Exploring North Korea's Surveillance Technology

Florian Grunow & Niklaus Schiess
ERNW GmbH

Disclaimer

- We never visited DPRK
  - What we say about DPRK is mostly speculation or
  - based on publications of others.
- 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

- Introduction
- Surveillance
- Censorship
- Conclusions

Motivation

- Shed some light on repressive technology, even in 2017
- Overview of technical abilities to perform
  - Surveillance of their citizens
  - Censorship on a large scale
- Lack of public, in-depth research about technology by DPRK
- Disclosure to the public of potential surveillance and censorship

Previous Research

- Research done by us
  - Lifting the fog on Red Star OS (32C3)
  - Woolim: Lifting the fog on DPRK's latest tablet PC (33C3)

Previous Research

- Research done by us
  - Lifting the fog on Red Star OS (32C3)
  - Woolim: Lifting the fog on DPRK's latest tablet PC (33C3)
- Research done by others
  - Multiple publications concerning Red Star OS security (@hackerfantastic)
  - Art based on our Red Star OS research: Inter Alias (www.interalias.org)
  - Compromising Connectivity: Information Dynamics between the State & Society in a Digitizing North Korea - U.S.-Korea Institute (USKI) at SAIS

Modern Devices in a Repressive State

- DPRK started at around ~2000
- PCs, tablet PCs, mobile phones
- The problem: devices allow
  - access to media (photos, videos, audio),
  - sharing of media files and
  - potentially access information from outside of DPRK.
- Potential solutions:
  - Surveillance: tracking the distribution of unwanted/impure media
  - Censorship: prevent the distribution of unwanted/impure media

Red Star OS

Tracking the distribution of media files

Red Star OS

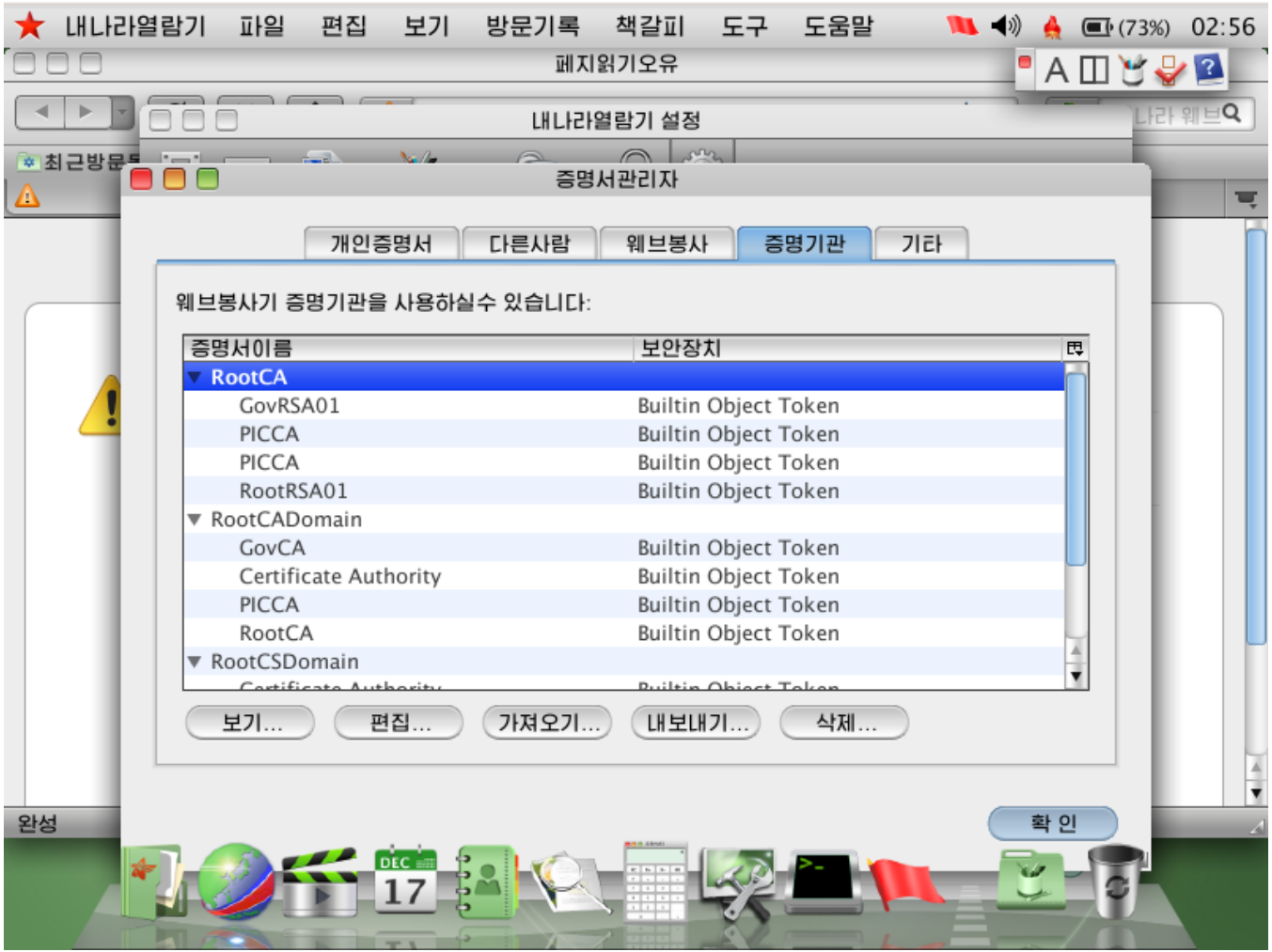
- Different leaked versions
  - Server (3.0) and Desktop (2.0 (and 2.5?) and 3.0)
  - We focused on Desktop 3.0
- General purpose desktop system based on Fedora and KDE
  - Look and Feel of Mac OS X
  - Email client, calendar, word processor, media player…
- Latest package builds in 2013
- Public leak in December 2014

TROOPERS


KFinder File Edit View Go Window Help
(85%) 02:28
Applications
Address Book
AppLink
Calculator
CHMViewer
Font Book
Grab
kCal
kPhoto
Mail
Naenara...wser 3.5
PDFEditor
Preview
QuickTime Player
Simple Text
Software Manager
Sogwang Office
Stickies
System ...ferences
UnBangUI
Utilities

TROOPERS

TROOPERS


내나라열람기 파일 편집 보기 방문기록 책갈피 도구 도움말
(73%) 02:56
페지읽기오유
내나라열람기 설정
증명서관리자
개인증명서
다른사람
웹브봉사
증명기관
기타
웹브봉사기 증명기관을 사용하실수 있습니다:
증명서이름
보안장치
RootCA
GovRSA01 Builtin Object Token
PICCA Builtin Object Token
PICCA Builtin Object Token
RootRSA01 Builtin Object Token
RootCADomain
GovCA Builtin Object Token
Certificate Authority Builtin Object Token
PICCA Builtin Object Token
RootCA Builtin Object Token
RootCSDomain
보기...
편집...
가져오기...
내보내기...
삭제...
확 인
완성
DEC
17

TROOPERS


KFinder File Edit View Go Window Help
(84%) 02:29
검사
파일검사를 완료하였습니다.
파일경로: /Users/kim/Download/.localized
결과
파일이름 경로
검사한 개수: 2
발견한 개수: 0
검사
일시정지
정지
제목없음 련결
DEC
17

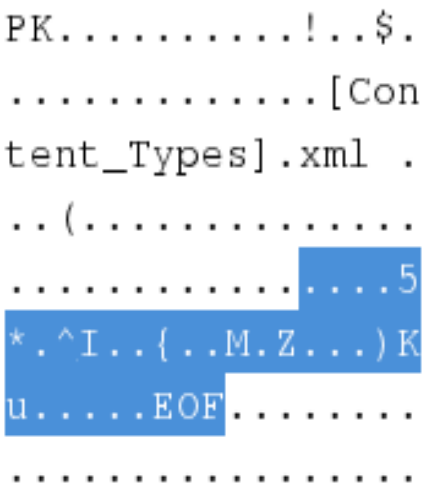
TROOPERS

Red Star OS Recap

→ Suspicious non-killable processes running

→ Integrity checking for core processes and files

→ Research revealed Red Star OS changes files



Original

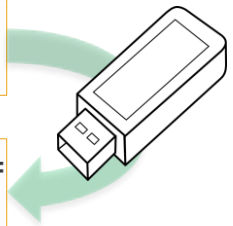
```
A5AD1102776A2E8FD5E5F5CF94FF003D ¥...wj..ÕåõÏ.ÿ.=
CBEB9F29FE7B97D73E53FCF72FAE7FA1 Ëë.)þ{.×>Sü÷/®.¡
DDFE7BFD5E0CFFD9                 Ýþ{ý^.ÿÙ
```

ERNW providing security.

TROOPERS

Original

```
A5AD1102776A2E8FD5E5F5CF94FF003D ¥...wj..ÕåõÏ.ÿ.=
CBEB9F29FE7B97D73E53FCF72FAE7FA1 Ëë.)þ{.×>Sü÷/®.¡
DDFE7BFD5E0CFFD9                 Ýþ{ý^.ÿÙ
```



First User
WMAC9A58CDZ364C

```
A5AD1102776A2E8FD5E5F5CF94FF003D ¥...wj..ÕåõÏ.ÿ.=
CBEB9F29FE7B97D73E53FCF72FAE7FA1 Ëë.)þ{.×>Sü÷/®.¡
DDFE7BFD5E0CFFD9E3E0D90455 9D35F9 Ýþ{ý^.ÿÙãàÙ.U.5ù
9B3BFDDA6BD6B6A95A13A0E6294B75B1 .;ýÚkÖ¶©Z. æ)Ku±
18000000454F46                   ....EOF
```

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

ERNW providing security.

TROOPERS

Original

```
A5AD1102776A2E8FD5E5F5CF94FF003D ¥...wj..ÕåõÏ.ÿ.=
CBEB9F29FE7B97D73E53FCF72FAE7FA1 Ëë.)þ{.×>Sü÷/®.¡
DDFE7BFD5E0CFFD9                 Ýþ{ý^.ÿÙ
```

First User
WMAC9A58CDZ364C

```
A5AD1102776A2E8FD5E5F5CF94FF003D ¥...wj..ÕåõÏ.ÿ.=
CBEB9F29FE7B97D73E53FCF72FAE7FA1 Ëë.)þ{.×>Sü÷/®.¡
DDFE7BFD5E0CFFD9E3E0D90455 9D35F9 Ýþ{ý^.ÿÙãàÙ.U.5ù
9B3BFDDA6BD6B6A95A13A0E6294B75B1 .;ýÚkÖ¶©Z. æ)Ku±
18000000454F46                   ....EOF
```

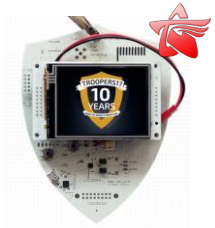
Second User
WM8295FF513293A

```
A5AD1102776A2E8FD5E5F5CF94FF003D ¥...wj..ÕåõÏ.ÿ.=
CBEB9F29FE7B97D73E53FCF72FAE7FA1 Ëë.)þ{.×>Sü÷/®.¡
DDFE7BFD5E0CFFD9E3E0D90455 9D35F9 Ýþ{ý^.ÿÙãàÙ.U.5ù
9B3BFDDA6BD6B6A95A13A0E6294B75B1 .;ýÚkÖ¶©Z. æ)Ku±
7908DFD0E092B2D128247E20315975B2 y.ßÐà.²Ñ($~ 1Yu²
5A13A0E6294B75B130000000454F46   Z. æ)Ku±0...EOF
```

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

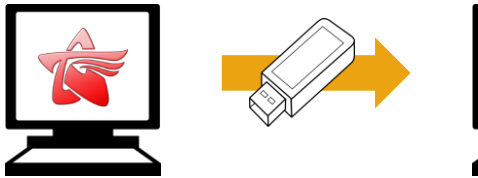
Tracking the Distribution of Media Files

User 1



Troopers.jpg

Tracking the Distribution of Media Files



User 1

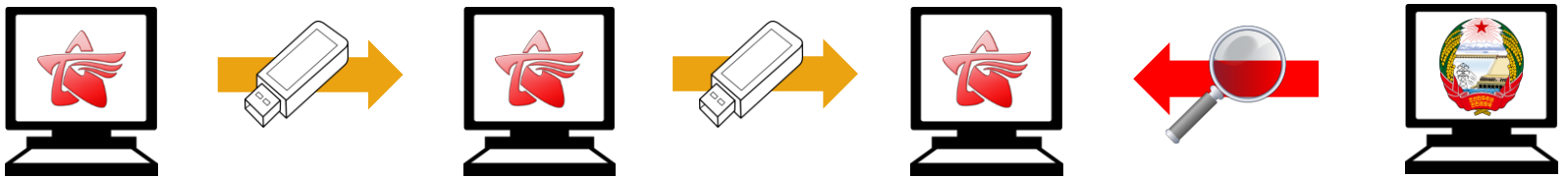
User 2

Troopers.jpg

Tracking the Distribution of Media Files

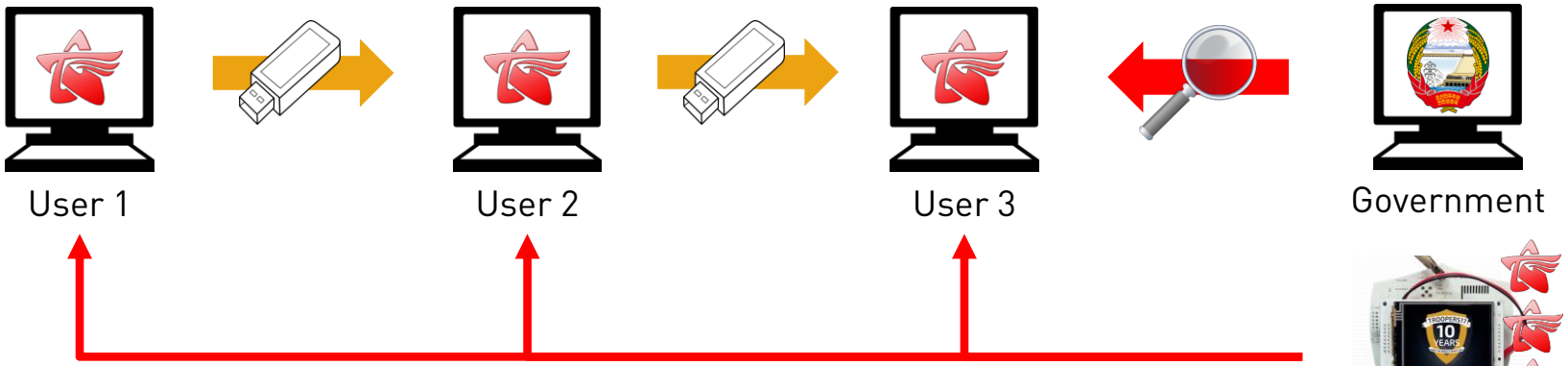
Troopers.jpg

Tracking the Distribution of Media Files



Troopers.jpg

Tracking the Distribution of Media Files



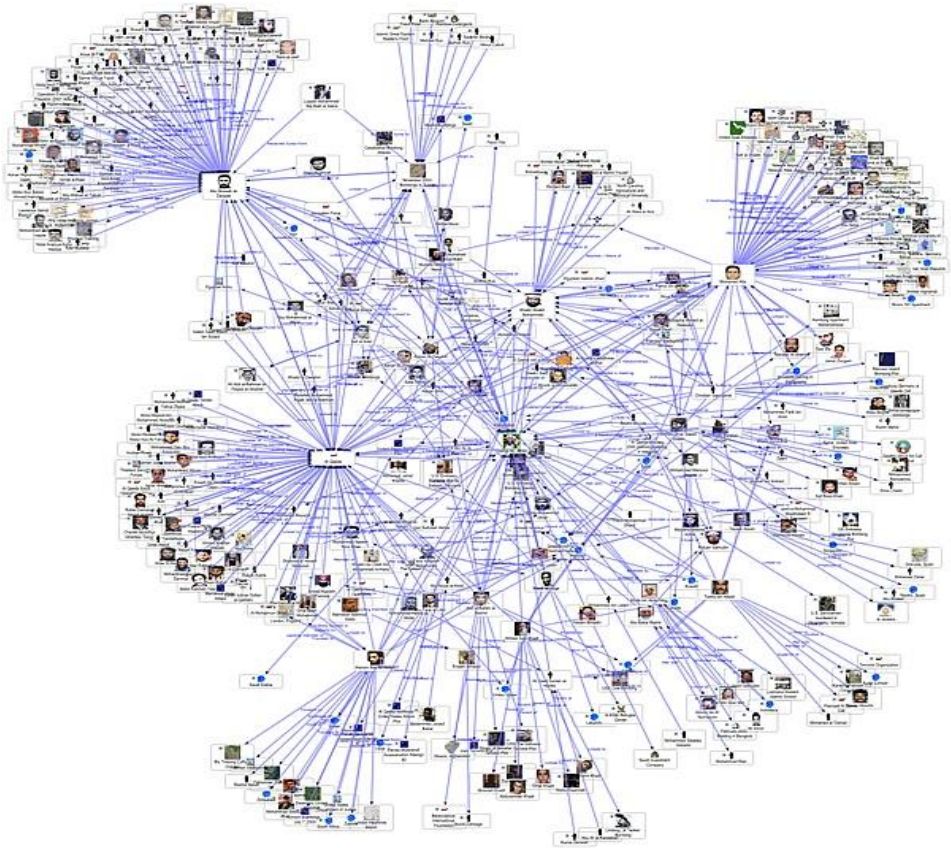
Troopers.jpg

ERNW
providing security.

TROOPERS

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

Problems with Red Star OS Watermarking

- Only affects media files
  - No binaries/applications -> users can install software
- Not really sophisticated
  - Can be removed/bypassed easily
- “AntiVirus” could prevent distribution of certain files
- Watermarking only allows to **track** the distribution of media
  - Does **not prevent** distribution of media

Woolim

Prevent the distribution of media files

Source: http://bilder4.n-tv.de/img/incoming/crop10413391/8721322747-cImg_16_9-w1200/RTR3EQ0B.jpg

Woolim

- Name of a waterfall in DPRK
- Manufacturer: Hoozo (Z100) from China
- Similar products sell for ~180€ to ~260€ online
- Software from/modified by DPRK
- Android 4.4.2 with Kernel 3.4.39
- System Information
  - Allwinner A33 (ARMv7) SoC
  - 8GB SK Hynix flash
  - MicroSD and power plug
- Connectivity only available via dongles (no WIFI/Bluetooth built-in)

Exploring “This is not signed file.”

- Introduces file signatures
  - Using asymmetric cryptography (RSA)
  - Goal: **PREVENT** the distribution of media files

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

Exploring “This is not signed file.”

- 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

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

Exploring “This is not signed file.”

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

ERNW
providing security.

TROOPERS

Signature Checking

- Java interface with native JNI library
  - Called by apps e.g. during file opening/saving
  - Sometimes concealed as “license checks”

Signature Checking

- Java interface with native JNI library
  - 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

Signature Checking

- Java interface with native JNI library
  - 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

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

```
 7 package gov.no.media.natsign;
 8
 9
10 public class MnsNative
11 {
12
13     public MnsNative()
14     {
15     }
16
17     public static native void getIMEIandIMSI(String s, String s1);
18
19     public static native int getNatSignInfoLen(String s, int ai[]);
20
21     public static native int isMagicCorrect(String s, int ai[]);
22
23     public static native int isNatSignFile(String s, int ai[]);
24
25     public static native void saveKeyToFile(byte abyte0[], int i);
26
27     public static native void savePatternToFile(byte abyte0[], int i);
28
29     public static native void saveSelfKeyToFile(byte abyte0[], int i);
30
31     private static final boolean D = true;
32     public static final String TAG = "MnsNative";
33
34     static
35     {
36         System.loadLibrary("medianatsign");
37     }
38 }
```

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

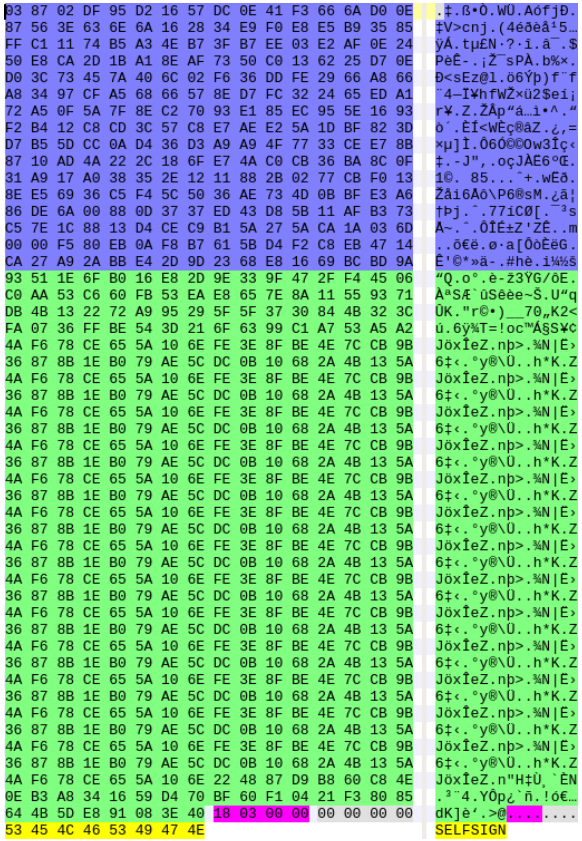
- Combination of
  - Symmetric encryption (Rijndael 256)
  - Asymmetric signatures (RSA)
  - Hashing (SHA224/SHA256)
- Device identity stored in legalref.dat
  - Comprised of IMEI and IMSI
  - Each device's „legal reference"
- Files created on the device itself can be opened
  - Camera images, office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

ERNW
providing security.

TROOPERS

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



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"
};
```

ERNW
providing security.

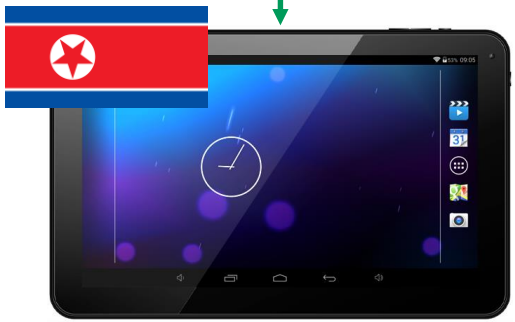
TROOPERS

Absolute Control of Woolim's Media Sources

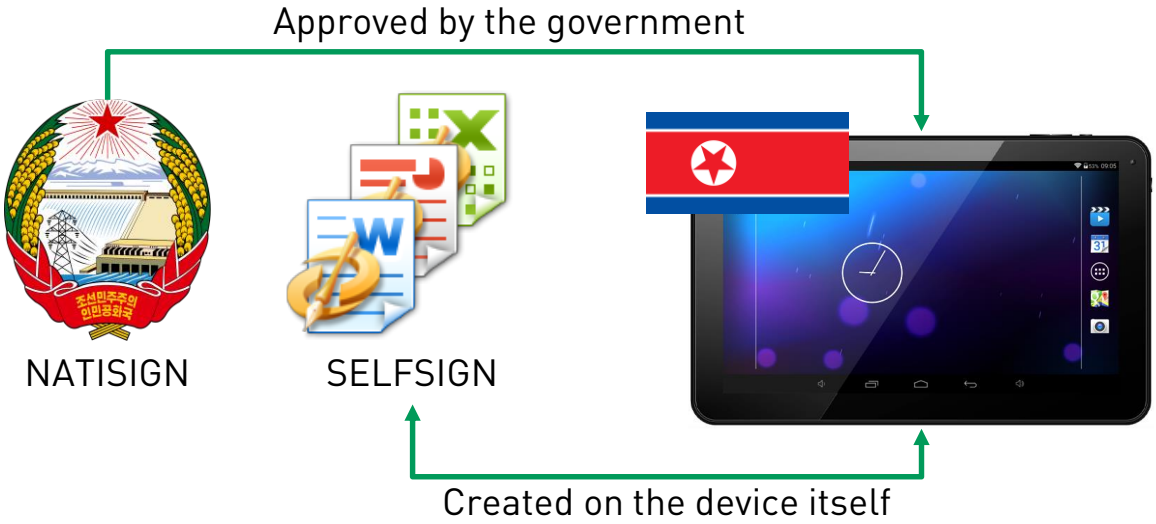
Absolute Control of Woolim's Media Sources

Approved by the government

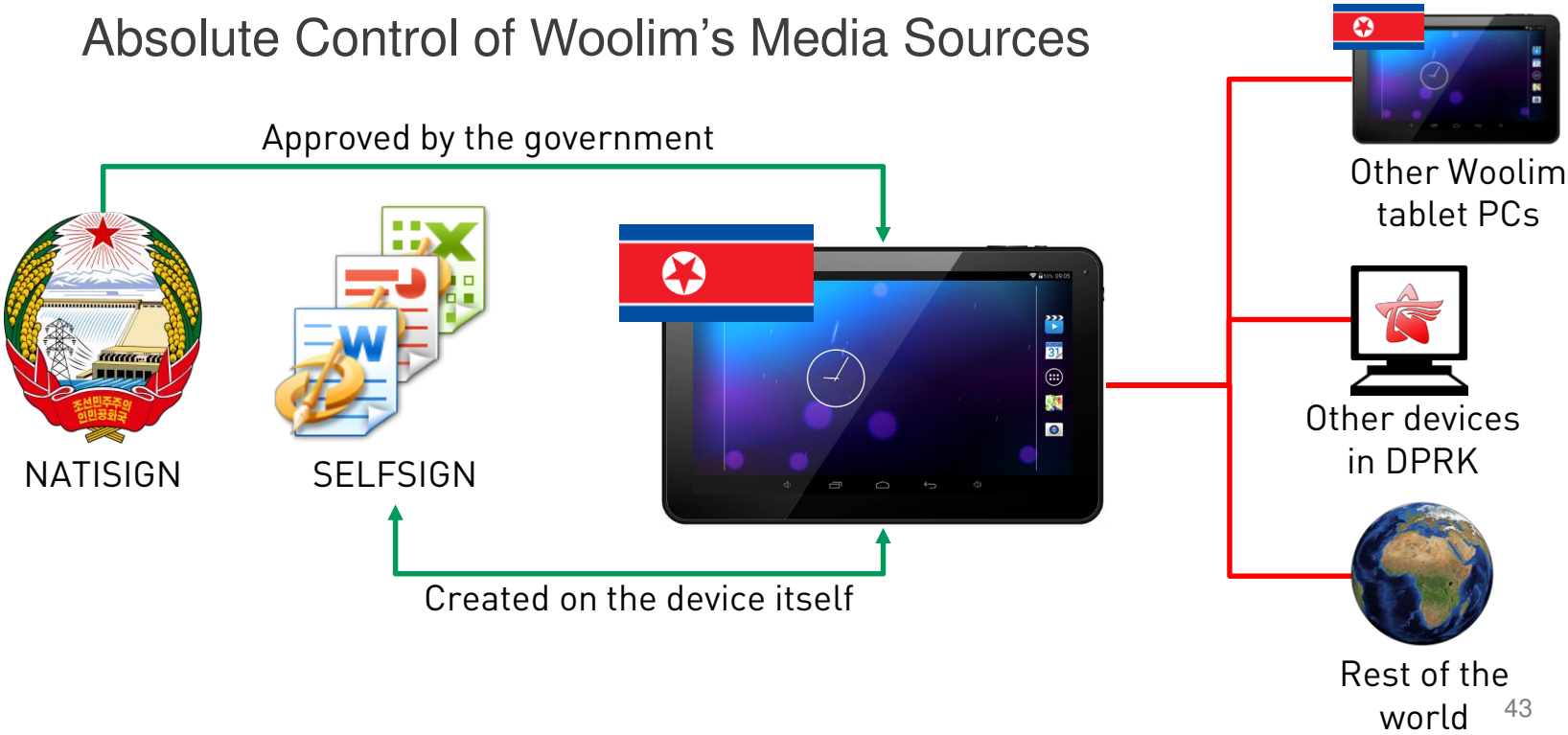
NATISIGN



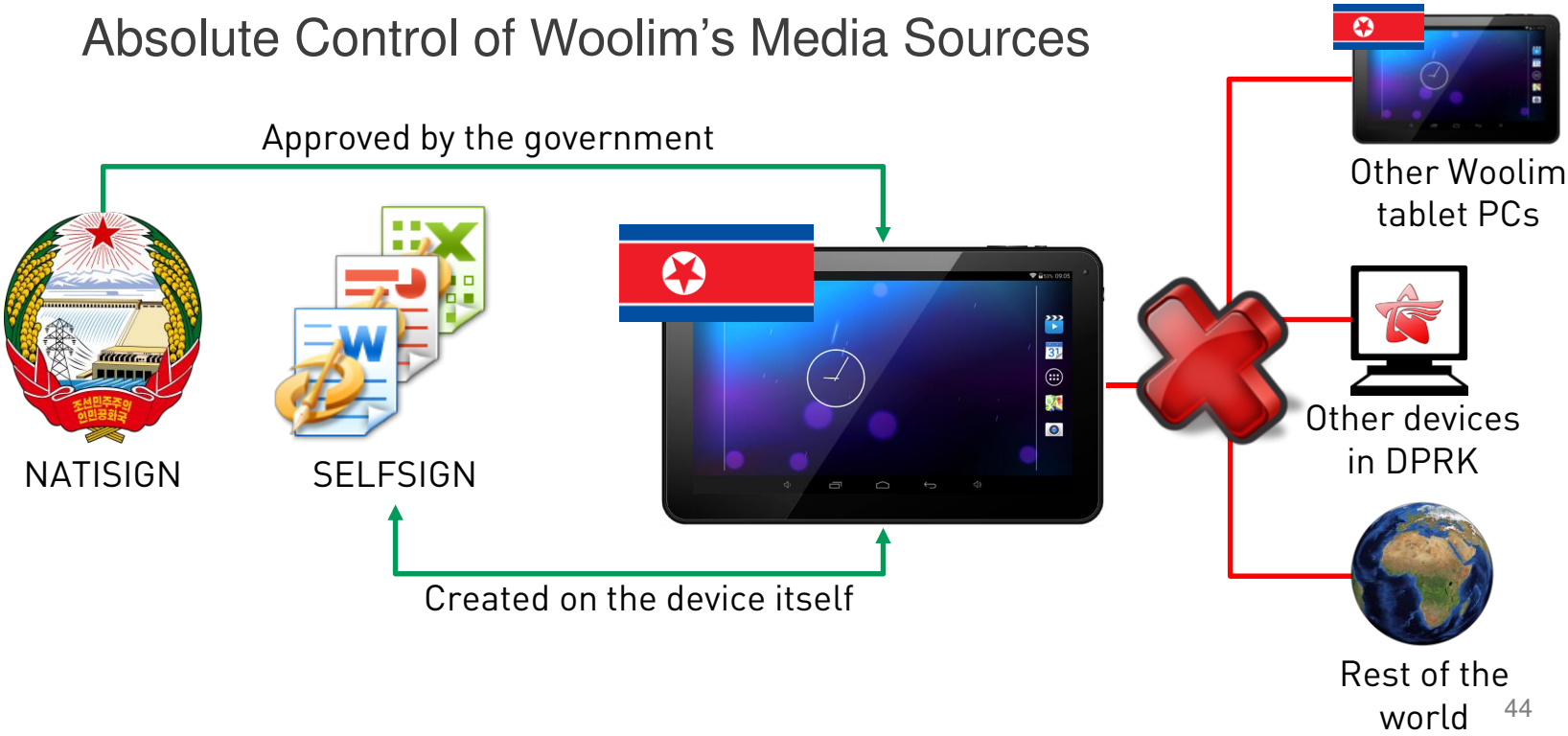
Absolute Control of Woolim's Media Sources



Absolute Control of Woolim's Media Sources



Absolute Control of Woolim's Media Sources



Network-level Surveillance and Censorship

- Network is controlled by the government
- No Internet access for most users
- Route all traffic over central nodes/proxies
- Only a few government-owned Certificate Authorities

Human-level Surveillance?

Human-level Surveillance

- Woolim includes TraceViewer
  - Take screenshots of apps
  - Records browser history
- Random physical inspections of mobile devices
  - Ranging from school teachers to members of special security units
  - Could identify inappropriate usage within minutes
- Prevents hiding impure files in removable media
  - Detecting inappropriate use is still possible if media will be removed
- Recorded histories and screenshots cannot be removed

Conclusions

Surveillance and Censorship

Source: https://www.zdf.de/assets/kim-jong-un-104~1920x1080

Surveillance and Censorship on Multiple Levels

- Network level
  - Government-controlled network
- Device level
  - Track distribution of media files via watermarks and signatures
  - Prevent distribution of media files with signatures
- Human level
  - Take screenshots and record browser histories
  - Make them easily accessible for random inspections via TraceViewer

Thanks for Supporting our Research

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

Future Work

- Dump of multiple devices (tablets and smartphones)
  - We don't have access to these devices
- AntiVirus software

- Anybody got a smartphone from DPRK?
- Anybody got software from DPRK?
- "signed XP"?

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

Thank you for your Attention!

{fgrunow,nschiess}@ernw.de

www.ernw.de

@0x79
@_takeshix

www.insinuator.net