1.0" encoding="utf-8" standalone="no"?><manifest xmlns:android="http://schema
ndroid" android:sharedUserId="com.google.uid.shared" package="com.google.android.backuptranspor
Code="23" platformBuildVersionName="6.0.1">
Match found in GoogleCale_AndroidManifest.xml
1:<?xml version="1.0" encoding="utf-8" standalone="no"?><manifest xmlns:android="http://schema
ndroid" android:sharedUserId="com.google.android.calendar.uid.shared" package="com.google.andro
r" platformBuildVersionCode="23" platformBuildVersionName="M-2103336">
Match found in GoogleLogi_AndroidManifest.xml
1:<?xml version="1.0" encoding="utf-8" standalone="no"?><manifest xmlns:android="http://schema
ndroid" android:sharedUserId="com.google.uid.shared" android:sharedUserLabel="@string/sharedUse
ogle.android.gsf.login" platformBuildVersionCode="23" platformBuildVersionName="6.0.1">
Match found in GoogleServ_AndroidManifest.xml
1:<?xml version="1.0" encoding="utf-8" standalone="no"?><manifest xmlns:android="http://schema
ndroid" android:sharedUserId="com.google.uid.shared" package="com.google.android.gsf" platformB
atformBuildVersionName="6.0.1">
SP Match found in HwAppObser_AndroidManifest.xml
```

Análisis del sistema de archivos

- SETUID
- SETGID
- Sticky bit

/app	Stock apps installed
/bin	Native binaries and daemons
/etc	Configuration files
/fonts	TTFs
/framework	Android framework .jar files
/lib	Native libraries
/usr	Miniature "/usr"
/xbin	Optional/Extra binaries

Protecciones de Linux

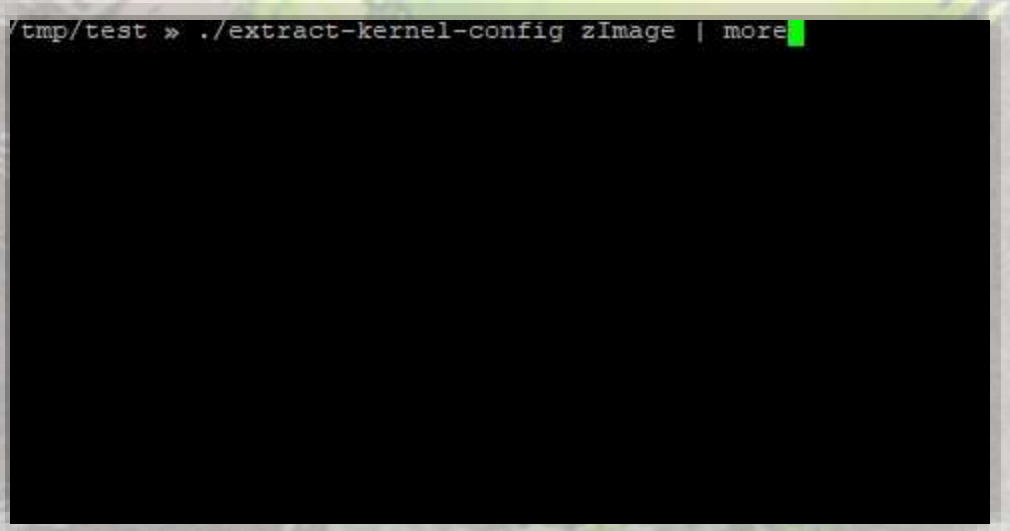
- Se extrae la información de boot.img en la imagen del firmware.
- Kernel Module Signing
  - Comprueba la firma de los módulos que se cargan durante el arranque del sistema.
- Security-Enhanced Linux
  - Control de acceso MAC complementario al sistema tradicional.

Protecciones de Linux

- Extraer boot.img usando abootimg

```
/tmp/test » abootimg -x boot.img
writing boot image config in bootimg.cfg
extracting kernel in zImage
extracting ramdisk in initrd.img
```

- Extraer kernel config de zImage



- ✓ https://github.com/torvalds/linux/blob/master/scripts/extract-vmlinux
- ✓ https://github.com/ggrandou/abootimg

Protecciones de Linux

- Resultado de analizar la configuración de SELinux

Address Space Layout Randomization

- Comprobación de los parámetros de configuración.
- Test de aleatoriedad de las diferentes partes de la ASLR.

```
Linker
7f79798000-7f797ca000 r-xp 00000000 103:06 241                           /system/bin/linker64
7f797da000-7f797db000 r--p 00032000 103:06 241                           /system/bin/linker64
7f797db000-7f797dd000 rw-p 00033000 103:06 241                           /system/bin/linker64
7fad5ac000-7fad5de000 r-xp 00000000 103:06 241                           /system/bin/linker64
7fad5ee000-7fad5ef000 r--p 00032000 103:06 241                           /system/bin/linker64
7fad5ef000-7fad5f1000 rw-p 00033000 103:06 241                           /system/bin/linker64
7f93690000-7f936c2000 r-xp 00000000 103:06 241                           /system/bin/linker64
7f936d2000-7f936d3000 r--p 00032000 103:06 241                           /system/bin/linker64
7f936d3000-7f936d5000 rw-p 00033000 103:06 241                           /system/bin/linker64
```

Address Space Layout Randomization

- Modo de compilación de los binarios.

```
#### SRC-IG-0402: Prueba del modo de compilación de los binarios ####

Resultados en ./input/binaries
 Extrayendo binarios de /system/bin...
    Extrayendo 79b77788-9789-4a7a-a2be-b60155eef5f4.sec
```

```
 input [master] ⚡  tree binaries
binaries
├── acpi
├── agnsscontrol
├── agnsslog
├── am
├── applypatch
├── appops
├── app_process
├── app_process32
├── app_process64
├── appwidget
├── atcmdserver
├── atrace
```

Address Space Layout Randomization

- Modo de compilación de los binarios.

```
#### SRC-IG-0402: Prueba del modo de compilación de los binarios ####

./input/binaries
  acpi: DYN
  agnsscontrol: DYN
  agnsslog: DYN
  am: DYN
  applypatch: DYN
  appops: DYN
  app_process: DYN
  app_process32: DYN
  app_process64: DYN
  appwidget: DYN
  atcmdserver: DYN
  atrace: DYN
  basename: DYN
  bcc: DYN
  blkid: DYN
  blockdev: DYN
  bmgr: DYN
  bootanimation: DYN
  bu: DYN
  bugreport: DYN
  bzcat: DYN
  cal: DYN
  cat: DYN
  chargelogcat: DYN
```

```
expr: DYN
factory_log_service: EXE
fallocate: DYN
false: DYN
```

```
 binaries [master] ⚡  readelf -h yes
ELF Header:
  Magic:   7f 45 4c 46 02 01 01 00 00 00 00 00 00 00 00 00
  Class:                             ELF64
  Data:                              2's complement, little endian
  Version:                           1 (current)
  OS/ABI:                            UNIX - System V
  ABI Version:                       0
  Type:                              DYN (Shared object file)
  Machine:                           AArch64
  Version:                           0x1
  Entry point address:               0xa2d4
  Start of program headers:          64 (bytes into file)
  Start of section headers:          321448 (bytes into file)
  Flags:                             0x0
  Size of this header:               64 (bytes)
  Size of program headers:           56 (bytes)
  Number of program headers:         9
  Size of section headers:           64 (bytes)
  Number of section headers:         27
  Section header string table index: 26
```

Comprobaciones sobre el cifrado

- Full Disk Encryption
- File Based Encryption

```
#### SRC-IG-0300: Información sobre el cifrado ####

Encryption state: encrypted
Encryption type: block
```

```
#### SRC-IG-0301: Configuración cifrado basado en HW ####

config_dm_req_crypt= y
config_crypto_xts= y
config_crypto_dev_qcrypto= y
```

Android Verified Boot (AVB)

- Comprobación de los parámetros que habilitan AVB.

```
#### SRC-IG-0500: Comprobación del AVB ####

CONFIG_DM_VERITY: OK
veritymode: not found
```

Posibles mejoras

- Análisis del código de las aplicaciones
- Mayor profundidad de análisis de SELinux
- Mejorar las pruebas sobre la ASLR
- Pruebas simples de fuerza bruta
- Prueba de AVB con modificaciones

Datos de contacto

jtsec: Beyond IT Security

c/ Abeto s/n Edificio CEG Oficina 2B

CP 18230 Granada – Atarfe – Spain

hello@jtsec.es

@jtsecES

www.jtsec.es