CHARGE YOUR DEVICE WITH THE LATEST MALWARE

André Pereira, Manuel E. Correia and Pedro Brandão
@whoami

- C3P member
  - c3p.up.pt
- CRACS researcher
  - cracs.fc.up.pt

André Pereira apereira[at]dcc.fc.up.pt
Introduction
Increased usage of Smartphones

- New features like phone banking, e-mail, GPS and Web Browsing.
- Leads us to expose more information, that we think we hold as private.
Why Android

- Android composes 80% of the market share.
- Possesses physical attack surface, like **USB** and **NFC**.
- **Open-Source**, it is in the best interest of the community to discover vulnerabilities.
Android vendor customization

- **Good**, because allows vendors to differentiate their products, not just in terms of hardware, but also in software.

- **Bad** for security. Late or no patches. Extension of the attack surface.
Dangers of physical attacks through USB

● Often overlooked by security experts.

● Proved as a serious attack vector, with attacks such as Stuxnet.

● Incorporated in ubiquitous devices such as Android and USB pen drives.
Vulnerabilities
ADB enabled

- Stands as an interface through USB, between a computer and Android.
- With it we are able to install applications, access logcat, get shell access.
- It is estimated that 20% of the Android users have it enabled.
AT commands

- Today AT commands stand as a standard language to talk with the modem.
- Enables the usage of protocols like 3GPP and GSM.
- With the ability to issue these commands to the modem, we can issue calls, send SMS, obtain contacts inside the SIM card.
AT commands

• Today smartphones are composed by two processors, the **AP** (application processor) and the **BP** (Baseband processor).

• AT commands is the preferred interface for communication between these two processors.
Radio Interface Layer

- The RILD is responsible for handling the communication with the modem inside the AP.
- It provides an abstraction layer for the Android application to talk with the modem.
- Issues AT commands through Linux IP stack to the modem.
Radio Interface Layer

1. Phone
   - Dial(): Unix sockets

2. rild
   - Dial(): func call
   - Immediate return

3. RIL impl
   - onRequest(): +AT0 or other IPCs

4. baseband
   - Start Dial

5. Android
   - Dial complete
   - Async return

6. Vendor RIL
   - Listen thread
   - "CONNECT" or other IPCs

7. Vendor RIL
   - Dial Finishes

8. Vendor RIL
   - Dial Finishes
AT commands over USB

- Some manufacturers allow AT commands to be issued through the USB connection.
- Enables the connected PC to talk with the device's modem
- Poses a risk in the connection, since attackers could profit from it.
Samsung AT proprietary commands

- Added by Samsung, so that Kies software communicates over USB with the smartphone.

- To obtain **contacts**, **files**, **update firmware**.
Eavesdropped Kies USB communication - AT+PROF

AT+PROF="Phonebook"
Eavesdropped Kies USB communication - Get device info
Command AT+DEVCONINFO?

- One of the first used by Kies when trying to establish communication with the smartphone.
- Mounts the external storage.
- Returns relevant information such as the IMEI, and the device version.
Command AT+FUS?

- Places the device in download mode.
- Normally to place the device in such a way mechanical key pressing by the user is necessary.
Attack scenario

- Public fake charging kiosk
- Where large numbers of users are prone to be infected
- Easy acceptance by the victim
Implementation
Architecture

The system inside the public kiosk needs to:

● Match the vulnerabilities found in the device
● Be fully automated

We use a virtual machine to make use of two OS’s

● Host Windows 7
● Guest Xubuntu.

Windows 7 had to be the host, so that Odin has direct access to devices.
Architecture

The script running on the guest (Xubuntu) is responsible for:

- Detecting plugged USB devices;
- Identifying the type of device;
- Communicating with the host, when Odin is necessary;
- Copying data from the SD card.
Architecture

The host (Windows 7) is responsible for:

● Communicating with the guest, to know which device to flash;
● Identifying the flash image that matches the device and its firmware;
● Identifying the correct version of Odin for flashing;
● Using GUI automation tools, like Pywinauto, to automate the process that needs GUI input;
Having the AT command interface.

- The purpose of the attack is to steal money from the victim.
- Issuing AT commands over USB to make calls and send SMS messages to added cost numbers.
- For SMS we issue:
  
  AT+CMGF=1
  
  AT+CMGS=+<ADDED_SMS_COST_NUMBER>
  
  <SMS_TEXT>

- For calls we issue:

  ATD + <ADDED_COST_CALL_NUMBER>
Flashing a compromised boot partition with “AT+FUS?”

Pre attack:
1. Unpack a boot partition
2. Add malicious code
3. Pack the altered boot partition

When attacking:
4. Flash it on the device
By changing the boot partition we accomplish three objectives

1. Make **ADB** always enabled.

2. Gain root access.

3. Install an uninstallable surveillance application.
1) Make ADB always enable

Change the init.rc file to have:

on property:persist.service.adb.enable=0
    stop adbd
    start adbd
2) Have root access

Added the su binary to the boot partition and changed the init.rc file to have:

copy /su /system/xbin/su
chmod 06755 /system/xbin/su
chown root /system/xbin/su
3) Install an uninstallable surveillance application

Added androrat to the ramdisk and changed the init.rc with:

```
copy /androrat.apk /system/apps/androrat.apk
```
Tested devices

Verified the following devices by attack:

- Samsung GT-S5839i
- Samsung GT-I5500
- Samsung GT-S7500
- Samsung GT-S5830
- Samsung I9100
- Samsung S7560M
- Samsung I9300 Galaxy S3
Tested Antivirus apps.

We tested with several antivirus apps for Android, namely AVG, Avast, CM Security and virus scanner.

- **AVG** detected that Androrat was installed, but could not remove it.
- The rest didn’t detect anything wrong with the device.
Conclusion

- USB connection is a threat that should not be overlooked
- Vendor customization could lead to serious vulnerability
- Clearly these added features have dangers as shown
- They were designed that way and are not a bug in the system.
Thank you

Questions?

André Pereira apereira@dcc.fc.up.pt