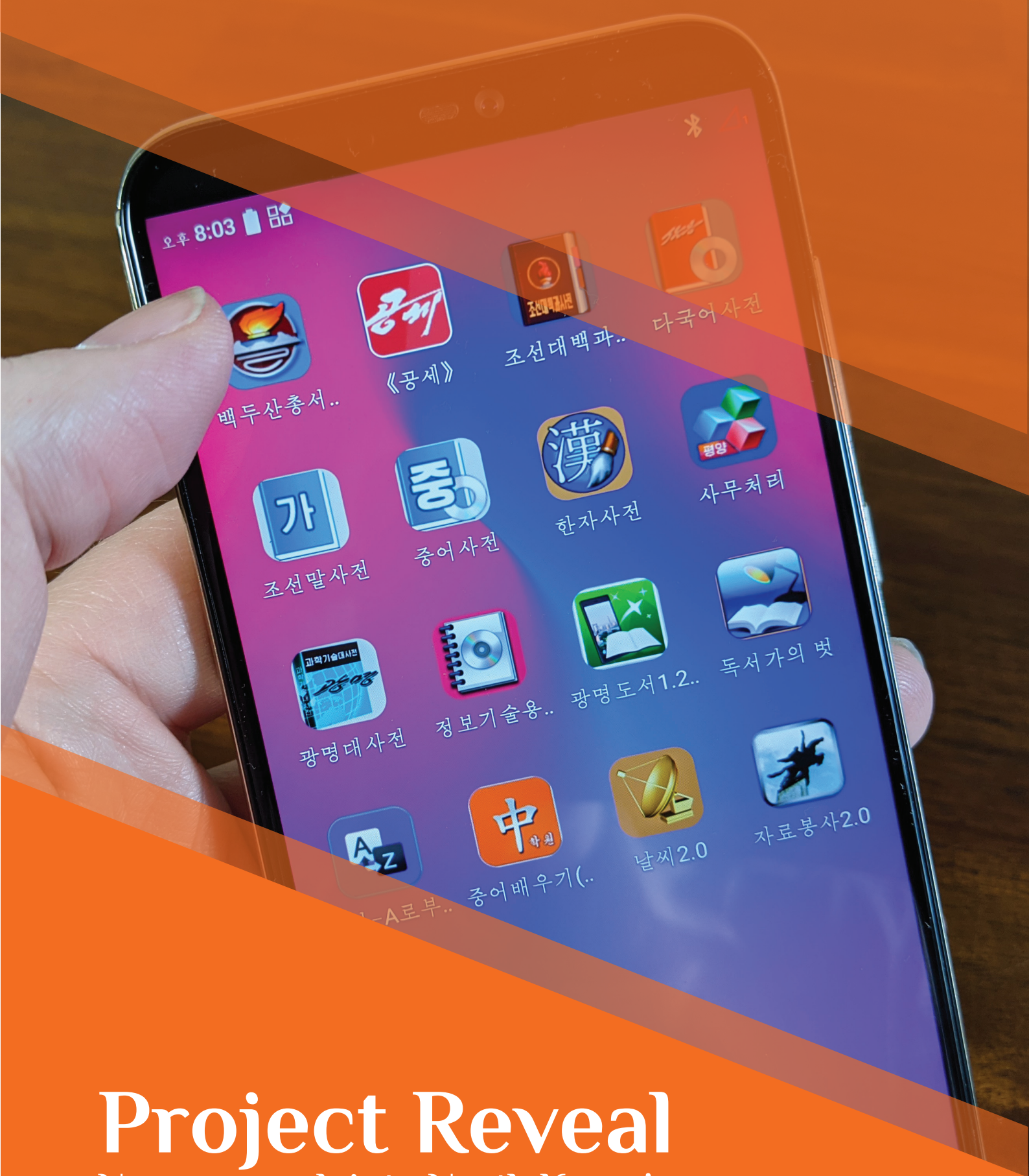


Project Reveal

New research into North Korea's digital control system

Martyn Williams and Niklaus Schiess

Project Reveal

New research into North Korea's digital control system

Martyn Williams and Niklaus Schiess

CONTENTS

EXECUTIVE SUMMARY

The availability of the Internet and smartphones has transformed societies around the world. Citizens now can access knowledge from around the globe, seek out independent news coverage and voice their opinion with little filter. While state controls exist to varying degrees in some countries, nowhere is the control as complete and restrictive as North Korea.

While the smartphones available in Pyongyang are little different to those available in other countries, the installation of custom software, a closed communications network and constant monitoring, mean the device in North Korea is useful to consumers for little more than consumption of state-approved propaganda.

However, for the state, smartphones constitute a potentially potent vector for remote surveillance at scale. To date, there is no evidence that metadata is being exploited at a large scale for surveillance purposes, but this is an area that must be monitored.

Much of North Korea's information control system is based on the same technologies that underpin the Internet and smartphones globally but rather than expanding access to knowledge, North Korean engineers have removed or modified features to block it.

In our research, we examined two current North Korean devices to determine recent changes in the information control landscape.

• WI-FI

One of the most interesting changes has been the reintroduction of Wi-Fi to North Korean devices. It had been disabled for years but the Taeyang 8321 tablet includes an app for Mirae, a new Wi-Fi network in central Pyongyang.

Analysis of the app reveals subscribers are required to use a username, password, SIM Card and be using an approved device to gain access to the network. The use of a SIM Card is unusual, but the engineers chose an international standard for the authentication. The Wi-Fi network settings are hard coded into the app and cannot be changed by the user. The Wi-Fi portion of the settings app has been disabled removing the ability to search for other networks.

As a result, the tablet can be used to connect to the Mirae network but no others. This allows North Korean authorities the ability to provide wifi-based intranet connectivity while preserving a level of network access control consistent with mobile provider-based intranet data access.

This demonstrates that North Korean engineers continue to take existing technology and modify it to their needs, typically by removing or restricting features. Certain technological features generally appear to be reintroduced only when the level of control and security is sufficient.

• HACKING

In the course of our research, we interviewed two North Korean escapees who revealed the existence of a small hacking culture inside North Korea. It had previously been assumed that North Koreans, lacking access to the Internet, would find it difficult to gain the knowledge to hack Android smartphones but that is not the case. However, the nature of the "hacks" are notable as they must be conducted locally on the device, leveraging at most a second linked device, rather than more traditional hacks which leverage network connectivity to exploit vulnerabilities. In other words, the techniques they developed, were extremely specific to the nature of North Korean devices and software in their purpose and execution.

One of the escapees worked in China as a software engineer for a state enterprise and smuggled Chinese hacking software back into the country upon his return. Another was part of the group of computer science students at the prestigious Kim Il Sung University that swapped tools and tips amongst themselves.

The motivation for hacking wasn't always related to breaking the state's control on unrestricted consumption of illicit media. Sometimes, handsets were hacked to clear the memory of files so the phones could reach a higher price on the secondhand market.

Both escapees interviewed said that the number of people actively able to hack phones was small, but it is notable that it existed.

• TECHNICAL RESPONSE

Among the state's technical responses to hacking appears to be the disabling of USB file transfer functions on smartphones. Technical analysis of a Pyongyang 2425 handset, released in 2019, was severely hampered by the inability to access the phone memory over USB. In previous North Korean handsets, the USB interface had always provided access but the same wasn't possible in the latest handset.

The escapees we interviewed said that they disabled the state control software by installing software via the USB interface, so it is possible that state engineers responded by disabling this route into the phone.

This was the case with Wi-Fi. When it was discovered that it was being used to access the open Internet, the state disabled it in all phones. It was only reintroduced recently, as previously mentioned, once controls had been designed to ensure it could only be used for approved purposed.

•NEW LAWS

Another measure of the degree to which hacking is becoming an issue came in the Reactionary Ideology and Culture Rejection Law that was enacted in 2020.

The law seeks to punish those found in possession of foreign culture with anywhere from years in labor reform to death. Included in the law is specific prohibition against "Illegally installing a phone manipulation program." While it is difficult to estimate the number of North Koreans modifying their phones and interviewees did not seem to think the practice was widespread, the existence of this specific wording would imply it is happening at a scale where authorities are aware and potentially concerned.

The law also takes issue with a number of associated issues related to foreign media access and consumption and offers other clues as to current issues inside the country.

One article imposes a fine if people are found with a smartphone that doesn't contain the state software for blocking "impure publications and propaganda."

And companies are also threatened with fines for "not correctly controlling Internet or computer network management," which hints that there might have been issues regarding people using company Internet connections for other than approved use.

• OFFICIAL SOFTWARE

Given the extreme rigidity of the North Korean digital control system, it is likely that authorities needed to design some means by which to allow for limited exceptions to the controls for approved purposes. They appear to have done so by way of officially produced apps. The apps allow for content such as audio files and images to be tagged with the individual digital signature of a particular phone and loaded onto that phone and their compatibility with phones several years apart indicates the system continues to serve its purpose.

By analyzing two similar software applications of the variety used for loading content onto North Korean smartphones, we find that the basic functionality of the digital signature system used to control content access has remained unchanged.

ABOUT THE AUTHORS

Martyn Williams is a journalist and researcher who has been following North Korea's information technology development for more than 20 years. In 2008 as the country got its first Internet connection, he started the North Korea Tech website to catalog the gradual emergence of the country onto the web and its slow embrace of technology.

He is currently based in Washington, D.C. and is a fellow at The Stimson Center where he regularly speaks and writes on North Korean technology issues. Previously he spent 8 years in the San Francisco Bay Area and 16 years in Tokyo, Japan.

Niklaus Schiess is a Security Analyst at ERNW in Heidelberg, Germany, focusing on application and network security. He has vast experience in assessing complex, large-scale network infrastructures, protocols, and applications. Besides conducting penetration tests for ERNW, he spends quite some time participating in capture the flag hacking contests.

He began exploring North Korean software and security in 2015 and has presented on the subject at international security conferences.

Lumen is a US-based non-profit organization whose mission is to provide all North Koreans with access to uncensored information and media as well as safe channels of communication. Its vision is to achieve a world where every North Korean can think, act, and move freely. Its focus is to develop delivery and distribution methods.

ERNW is an independent IT Security service provider based in Heidelberg, Germany. Since its founding in 2001, the focus has been on consulting and testing in all areas of IT security.

Acknowledgements

This report wouldn't have been possible without the generous support of numerous people and organizations. In particular, the authors would like to thank **Sarah Yun** and the staff of the **National Endowment for Democracy**, and **Nat Kretchun** and the staff of the **Open Technology Fund** for their support and funding to realize the project.

We would also like to thank **Jieun Baek, Hayun Sung** and the team at **Lumen**, **Florian Grunow** at **ERNW**, **Sokeel Park** at **Liberty in North Korea**, and the brave North Koreans who helped us obtain phones and who we interviewed for this report.

Graphic design by **Maria Francisco**. Korean translation by **Kyong Jin Seo**.

MOBILE PHONE CONTROL IN NORTH KOREA

North Korea's smartphone control system includes restrictions at the network level and at the smartphone level.

On the network, users are permitted to access nothing but state-approved services. Phones and computers connect to a closed intranet that includes some of the features of the Internet, such as websites and video streaming, but with none of the freedom.

While reports from the country indicate that the number and variety of websites and services is expanding, nothing exists beyond state-sanctioned services and access to the Internet is blocked.

The smartphone controls are accomplished with a customized version of the open-source Android operating system that runs on every North Korean smartphone. It includes several restrictions not found on phones in the rest of the world.

THE DIGITAL SIGNATURE SYSTEM

One of the most important control mechanisms employed by the North Korean state is a digital signature system that verifies whether apps can be installed or whether media can be displayed. It underpins most of the control on the devices and has been relatively successful in preventing North Koreans from using their smartphones for anything other than approved purposes.

It wasn't present on the first smartphones available in North Korea but was introduced around 2012, likely as a result of authorities observing that smartphones were handy devices for illicit media consumption.

Beginning in 2012 and through to 2014, authorities pushed users to upgrade the software on their phones to a version that included the signature system. After the upgrade, phones were much less useful for non-approved purposes.

In recent years, the signature system has transitioned from the individual app layer to a deeper level in the operating system. As a result, use of the system is more universal across a handset rather than just in specific apps. This move means some of the original methods used to bypass the system, such as opening some files in a web browser, no longer work.

---

[1] Lifting the Fog on Red Star OS, Chaos Computer Club, December 2015
[2] Woolim: Lifting the fog on DPRK's latest tablet PC, Chaos Computer Club, December 2016
[3] Exploring North Korea's Surveillance Technology, ERNW, March 2017

Use of the signature system in Android-based smartphones and Red Star OS-based computers has been well documented in previous research. [1] [2] [3]

In the Android realm, files are required to be digitally signed by one of two signatures to be accepted as valid and to be executed or viewed on a device.

The `SELFSIGN` signature is generated by the smartphone itself and appended to media files such as photographs taken with the device. The second signature, `NATISIGN`, is generated by the government and used on all official content and apps.

When a file is transferred to a North Korean smartphone, the phone immediately checks that it is one of a number of accepted file types and, if so, for a valid signature. If the file fails these checks it will be deleted.

Accepted file types are:

- Audio and Video: .3g2, .3gp, .aac, .ac3, .amr, .ape, .asf, .avc, .avi, .awb, .cda, .dat, .divx, .dts, .flac, .flv, .ifo, .m4a, .m4b, .m4p, .m4r, .m4v, .mid, .midi, .mka, .mkv, .mmf, ,mov, .mp2, .mp2v, .mp3, .mp4, .mpa, .mpc, .mpeg, .mpeg4, .mpg, .ofr, .ogg, .ogm, .ra, .ram, .rm, .rmvb, .smf, .swf, .tp, .ts, .tta, .vob, .wav, .wma, .wmv, .wv, .3gpp, .cwdx, .csdx, .cpdx
- Image formats: .bmp, .gif, .jpeg, .jpg, .pcx, .png, .tga, .tif, .tiff, .jps
- Text-based formats: .xlsx, .xml, .doc, .docx, .htm, .html, .pdf, .ppt, .pptx, .rtf, .txt, .xls, .odt, .ods, .odp
- Android files: .apk

A technical discussion of how this works is included in the appendix.

This simple mechanism means unapproved apps, such as those available overseas, or unapproved content, such as video and audio smuggled into the country, cannot be played on smartphones.

The system appears to be secure and is based on industry-standard 2048-bit RSA digital signatures.

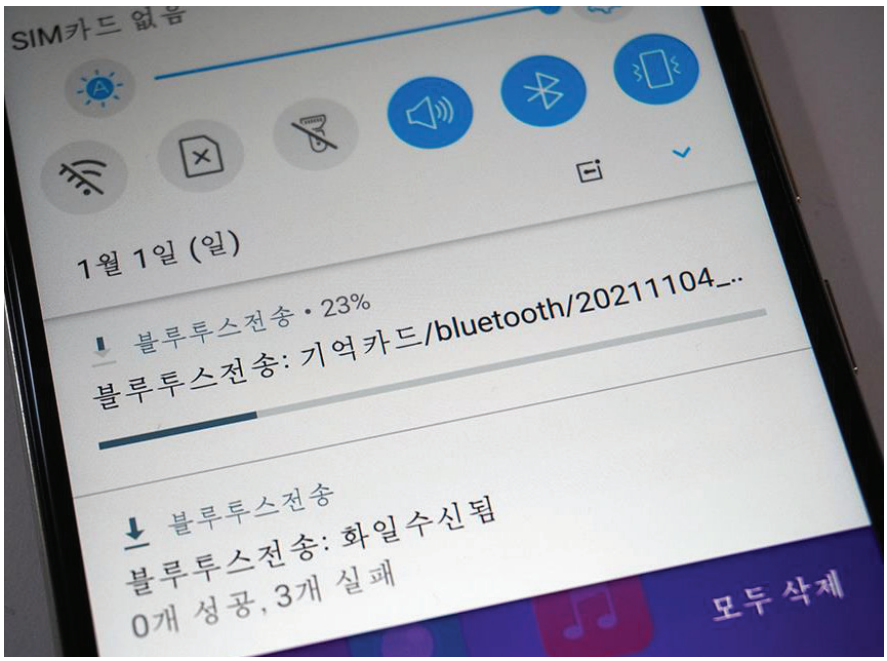


Figure 1
A file transfer over Bluetooth to a North Korean Pyongyang 2425 device. The phone has already rejected 3 files.

One notable change in recent versions has been a shift from signature checks conducted in certain apps on certain files to its place at a deeper level in the phone operating system.

Previously it had been possible to skirt the signature system by using, for example, the web browser to open some file types, but in more recent hardware the signature checks are at a lower level in the phone so encompass all activities on the device.

TRACE VIEWER

The ubiquitous Trace Viewer (열람리력) app is a standard feature of every North Korean smart phone and is an ever-present reminder that big brother is watching when the phone is in use.

The software randomly snaps photographs while the phone is switched on and stores them in a directory where they cannot be erased. [4]

Early versions of Trace Viewer allowed users to see the screenshots although more recent versions, including one on a Pyongyang 2425 handset that was examined as part of our research, do not allow users to see the images. They are presented as icons with a time and date of capture but clicking on them does nothing.

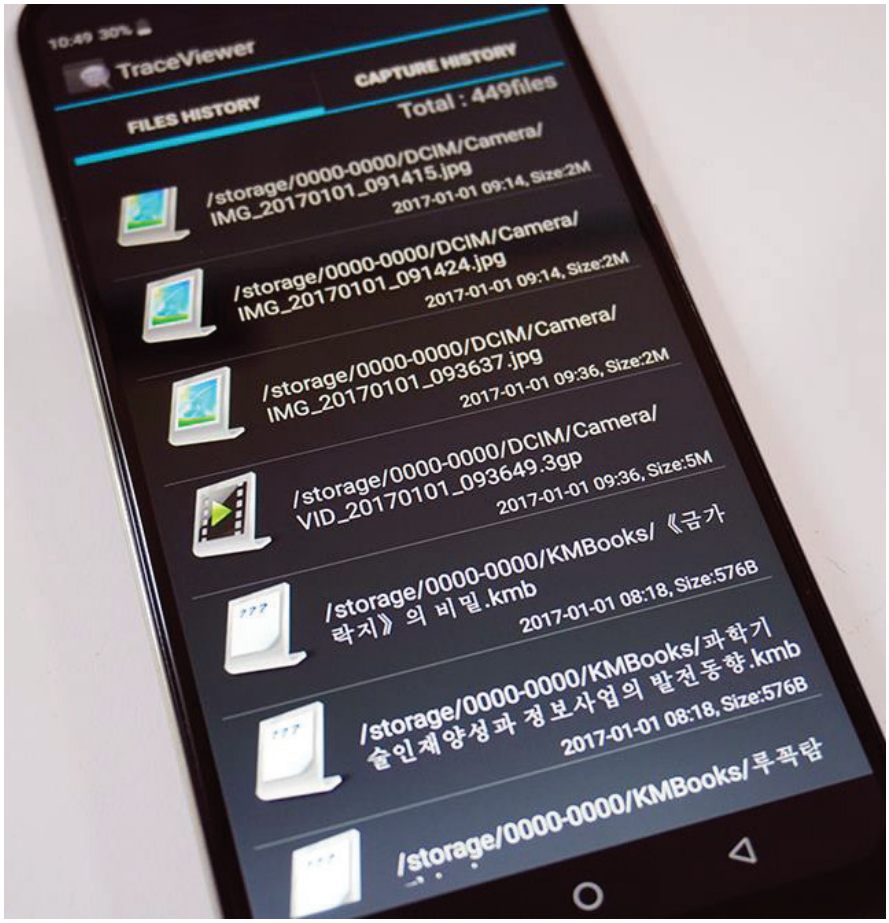


Figure 2
TraceViewer running on the Pyongyang 2425 smartphone

[4] All That Glitters Is Not Gold: A Closer Look at North Korea's Ullim Tablet, 38 North, March 3, 2017

RECENT CHANGES IN THE TECHNICAL LANDSCAPE

The state's grip on information control in North Korea does not appear to be slipping. Whilst our research has uncovered the existence of a nascent underground hacking culture in North Korea (detailed later in this report) the state continues to prove resourceful in countering new technologies that might give citizens a leg-up in their efforts to consume uncensored information.

In the previous section, we discussed how authorities reacted to the initial use of smartphones to view foreign content with the introduction of a digital signature system. In the last two years, we have seen a similar shift with Wi-Fi technology.

MIRAE WI-FI NETWORK

Several years ago, there were no state controls on WiFi. Few homes had computers, there waslittle network connectivity beyond cellular signals and the Internet was not widely available, but that lax attitude towards Wi-Fi changed abruptly in August 2014.
It appears that at least one foreign embassy had set up an open Wi-Fi hotspot and North Koreans were using it to access the Internet. The authorities reacted by instructing all embassies they had to immediately shut down Wi-Fi access points until they were inspected and approved. [5] [6]

Soon after, the ability to connect to Wi-Fi disappeared from smartphones. The Wi-Fi menu option is still there, but clicking it does nothing.

In 2018, Wi-Fi returned to Pyongyang. The Mirae (미래) Wi-Fi Network was established along Ryongmyong Street and was providing scientists with faster access to databases and research, according to Korean Central Television which showed the network in action.[7]

North Korean media reported it can deliver speeds of up to 70Mbps however, an app for the service claims speeds between 2Mbps and 33Mbps. Whichever is true, it is much faster thanwhat's possible with 3G cellular technology.

The television report claimed that the network uses a SIM Card-based authorization system. Such systems are the standard for mobile phone networks but haven't been seen in commercial Wi-Fi operations.

---

[5] Wi-Fi Access Sparks Housing Boom in Pyongyang, The Diplomat, August 14, 2014
[6] North Korea bans WiFi networks for foreigners, NK News, September 8, 2014.
[7] Korean Central Television News, October 21, 2018

Figure 3
A Mirae Wi-Fi access point in Pyongyang shown on Korean Central Television on October 21, 2018

Access to the Mirae Wi-Fi network requires three things:

- A supported device such as the Taeyang 8321
- A SIM cards from the network provider
- A username and password for authentication

In our research, we analyzed a North Korean Taeyang 8321 tablet computer with support for the Mirae service to discover how it works.

The Taeyang tablet we analyzed was one of the first devices available in North Korea with access to Mirae. Due to the low number of available devices, this is the only device where deeper analysis on Mirae has been performed. However, it is assumed that the implementation for accessing and using the network is identical on other devices.

Figure 4
A phone with Mirae Wi-Fi software shown on Korean Central Television on December 3, 2018

Figure 5
A SIM Card for the Mirae Wi-Fi network shown on Korean Central Television on October 21, 2018.

To connect to the network, the Mirae app first conducts a number of checks to ensure that legitimate devices and SIM cards are being used by verifying specific properties of the device.

The actual sign-on to the network uses cryptographic material that is stored on the SIM card.

Two industry-standard protocols are utilized:
- EAP-SIM (by default)[8]
- EAP-AKA (for 3G-enabled equipment)[9]

Both use SIM cards to authenticate devices on networks and are in use internationally. For example, Deutsche Telekom uses them to authenticate mobile subscribers on its public Wi-Fi hotspots.

The Mirae network app basically works the same way as international implementations but adds various additional steps to ensure that not only is the SIM card correct but it's being used on an approved device.

During our analysis no such SIM cards were available. However, the actual EAP-SIM/EAP-AKA mechanisms are the ones provided by Android. Changes in these implementations were not observed.

Additionally, the app also requests users enter a username and password, adding an additional level of security.

The combination of a physical SIM card, approved device and user account makes signing on to the network significantly more secure than just relying on one of those methods. It also makes it impossible to use an unapproved device and unlikely that anyone other than the legitimate account holder is using their account.

[8] RFC 4186 – "Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM)," Internet Engineering Task Force, January 2006
[9] RFC 4187 – "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)," Internet Engineering Task Force, January 2006

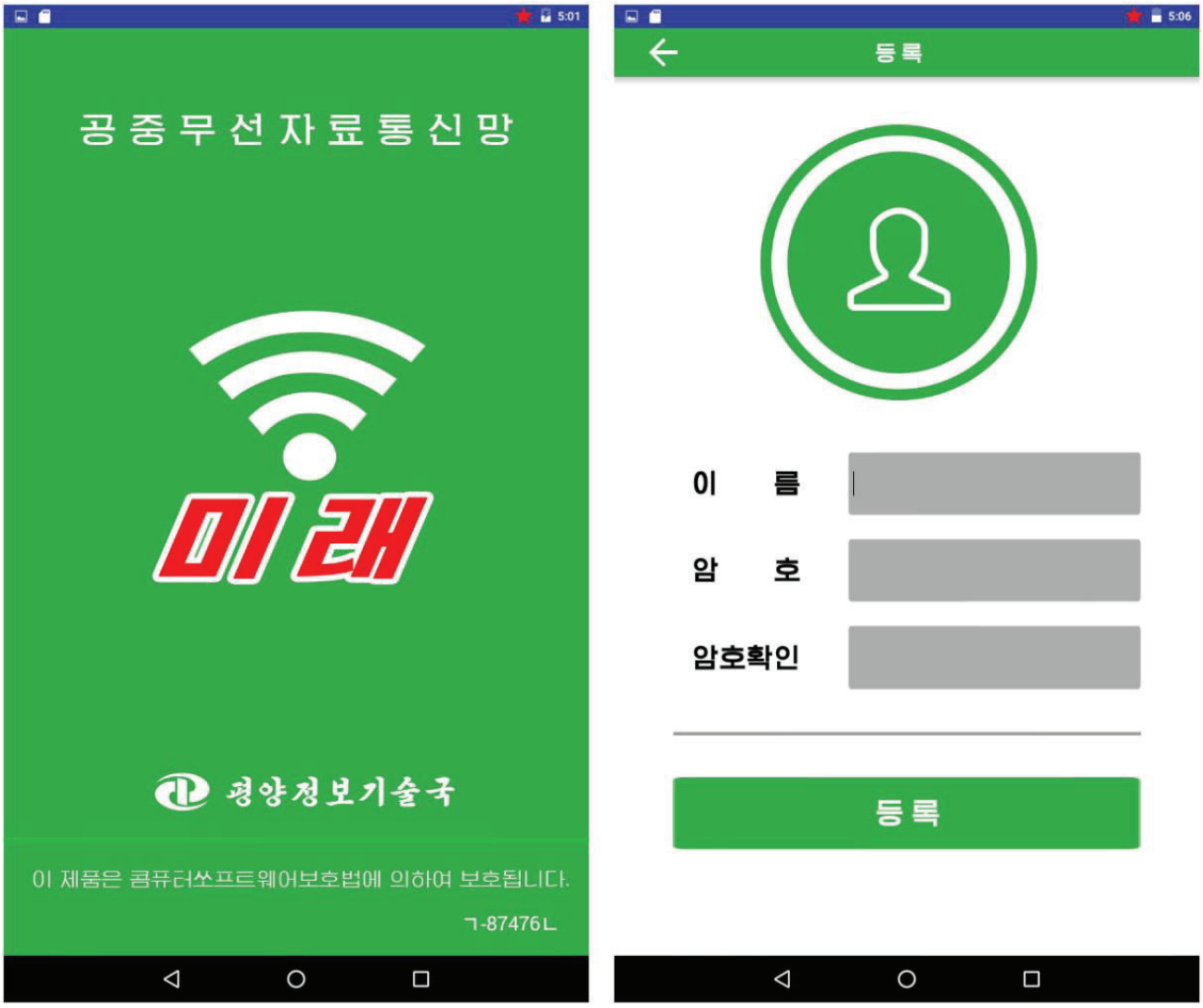


Figure 6
The splash screen and sign-on screen of the Mirae Wi-Fi app

Authorities have also made several modifications to the basic Android settings app. The changes include additions to the app but restrictions that either limit or completely remove existing features that are available in Android by default.

Some appear designed to ensure the reintroduction of Wi-Fi connectivity doesn't allow for unauthorized use by citizens such as was seen before.

These include the removal of WiFi-related settings in the app, such as the ability to search for a network, notifications when an open network is detected, VPN settings and tethering.

The reason for other changes is less clear. For example, the ability for the phone to auto rotate the screen has been removed as has the actual battery power usage. The capability to put the phone into Android's developer mode, which unlocks many settings usually hidden from users, has also been removed.

With the ability to search for networks and adjust WiFi settings removed, connection to the Mirae network relies on information hardcoded into the Mirae app.

This includes the wireless network name for the network ("PYY1026MIRAE00007") and authentication method.

Technical details of the changes are included in the technical appendix.

Overall, the reintroduction of Wi-Fi is another example of state engineers taking internationally available technology and modifying it so that it remains useful solely for their intended purpose. Rather than reinvent the wheel, the state is proving adept and subverting open technology, like Android and Wi-Fi, for their own use.

GETTING AROUND STATE CONTROLS

During our research we have come across two methods used to get around the previously described state controls on smartphones.

The state-sanctioned method uses software designed to add digital signatures to media fileswhile the illicit method involves the loading of software on to the phone to defeat the security checks.

Both are described in this section.

SIGNATURE SIGNING SOFTWARE

Software exists in North Korea that allows for various media to be installed on phones with the signature system. The signature signing software runs on a Windows computer and adds a `SELFSIGN` signature, so files are accepted.

We analyzed multiple versions of this software. The names, versions and release dates differ, they even have a specific timeframe where they are supposed to be valid. However, the signatures that can be created with these are still valid, regardless of the displayed expiration date.

They are valid on devices ranging from 2014 (Woolim) to 2019 (Taeyang 8321). This is an indication that the key material and the inner workings of the signature system have never been updated and no major modifications have been introduced. It could be possible that they are still the same since the day they've initially been released (the exact release date is unknown).

• IMPLEMENTATION

This software allows you to load a list of files and to specify an IMEI (International Mobile Equipment Identity) of the target device. The IMEI is a 15-digit number that identifies a phone and its serial number and is unique to each device.

By pressing a button, the software then processes each file and creates and applies a `SELFSIGN` signature. The process is the same as if the smartphone would create the file for itself, e.g., by taking a picture with the camera.

The key material used to create the signature is hardcoded into the application, and it just needs the IMEI. In case there is already a valid signature for another IMEI inside the file being processed, the new one will be appended into a list within the signature.

This is a built-in mechanism that allows IMEIs of multiple devices to be added to a signature so the file can be opened on more than one device. However, this mechanism does not enable a signature to be attached that allows a file to be opened by arbitrary devices.

The software just modifies the given files on the filesystem. This can either be on the computer itself or an SD card that can then be inserted into a smartphone or tablet PCs. It does not require a device to be connected to the computer and it does not interact with USB devices in case they would be connected to the system.

• CHAMMAE

This is the oldest version we've had to analyze. It is the v1.00 but it is unknown if there were any earlier versions available.

The following screenshot shows the main interface the software:

This interface is shown when the application starts up and there is not much more to see there.

On the left side it allows to switch between two modes:

- Cell phone: requires the device's IMEI
- Computer: requires a device number
-

Both create the same kind of SELFSIGN signatures. The software allows you to load a list of files that can be processed. Each file will get a signature, like the ones created on the devices.

The crypto material (especially the keys) is always the same, only the content a.k.a. the identity of the device within the signature differs.

The dates on the upper right indicate that the software is valid from January 1st, 2015, until December 31th, 2015. However, the signatures created with this software are valid for devices ranging from 2014 (Woolim) to 2019 (Taeyang). It is unclear if there is any enforcement on North Korean systems that use this software to don't make it accessible after it expires. Also, during the analysis no further restrictions in the software, e.g., limits to sign a specific number of files have been identified.

• PIGEON

Pigeon also exists alongside Chimae/Chammae. It is v1.01, however, the time period in the upper right shows that the validation range is October 1st, 2013 until September 30th, 2014. It is assumed that even though it is a newer version, the older ones are still in use, and are shipped with updated validation periods.

Besides parsing and applying signatures compatible with the signature system described in section libmediaselfsign.so, this software is also compatible with Red Star OS watermarks.

Before applying signatures to the files, the code tries to parse a Red Star OS watermark which has a similar format to the signatures:

- Seek to the end of the file
- Read the last three bytes
- Compare them to the string "EOF"

There is also code that parses these watermarks. In case a valid watermark has been found, the code adjusts the file length without the appended watermark at the end (typically 24 bytes).

The reason for the existence of Pigeon and Chammae is unclear. One could be a successor to the other of the different branding could be used by different smartphone vendors.

SMARTPHONE HACKING IN NORTH KOREA

Previously it had been assumed that, shut off from the Internet, North Koreans lacked the knowledge and tools to be able to mount an effective attack on state information control mechanisms, but during the course of our research we discovered that is not correct.

We interviewed two escapees who independently told us how groups of friends or associates would help each other to get around the state controls on smartphones. The scale of the hacking still appears to be minor, but recent changes to North Korean law indicate national authorities view it as a serious problem.

The interviewees, Mr. Kim and Mr. Park (pseudonyms) were both technically literate. Mr. Kim had been a programmer for the North Korean government and Mr. Park was a university student who had access to computers for over 10 years inside North Korea.

Both described using a similar method to bypass the state security applications.

Smartphones would be connected to a laptop computer via a USB cable to transfer an application onto the phone. If the phone was tricked in the correct way, the application could be transferred and launched without being detected and deleted by the phone's security software.

Once launched, the application provided the user with root access, which gives complete control over the entire phone and the ability to add, modify or delete any file. Mr. Kim described using a Chinese application called "Root 方手," although he stressed a variety of different rooting applications could be used to accomplish the task.

The motivation for doing this was to bypass phone security and be able to install different applications, photo filters and media files that would otherwise not be permitted.

Mr. Park said the application was shared among university students, but installation was not straightforward. His attempts were twice blocked by the phone before succeeding on the third attempt, he said.

"The program wasn't widely available to the general public," he said. "It was shared among certain university students who have knowledge in the area of computer science. The limiting factor was because it was technically challenging. Others didn't use it simply because they didn't know how to use it."

Mr. Kim described how some people offered this as a service to non-technical users who wanted apps or files installed on their phones or to increase the value of a device before selling it.

He gave the example of a North Korean phone imported from China that supports a dual-SIM function. The North Korean authorities might have disabled the function when they localized the phone but if it can be switched back on, the phone's value on the second-hand market rises considerably.

The resale value of a phone could also be increased by accessing and deleting screenshots automatically taken with the "Trace Viewer" application that is in each North Korean smartphone. The app takes random snapshots to try and dissuade illicit activities and the images cannot be deleted by the user.

"The number of screenshots in the phone helps determine how old a phone is. So, if it has a lot of screenshots that means the price will go down. If the phone looks new from the outside and the seller wants to delete the files inside. they can get a better price for the phone," he said.

Both escapees stressed that rooting is far from common in North Korea. Kim estimated less than 10 percent of people might have attempted it while Park estimated around 30 percent of the university students he knew had done it.

In part, this is due to its technical complexity and the requirement to have a PC.

"Most North Koreans are far from technology," said Kim. "The major generation are working in their 30s but didn't get experience with technology when they were growing up. So even if they have computers and know how to use them, they are probably not aware of how to work with a smartphone. When they want to do that, they'll usually approach someone who understands it because they work in the field."

Besides the monetary aspect detailed above, the reasons for rooting aren't always associated with information consumption. Sometimes people just want a different start-up screen on their phone, or a particular game or photo filter installed, said Kim.

Ironically, the knowledge on rooting and how to do it is gained by North Korean programmers who get sent overseas by their government. Many end up in China working on software outsourcing businesses that do work on behalf of Chinese and western companies. The customers believe they are contracting a Chinese developer when in fact it's a North Koreanbacked company.

"If you're working abroad and you're coming back to North Korea, it's encouraged by the government to bring part of the Internet back," said Kim. "You bring Internet sources back and they add them to a database, so we have the information here."

Programmers will typically fill hard drives with data for the government and the institution they work for. Typically, they will also hide some for themselves and that can include entertainment but also the types of applications needed to hack Android phones, he said.

While only a minor percentage of North Korean smartphone users might have engaged in rooting, the authorities do appear to have fought back.

This has happened on both the technical and legal front.

Park said he had success with an Arirang smartphone and Pyongyang 2413 phone, which likely went on sale around 2016 or 2017. Kim said the USB transfer method he described worked until the Pyongyang 2419 smartphone but didn't work after that. The 2419 went on sale in 2017, so then or 2018 appears to be the time authorities caught up with the particular method.

In the process of our research, the Pyongyang 2425 phone is the first post-2017 smartphone we have obtained, so this could explain why all previous methods to connect via USB failed on this handset.

Perhaps more interestingly, and hinting at a larger problem, the issue was also specifically called out in North Korea's new Reactionary Ideology and Culture Rejection Law that went into effect in late 2020. The law is part of a major new offensive on foreign content and influence.

The law specifies a punishment of at least 3 months of labor education for the crime of "illegally installing a mobile phone manipulation program." [10]

It also allows a fine of between 50,000 and 100,000 won to be imposed if a phone is discovered during a inspection that has "an impure publication and a propaganda material blocking program."

This is believed to be the first time that such activities have been specifically called out as crimes in North Korean laws.

[10] North Korea Intensifies War Against Foreign Influence, 38 North, November 10, 2021

SMARTPHONE PURCHASE AND SALE

The process for obtaining a smartphone is not a quick one. Citizens who wish to obtain a phone are first required to apply for permission to have one. Mr. Park, one of the two escapees interviewed on the subject of hacking, explained the procedure he had to go through when he obtained a phone:

"First, you're required to fill out a cellular subscription application. It has questions about your name, address, occupation. Then you have to obtain stamps from the local police station and security agency, and then you can apply for particular models of phones. This takes about 3 months because the application is sent to the International Communications Bureau and they assign you a number under your name. Then, when you get a notification you can go there and wait to get a cell phone."

Park arrived in South Korea in 2017. His experience is mirrored in published reports from the time, although one report from mid-2017, after he had left the country, says the procedure has been sped up. [11] [12]

Park said the supply of phones from official sources is limited because some are diverted to the markets for a profit.

"When cell phones, say 100, are imported from China, the store has a quota to sell but it cannot sell 100. They take about 70 to 80 phones and sell them to brokers who sell them at the markets at an inflated price. So even though 100 phones were available, there are only 20 to 30 phones available for people to buy at the store."

Due to the security software on phones and the North Korean cellular network, users are limited to using those phones marketed by domestic brands.

• INSPECTION CERTIFICATES

Various devices we've analyzed had inspection stickers on them. The stickers appear to provide visual confirmation that a device has been inspected, modified and approved for use in North Korea. Similar stickers can be seen on other electronics items, such as computer monitors, in state TV broadcasts.

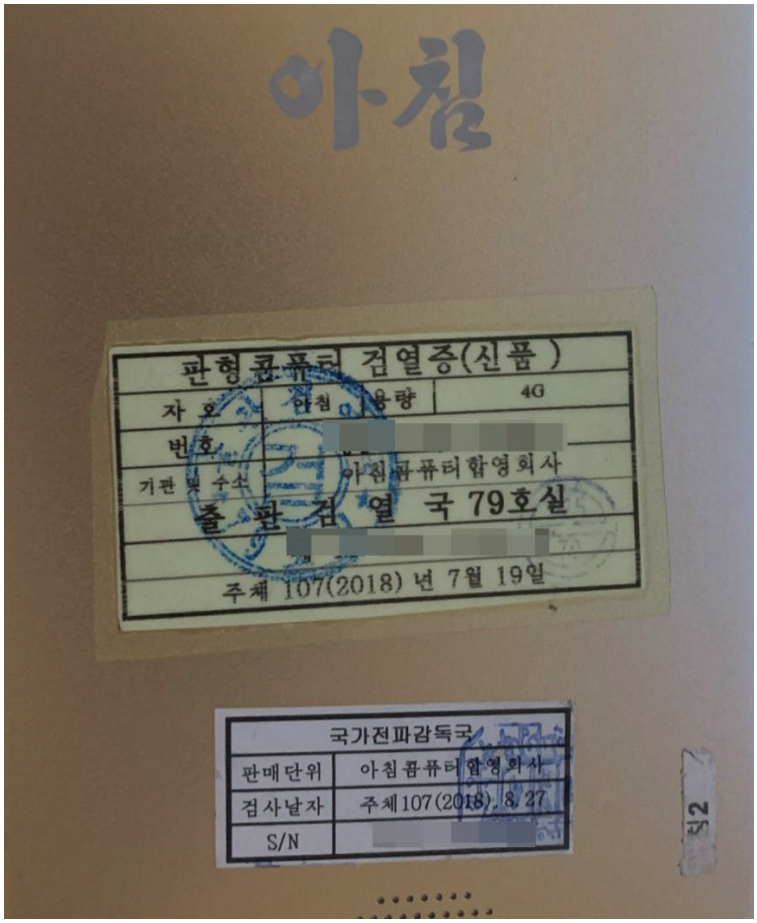
[11] Cell phone purchases up despite prohibitive costs, Daily NK, April 28, 2017
[12] Soldiers circumvent real-name registration rules for mobile phones, Daily NK, August 11, 2017

In the case of smartphones and tablets, the inspection includes that the signature system is installed and running, as well as various other precautions that ensure that only approved media is consumable on these devices.

We learned from interviews with North Korean defectors that Group 109 is one of the governmental institutions that is responsible for the device inspections.

There are various things we can learn from these inspection certificates:

EXAMPLE



This is a label from an “Achim” (Morning) brand tablet PC. Some details on the label have been obscured to protect the source of the tablet.

The top label reads:

Tablet computer inspection certificate (new)
Brand: Achim / Capacity: 4G
Number: <redacted serial number>
Organization: Achim Computer JV
Publication Censorship Bureau, Room 79
<redacted number>
Juche 107 (2018) July 19

The lower sticker reads:

Bureau of National Radio Supervision
Sales unit: Achim Computer JV
Date of Inspection: Juche 107 (2018) August 27
S/N: <redacted serial number>

The inspection dates are already a good indicator about how old the devices are (despite the release of the actual hardware). But the inspection entity is also an interesting part of these stickers: it might reveal which governmental institutions are part of either developing or surveilling these devices.

Room 79 of the Publication Censorship Bureau (출판검열국 79 호실) is believed to be involved with the censorship of content that comes into the country from overseas so this sticker appears to convey approval of the software contents of the tablet.

The Bureau of National Radio Supervision (국가전파감독국) appears to be the agency that approved the tablet hardware for use in the country.

PYONGYANG 2425 SMARTPHONE PROFILE

The Pyongyang 2425 is the most modern smartphone yet analyzed by the engineering team and one of the newest available in North Korea. It has proved to be the most well-protected against analysis. Unlike previous phones, North Korean authorities have gone to considerable length to disable the ability to dump the memory of the phone to a computer via USB.

Upon connecting to the phone via USB, a computer will successfully display the name “2425” and list the phone in the file explorer, but attempts to access the phone memory open an empty directory with no files inside.

The phone shows a limited amount of information in the “Properties” screen but no other interrogation of the device appears possible.

As a result of this, all known methods for accessing the memory and storage in the phone have failed and we have been unable to access the contents of the phone for analysis. Work continues on this task.

In previous analysis of North Korean technology, it has become clear that changes in the way the state does things is usually as a result of a problem with the existing method. That appears to be true in this case and the extra defenses against memory access indicates that this is an area of concern for the authorities.

Based on the escapee interviews detailed later in this report, some North Koreans had discovered a way to bypass the security system on devices. This method necessitated connecting the phone to a computer via USB and installing a Chinese smartphone app that passed control of the device to the user.

The tougher defenses against USB connection on the Pyongyang 2425 are almost certainly the state's reaction to this domestic hacking.

PHONE PROFILE

The Pyongyang 2425 is one of the most modern smartphones on sale in North Korea. It was released in 2019 and appears to be based on a model from China's Gionee, which has been customized for the North Korean market. [13]

While no identical Gionee smartphone was found in the company's line-up, the phone's IMEI number references Gionee as the manufacturer. Gionee also produced the prior Pyongyang 2423 smartphone. [14]

The phone has similar specifications to most mid-range smartphones on sale around the world today. It runs version 8.1 (Oreo) of the Android operating system and has a 6.2 inch screen, 16 megapixel front and rear cameras, a fingerprint sensor and wireless charging.

[13] North Korea's latest smartphone made by Chinese manufacturer, Daily NK, June 19, 2019
[14] The origins of the Pyongyang 2423 smartphone, North Korea Tech, February 5, 2019

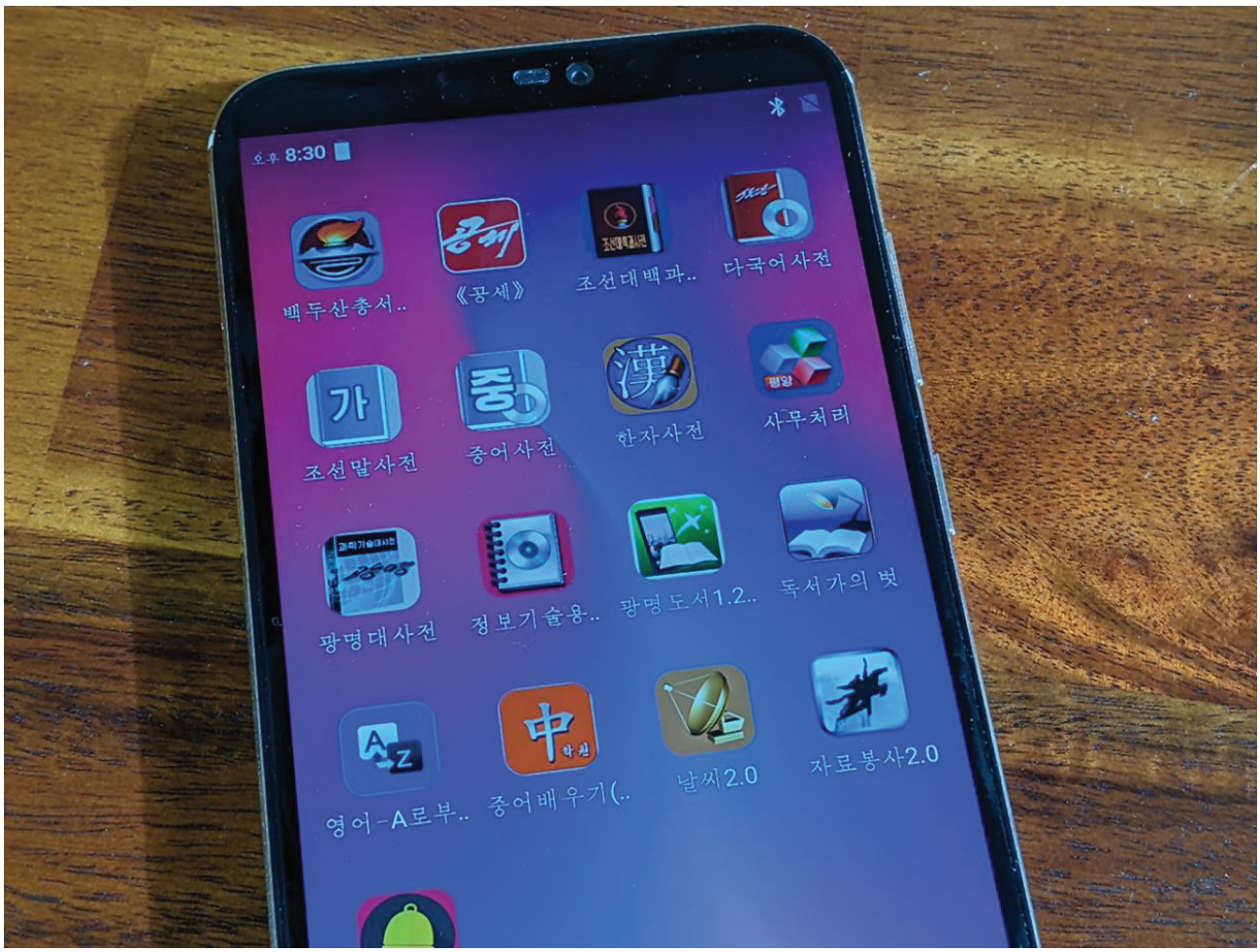
Figure 7
The Pyongyang 2425 smartphone pictured in North Korean media (Image: Sogwang)

APPS

The Pyongyang 2425 contains two screens of domestic apps. Screen one is shown above. The North Korean apps are mostly concerned with education and include several dictionaries and electronic book apps.

There are also five games, four of which were developed by the Samhung IT Exchange Center. The organization is based in Pyongyang and is a prolific producer of software. Its other apps, not installed on this phone, include a video streaming app that has been likened to Netflix.

Two of the apps were produced by Mangyongdae IT Corp (만경대정보기술사), which is the company behind the Jindallae-brand smartphones. Their inclusion on the Pyongyang phone indicates that while some phone brands produce their own apps, they are not necessarily exclusive to their own handsets.



Top row:

- 백두산 총서 1.25 – An anthology of works and speeches by North Korean leaders (2017, Central Scientific and Information Agency, 중앙과학기술통보사)
- 공세 – North Korean newspaper and magazine app (requires subscription) (Rodong Sinmun, 로동신문사)
- 조선대백과사전 - Chosun Encyclopedia (2013, Scientific Encyclopedia Publishing House, 과학백과사전출판사)
- 다국어사전 – Multiligual dictionary with Korean to English, Russian, Chinese, Japanese, German and French (2013, Pyongyang University of Foreign Studies, Foreign Language Publishing House, Management Research Institute, 평양외국어대학, 외국문도서출판사, 경영업무연구소)

Second row:

- 조선말사전 1.1 – Korean dictionary (2017, Scientific Encyclopedia Publishing House, 과학백과사전출판사)
- 중어사전 – Chinese dictionary (2014, Pyongyang University of Foreign Studies, 평양외국어대학)
- 한자사전 1.0 – Chinese character dictionary (2016, Pyongyang Informatics Center, 평양정포기술국)
- 사무처리 1.0.1 – Office app suite (no publisher listed)

Third row:

- 광명대사전 3.0 – Kwangmyong scientific app (Central Scientific and Information Agency, 중앙과학기술통보사)
- 정보기술용어사전 – Dictionary of technical terms (Published by Education Information Exchange)
- 광명도서 1.22 – Science book reader app (2013, Central Scientific and Information Agency, 중앙과학기술통보사)
- 독서가의벗 – E-book app (Published by Korea Publications Export and Import Corp.)

Fourth row:

- 영어 -A 로부터 Z 까지 – English learning app (2016, Mangyondae IT Corp., 만경대정보기술사)
- 중어배우기(외국어학원용) – Chinese learning app app (2014, Mangyondae IT Corp.,만경대정보기술사)
- 날씨 2.0 – Weather app (Weather Information Exchange Service, 기상정보교류소)
- 자료봉사 2.0 – App and media catalog (Published by Checom Technology JV)

Fifth row:

- 금방울 1.0 – Smartphone loss prevention app (Yonphung Business Information Technology Centre, 연풍상업정보기술사)

Second page, first row:

- 5 인주배놀이 4.1 – Five player boat game (2017, Samhung IT Exchange Center, 삼흥정보기술교류소)
- 별찌까기 – Puzzle game (Samhung IT Exchange Center, 삼흥정보기술교류소)
- 장기명수 – Puzzle game (2017, Management Research Center, 경영업무연구소)
- 풀면 수재 2048 – Number puzzle (Samhung IT Exchange Center, 삼흥정보기술교류소)

Second page: second row:

- 14 맞추기 – Card game (Samhung IT Exchange Center, 삼흥정보기술교류소)

DEVELOPMENTS TO WATCH IN NORTH KOREAN COMMUNICATIONS

During our research, a number of noteworthy developments occurred in the North Korean mobile communications space.

MOBILE PAYMENTS

The use of Koryolink airtime credits as an informal digital currency and mobile money system has been documented previously. [15]

Figure 8
Gas pumps in Hamhung advertise the acceptance of phone payments shown on Korean Central Television on September 20, 2020

However, in late 2020 it was reported that the state had moved to curtail the buying and selling of such credit in July of the same year. The report said that wealthy *Donju* were selling airtime top-up cards at a premium to people who could not go to the Post Office to purchase them.

[15] North Koreans build nascent fintech infrastructure with "mobile money", Daily NK, January 28, 2019

The restrictions limited a subscriber to transferring credit to a maximum of one other user per day, to purchasing no more than 100 minutes of airtime and to cashing in unused airtime at all. [16] [17]

The restrictions appear to be related to the introduction of state-run mobile payments systems that were introduced the same year.

One system was showcased in use at a store in Pyongyang on state television in November 2020. The Manmulsang system is a product of Yonpung Commercial Information Technology Company and uses QR Codes to enable payments for goods. In the example broadcast on TV, the QR Code appears to contain data for a 43-inch television at a price of 264,000 won.

Figure 9
A smartphone reads a QR Code for Manmulsang payment, shown on Korean Central Television on November 15, 2020.

Another new mobile system is an extension of the Jonsong (전성) Card that previously existed as a IC-based payment card. The mobile variant was developed by the country's central bank and Pyongyang Information Technology Bureau (평양정보기술국의), according to state media.

The company is also behind most of North Korea's electronic payment cards.

---

[16] Donju on the losing end of recent ban on "mobile money", Daily NK, October 21, 2020
[17] Donju and ordinary people impacted by recent ban on mobile money, Daily NK, October 28, 2020

In May 2021, Korean Central Television broadcast a news report that showed a poster for the system on display in a shop. Above the poster was a smaller sign featuring a QR Code barcode suggesting the system is based on barcodes. [18]

The launch of electronic payment systems by state-run companies is likely an attempt to regain some control and oversight of the digital payment market. The use of mobile phone credits as a form of electronic payment was an unintended use of the system but one that worked for traders and provided benefits over cash. It also took some control away from the state. The new payment platforms, if adopted, will give some of that oversight back.

Figure 10
A close-up of a poster for a mobile payments system shown on Korean Central Television on May 30, 2021

NEW LAWS

REACTIONARY IDEOLOGY AND CULTURE REJECTION LAW

In late 2019, the North Korean authorities launched a major new offensive on foreign information with the introduction of the Reactionary Ideology and Culture Rejection Law. [19]

[18] Korean Central Television news, May 30, 2021
[19] North Korea Intensifies War Against Foreign Influence, 38 North, November 10, 2021

The law is part of a multi-pronged effort to clamp down on the influence of foreign culture inside the country and goes together with other measures such as a strengthening of physical border controls to prevent smuggling.

The law specifies stiff penalties for the possession of foreign media, up to and include death for those convicted of smuggling, distributing, or organizing group viewing of South Korean content.

Of interest to our research are several fines levied on individuals and institutions that subvert information control laws in different ways.

MOBILE PHONES

Individuals caught with foreign mobile phones or phones with a "mobile phone manipulation program" can be sentenced to up to three months of reform through labor. The former refers to Chinese mobiles phones typically used in the border region to make international calls and send messages overseas while the latter is believed to relate to attempts by North Koreans to hack their phones, as detailed earlier in this report.

The creation of a specific item to counter installation of such software indicates that it had become a fairly significant problem for the state. While our interviewees indicated it was not in widespread use, it was likely more common among technically literate citizens.

The law imposed a fine of between 50,000 and 100,000 NK won for using a mobile phone "not loaded with an impure publication and propaganda material blocking program."

UNMODIFIED HARDWARE

North Korea has long imposed restrictions on the use of TVs and radios from overseas to prevent the consumption of foreign information. Broadcast receivers from overseas are required to be inspected by authorities and undergo hardware modifications that make it difficult or impossible for them to receive foreign broadcasts. The law also extends to computers, which are required to run domestic software that monitors computer use.

The new law imposes fines of between 50,000 and 100,000 NK won for "using equipment such as TVs, radios and computers in violation of the registration and inspection order regarding electronic, radio, broadcasting and communications equipment."

There are larger fines of between 1 million and 1.5 million NK won on companies and institutions that ignore the rules on import inspections of such equipment. The targeting of fines on institutions suggests there may have been cases where enterprises have imported foreign consumer electronics and ignored laws on inspection and modification.

WORKPLACE COMPUTER USE

Most North Koreans don't own personal computers, but the devices are becoming more common in the workplace, particularly in the ubiquitous "Science and Technology Dissemination Rooms" that feature in many companies and are centers for distance education and online study.

One aspect of the new law threatens a fine of between 1 million and 1.5 million NK won on companies or organizations that "create space for bringing in and distributing reactionary ideology and culture ... by not correctly controlling Internet or computer network management."

The inclusion of Internet stands out here as few North Korean enterprises or organizations are thought to have access. Internet is understood to be available at companies involved in international trade, major universities and government agencies. In all cases, Internet access is understood to be closely monitored, although the institutional fines specified in the new law hint that such monitoring hasn't always been perfect.

LAW ON MOBILE COMMUNICATIONS

Alongside that law, the Supreme People's Assembly in December 2019 also considered a new law on mobile communications.

"The law on mobile telecommunications deals with the principled issues arising in the mobile telecommunications including the set-up, management and operation of mobile telecommunications facilities, modern perfection of mobile telecommunications network, diversification of mobile telecommunications, service and use of mobile telecommunications and registration of mobile telecommunications equipment," said the Korean Central News Agency. [20]

The term mobile communications could cover both cellular and Wi-Fi, so it is unclear whether this law is focused on enabling the faster roll-out of Wi-Fi or an expansion of the cellular network.

[20] 12th Plenary Meeting of 14th Presidium of DPRK Supreme People's Assembly Held, KCNA, December 5, 2019.

NETWORK UPGRADES

As mobile telecom operators around the world roll out 5G technology with multi-gigabit per second speeds, North Korea's cellular network remains based on the 3G W-CDMA technology.

While the technology underwent several enhancements during its life, the service deployed in North Korea is not thought to be possible of data transmission speeds above 384kbps.

At the 8th Congress of the Workers' Party of Korea in January 2021, Kim Jong Un told delegates that the telecommunications sector needs to upgrade its infrastructure.

"The field should step up technical updating of its infrastructure and turn mobile communications into a next-generation one as early as possible by developing the relevant technology," he said according to the Korean Central News Agency. — KCNA, January 9, 2021.[21]

The pronouncement came with no additional details and state media has not expanded on any plans for a network upgrade but the current network, which went into service in late 2008, is long overdue an upgrade.

Kim's speech came a month after the new law on mobile telecommunications was discussed at the Supreme People's Assembly. That is discussed in the prior section and covers, in part, modernization of the network.

In the aftermath of several powerful typhoons in August 2020, Korean Central Television showed repair work taking place at a local telephone switching house and Koryolink cellular tower. In one of the images, an operator could be seen using a switchboard to connect phone calls.

[21] On Report Made by Supreme Leader Kim Jong Un at 8th Congress of WPK, KCNA, January 9, 2021

Figure 11
A North Korean telephone switching center seen on Korean Central Television on August 31, 2020

A second image showed workers repairing machinery that appears to be several decades old.

Figure 12
A North Korean telephone switching center seen on Korean Central Television on August 31, 2020

A February report said Kim's instruction to update telecommunications infrastructure is targeted at eliminating such manual switchboards that are in use in small towns and rural areas. [22]

MINISTRY OF INFORMATION INDUSTRY

While no official announcement on the creation of a new ministry was made in state media, the Rodong Sinmun newspaper mentioned the "Ministry of Information Industry" (정보산업성) for the first time in a report on May 17, 2021.

The ministry appears to be either the creation of a split of the Ministry of Posts and Telecommunications or a renaming of that ministry. In September, Korean Central Television broadcast an image of the Ministry of Information Industry name on one side of the building that previously housed the Ministry of Posts and Telecommunications.
The creation of the new ministry most likely happened at the Party Congress in January, when North Korean covered several issues related to telecommunications.

Figure 13
The Ministry of Information Industry building in Pyongyang, seen on KCTV on September 17, 2021.

[22] North Korea's efforts to improve telecommunications environment face many hurdles, Daily NK, February 19, 2021

CONCLUSION

The North Korean state continues to play a balancing act with technology.

On one side, technology promises to bring some badly needed efficiency and benefit the spluttering domestic economy, while on the other the state realizes that uncontrolled access to information and communications technology poses perhaps the biggest threat to the absolute power enjoyed by Kim Jong Un and the Workers' Party of Korea.

In this research there are several examples of this balance.

The initial introduction, subsequent banning and recent reintroduction of WiFi is one such case.

It would have been easy to keep WiFi banned, but authorities apparently realized there is a lot to gain from the technology and came up with a way to reintroduce it while minimizing risks.

Changes in the USB interface on the Pyongyang 2425 smartphone appear to be another example of a reaction to the ingenuity of citizens to use technology in a way other than it was intended.

Importantly, the hacking of smartphones detailed in the research represents a step up in the level of aggressiveness shown by citizens. In the past, most unapproved use of technology has involved workarounds or simple bypasses around obstacles, but the smartphone hacking is much more direct and involves attacking the security software itself through the installation of an additional app.

Additionally, the hackers responsible had those technical skills because of training they received from the state itself. In the case of one of the interviewees, he was specifically trained as a hacker for the benefit of the state.

For those involved in information dissemination and freedom of information issues in North Korea, this is a positive development. As North Korea pushes to train citizens in information technology, some of that knowledge will inevitably be funneled towards bypassing some of the digital controls currently imposed on citizens.

However, just as a more technically literate population might be a double-edged sword for the state, so is the state's increasing use of technology for the people. North Korean engineers have proved adept at modifying technology to fit within the surveillance state and continued adoption could further erode what little privacy North Koreans already have.