Mateusz TYBURA
RZESZOW UNIVERSITY OF TECHNOLOGY
2 W. Pola St., 35-959 Rzeszów

Analysis of selected aspects of mobile security on Android and Windows

Abstract

The purpose of this work was to analyze built-in security and privacy protection methods in mobile devices such as smartphones and tablets with Windows and Android operating systems. It was performed only with default settings and without any external software such as antiviruses.

Keywords: mobile, security, authorization.

1. Introduction

Nowadays there are many mobile devices. Using them we must be aware of privacy and security which are both complicated things. Breaking them could lead to full access to devices with the all stored data. Maybe tablets or smartphones are not main devices to work or gather data but they are also used all around the world. Many of them are usually connected to the same internal network as PC computers or laptops. This can enable getting a WiFi password and then analyzing all packages sent by this network. There are even more things to be concerned about when thinking about privacy or security. Some of them were chosen to be tested and described.

2. Security basics

It is quite obvious that security is the way of minimizing possibilities and effects of attack. In this way security (*S*) could be measured as the sum of security levels (*SL*) divided by a danger level (*DL*):

$$S = \sum_{n}^{i=1} \frac{SL_i}{DL_i} \tag{1}$$

This simple model shows that even very simple type of attack on a security system is highly dangerous if there is nothing to prevent it. On the other hand, there is also something else. Even if someone successfully breaks thought all security systems, it is not the end of world. The attack would be as strong as the possibilities gained with the access to our system. So for a single element it could be measured as multiplication of the possibilities gained (*PG*), normalized to values from 0 to 1, and the security (*S*):

$$RS = S \cdot PG \tag{2}$$

It is very difficult to measure security. There is no universal way to make all systems both highly usable and secure. Only a few things are sure like the fact that a device which is separated from other devices in the network and with no critical data in its memory is not very important in the process of rising the security. So we could put 0 in *PG* value of the equation. Unlike some very crucial systems, such as hospital infrastructure, where the risk is not only technical thing but it also involves humans health and life.

Security and privacy seems to be impossible thing when thinking about tablets and smartphones. End users got into their hands the devices with very poor security systems and a wide range of communication systems. Classic mobile phones gave the possibility to use a mobile network and Bluetooth or IR. Now there are many more things. Modern devices have many built-in sensors such as proximity sensors, accelerometers, gyroscopes and they have the possibility to use WiFi, NFC or GPS. It simply could make someone gain a lot of data about the selected user.

3. Authorization

All the analysed mobile systems have built-in authorization process but, unfortunately, it is turned off by default. In Android there are 5 ways of device blockade but only 3 are secure. The simplest way is just clicking or moving the icon presented on the screen.

Fig. 1. Unlock pattern

The unlock pattern is one of secure methods (Fig. 1). The entire security is based on the path between the start and end points chosen from 9 presented in 3 rows and 3 columns. This can be treated as a 9 vertices graph with no edges. Indexing them from up left to down right with natural numbers can be used to measure their degrees as shown below:

$$\deg(v_i) = \begin{cases} 3 \text{ for } i \neq 5 \\ 8 \text{ for } i = 5 \end{cases} \tag{3}$$

It can be simplified further into the degree equal to 3 for all the edges because all degrees are greater than or equal to 3. With this simplification, combinations count (*Cc)* is calculated as

$$C_c(n) = \begin{cases} 9 \text{ for } n = 1 \\ 3 * C_c(n-1) \text{ for } n > 1 \end{cases} \tag{4}$$

For the first edge, it is possible to choose from all, so there is 9 for combinations count. For the others, there are 3 possible ways to choose the next edge. It can be treated as a sequence with the starting values: 9, 27, 81, 243, 729, 2187, 6561, 19683, 59049, 177147 and so on. It can easily be seen that all these numbers are powers of number 3, so *Cc* can be simplified to:

$$C_c(n) = 3^{n+1} \tag{5}$$

This shows that the blockade pattern is less secure than a password built with just numbers which has 10^n combinations. There are also some concerns about human memory. Even thing such as a pattern must be remembered and repeated all time. Too complicated pattern are not easy to be used. It is quite obvious that there could be some well-known patterns just like “1234” or “password”. The pattern security can be calculated by a special strength meter whose values are from 6.6 to 46.8 [1].

Other interesting way of securing a device is presented in Windows 8 [2]. It is a password based on the gesture pattern and the image selected by the user (Fig. 2). There are 3 gestures which can be used: a line, a circle and a single point touch. It can be seen as less secure than the Android’s pattern but it is not limited by just 9 points. The user can use the whole screen resolution which is much higher than 3×3. It is of course limited by the area of

a single touch which cannot be calculated because of different sizes of fingers and different sizes of screens. But still there are much more possibilities.

Fig. 2. Picture password

Only one thing is the same – the human memory. Because the pattern must be repeated, the user must choose some characteristic points of the selected image to navigate through. So it is possible for some other person to make a guess. And, after all, the pattern is very limited and can be easily broken.

4. Access to user data

The first test was about accessing the user data when the device was connected to a USB port of a laptop. It is one of the ways to charge batteries but also a possibility to look through phone or tablet memory.

We started with connecting a smartphone with the Android operating system to a computer. The first thing to see is the fact that the device was detected incorrectly as audio devices but with correct information about both producer and model. The internal memory and SD card were also shown as distinct things. Unfortunately, there were no other data gathered. Some folders were fully accessible but there was not any information about the file system type or the folders which could be similar to those on Linux. The device was listed by the operating system when we used the *lsusb* command in prompt but using the *mount* it was not shown (Fig. 3) and the data given by the folder properties did not help. The location listed in the properties was not accessible from the prompt so there was no way to make a full copy of the data by *dd*.

Fig. 3. Prompt showing the result of the *mount* command

The Nokia Lumia with Windows Phone 8.1 operating system was also successfully detected. There was a message telling that device could not be mounted but it was done. It was detected as a type of a digital device such as a camera. Looking into the device memory gave a little bit more information (Fig. 4). The folder named *System Volume Information* suggested that the NTFS file system was used for the internal phone memory [4].

Fig. 4. Folders in the Windows Phone device memory

This phone was also listed in USB devices when we used *lsusb* but gaining more information by *mount* or the folder properties was not done. It made it all clear that both phones were secured from gaining the full access to the user data just after connecting to a laptop.

5. Internet sharing security

These test checked the security of internet sharing functions of mobile phones. It could be done by WiFi or Bluetooth but only the first possibility was tested. The reason for that is fact that WiFi is also used in computers and tablets while Bluetooth is available only in selected computers.

There are very few settings in the internet sharing option. The user can just turn on and off this function and change both network name and password. It is impossible to use the methods like hiding SSID, filtering connections by IP or MAC addresses or use the certificates for authentication [3]. After turning on there is only a simple counter showing how much devices is connected.

Networks are by default named with the producer, the model of phone and some random numbers. It is very insecure because of a lot of data gathered just by knowing what type of device is working as AP, especially when working with mobile phones with Windows Phone. It is because the password is built with just 8 numbers which are even worse shown as a plain text when getting into Settings screen. On the Android, the password is longer, more complicated and secured from reading by covering with the standard password hiding characters. It can be read only after checking the checkbox.

We decided to attack only the Windows Phone's shared network because the Android prompted for changing the password which made it impossible to check security while using all default settings. The attack was simple, performed using one single laptop and took less than 1 h 30 min which was absolutely unacceptable (Fig. 5).

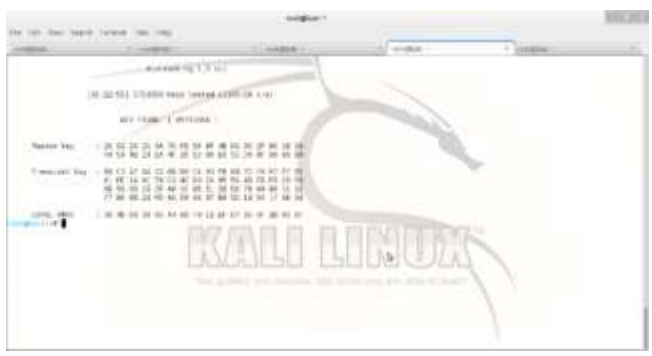

Fig. 5. Breaking the WiFi network password

For testing both devices we chose to measure the stability of networks while being under DoS attack. The networks built of a mobile phone and a tablet were tested by using the *ping* command.

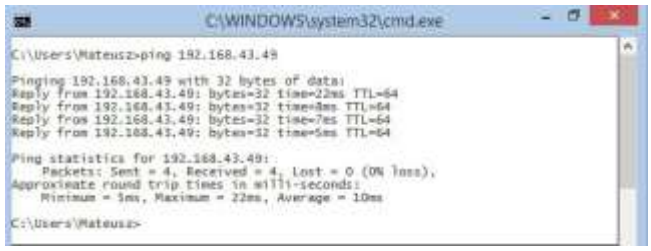

Fig. 6. *Ping* before attack on the Android's network

Before the test they were both working and answering. While testing only the Windows Phone's network was doing well with 10% loss of packages. They were delivered in time from 12 ms to almost 4 s with the average time of 225 ms. It was slower than before the attack but only in the average and maximum time. The minimum time was smaller than before.

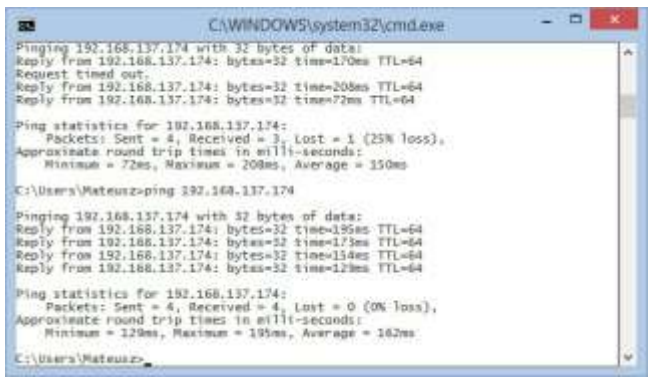

Fig. 7. *Ping* before attack on the Windows Phone's network

The Android had problems with reaching the pinged host so there was not any statistics about the time.

6. Availability of updates

It is considered as impossible to make a program without any bug in so it is crucial for users to have full access to all updates. Each not fixed bug would became more and more harmful. In the ideal situation, all devices would get every update of software making them fully updated and immune to any already found type of malware or a remote attack.

The Windows Phone is in a better situation because of fewer devices and a shorter history when we consider its 8th version as a totally new operating system. The Android is older and installed in so many devices that it seems to be unachievable to secure them all.

For more information about it, we gathered the data about operating systems installed in smartphones and tablets available on sale in 3 stores.

On smartphones there are almost 82% of devices with the Android (Fig. 8), which makes it a dominating operating system. Unfortunately, only 1% of them have the newest version. It is less than almost 2% of devices with the Android in versions from 2.1 to 2.3, which have been available since 2010. So it is absolutely possible to buy devices which have not been updated for 5 years. That makes them very insecure. The Windows Phone has only 18% of devices and only 2 devices have the oldest version of this operating system.

Tablets showed almost the same data (Fig. 9). One of the differences was no device with Android 5.0, more devices with Android 4.2 than with its 4.4 version and one device with Windows 7.

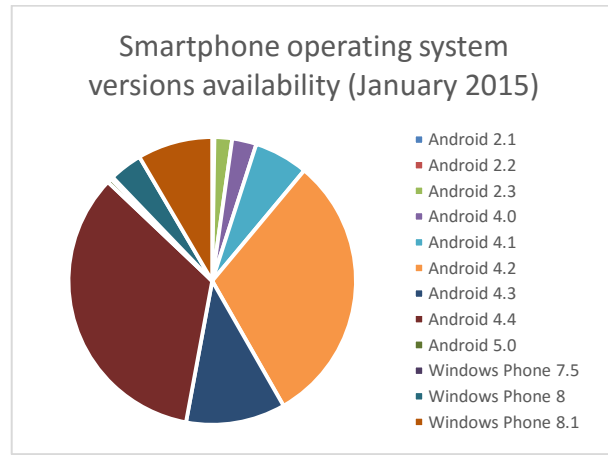

Fig. 8. Availability of smartphone operating system versions (January 2015)

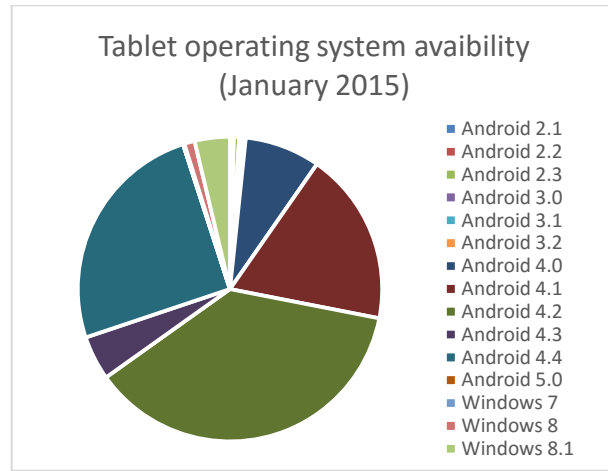

Fig. 9. Availability of tablet operating systems (January 2015)

There are also official Google's data about the Android [5] (Fig. 10). It can easily be noted that even after a few months researches are actual in comparison to the actual Google data. There are still devices with Android 2 and 4. Versions 4.4 and 4.2 are still most popular. One of the differences is more devices with Android 5, but now there are only about 25% devices with the newest version of this operating systems which is not a good news for the mobile security.

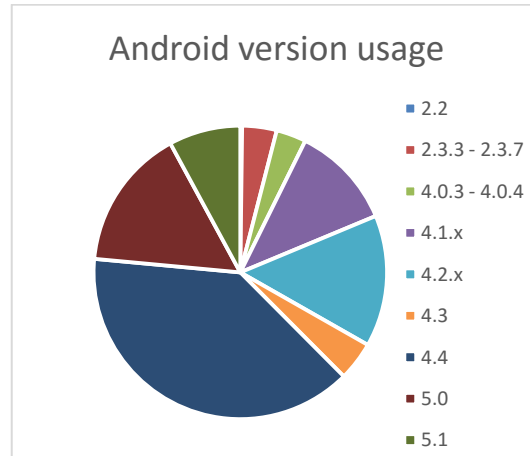

Fig. 10. Usage of Android versions (official Google's data)

Some changes are taking place but seeing the same old versions makes a thesis that they will be used as long as some users will use their old devices.

7. Remote finding and device blockade

Losing a device is one of possible ways of making the private data available for someone who is not allowed. Because of that, modern devices have special functions made especially for finding lost devices, blocking them and even removing all data from the memory.

It is necessary to know about the security of these functions. Only the user must be allowed to do that. Every other person with the possibility of doing that would make a lot of troubles. Mobile devices are used for paying, accessing bank accounts or in a double verification system, when the user get a code to confirm his right to log in to some account. It is widely used by banks or sites like Facebook.

For Android devices there is a special site available on https://google.com/android/devicemanager. Almost all this site is covered by a map which shows the last location of devices. It also gives the information about the time when a phone or a tablet sent its latest geographical position. There are 3 actions for the user to perform. The first one is to make a call. After confirmation the device is ringing in its max volume for all the time, even if it was muted before. There is no information about who is calling. It is just the voice call screen and a very loud sound. The second one gives the user opportunity to make a device unusable by setting a new password. It can also show the optional text and pthe hone number for someone who found the user's smartphone or tablet. The last one is very dangerous because it deletes data. Its usage should be limited. One strange thing about it is the fact that the device shows a special notification icon telling that it is found by the Android device manager. Anyone would in fact know about that.

The Windows Phone gives the user almost the same features on its own site: https://www.windowsphone.com. A phone can be located, locked or erased. The location is as precise as on the Androids website. There is also a special option of printing it. Ringing also does not show any information about who is calling. The device just shows the standard voice call screen without exact information about the caller. Locking is less functional because it only makes it possible to put some text on the phone screen and call the locked phone. There is also information that the user will get a mail about it.

Managing from the website makes it reasonable to think that all these functions are useful as long as the device is connected to the internet. There is no documentation of how exactly it works but if the user went to settings on the Windows Phone device, he would see information about using push notifications rather than sms messages to manage it.

This makes a theoretical possibility of managing the phone by someone who would first change the phone settings to use sms instead of push notifications and send them as it was sent from the managing site. Other possible attack scenario is to overwrite networks DNS to make push notifications being received and sent by a special server.

8. Conclusions

Mobile devices are not secured well. It seems that years will pass before we see them more as more secure. There are many reasons for that. One is the limitation of users input just to touch the screen. Other thing is the less computation power than PCs. Mobile devices are also younger so it makes all their constructors and people who makes software for them less experienced in securing them. There are also many more things to make research on. One of them is the attack scenario mentioned in Section 7.

There are also good points of the mobile security. The user data seems to be secured well from simply copying it by connecting to a USB port of a computer. Other thing is the whole system of finding and locking a device when lost. It is shown that it is secured from the unauthorized access and works fast.

9. References

[1] Chen Sun, Yang Wang, Jun Zheng: Dissecting pattern unlock: The effect of pattern strength meter on pattern selection. Journal of Information Security and Applications, vol. 19, no. 4-5, pp. 308-320, 2014.
[2] Pogue D.: Windows 8 the missing manual, O'Reilly, 2013.
[3] Chaouchi H., Laurent-Maknavicius M.: Wireless and mobile network security, ISTE, 2009.
[4] Russinovich M., Solomon D., Ionescu A.: Windows Internals Part 2, 6th edition, Microsoft Press, 2012.
[5] Documentation of Android versions usage, https://developer.android.com/about/dashboards/index.html, 2015

Received: 18.06.2015 *Paper reviewed* *Accepted: 03.08.2015*

Mateusz TYBURA, MSc

Mateusz Tybura graduated in IT (MSc 2015) from Rzeszow University of Technology. Currently he is studying for PhD degree at the same university. He is a member of KNEiTI scientific circle. His main research areas are security and mobile technologies.

e-mail: tyburam@hotmail.com