Governmental Control of Digital Media Distribution in North Korea: Surveillance and Censorship on Modern Consumer Devices

Niklaus Schiess
ERNW GmbH

Abstract

Modern devices like PCs and tablet PCs enable users to consume a wide range of media like videos, audio and documents. Introducing such devices in repressive regimes like North Korea [10] (officially Democratic People's Republic of Korea, DPRK) contradicts the objective of controlling and suppressing information within the country and particularly information imported from the outside world. This can be generalized as any information that has not been reviewed and approved by the government. This paper is an effort to evaluate the technical challenges that arise while enabling users to consume or create potentially unwanted media and analyzes two media-controlling mechanisms developed by North Korean government organizations. The analysis covers implementations found in Red Star OS, a Linux-based operating system developed by the Korean Computer Center, and Woolim, an North Korean tablet PC that is based on the Android operating system. We will conclude about the effectiveness and implication on the distribution of digital media within North Korea and how these mechanisms have evolved in the analyzed products over the past several years.

1 Introduction

The lack of openly available, in-depth reports of modern technology developed and deployed by repressive regimes makes it difficult to assess the capabilities and scale of surveillance and censorship carried out today. As consumer devices that allow to interconnect individuals and groups of people to form social networks are prevailing, sharing information and media becomes easier than ever. To thwart the distribution of unwanted, or impure [11], media, North Korea has begun to develop countermeasures over the past decade [11].

A well-established approach for media-control is censorship on the network level, as it is known that repressive regimes like China [14], Iran [7] or Turkey [6] are using national telecommunication networks as an instrument to interfere with information flows within their country and even across borders [13]. In the case of North Korea, which is considered one of the most repressive states [11], where typical users only get access to a nationwide intranet that is entirely controlled by the government. Full Internet access, without any governmental regulations and restrictions of the consumable content, is only possible for a chosen few [12].

1.1 Motivation

Although network-level control over media distribution can be effective even on a nationwide scale, the effectiveness is limited in a technical less advanced environment like North Korea today [11]. For a country that still lacks proper coverage of telecommunication networks, especially outside of larger cities like Pyongyang [11], a multitude of devices will most likely never be connected to any network. As media from the outside world was historically shared and consumed via removable media like flash drives and memory cards on devices like DVD players [11], network-level measures are de facto superfluous. Device level measures for media control have been implemented in North Korean products to complement the network measures.

1.2 Contributions

This paper examines measures that have been introduced in North Korean products to develop surveillance and censorship mechanisms that adapt to the country's environment. The analysis is an effort to uncover the inner workings of the media controling capabilities of North Korean software. It is meant to provide a better understanding how North Korea uses open-source software to suppress free speech. Especially for organizations that dedicate their work to importing information into North

Korea [5, 2], it is important to understand how modern devices might try to prevent spreading digital media within the country. The analysis follows a reverse-engineering approach because the source of the North Korea software is not available. The focus lies on privacy aspects and does not cover the security-related topics. Therefore, the results might not cover all implementational details as these are either not available or could not be extracted via reverse-engineering completely.

1.3 Related Work

The overall concept of surveillance and censorship of media and communication on modern devices has been analyzed with a focus on governmental capabilities to control nation-wide telecommunication networks. [14, 7, 6, 12] This work focusses on the technical analysis of software and devices either developed or distributed by North Korean government organizations. These have either been leaked to the Internet or are not known to be available for analysis to the outside world. At the point of this writing there is no comparable research that covers North Korean technology in a similar depth.

2 General Insights

This work is based on two North Korean products that, based on information that has been extracted from the analyzed software, have been mainly developed by government-controlled organizations. Background information about the inner workings of these products is crucial to understand the effectiveness and limitations in terms of their surveillance and censorship capabilities.

2.1 Red Star OS

In late 2014 the ISOs of Red Star OS have been leaked to the public [4]. Prior to this leak there was barely any information available as it is not available outside of North Korea. The release included a desktop and a server edition, both based on the Fedora Linux distribution [1]. This work focusses on version 3 of the desktop edition (an older version 2 is also publicly available) that provides a KDE-based graphical environment that reassembles the looks of OS X. The default installation ships with a suite of software that enables users to utilize it as a general-purpose operating system.

The system implements a sophisticated architecture of processes that are monitoring each other to preserve the integrity of the system. The integrity of files that are responsible for starting these processes is ensured by SELinux rules and a daemon called *securityd* that checks the integrity of various files with a hardcoded list of checksums. Even after disabling SELinux, altering one of these files will result in an instant reboot of the system. As these checks are also done during the boot process, the system will be trapped in a reboot loop which renders the system unusable. These processes are using a kernel module (rtscan.ko) that provides an interface (/dev/res) that allows to protect files and services from altering and killing, even for the root user.

The goal of these integrity measures is to protect two processes. One is *scnprc*, which is disguised as a antivirus tool, that runs in the background and checks files against a list of patterns. It also provides a GUI component that can be used to interact with the process to some extent. The second one is *opprc*, a process that is started by *scnprc*, which carries out activities that are decoupled from its parent process. The main feature of *opprc* is to apply watermarks to media files. These watermarks are comprised of the hard disk serial that allows third parties to identify a specific Red Star OS instance. Depending on the media file type the process uses different strategies to determine where these watermarks are applied but the structure of the watermarks is always the same. For the sake of simplicity, the rest of this paper will assume watermarking of JPEG files, where watermarks are simply appended to the end of a file. As the JPEG standard defines magic bytes to determine the end of a file (`0xFFD9`), the difference between the original file and any appended watermarks is easily recognizable.

Prior to appending watermarks to media files, *opprc* encrypts them with DES and a hardcoded encryption key. The developers might attempt to obscure the content of the watermarks or make it more difficult to tamper with them. But due to the hardcoded key, these watermarks can be forged with little effort.

2.2 Woolim

Woolim (alternatively translated to Ulrim) is a North Korean tablet PC. At the time of writing, it is one of the latest models in a range of approximately four different generations of North Korean tablet PCs. The hardware of Woolim is an import from the Chinese manufacturer Hoozo [3] and is sold under the model name Z100. It is running Android 4.2 (KitKat) and the build dates of the analyzed device date back to the end of 2015.

Woolim implements mechanisms to append device identifying data to media files like Red Star OS. But the structure is fundamentally different because it contains more data and is therefore larger in size and it uses stronger cryptographic algorithms to obscure its content. Compared to Red Star OS, this data is not only encrypted but it also includes a signature to ensure the authenticity and integrity of the appended data. Woolim supports two types of signatures that are denoted by an ASCII encoded string suffix that is appended to each signature:

- *NATISIGN* signatures, also referenced as *gov_sign* in the analyzed code, are applied to media files by the government in order to determine files that have been approved for distribution. NATISIGN is a simple RSA signature that is appended to media files together with some minor structure information.

- *SELFSIGN* signatures are applied to media files to allow Woolim devices to consume media that has been created on the device itself (e.g. camera photos or document files). SELFSIGN signatures also include a watermark that identifies the device that created the media file or the signature respectively.

Compared to NATISIGN, the SELFSIGN signature carries slightly more information that allows to identify the device that created the signature. As this is not required for the NATISIGN mechanism, the structure of both signature types differ. The C struct shown in Listing 1 defines the format of a SELFSIGN signature.

```
struct SELFSIGN {
  char rsa_signature[256];
  char encrypted_identity[520];
  int32_t signature_length; /* 792 */
  int32_t padding; /* NULL */
  char suffix[8]; /* "SELFSIGN" */
};
```

Listing 1: SELFSIGN signature struct

The encrypted identity is comprised of the IMSI [9] and IMEI [9] of the creating device and is encrypted with the Rijndael [8] block cipher using 256 bit blocks and a hardcoded 256 bit encryption key. Besides the identity information and the used encryption algorithm, the encryption scheme and used keys are like the implementation of Red Star OS. Although the device has no built-in networking or telecommunication functionality, the implementation is likely using IMSI and IMEI for device identification because the same implementation could be used by other Android-based North Korean devices like smartphones.

The signatures are applied and checked by a system library that is used by various applications. These applications must make sure that they explicitly check signatures. Unlike the watermarking implementation of Red Star OS, that is done implicitly by processes running in the background, each application is responsible for properly applying and checking these signatures. The library is generally used by all applications that are meant to consume media files like the image viewer (*Gallery2.apk*), music player (*Music.apk*) or text editor (*TextEditor.apk*). In addition to these media-related applications there are also system related applications like a file manager (*FileBrowser.apk*) and even an application installer (*PackageInstaller.apk*) that implement these signature checks. Therefore, the North Korean government can not only control the types of media files that can be consumed on Woolim devices, but also the applications that can be installed.

3 Implications on Media Distribution

The previously discussed implementations of media-controlling mechanisms can influence media distribution in different ways. In the following we will assess the impact of these implementations based on two aspects:

Surveillance Tracking the distribution of digital media files to identify sources of impure media and create social networks by tracing the transfer from system to system. It allows to identify who had access to a specific media file, the path of distribution and eventually allows to shut down the sources that create or import such media files.

Censorship Preventing the distribution of media by attaching cryptographically signed data to digital media files. Valid signatures can only be created by authoritative organizations that have access to the private part of a preinstalled key pair whereas consumer devices verify them with the public part. Censorship makes sure that the distribution of digital media files is only possible if they have been reviewed and approved by the government. Non-approved media files cannot be opened on devices that implement compatible signature checks.

The following sections will discuss in detail how the developers of Red Star OS and Woolim achieving these goals. The discussion will also highlight the issues and limiting factors of the analyzed implementations.

3.1 Tracking the Distribution of Digital Media Files

Applying watermarks to media files that identify a system is a quite effective way to track which system had access to an allegedly impure media file. An even more interesting property of Red Star OS is that if a media file already includes one or more watermarks, it will continue to append the current system's watermark (provided it is not equal to the most recent watermark). Transferring a media file between multiple systems running Red Star OS therefore results in a list of watermarks appended to this file. This list will then allow to trace back and identify all systems that had access to this file. Figure 1 illustrates how the list of watermarks appended to a media file extends when it will be transferred between multiple systems in line via removable media.

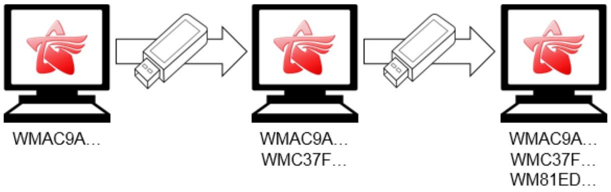

Figure 1: Watermarking on Red Star OS

Apart from identifying parties involved in the media distribution this list of watermarks also allows to reconstruct the line of distribution. It shows which user gave media files to other users and it reveals the very first Red Star OS based system that had access to a potentially forbidden file. The first user in the list of watermarks is therefore not necessarily the one who created or imported the media file. So, this measure is ineffective for systems that do not run Red Star OS or any other OS that implements watermarking mechanisms compatible to Red Star OS.

When the North Korean government gets hold of impure media files e.g. by accessing a suspect's system that is running Red Star OS, it allows them to identify where they got the file from. If the file has traversed multiple systems, it might also allow to identify connections between dissidents that may lead to further investigations and shutdowns of sources of impure media files.

Although tracking the distribution of media files with watermarks can be effective to some extent, there are various limitations that reduce the effectiveness. As watermarks are only applied by Red Star OS based systems and devices that implement compatible mechanisms, this does not apply to any other systems. Therefore, all other systems that are operated will not append any watermarks which makes them not traceable via this mechanism. Another problem is that watermarks are not mandatory so they can just be removed from media files. Even if this is done on Red Star OS, where the watermark of the current system will be applied even if the list of watermarks will be removed or is empty in the first place, it allows to hide any other systems that had access to the file previously.

In terms of hiding users that participate in the distribution of media files, watermarks can be forged easily. Encrypting random watermarks and append them to media files is simple and can be done even on Red Star OS. This allows to erase all traces of Red Star OS based systems that previously had access to impure files. From a technical point of view the Red Star OS watermarking mechanism can be bypassed and forged without much effort. But it is hard for North Korean citizens that do not have access to information on the Internet and systems that allow to properly analyze the corresponding implementations.

3.2 Preventing the Distribution of Digital Media Files

Tracking the distribution of media files allows to identify parties that participate in the distribution but could not prevent any loss of control in terms of digital media distribution. Especially imported media from the outside world is a threat to the North Korean regime, therefore the goal shifts from simple surveillance to full censorship of unwanted media [11]. The NATISIGN signatures applied and checked by Woolim provide a strong control over media sources for the North Korean government. Media files that can be distributed to users of Woolim devices must be approved and signed by an authoritative organization. All other media files can not be consumed these devices.

Whenever a user tries to open a media file on a Woolim device, the application looks for a signature at the end of the file. If there is a signature, it first checks whether the signature is a valid NATISIGN signature and then tries to check if it is a valid SELFSIGN signature. Figure 2 illustrates the process of signature checking of media files on Woolim.

If the signature check fails, the applications will refuse to open the media files. In the case of files that contain a valid SELFSIGN signature, the media file has been created on the device itself. Even though the signature will be created with a preinstalled private key that is most likely the same on all devices, the signature checks can determine the device that created the file with the encrypted identity that contains the IMSI and IMEI. In any other case, e.g. the file has been copied from removable media to the Woolim device, the file requires a valid NATISIGN signature. These are files that have been approved by an authoritative government organization at some point in time. This gives the government absolute control over media files that can be distributed to Woolim devices and all systems that implement compatible signature checking mechanisms. Any file that lacks this approval, like files that have been imported illegally, will not be consumable on any Woolim device.

4 Conclusions

4.1 Summary

The presented work gives a brief insight into recent developments of surveillance and censorship mechanisms for media files on two modern, North Korean devices. It

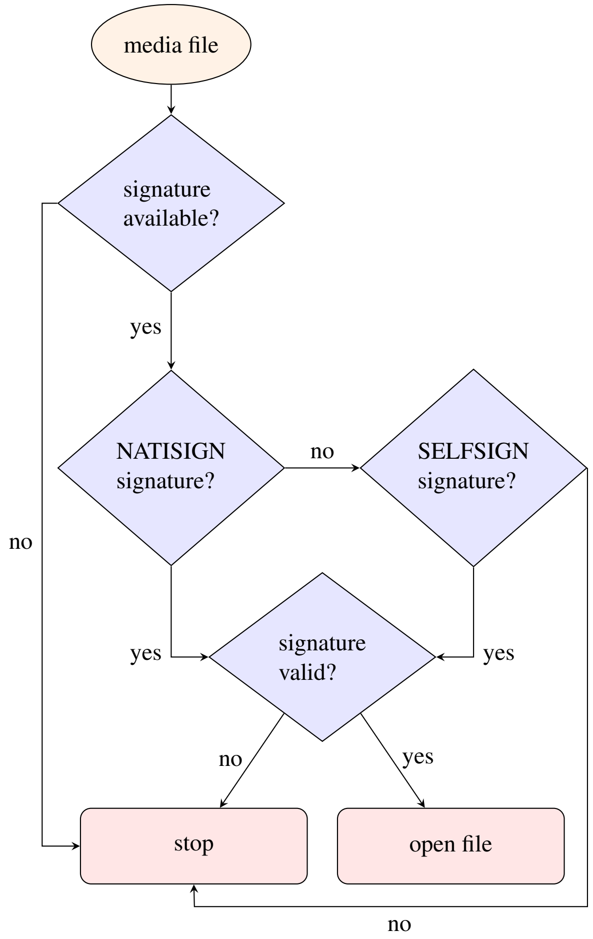

Figure 2: Signature checking on Woolim

demonstrates how a government might try to gain control over digital media sources to reduce the potential loss of control by providing access to modern devices. The North Korean government tries to reduce the impact of information imported from the outside world but still tries to enable its citizens to experience the advances of a modern, connected world.

Even with the known infrastructural deficiencies within the country, that makes comprehensive propagation of modern networked devices and systems almost unfeasible, they try to expand their controlling mechanisms to the device level. The adaption of surveillance and censorship to devices that will probably never be connected to any network is a remarkable step to increase the effectiveness of a nationwide control over media sources.

The outcomes of this work also show that the two North Korean products share large parts of functionalities and implementational principles. Analyzing Red Star OS and Woolim shows that Woolim is in various was an extended and improved version of functionality that was already available in Red Star OS. Woolim seems to be a further step in the evolution of North Korean devices that are built to obey governmental media restrictions on devices and systems that are built on open source software.

Various aspects in analyzed implementations show that both Red Star OS and Woolim have most likely been developed by the same group of developers or at least the same governmental organization. An illustrative example are the similarities found in the encryption algorithms and schemes that are used to obscure device identifying information in watermarks and signatures. Red Star OS uses the DES block cipher whereas Woolim uses the Rijndael block cipher, the base algorithm for the successor standard of DES called AES [8]. Regardless of the implementation both use a hardcoded encryption key, which in both cases is just a consecutive string of numbers ranging from one to seven for DES and 31 for Rijndael respectively. The patterns are identical and the size difference is just based on the supported key sizes of the used encryption algorithms.

4.2 Limitations

Due to the fact that the source code of the analyzed products is not available, this work might not cover all implementational aspects. It is possible that there are additional measures that could not yet be identified by reverse-engineering. The implications on media distribution are also only covered from a technical perspective. Therefore, this work only shows what the media controlling measures could accomplish and not what is actually enforced by the North Korean government today.

4.3 Future Work

It is planned to release further research about North Korean software, focusing on anti-virus products. This is currently still work in progress and will hopefully be released towards the end of this year.

5 Acknowledgments

The analysis of the Woolim tablet PC and other devices and software have been enabled by ISFINK. The author would like to thank them for their support and valuable input during this research.

References

[1] Fedora linux. https://getfedora.org/. Accessed: 2017-05-26.

[2] Flash drives for freedom. http://www.flashdrivesforfreedom.org/. Accessed: 2017-05-26.

[3] Hoozo. http://hoozo.cn/. Accessed: 2017-05-26.

[4] I managed to get a hold of the latest version of that north korean linux distro, in some shape or form. here's a torrent of red star os 3.0 server. https://www.reddit.com/r/linux/comments/272zxf/i_managed_to_get_a_hold_of_the_latest_version_of/. Accessed: 2017-05-26.

[5] International solidarity for freedom of information in north korea. http://isfink.org/. Accessed: 2017-05-26.

[6] Akdeniz, Y. Report of the osce representative on freedom of the media on turkey and internet censorship. *Organizace pro bezpečnost a spolupráci v Evropě, publikováno 18*, 1 (2010).

[7] Aryan, S., Aryan, H., and Halderman, J. A. Internet censorship in iran: A first look. In *FOCI* (2013).

[8] Daemen, J., and Rijmen, V. *The design of Rijndael: AES-the advanced encryption standard*. Springer Science & Business Media, 2013.

[9] Koien, G. M. An introduction to access security in umts. *IEEE Wireless Communications 11*, 1 (2004), 8–18.

[10] Mansourov, A. *Bytes and Bullets: Information Technology Revolution and National Security on the Korean Peninsula*. Asia Pacific Center for Security Studies, 2005.

[11] Nat Kretchun, Catherine Lee, S. T. Compromising connectivity: Information dynamics between the state & society in a digitizing north korea.

[12] Warf, B. The hermit kingdom in cyberspace: unveiling the north korean internet. *Information, Communication & Society 18*, 1 (2015), 109–120.

[13] Winter, P., and Lindskog, S. How the great firewall of china is blocking tor. In *FOCI* (2012).

[14] Xu, X., Mao, Z. M., and Halderman, J. A. Internet censorship in china: Where does the filtering occur? In *International Conference on Passive and Active Network Measurement* (2011), Springer, pp. 133–142.