Woolim – Lifting the Fog on DPRK's Latest Tablet PC

Disclaimer

- We never visited DPRK
  - What we say about DPRK is mostly speculation
- This is not about making fun of them
  - Not about the developers …
  - … and certainly not about the people of DPRK
- No focus on security in this talk -> Privacy

Agenda

- Red Star OS updates
- Woolim
  - Hardware
  - Software
- Gaining access to the data
- Distribution of media
- Q&A

Source: http://i3.kym-cdn.com/photos/images/original/000/979/926/81d.jpg

Red Star OS Updates

- Multiple publications concerning Security (@hackerfantastic)
  - Code Execution in Naenara Browser (old FF)
  - Command Injection in *mailto:* handler
  - Shellshock in RSSMON & BEAM in Server Version

Red Star OS Updates

- Multiple publications concerning Security (@hackerfantastic)
  - Code Execution in Naenara Browser (old FF)
  - Command Injection in *mailto:* handler
  - Shellshock in RSSMON & BEAM in Server Version
- Inter Alias (www.interalias.org)
  - Used watermarking to create artifacts in pictures

Red Star OS Updates

- Multiple publications concerning Security (@hackerfantastic)
  - Code Execution in Naenara Browser (old FF)
  - Command Injection in *mailto:* handler
  - Shellshock in RSSMON & BEAM in Server Version
- Inter Alias (www.interalias.org)
  - Used watermarking to create artifacts in pictures
- Watermarking in the wild
  - http://cooks.org.kp/
  - 6 different watermarks appended to JPGs

Motivation

- No in-depth analysis yet
  - Just some general information available
- Related to our previous research
  - Lifting the Fog on Red Star OS (32c3)
- Findings from Red Star OS left open questions
  - Dead code and unused crypto?
  - More advanced watermarking?

울림 - Woolim – Ul-rim – Ul-lim - *Echo*

- Name of a waterfall in DPRK
- One of probably 4 Tablet PCs from DPRKs
    - We have hands on for 3
- Manufacturer
    - Hoozo in China
    - Z100
- Similar products sell for ~180€ to ~260€
- Software from/modified by DPRK

울림

Product Presentation

Woolim

울림

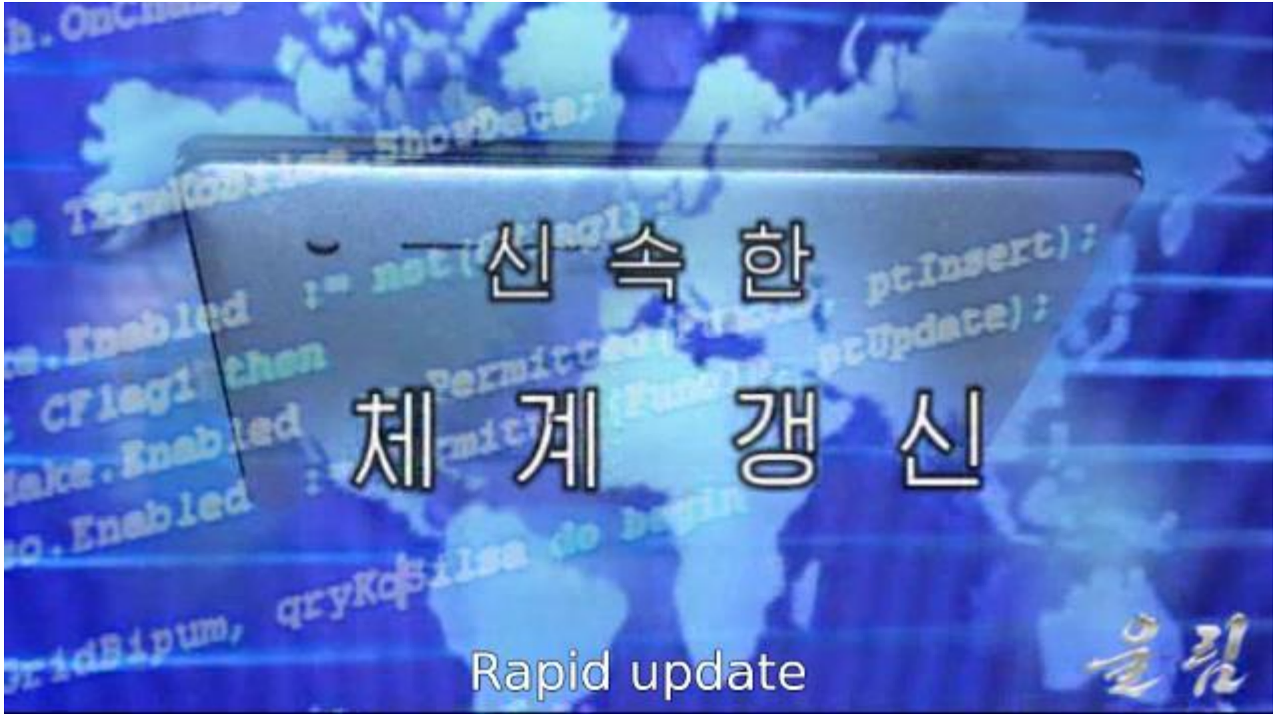
A few side notes …

Don’t drive and watch TV …

울림

A few side notes …

Updates and Patches available?

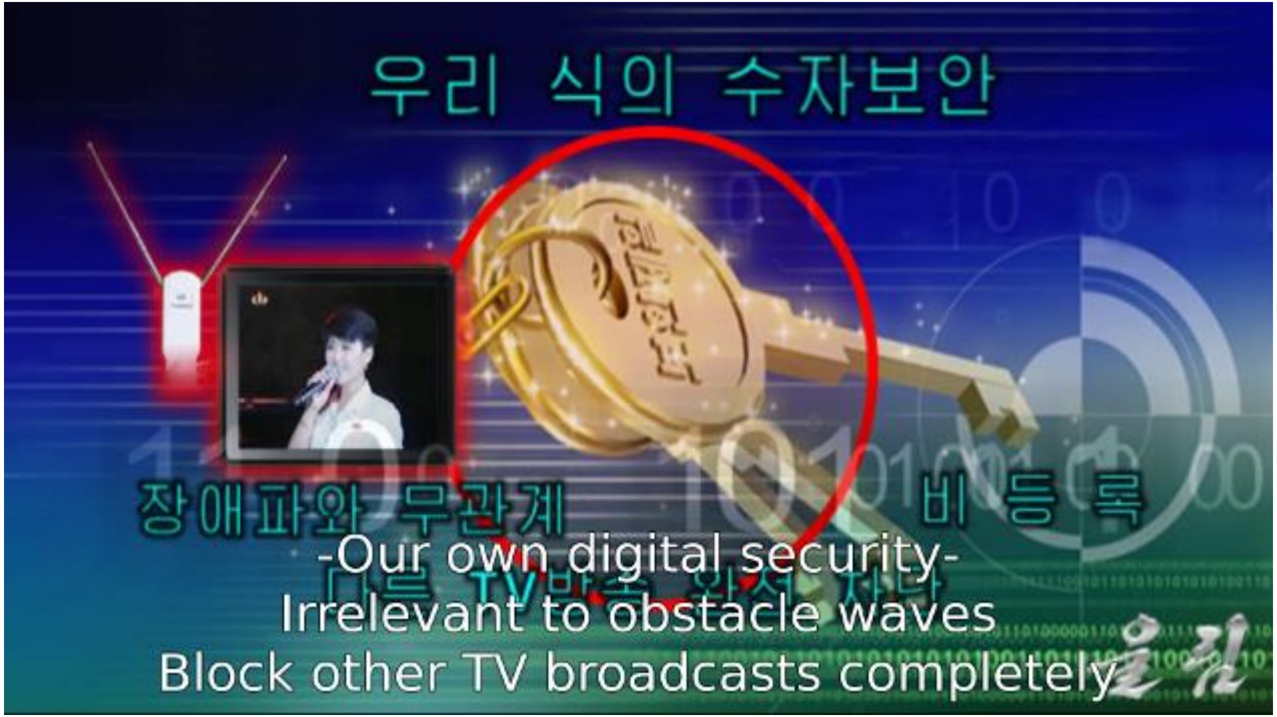


울림

A few side notes …

Free warrantee service

울림


우리 식의 수자보안
장애파와 무관계
비 등록
다른 TV방송 완전 차단
-Our own digital security-
Irrelevant to obstacle waves
Block other TV broadcasts completely
울림

A few side notes …

DVB-T Crypto?

Sells as a feature!

Remember RedStar AV?

Architecture - Hardware

- System Information
  - Allwinner A33 (ARMv7) SoC
  - 8GB SK Hynix flash
  - MicroSD and power plug
  - Not so responsive touchscreen
  - No communication interfaces

Architecture - Hardware

- System Information
  - Allwinner A33 (ARMv7) SoC
  - 8GB SK Hynix flash
  - MicroSD and power plug
  - Not so responsive touchscreen
  - No communication interfaces

- USB peripherals available
  - Modem
  - Wifi
  - LAN
  - DVB-T
  - HDMI (?)

Architecture - Software

- Android 4.4.2
- Kernel 3.4.39
- Build: Sep 10, 2015

Architecture - Software

- Android 4.4.2
- Kernel 3.4.39
- Build: Sep 10, 2015

- Preinstalled applications
  - Camera
  - “Education”
  - Games
  - Browser

Application Demos

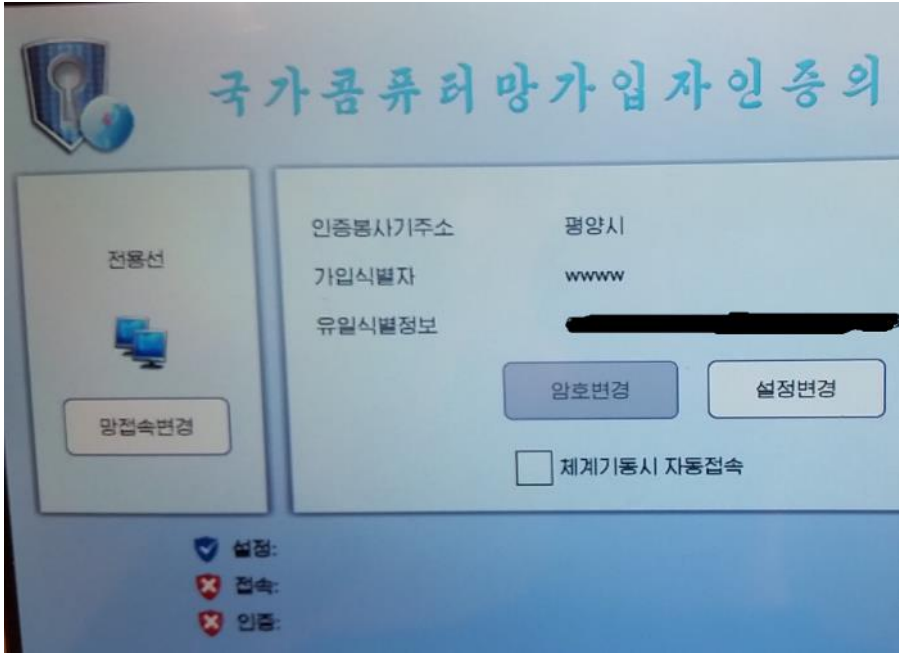
Woolim

Source: http://static3.businessinsider.com/image/5597ee366bb3f7324101480f-1200-924/kim-jong-un-135.jpg

울림

NAC

- Probably used for access to Kwangmyong
- PANA / PPPoE / Dialup
- Login credentials
- Different access points for different regions



국가콤퓨터망가입자인증의

인증봉사기주소 평양시

가입식별자 wwwww

유일식별정보 [redacted]

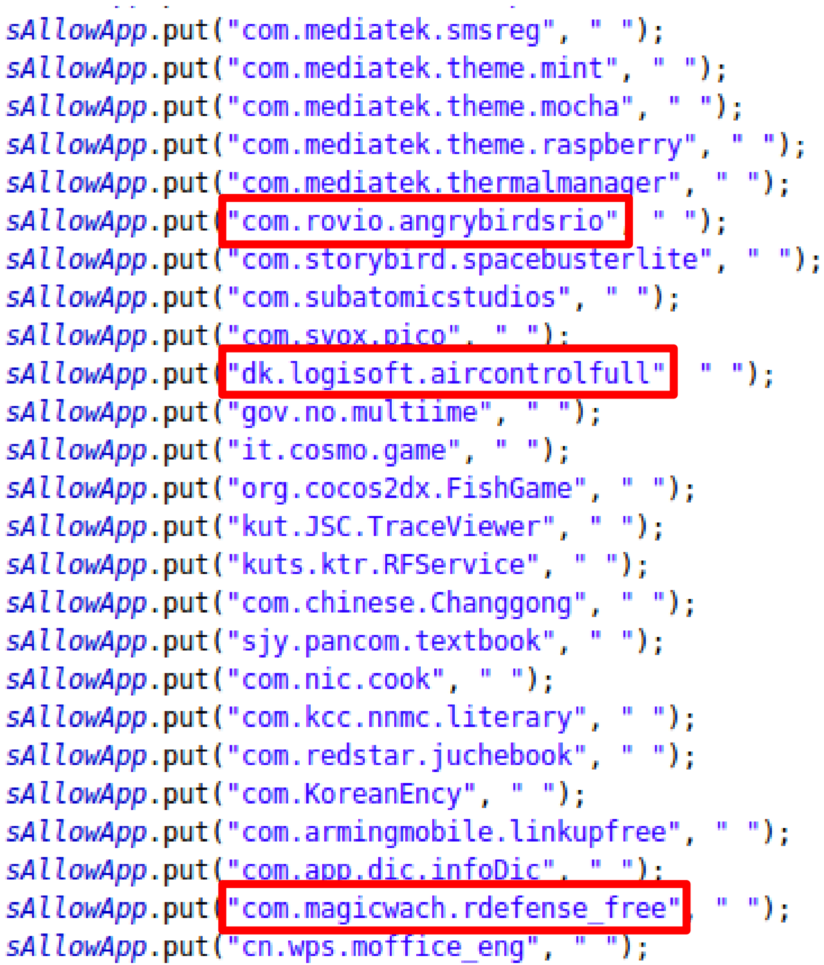
□ 체계기동시 자동접속

Red Flag 🚩

- Schedules thread
  - Takes screenshots in the background
  - Logs the Browser history
- Get IMEI, IMSI and android_id
- Copies key material
- “Integrity Check” -> Shutdown system
- Whitelist check for applications

Whitelist examples

RedFlag Service



```
sAllowApp.put("com.mediatek.smsreg", " ");
sAllowApp.put("com.mediatek.theme.mint", " ");
sAllowApp.put("com.mediatek.theme.mocha", " ");
sAllowApp.put("com.mediatek.theme.raspberry", " ");
sAllowApp.put("com.mediatek.thermalmanager", " ");
sAllowApp.put("com.rovio.angrybirdsrio", " ");
sAllowApp.put("com.storybird.spacebusterlite", " ");
sAllowApp.put("com.subatomicstudios", " ");
sAllowApp.put("com.svox.pico", " ");
sAllowApp.put("dk.logisoft.aircontrolfull", " ");
sAllowApp.put("gov.no.multiime", " ");
sAllowApp.put("it.cosmo.game", " ");
sAllowApp.put("org.cocos2dx.FishGame", " ");
sAllowApp.put("kut.JSC.TraceViewer", " ");
sAllowApp.put("kuts.ktr.RFService", " ");
sAllowApp.put("com.chinese.Changgong", " ");
sAllowApp.put("sjy.pancom.textbook", " ");
sAllowApp.put("com.nic.cook", " ");
sAllowApp.put("com.kcc.nnmc.literary", " ");
sAllowApp.put("com.redstar.juchebook", " ");
sAllowApp.put("com.KoreanEncy", " ");
sAllowApp.put("com.armingmobile.linkupfree", " ");
sAllowApp.put("com.app.dic.infoDic", " ");
sAllowApp.put("com.magicwach.rdefense_free", " ");
sAllowApp.put("cn.wps.moffice_eng", " ");
```

Gaining Access

Extract all the Things!

Source: http://guardianlv.com/wp-content/uploads/2013/08/kimjongunnorthkorea005.jpg

The obvious things …

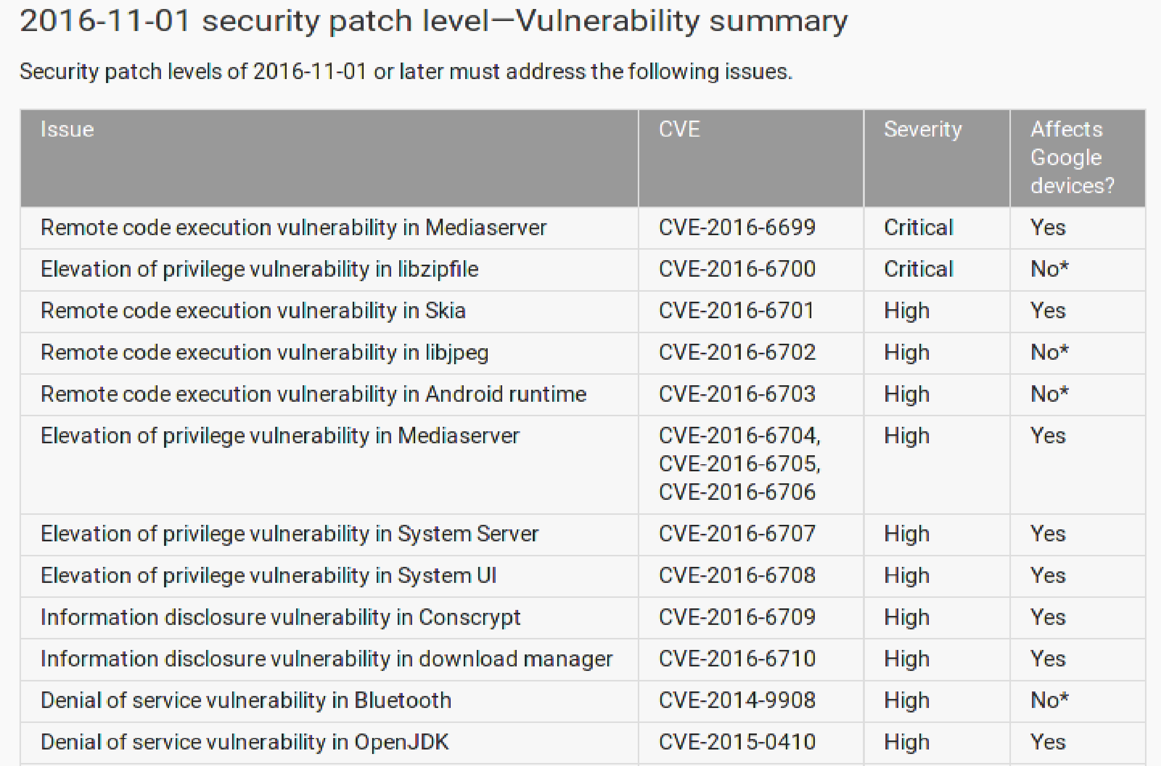
- ADB enabled?
- Can we enable it?
- Developer options?
- Can we install APKs?
- Is there a recovery/download mode?

The more advanced things …

- File open dialogs in Apps
- Attacks via archives
  - Symlinks
  - Directory Traversal
- Suspicious shell commands in configuration files
- Java Deserialization for Tetris
- Flash application
- XLS macro injections
- … even more …

Exploiting Vulnerabilities?

Android Security Bulletins 11/2016



2016-11-01 security patch level—Vulnerability summary

Security patch levels of 2016-11-01 or later must address the following issues.

Issue	CVE	Severity	Affects Google devices?
Remote code execution vulnerability in Mediaserver	CVE-2016-6699	Critical	Yes
Elevation of privilege vulnerability in libzipfile	CVE-2016-6700	Critical	No*
Remote code execution vulnerability in Skia	CVE-2016-6701	High	Yes
Remote code execution vulnerability in libjpeg	CVE-2016-6702	High	No*
Remote code execution vulnerability in Android runtime	CVE-2016-6703	High	No*
Elevation of privilege vulnerability in Mediaserver	CVE-2016-6704, CVE-2016-6705, CVE-2016-6706	High	Yes
Elevation of privilege vulnerability in System Server	CVE-2016-6707	High	Yes
Elevation of privilege vulnerability in System UI	CVE-2016-6708	High	Yes
Information disclosure vulnerability in Conscrypt	CVE-2016-6709	High	Yes
Information disclosure vulnerability in download manager	CVE-2016-6710	High	Yes
Denial of service vulnerability in Bluetooth	CVE-2014-9908	High	No*
Denial of service vulnerability in OpenJDK	CVE-2015-0410	High	Yes

Source: https://source.android.com/security/bulletin/2016-11-01.html

울림

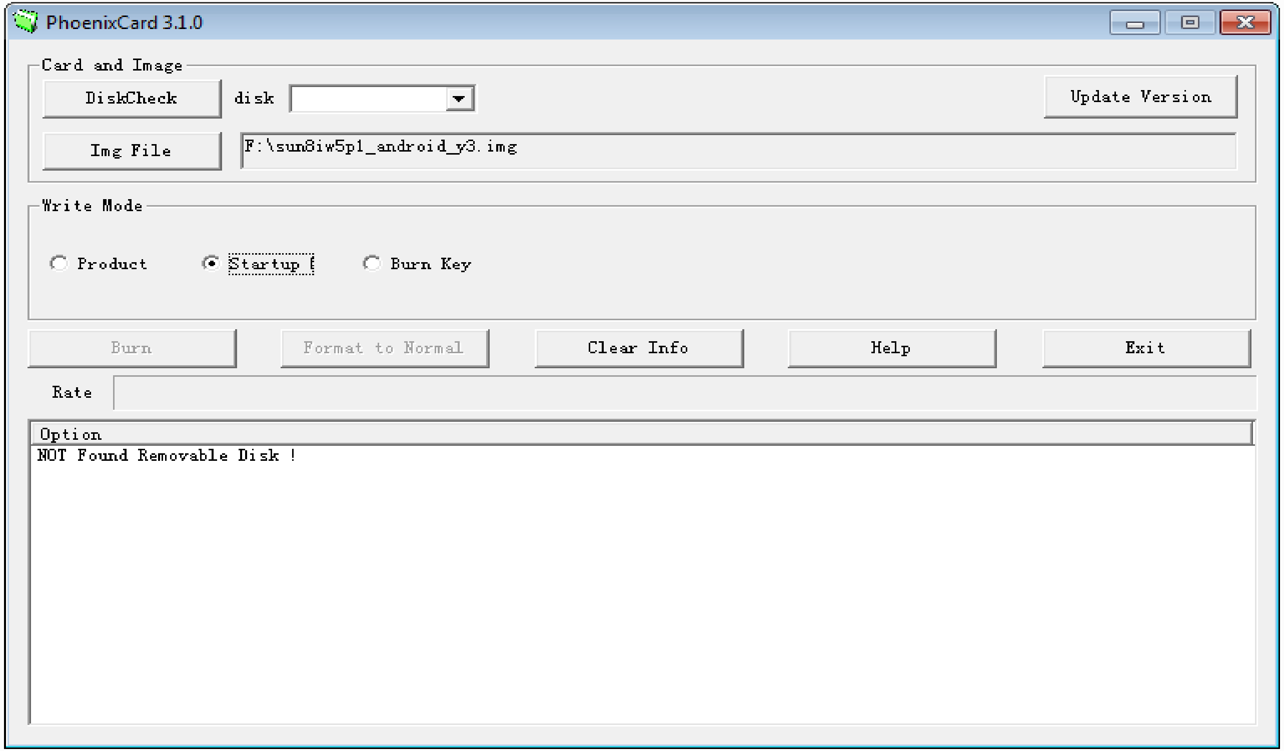
Hardware

Avoid Hardware Tampering!

Source: http://kimjongunlookingatthings.tumblr.com/image/140761766154

PhoenixCard

Create Bootable Images for Allwinner Devices



PhoenixCard 3.1.0

Card and Image

F:\sun8iw5p1_android_y3.img

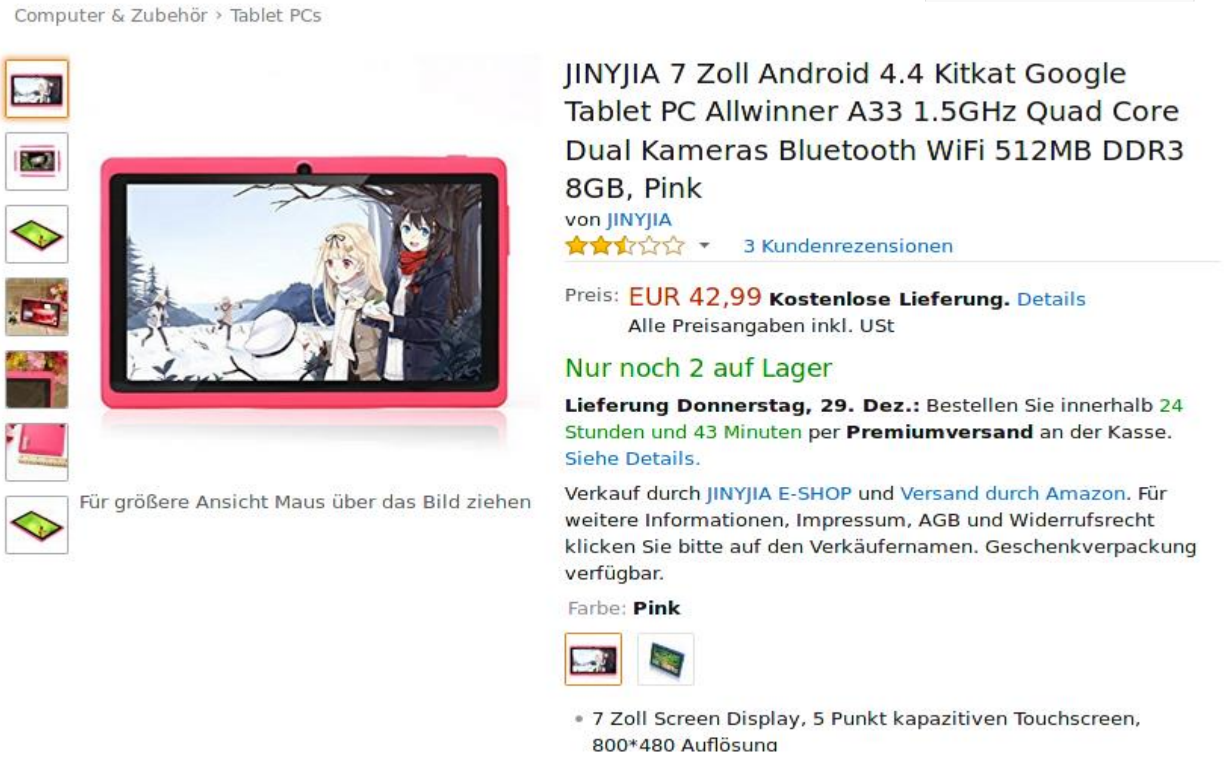
Write Mode

○ Product ● Startup ○ Burn Key

```
NOT Found Removable Disk !
```

Source: https://androidmtk.com/download-phoenixcard-tool

울림



Computer & Zubehör › Tablet PCs

Für größere Ansicht Maus über das Bild ziehen

JINYJIA 7 Zoll Android 4.4 Kitkat Google Tablet PC Allwinner A33 1.5GHz Quad Core Dual Kameras Bluetooth WiFi 512MB DDR3 8GB, Pink

von JINYJIA

★★⯪☆☆ ▾ 3 Kundenrezensionen

Preis: EUR 42,99 **Kostenlose Lieferung.** Details

Alle Preisangaben inkl. USt

Nur noch 2 auf Lager

Lieferung Donnerstag, 29. Dez.: Bestellen Sie innerhalb 24 Stunden und 43 Minuten per **Premiumversand** an der Kasse. Siehe Details.

Verkauf durch JINYJIA E-SHOP und Versand durch Amazon. Für weitere Informationen, Impressum, AGB und Widerrufsrecht klicken Sie bitte auf den Verkäufernamen. Geschenkverpackung verfügbar.

Farbe: **Pink**

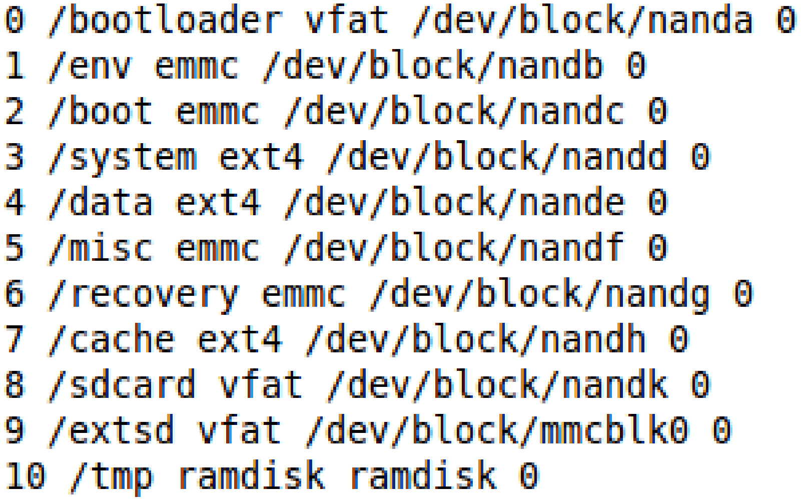
- 7 Zoll Screen Display, 5 Punkt kapazitiven Touchscreen, 800*480 Auflösung

Test Environment

Cheap A33 Tablet with similar functionality

Source: https://www.amazon.de/gp/product/B01C84JN5S/ref=oh_aui_detailpage_o07_s00?ie=UTF8&psc=1

Storage Layout



```
0 /bootloader vfat /dev/block/nanda 0
1 /env emmc /dev/block/nandb 0
2 /boot emmc /dev/block/nandc 0
3 /system ext4 /dev/block/nandd 0
4 /data ext4 /dev/block/nande 0
5 /misc emmc /dev/block/nandf 0
6 /recovery emmc /dev/block/nandg 0
7 /cache ext4 /dev/block/nandh 0
8 /sdcard vfat /dev/block/nandk 0
9 /extsd vfat /dev/block/mmcblk0 0
10 /tmp ramdisk ramdisk 0
```

Source: http://kimjongunlookingatthings.tumblr.com/image/126030443459

Distribution of Media files in DPRK

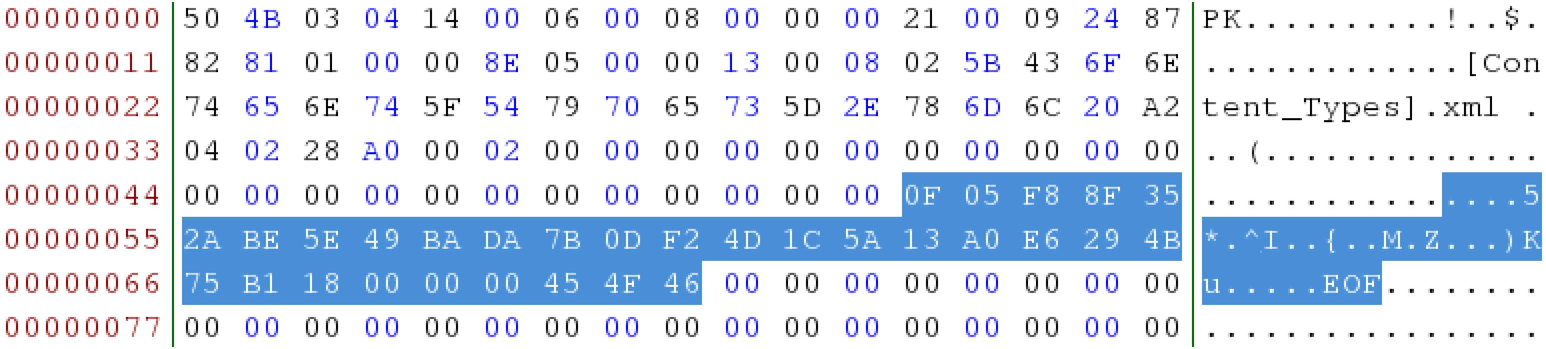
Achieving absolute control

Source: http://static5.businessinsider.com/image/5208f238eab8ea0649000011-1200-924/kim-jong-un-inspects-north-korea-smartphone-factory-2.jpg

Multiple Ways of Tracing Media Distribution

- Watermarking introduced in Red Star OS
  - Append simple watermarks to media files
  - Compatible code available on Woolim (librealtime_cb.so)
  - Seems to be refactored out of multiple services of Red Star OS 3.0
  - Seems like watermarking parts are not used by default
- Technically more advanced, more restrictive way of Woolim
  - Based on cryptographic signatures
  - Gives the government more power over media sources

Red Star OS Watermarking Recap



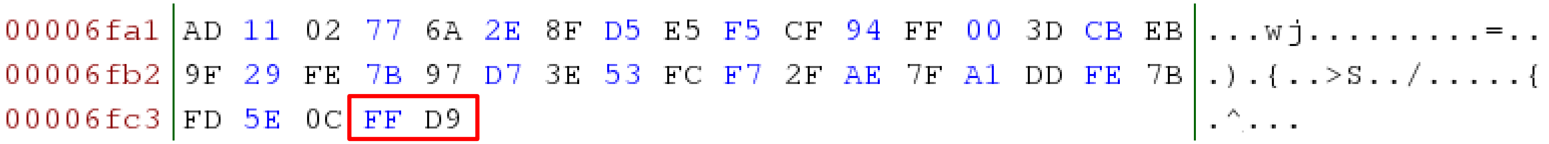
```
00000000 50 4B 03 04 14 00 06 00 08 00 00 00 21 00 09 24 87 PK..........!..$.
00000011 82 81 01 00 00 8E 05 00 00 13 00 08 02 5B 43 6F 6E ..............[Con
00000022 74 65 6E 74 5F 54 79 70 65 73 5D 2E 78 6D 6C 20 A2 tent_Types].xml .
00000033 04 02 28 A0 00 02 00 00 00 00 00 00 00 00 00 00 00 ..(..............
00000044 00 00 00 00 00 00 00 00 00 00 00 00 0F 05 F8 8F 35 ................5
00000055 2A BE 5E 49 BA DA 7B 0D F2 4D 1C 5A 13 A0 E6 29 4B *.^I..{..M.Z...)K
00000066 75 B1 18 00 00 00 45 4F 46 00 00 00 00 00 00 00 00 u.....EOF........
00000077 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .................
```

Plaintext: **WMB48Z789B3AZ97**

Decryption tool: https://github.com/takeshixx/redstar-tools

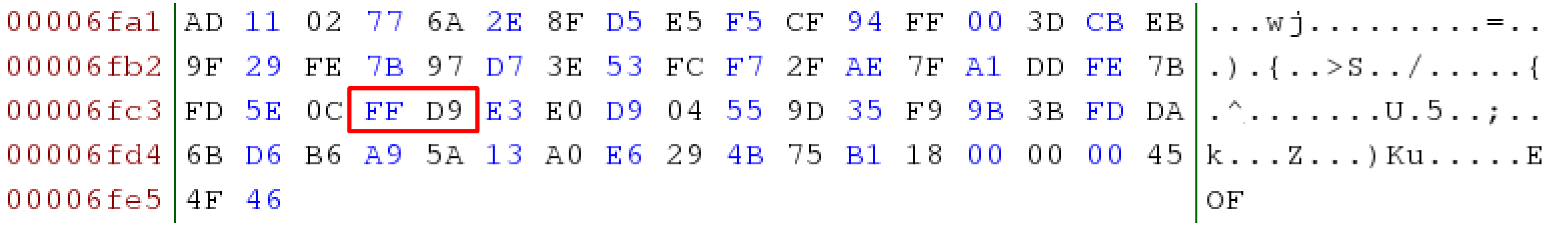
울림

Original



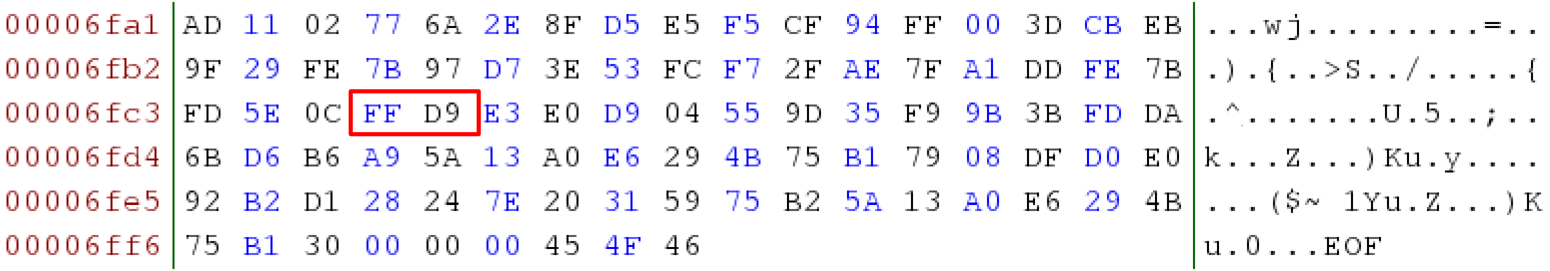
```
00006fa1 AD 11 02 77 6A 2E 8F D5 E5 F5 CF 94 FF 00 3D CB EB ...wj.........=..
00006fb2 9F 29 FE 7B 97 D7 3E 53 FC F7 2F AE 7F A1 DD FE 7B .).{..>S../.....{
00006fc3 FD 5E 0C FF D9                                     .^...
```

First user



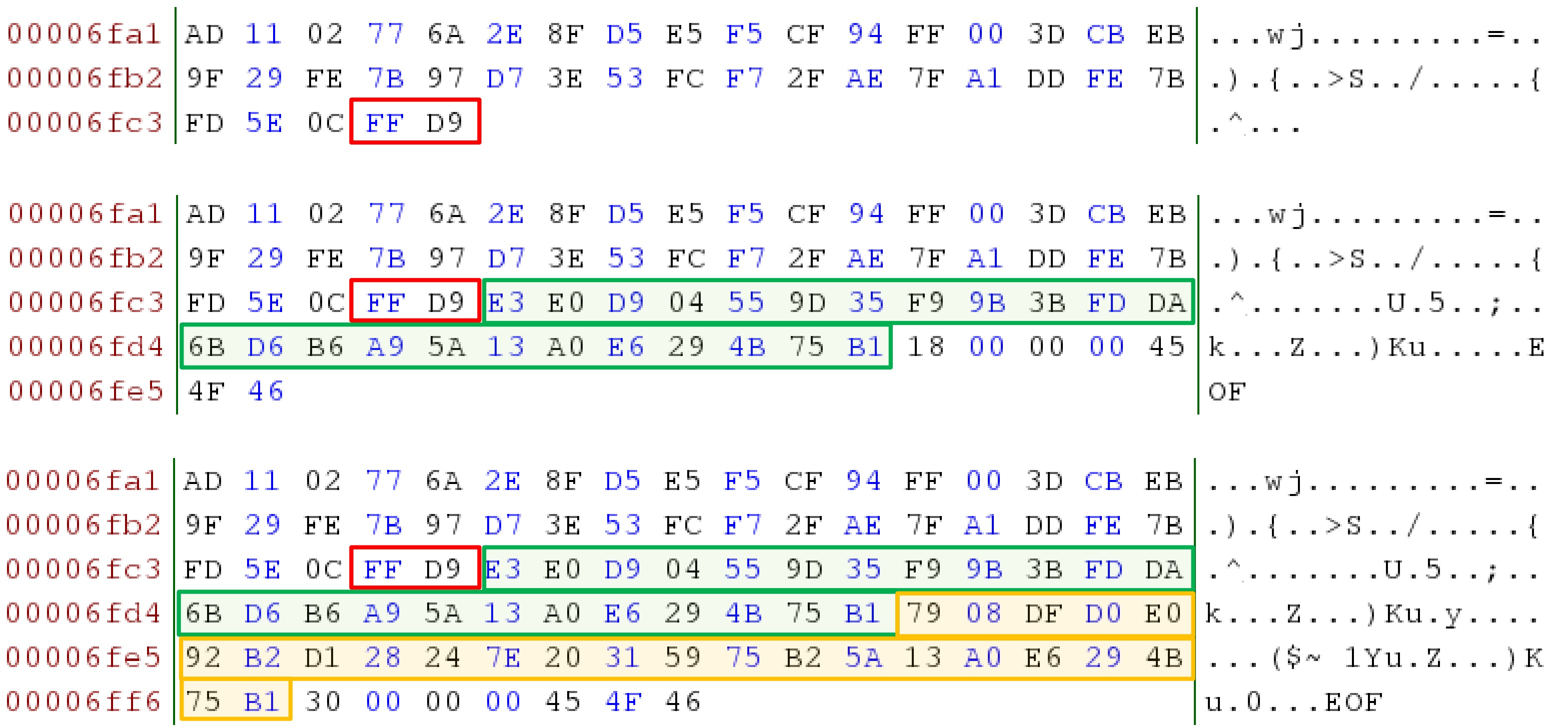
```
00006fa1 AD 11 02 77 6A 2E 8F D5 E5 F5 CF 94 FF 00 3D CB EB ...wj.........=..
00006fb2 9F 29 FE 7B 97 D7 3E 53 FC F7 2F AE 7F A1 DD FE 7B .).{..>S../.....{
00006fc3 FD 5E 0C FF D9 E3 E0 D9 04 55 9D 35 F9 9B 3B FD DA .^.......U.5..;..
00006fd4 6B D6 B6 A9 5A 13 A0 E6 29 4B 75 B1 18 00 00 00 45 k...Z...)Ku.....E
00006fe5 4F 46                                              OF
```

Second user



```
00006fa1 AD 11 02 77 6A 2E 8F D5 E5 F5 CF 94 FF 00 3D CB EB ...wj.........=..
00006fb2 9F 29 FE 7B 97 D7 3E 53 FC F7 2F AE 7F A1 DD FE 7B .).{..>S../.....{
00006fc3 FD 5E 0C FF D9 E3 E0 D9 04 55 9D 35 F9 9B 3B FD DA .^.......U.5..;..
00006fd4 6B D6 B6 A9 5A 13 A0 E6 29 4B 75 B1 79 08 DF D0 E0 k...Z...)Ku.y....
00006fe5 92 B2 D1 28 24 7E 20 31 59 75 B2 5A 13 A0 E6 29 4B ...($~ 1Yu.Z...)K
00006ff6 75 B1 30 00 00 00 45 4F 46                         u.0...EOF
```

울림



Original

```
00006fa1 AD 11 02 77 6A 2E 8F D5 E5 F5 CF 94 FF 00 3D CB EB ...wj.........=..
00006fb2 9F 29 FE 7B 97 D7 3E 53 FC F7 2F AE 7F A1 DD FE 7B .).{..>S../.....{
00006fc3 FD 5E 0C FF D9                                     .^...
```

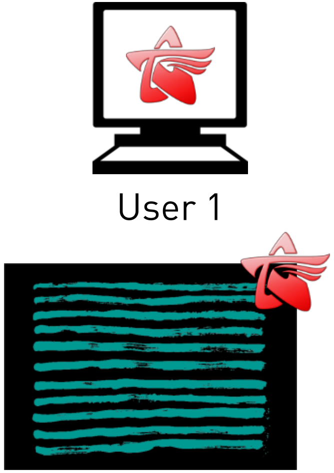
First user

```
00006fa1 AD 11 02 77 6A 2E 8F D5 E5 F5 CF 94 FF 00 3D CB EB ...wj.........=..
00006fb2 9F 29 FE 7B 97 D7 3E 53 FC F7 2F AE 7F A1 DD FE 7B .).{..>S../.....{
00006fc3 FD 5E 0C FF D9 E3 E0 D9 04 55 9D 35 F9 9B 3B FD DA .^.......U.5..;..
00006fd4 6B D6 B6 A9 5A 13 A0 E6 29 4B 75 B1 18 00 00 00 45 k...Z...)Ku.....E
00006fe5 4F 46                                              OF
```

Second user

```
00006fa1 AD 11 02 77 6A 2E 8F D5 E5 F5 CF 94 FF 00 3D CB EB ...wj.........=..
00006fb2 9F 29 FE 7B 97 D7 3E 53 FC F7 2F AE 7F A1 DD FE 7B .).{..>S../.....{
00006fc3 FD 5E 0C FF D9 E3 E0 D9 04 55 9D 35 F9 9B 3B FD DA .^.......U.5..;..
00006fd4 6B D6 B6 A9 5A 13 A0 E6 29 4B 75 B1 79 08 DF D0 E0 k...Z...)Ku.y....
00006fe5 92 B2 D1 28 24 7E 20 31 59 75 B2 5A 13 A0 E6 29 4B ...($~ 1Yu.Z...)K
00006ff6 75 B1 30 00 00 00 45 4F 46                         u.0...EOF
```

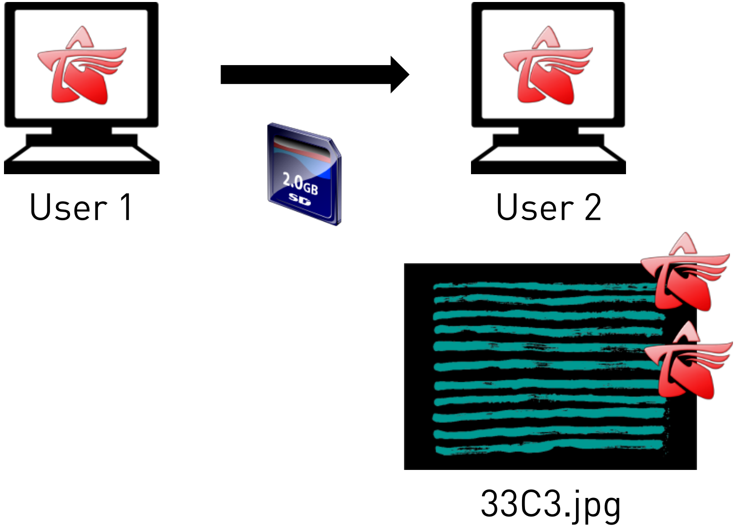
Tracking the Distribution of Media Files



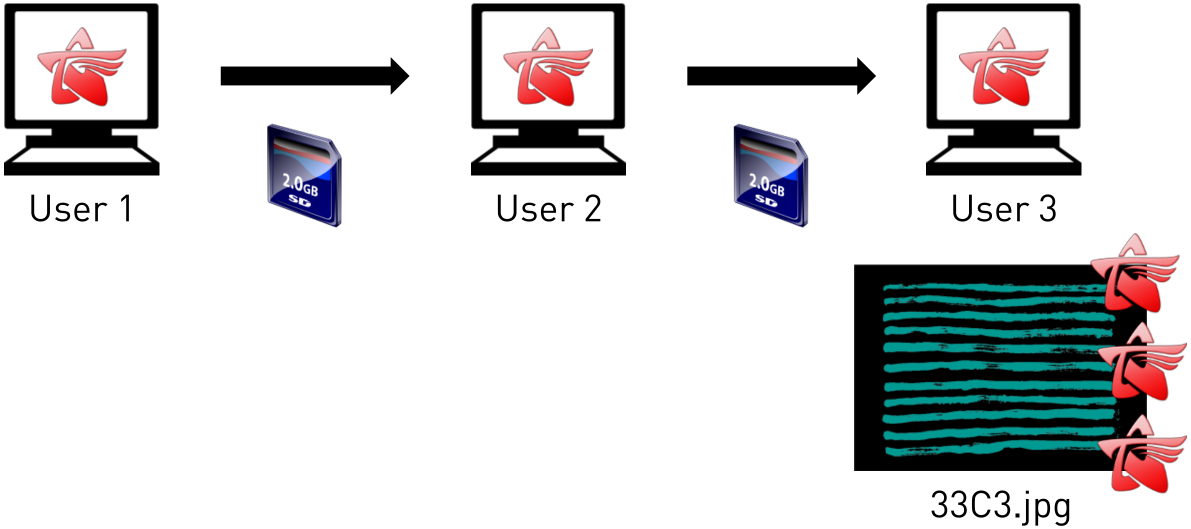
User 1

33C3.jpg

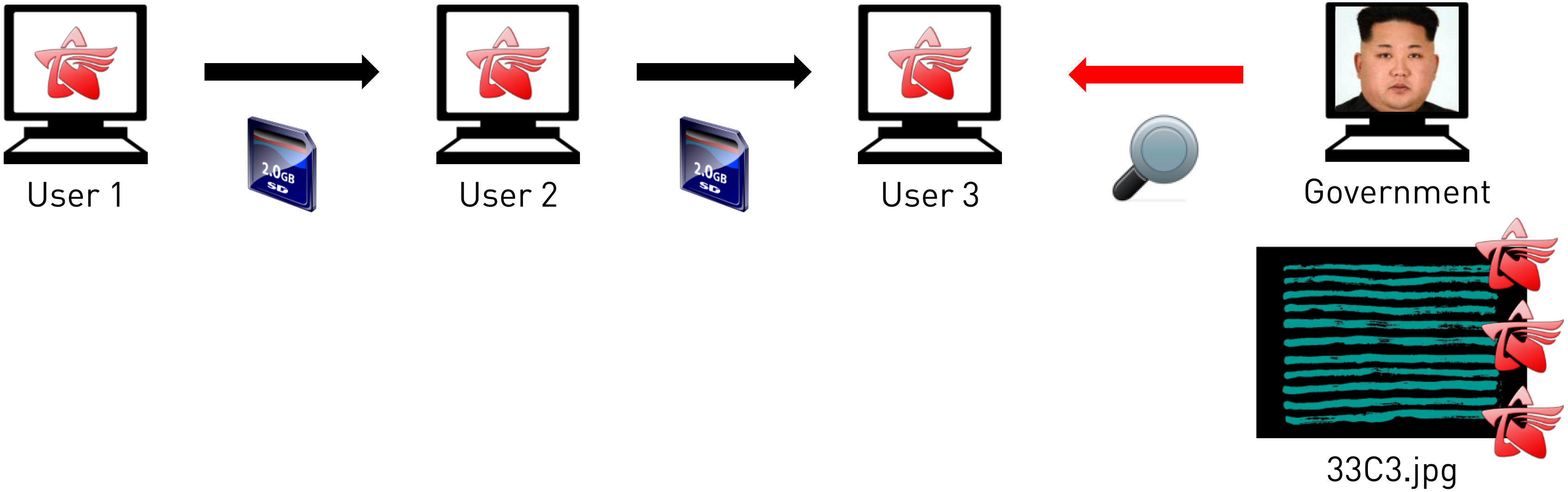
Tracking the Distribution of Media Files



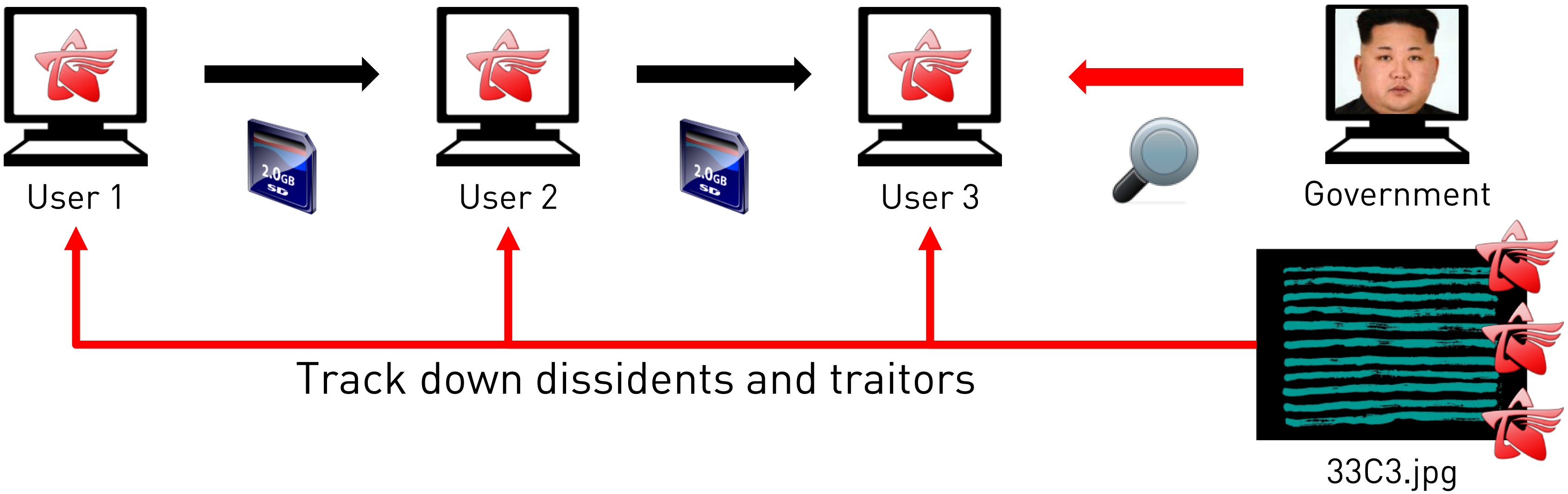
Tracking the Distribution of Media Files



Tracking the Distribution of Media Files



Tracking the Distribution of Media Files



User 1

User 2

User 3

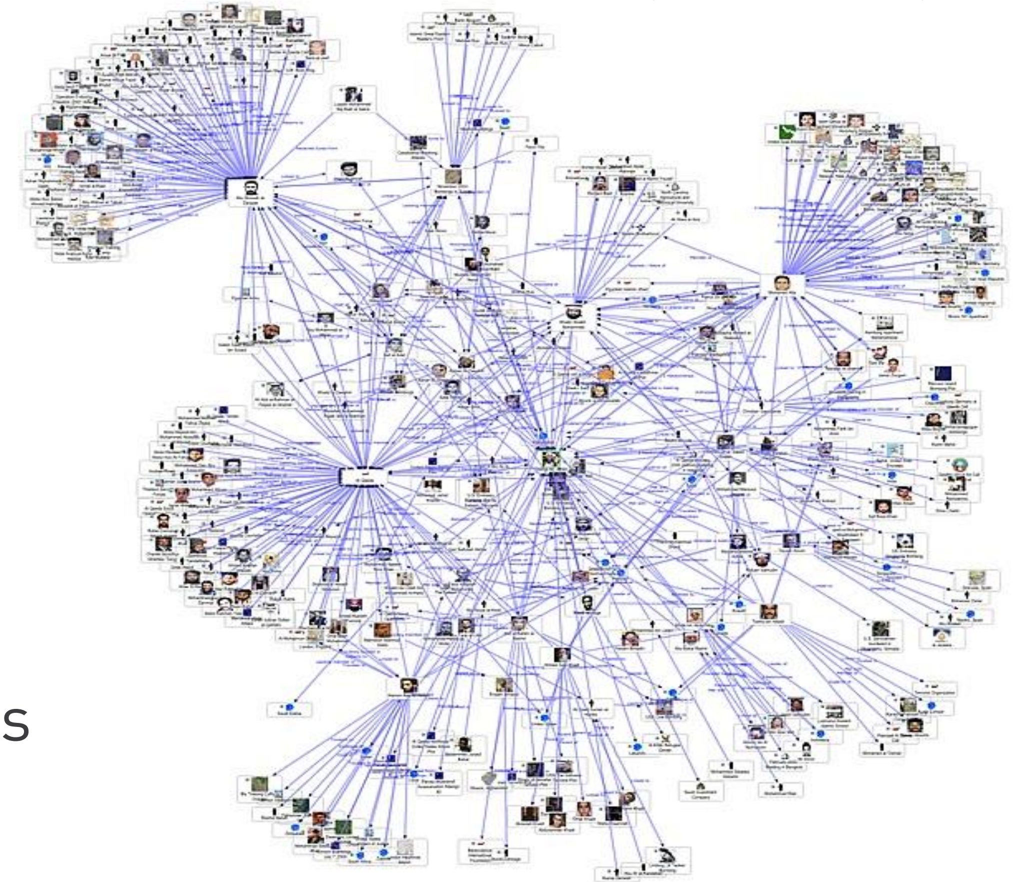
Government

33C3.jpg

Track down dissidents and traitors

Tracking the Distribution of Media Files

- Create social networks
- Construct connections between dissidents
- Track down sources that create/import media files
- Shutdown dissidents/traitors



Source: https://i.stack.imgur.com/xWMRJ.jpg

Woolim is More Restrictive

- Introduces file signatures
  - Using asymmetric cryptography (RSA)
  - Goal: **PREVENT** the distribution of media files
- Government has full control over signatures
  - Absolute control over media sources
- Explicit signature checks on Woolim
  - Apps have to take care of checks
  - Unlike Red Star OS's kernel module

Source: http://s.newsweek.com/sites/www.newsweek.com/files/2015/02/23/0227kimjongun01.jpg

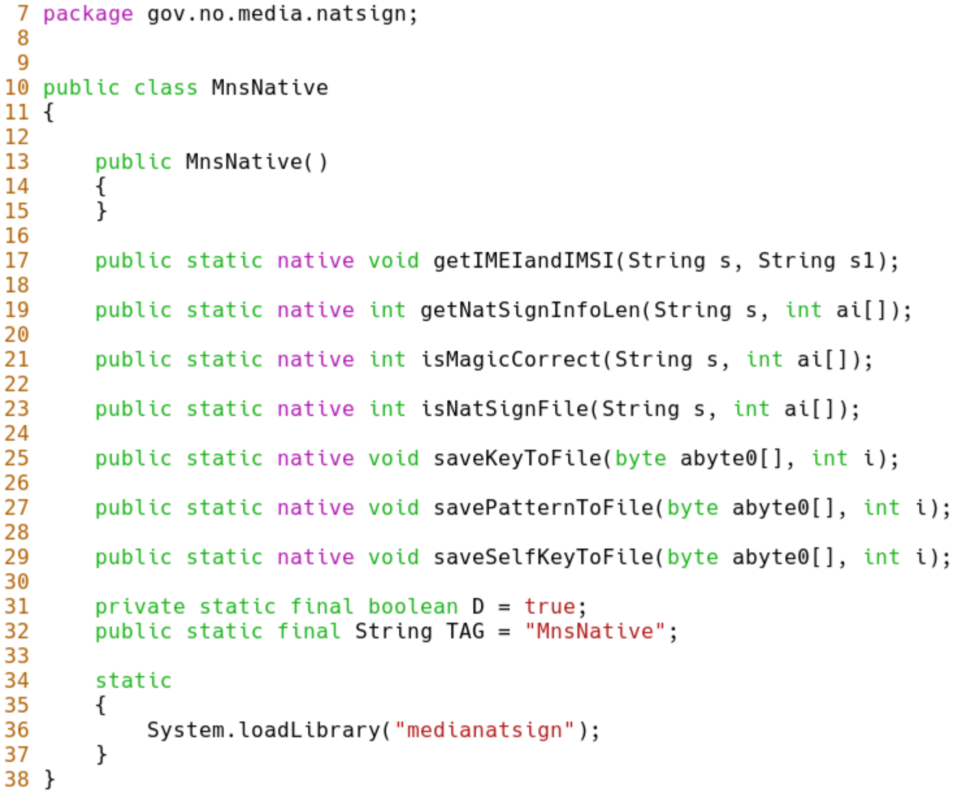
Signature Checking

- Java interface with native JNI library (gov.no.media.Sign)
  - Called by apps e.g. during file opening/saving
  - Sometimes concealed as “license checks”
- Multiple ways of signing
  - NATISIGN: Files signed by the government
  - SELFSIGN: Files signed by the device itself
- Files without proper signatures cannot be opened
  - By apps that do signature checks

Source: http://i.imgur.com/FjOuSdy.jpg

Java Native Interface Libraries

- Check if file has a proper signature
- Used by various applications, e.g.:
  - FileBrowser.apk
  - Gallery2.apk
  - Music.apk
  - PackageInstaller.apk
  - PDFViewer.apk
  - RedFlag.apk
  - SoundRecorder.apk
  - TextEditor.apk



```java
package gov.no.media.natsign;


public class MnsNative
{

    public MnsNative()
    {
    }

    public static native void getIMEIandIMSI(String s, String s1);

    public static native int getNatSignInfoLen(String s, int ai[]);

    public static native int isMagicCorrect(String s, int ai[]);

    public static native int isNatSignFile(String s, int ai[]);

    public static native void saveKeyToFile(byte abyte0[], int i);

    public static native void savePatternToFile(byte abyte0[], int i);

    public static native void saveSelfKeyToFile(byte abyte0[], int i);

    private static final boolean D = true;
    public static final String TAG = "MnsNative";

    static
    {
        System.loadLibrary("medianatsign");
    }
}
```

NATISIGN

- Files that have been approved by the government
  - Also referred to as "gov_sign"
- Files are signed with a 2048 bit RSA key
- Device holds the public key to verify signatures
  - Deployed on the device (0.dat)
- Code does some additional obfuscation
  - Probably to make manual signing harder

Source: https://en.wikipedia.org/wiki/North_Korea#/media/File:Emblem_of_North_Korea.svg

SELFSIGN'ing

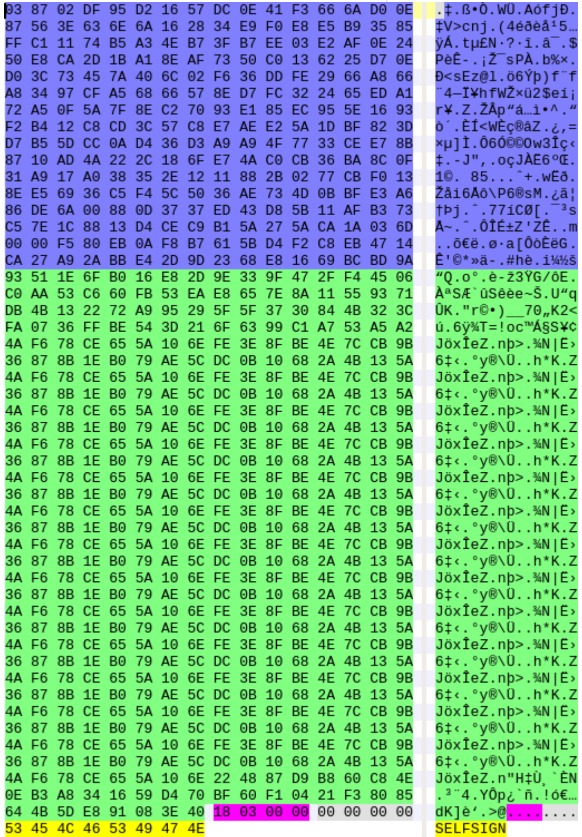
- Combination of
  - Symmetric encryption (Rijndael 256)
  - Asymmetric signatures (RSA)
  - Hashing (SHA224/SHA256)
- Device identity stored in /data/local/tmp/legalref.dat
  - Comprised of IMEI and IMSI
  - Each device's „legal reference"
- Files created on the device itself can be opened
  - Camera images, office documents, PDFs, etc.

Source: http://s1.ibtimes.com/sites/www.ibtimes.com/files/2014/10/09/kim-jong-un.jpg

울림

SELFSIGN Signatures

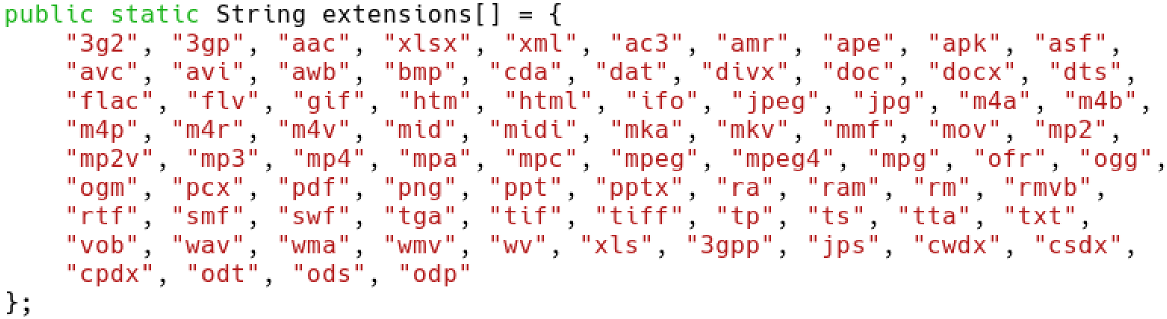
- RSA signature of file hash
- Encrypted device identity
  - Rijndael 256 (key and blocks)
  - IMEI and IMSI
- Trailer
  - Signature size
  - ASCII suffix “SELFSIGN“
- Fixed size of 792 bytes



```
03 87 02 DF 95 D2 16 57 DC 0E 41 F3 66 6A D0 0E   .‡.ß•Ò.WÜ.AófjÐ.
87 56 3E 63 6E 6A 16 28 34 E9 F0 E8 E5 B9 35 85   ‡V>cnj.(4éðèå¹5…
FF C1 11 74 B5 A3 4E B7 3F B7 EE 03 E2 AF 0E 24   ÿÁ.tµ£N·?·î.â¯.$
50 E8 CA 2D 1B A1 8E AF 73 50 C0 13 62 25 D7 0E   PèÊ-.¡Ž¯sPÀ.b%×.
D0 3C 73 45 7A 40 6C 02 F6 36 DD FE 29 66 A8 66   Ð<sEz@l.ö6Ýþ)f¨f
A8 34 97 CF A5 68 66 57 8E D7 FC 32 24 65 ED A1   ¨4—Ï¥hfWŽ×ü2$eí¡
72 A5 0F 5A 7F 8E C2 70 93 E1 85 EC 95 5E 16 93   r¥.Z.ŽÂp“á…ì•^.“
F2 B4 12 C8 CD 3C 57 C8 E7 AE E2 5A 1D BF 82 3D   ò´.ÈÍ<WÈç®âZ.¿‚=
D7 B5 5D CC 0A D4 36 D3 A9 A9 4F 77 33 CE E7 8B   ×µ]Ì.Ô6Ó©©Ow3Îç‹
87 10 AD 4A 22 2C 18 6F E7 4A C0 CB 36 BA 8C 0F   ‡.-J",.oçJÀË6ºŒ.
31 A9 17 A0 38 35 2E 12 11 88 2B 02 77 CB F0 13   1©. 85...ˆ+.wËð.
8E E5 69 36 C5 F4 5C 50 36 AE 73 4D 0B BF E3 A6   Žåi6Åô\P6®sM.¿ã¦
86 DE 6A 00 88 0D 37 37 ED 43 D8 5B 11 AF B3 73   †Þj.ˆ.77íCØ[.¯³s
C5 7E 1C 88 13 D4 CE C9 B1 5A 27 5A CA 1A 03 6D   Å~.ˆ.ÔÎÉ±Z'ZÊ..m
00 00 F5 80 EB 0A F8 B7 61 5B D4 F2 C8 EB 47 14   ..õ€ë.ø·a[ÔòÈëG.
CA 27 A9 2A BB E4 2D 9D 23 68 E8 16 69 BC BD 9A   Ê'©*»ä-.#hè.i¼½š
93 51 1E 6F B0 16 E8 2D 9E 33 9F 47 2F F4 45 06   “Q.o°.è-ž3ŸG/ôE.
C0 AA 53 C6 60 FB 53 EA E8 65 7E 8A 11 55 93 71   ÀªSÆ`ûSêèe~Š.U“q
DB 4B 13 22 72 A9 95 29 5F 5F 37 30 84 4B 32 3C   ÛK."r©•)__70„K2<
FA 07 36 FF BE 54 3D 21 6F 63 99 C1 A7 53 A5 A2   ú.6ÿ¾T=!oc™Á§S¥¢
4A F6 78 CE 65 5A 10 6E FE 3E 8F BE 4E 7C CB 9B   JöxÎeZ.nþ>.¾N|Ë›
36 87 8B 1E B0 79 AE 5C DC 0B 10 68 2A 4B 13 5A   6‡‹.°y®\Ü..h*K.Z
4A F6 78 CE 65 5A 10 6E FE 3E 8F BE 4E 7C CB 9B   JöxÎeZ.nþ>.¾N|Ë›
36 87 8B 1E B0 79 AE 5C DC 0B 10 68 2A 4B 13 5A   6‡‹.°y®\Ü..h*K.Z
4A F6 78 CE 65 5A 10 6E FE 3E 8F BE 4E 7C CB 9B   JöxÎeZ.nþ>.¾N|Ë›
36 87 8B 1E B0 79 AE 5C DC 0B 10 68 2A 4B 13 5A   6‡‹.°y®\Ü..h*K.Z
4A F6 78 CE 65 5A 10 6E FE 3E 8F BE 4E 7C CB 9B   JöxÎeZ.nþ>.¾N|Ë›
36 87 8B 1E B0 79 AE 5C DC 0B 10 68 2A 4B 13 5A   6‡‹.°y®\Ü..h*K.Z
4A F6 78 CE 65 5A 10 6E FE 3E 8F BE 4E 7C CB 9B   JöxÎeZ.nþ>.¾N|Ë›
36 87 8B 1E B0 79 AE 5C DC 0B 10 68 2A 4B 13 5A   6‡‹.°y®\Ü..h*K.Z
4A F6 78 CE 65 5A 10 6E FE 3E 8F BE 4E 7C CB 9B   JöxÎeZ.nþ>.¾N|Ë›
36 87 8B 1E B0 79 AE 5C DC 0B 10 68 2A 4B 13 5A   6‡‹.°y®\Ü..h*K.Z
4A F6 78 CE 65 5A 10 6E FE 3E 8F BE 4E 7C CB 9B   JöxÎeZ.nþ>.¾N|Ë›
36 87 8B 1E B0 79 AE 5C DC 0B 10 68 2A 4B 13 5A   6‡‹.°y®\Ü..h*K.Z
4A F6 78 CE 65 5A 10 6E FE 3E 8F BE 4E 7C CB 9B   JöxÎeZ.nþ>.¾N|Ë›
36 87 8B 1E B0 79 AE 5C DC 0B 10 68 2A 4B 13 5A   6‡‹.°y®\Ü..h*K.Z
4A F6 78 CE 65 5A 10 6E FE 3E 8F BE 4E 7C CB 9B   JöxÎeZ.nþ>.¾N|Ë›
36 87 8B 1E B0 79 AE 5C DC 0B 10 68 2A 4B 13 5A   6‡‹.°y®\Ü..h*K.Z
4A F6 78 CE 65 5A 10 6E FE 3E 8F BE 4E 7C CB 9B   JöxÎeZ.nþ>.¾N|Ë›
36 87 8B 1E B0 79 AE 5C DC 0B 10 68 2A 4B 13 5A   6‡‹.°y®\Ü..h*K.Z
4A F6 78 CE 65 5A 10 6E FE 3E 8F BE 4E 7C CB 9B   JöxÎeZ.nþ>.¾N|Ë›
36 87 8B 1E B0 79 AE 5C DC 0B 10 68 2A 4B 13 5A   6‡‹.°y®\Ü..h*K.Z
4A F6 78 CE 65 5A 10 6E FE 3E 8F BE 4E 7C CB 9B   JöxÎeZ.nþ>.¾N|Ë›
36 87 8B 1E B0 79 AE 5C DC 0B 10 68 2A 4B 13 5A   6‡‹.°y®\Ü..h*K.Z
4A F6 78 CE 65 5A 10 6E FE 3E 8F BE 4E 7C CB 9B   JöxÎeZ.nþ>.¾N|Ë›
36 87 8B 1E B0 79 AE 5C DC 0B 10 68 2A 4B 13 5A   6‡‹.°y®\Ü..h*K.Z
4A F6 78 CE 65 5A 10 6E 22 48 87 D9 B8 60 C8 4E   JöxÎeZ.n"H‡Ù¸`ÈN
0E B3 A8 34 16 59 D4 70 BF 60 F1 04 21 F3 80 85   .³¨4.YÔp¿`ñ.!ó€…
64 4B 5D E8 91 08 3E 40 18 03 00 00 00 00 00 00   dK]è‘.>@........
53 45 4C 46 53 49 47 4E                           SELFSIGN
```

Files Types Affected by Signing

- All kinds of media files
- Text and HTML files
- Even APKs…

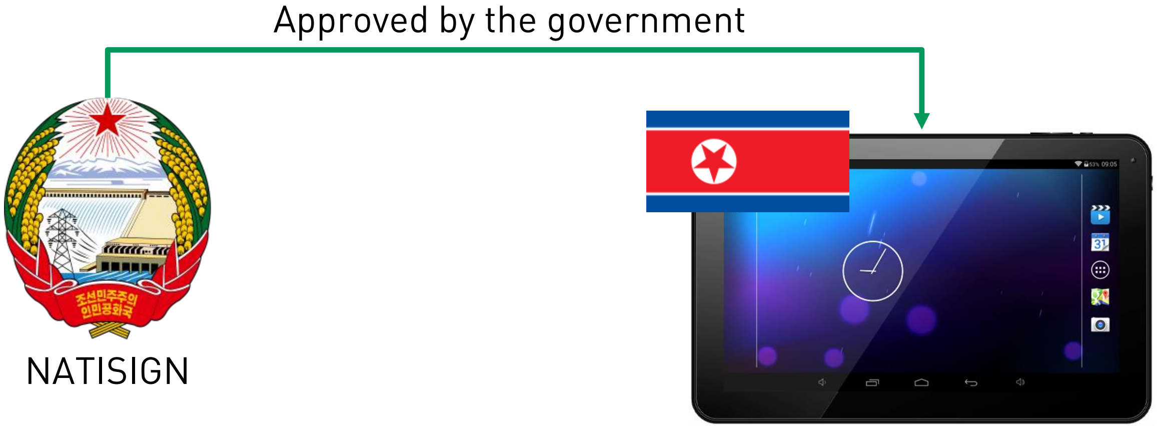


```
public static String extensions[] = {
    "3g2", "3gp", "aac", "xlsx", "xml", "ac3", "amr", "ape", "apk", "asf",
    "avc", "avi", "awb", "bmp", "cda", "dat", "divx", "doc", "docx", "dts",
    "flac", "flv", "gif", "htm", "html", "ifo", "jpeg", "jpg", "m4a", "m4b",
    "m4p", "m4r", "m4v", "mid", "midi", "mka", "mkv", "mmf", "mov", "mp2",
    "mp2v", "mp3", "mp4", "mpa", "mpc", "mpeg", "mpeg4", "mpg", "ofr", "ogg",
    "ogm", "pcx", "pdf", "png", "ppt", "pptx", "ra", "ram", "rm", "rmvb",
    "rtf", "smf", "swf", "tga", "tif", "tiff", "tp", "ts", "tta", "txt",
    "vob", "wav", "wma", "wmv", "wv", "xls", "3gpp", "jps", "cwdx", "csdx",
    "cpdx", "odt", "ods", "odp"
};
```

Absolute Control of Woolim’s Media Sources

Source: http://www.hoozo.cn/uploads/140908/1-140ZR24925135.jpg

Absolute Control of Woolim’s Media Sources

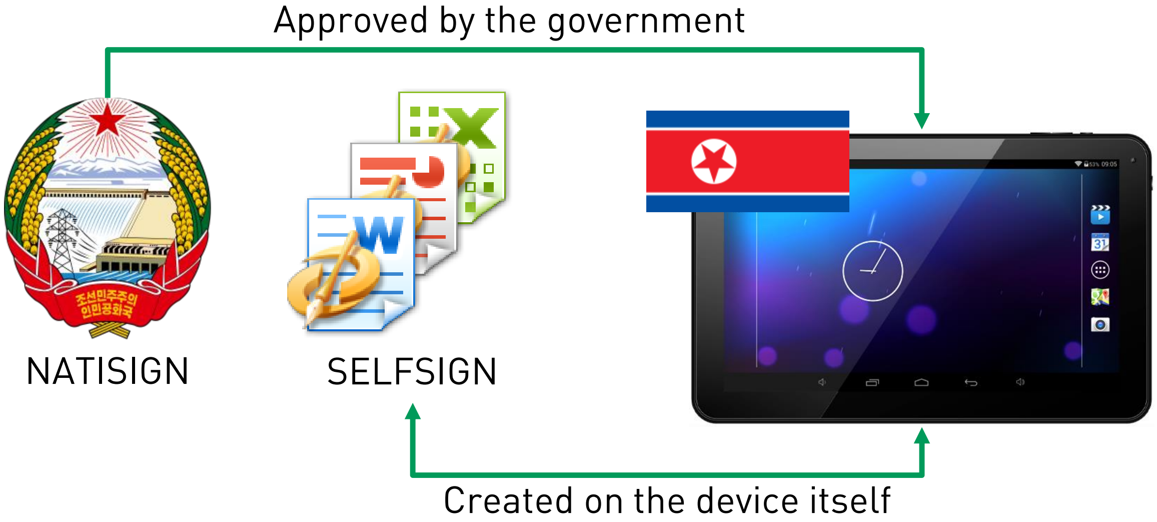


Approved by the government

NATISIGN

Source: http://www.hoozo.cn/uploads/140908/1-140ZR24925135.jpg

Absolute Control of Woolim’s Media Sources



Approved by the government

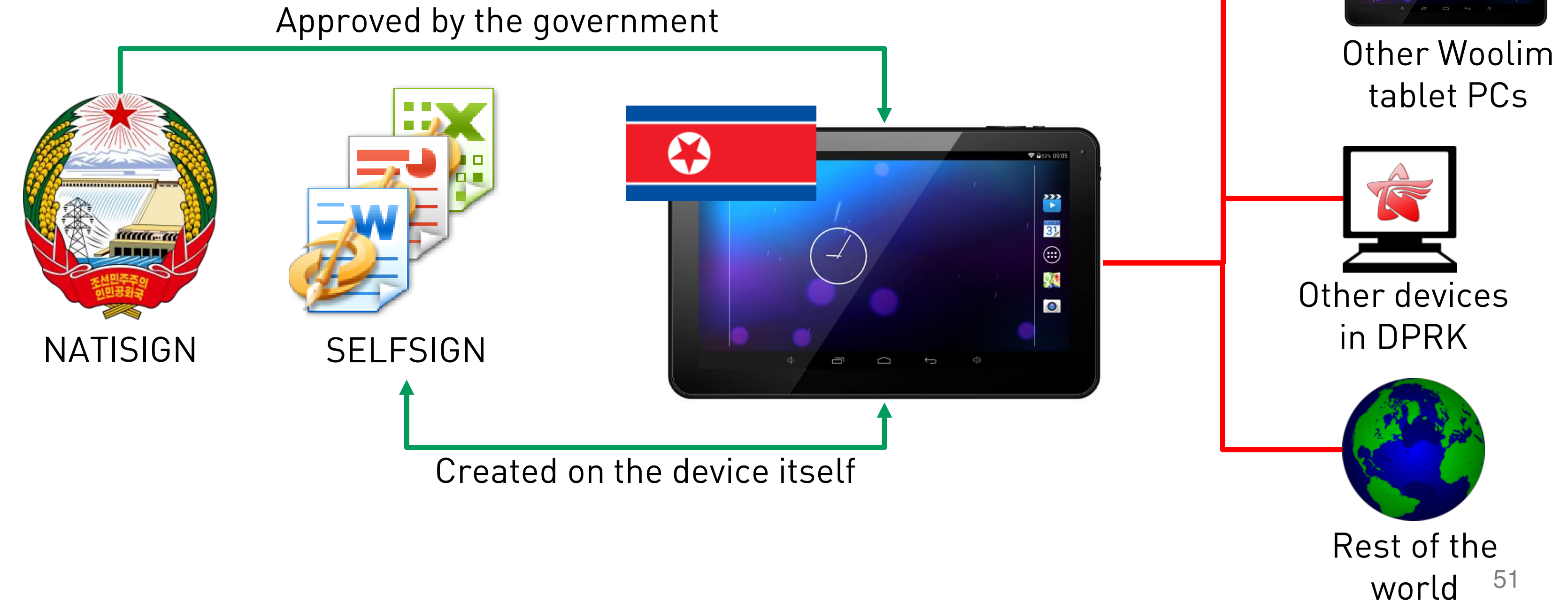
NATISIGN

SELFSIGN

Created on the device itself

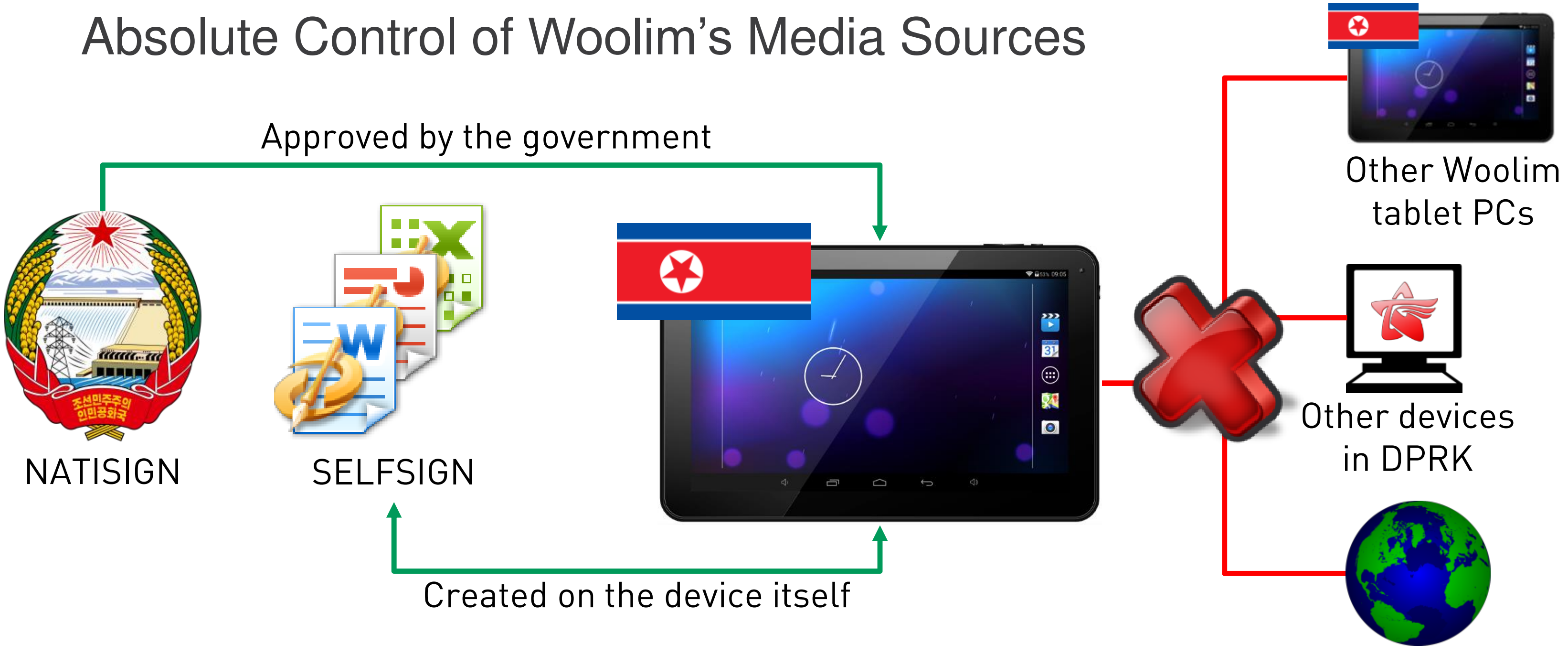
Source: http://www.hoozo.cn/uploads/140908/1-140ZR24925135.jpg

Absolute Control of Woolim's Media Sources



Source: http://www.hoozo.cn/uploads/140908/1-140ZR24925135.jpg

Absolute Control of Woolim's Media Sources



Approved by the government

NATISIGN

SELFSIGN

Created on the device itself

Other Woolim tablet PCs

Other devices in DPRK

Rest of the world

Source: http://www.hoozo.cn/uploads/140908/1-140ZR24925135.jpg

Thanks for Supporting our Research

- slipstream/RoL (@TheWack0lian)
  - For leaking the Red Star ISOs
- Will Scott (@willscott)
  - For translations and other information
- Iltaek
  - Translations
- ISFINK (www.isfink.org)
  - Freedom of Information in North Korea
  - Provided the tablet -> Big thank you!

Future Work

- Free some of the stuff from the tablet
  - Dictionaries
  - Books

Future Work

- Free some of the stuff from the tablet
  - Dictionaries
  - Books

- Anybody got a Smartphone from DPRK?
- Anybody got Software from DPRK?

→ We would love to take a look at more technology from DPRK!

ERNW providing security.

울림

33c3

Questions?

Florian:	@0x79
Niklaus:	@_takeshix
Manuel:	@MLubetzki

Source: http://1.bp.blogspot.com/-dySbc2VnF20/U-c8C7Z5nUI/AAAAAAAAE1k/imA6IocsiZw/s1600/kim-jong-un-looking-things+(2).jpg

Thank you for your attention!

Source: http://i.imgur.com/AEWrS7X.jpg