Mobile Firewall applications: an analysis of usability and effectiveness

Wouter Louman, Mitchell Vernee, Danique de Bruijn, Babette van 't Riet, Hani Alers
The Hague University of Applied Sciences
Bleiswijkseweg 37
2712 PB Zoetermeer, The Netherlands
+31704457244
{16071670, 16099567, 17100992, 17064953}@student.hhs.nl, HAL@hhs.nl

ABSTRACT
The amount of smartphone users worldwide exceeds three billion and that number is expected to grow. Sensitive data is often stored on the memory of smartphones and users of smartphones tend to be concerned about their data leaking out. Firewalls might prevent this, but do these firewalls work as expected? Do they block internet access for specific applications on the phone if requested? If these firewalls were to be used by technical and non-technical users, the user-friendliness is an important aspect as well. In order to examine the user-friendliness and effectiveness of the firewall applications in this research, usability tests and network traffic analyses are performed. The results of the network traffic analyses show that firewall applications do not blocks all network traffic when all applications are blocked. Usability tests indicate that the user-friendliness of firewall applications leaves much room for improvement.

CCS Concepts
CCS → Security and privacy → Network security → Firewalls

Keywords
Heuristic evaluation; Usability; Firewall; Mobile applications; Mobile security;

1. INTRODUCTION
According to the portal of statistics: Statista, the number of smartphone users worldwide today surpasses three billion and is forecast to further grow by several hundred million in the next few years [1]. Nowadays smart mobile devices are usually connected to a wireless network interface for data communication. This means that phones need to be protected at all times. Users and organizations need to keep accounts safe and databases encrypted.

Users are worried that their personal data is gathered without them knowing [2]. To ensure people that their data is kept safe, they can install a mobile firewall application. A firewall is a fit counter measure [3]. Computer firewalls have proven to work. They have been around for a long time and evolved with new problems. The mobile firewall applications on the other hand have not been around that long. Not every firewall application seems to do what it says. This research examines the effectiveness and user-friendliness out of the Android firewall applications. These firewall applications are supposed to block the in and outgoing data as requested by the user. The applications do not make their own decisions about which apps to block. Therefore, users need to engage with these firewall applications and select the mobile apps which are going to be blocked.

This work introduces a general method of evaluating the user-friendliness and effectiveness of the firewall applications. There are two lines of research handling usability aspects and the data protection aspect. First, the firewall applications are evaluated according to the heuristics of Jakob Nielsen [4]. These outcomes give the input for a usability test. This test is conducted with real world users, testing each firewall application by going through specific usage scenarios. The result from the usability test highlights areas where firewall applications are lacking in user friendliness. Besides the usability test, a network traffic test is also conducted. By analyzing the network traffic of the mobile device, it is possible to test the extent to which each firewall app succeeds in blocking the network traffic as promised.

2. METHODOLOGY
For this study, only non-root firewalls for the Android platform are considered. Rooting a device merely means to gain access to the root directory and having the appropriate permissions to take root actions [5]. This is a somewhat involved technical procedure. Non-root means that users only has to install an application without rooting their phone, which encompasses a much larger segment of the population. Five of the most popular firewall apps for Android were chosen for this study. The popularity was based on online reviews from technology editors and the number of downloads from users. The chosen apps are: "NoRoot Firewall", "Netguard", "InternetGuard Data Saver", "Droidwall" and "Protwall". The non-root firewall applications were chosen because of the target audience; the non-technical user. These users do want to protect their privacy, but do not possess a lot of technical skills way.

2.1 Usability testing
The five best-rated non-root firewall applications are subjected to a heuristic evaluation and a usability test.

2.1.1 Heuristic evaluation
The chosen applications are first evaluated against the Nielsen heuristics. The heuristic evaluation gave insight into the usability problems, guided by the problems scenarios could be set up. The heuristic evaluation results in the usability problems and a list of elements each application should contain.

2.1.2 Usability test
The usability of these applications is also measured using a usability test. 25 participants follow the scenarios guiding them

through the applications. Five participants rate each application, and the final score is averaged. All participants are Android users and have no knowledge of rooting their phone. The participants get a quick introduction to firewall applications. Then the participants go through the scenarios on the available Android phone. Each test is conducted on the same smartphone. The scenarios are:

- Allow all applications
- Allow all applications, except WhatsApp
- Disallow all applications
- Disallow all applications, except WhatsApp

The test is timed to measure how long it takes the participants to go through the scenarios. After finishing the test, each participant gives their opinion by rating the application from 0 - 10, with 0 meaning the participant would not ever use the application and 10 meaning they would use it.

2.2 Network traffic capturing test

In order to examine if the firewall applications are effective, two identical tests were performed with a network capturing tool called Wireshark (3.0.5) [6]. First, a hotspot was created on a laptop (Windows 10 64-bit). Subsequently, a phone (Huawei P10, Android 9.10) was connected to the aforementioned hotspot. All the firewall applications were installed on the given smartphone from the Google Play store [7]. The applications were started one by one and each firewall was set to four different configurations. These configurations are geared towards allowing or disallowing internet access for certain applications. They are the same as the four scenarios as mentioned in paragraph 2.1.2. These configurations were chosen because they made it less difficult to determine whether or not a firewall is working properly.

In addition, they represent the most fundamental options of all tested applications. In each configuration, the network traffic was recorded (1.20 minutes for each configuration) by using Wireshark on the laptop. The recorded network traffic was saved in trace files (.pcapng), which contained network packets. These were analyzed by examining:

- The protocols which were used.
  Certain protocols are often used for specific goals, therefore protocols can reveal information about what kind of traffic is going on.
- The IP addresses
  For looking up the IP addresses from the trace files, mxtoolbox.com [8] was used. With the help of this tool, PTR requests were performed to obtain the hostname corresponding to an IP address. ARIN reports were requested with the same tool to obtain information about the organization behind the IP address.
- The amount and size
  The amount and size of packets was retrieved from statistic tools within Wireshark. Also, filtering was applied for filter in or outgoing packets and packets from IP addresses owned by organizations such as Facebook.

The packets were filtered on the MAC address of the test phone so that only the traffic from and to the phone was displayed.

3. RESULTS

3.1 Heuristic evaluation results

The heuristic evaluation exposed a number of usability problems. The problems are listed below per application.

3.1.1 Netguard

The application does not give the user space to make errors. In certain situations, you get a confirmation option when you need to stop the battery optimizations on your phone. When a user drops down the options for the blocking: you can choose more settings. When you change something, the app will ask you if you want to confirm your action. When using NetGuard there is no option to disallow several apps or all apps at once. The user needs to manually tap the checkboxes to disallow. The app has some helpful tooltips, but no real explanation for some difficult functions. It also has no search function.

3.1.2 InternetGuard Data Saver

The firewall applications do not have many filtering options. Only in InternetGuard Data Saver there is a filter system. The users can filter on the UID or name. For a non-technical user, the term UID is not clear. It is not defined in the application. This application has small (not full screen) ads. As a user, you cannot select or deselect all the applications at once. This is done manually. The instructions are visible until you tap ok. Then the instructions are gone: As a user you cannot find the instruction anymore after tapping the OK button.

3.1.3 Droid Firewall

There are no real technical settings a user can alter. As a user you could only look into the application info from the phone itself. These settings can be changed. There is no error prevention, only a small explanation to use the application. The user cannot tweak real settings within the app. You can only tweak settings from the phone, reached through this app. The user can not alter this app to your liking. No error messages encountered. Also, there are no warnings when you press an icon accidently and are going to disallow Wi-Fi or network before you save. So, the user can erase or lose data by accident. There are no hints provided when opening the application, and the users are simply expected to discover the possibilities for themselves. There is also no “block all” function.

3.1.4 NoRoot Firewall

On the first page you can choose “stop” if you accidentally start the VPN. When you give permission to an application the user cannot undo it on the same page. The user has to search the app to undo it. If you disallow an app it is very intuitive to press the checkbox again to undo. This application has no search option.

This application does not have the option to block all applications or several applications at once. The app contains no dialogue/explanations. The user can only learn by trial and error.

3.1.5 Protwall

For expert users there are no real alterations possible. For both the experienced and inexperienced user the app needs to be used the same way. There is an “advanced options” at the menu. These are only levers, you can not alter IP addresses for examples. The more technical users will probably choose a rooted firewall application. Also, there is no help for novice users. When opening a new screen there is always an advertisement popping up. In the application you cannot block several or block all applications at once. This has to be done manually. No search function available.

Every time a new screen opens there is an ad. This really influences the experience for a user in a negative way.

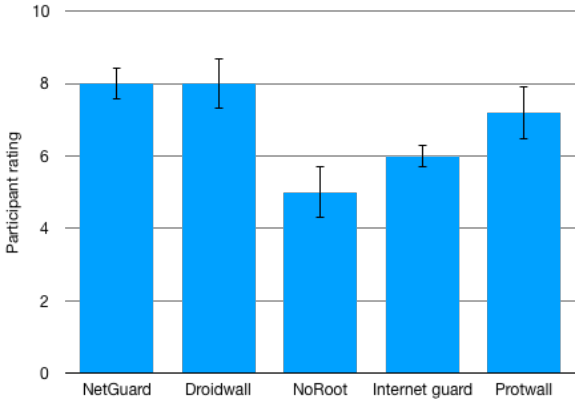

Figure 1. Average user rating per firewall application. Error bars represent the standard error of the mean.

3.2 Usability testing

3.2.1 User grading

Figure 1, shows the rating for each firewall app averaged over 5 participants for each application. Netguard and Droidwall have a shared position on being the top-graded apps by users. NoRoot Firewall scores the lowest when participants were asked about their opinion on the application. NoRoot firewall was stated to be the least preferable because of its looks. Netguard and Droidwall score similarly because of the similarity in their interface. The only difference between the two applications is the color scheme.

Table 1. Showcase of time testing of applications (in seconds)

	Disallow all	Allow all	Disallow WhatsApp only	Allow WhatsApp only
NetGuard	12.6	4.6	29.2	137.8
DroidWall	154.8	179.4	28.4	172.0
ProtWall VPN Safe	194.6	161.0	31.6	154.0
InternetGuard Data Saver	217.2	182.2	34.8	188.2
NoRoot Firewall	159.6	221.8	26.5	190.0

3.2.2 Time based testing

Table 1 shows that participants who tested Netguard were the quickest in fulfilling their task on three test subjects. Netguard is the only application which gives a button that allows the user to block or unblock all the applications running on your phone. Comparing the 'disallow all' step between applications, Netguard participants were 142.2 seconds quicker in blocking all the applications running on the phone. Users were even quicker when it came to allowing all the applications because unblocking only took 4.6 seconds. Compared to the second lowest scoring application this is a difference of 156.4 seconds.

3.3 Network traffic capturing test results

3.3.1 NetGuard

The results (Table 2) show that the total amount and size of packets coming from the phone are distinguishably lower when NetGuard is set to "disallow all applications" compared to when NetGuard is set to "Allow all applications". The amount and size of Facebook-related packets coming from the phone are lower when the firewall is set to "Allow all apps, except for WhatsApp", although a relatively small amount remains. The mode "Disallow all apps" shows lower amounts and sizes of packets related to Facebook as well. Packets are still going through, even when the firewall should block everything. Mainly, these are DNS, HTTP, TCP and UDP packets and are sent to IP addresses owned by companies such as T-systems International, Google and Facebook (according to ARIN reports corresponding to the IP addresses in the captured network traffic).

3.3.2 InternetGuard Data Saver

Table 2 shows that the total amount and size of packets coming from the phone is lower when InternetGuard Data Saver is configured to "Disallow all apps", compared to when set to "allow all apps". Furthermore, the amount and size of outgoing Facebook-related packets are lower for "Allow all apps, except WhatsApp" and "Disallow all apps" than for "Allow all apps". Notably, in the second test in mode "Disallow all apps" there are zero packets related to Facebook. Captured network traffic and ARIN reports shows that traffic (mainly HTTP, TCP, UDP and DNS) is still going out to IP addresses owned by T-Systems International, Google, Facebook and Akamai.

3.3.3 Droid Firewall

The results for Droid Firewall in Table 2 show that the size of outgoing packets in "disallow all apps", is lower than for "allow all apps", though M1 for "disallow all apps" shows a higher amount of outgoing packets than M2 for "allow all apps". The amount and bytes of packets related to Facebook are lower in tests for "disallow all apps" and "Allow all applications, except WhatsApp" than for "Allow all applications". It is notable that in test 2 for "Everything disallowed" and test 2 for "Allow all apps, except for WhatsApp" no Facebook-elated packets have been captured. The network traffic captures and ARIN reports show that outgoing traffic is mainly using UDP, DNS, TCP and HTTP protocols and is going to IP addresses owned by Facebook, T-Systems International.

Table 2. Amount and size of network packets per firewall

		Mode, Measurement moment, Firewall name							
		Allow all applications		Allow all applications, except WhatsApp		Disallow all applications		Disallow all applications, except WhatsApp	
		M1	*M2*	*M1*	*M2*	*M1*	*M2*	*M1*	*M2*
Packets	**Unit**	NetGuard							
Packets from phone	Amount	234	315	143	290	70	113	226	351
	Size (bytes)	34112	59920	17285	62162	6445	12181	23968	60933
Facebook-related packets from phone	Amount	73	42	15	1	5	1	76	74
	Size (bytes)	7319	3563	2260	54	270	114	7235	6663
		Internet Guard Data saver							
Packets from phone	Amount	428	346	219	269	104	306	225	193
	Size (bytes)	81056	71881	20876	53002	9285	67317	26002	24062
Facebook-related packets from phone	Amount	67	40	15	4	5	0	78	43
	Size (bytes)	6894	3575	1648	260	330	0	8387	3711
		Droid Firewall							
Packets from phone	Amount	337	125	142	50	164	68	215	392
	Size (bytes)	77964	19485	12671	4763	14354	6459	19628	89001
Facebook-related packets from phone	Amount	57	53	21	0	18	0	16	51
	Size (bytes)	6681	4633	1554	0	1332	0	1432	5067
		NoRoot Firewall							
Packets from phone	Amount	121	239	253	188	65	60	115	116
	Size (bytes)	12148	59554	61218	51344	13112	12993	18379	18353
Facebook-related packets from phone	Amount	59	44	10	0	0	0	36	41
	Size (bytes)	5906	3797	1251	0	0	0	3208	3734
		ProtWall							
Packets from phone	Amount	510	278	273	260	294	265	1071	289
	Size (bytes)	94623	57529	36468	54239	67655	61253	142851	58484
Facebook-related packets from phone	Amount	85	72	19	6	14	8	73	55
	Size (bytes)	8962	6898	1976	824	1638	3323	7347	7556

Note: M1 = Measurement (moment) 1, M2 = Measurement (moment) 2

3.3.4 NoRoot Firewall

The results in Table 2 showed that NoRoot is able to block some data. When looking into the results of "Disallow everything" it is shown that there are still packages going in and out, but it blocks all Facebook-related packets. The packets that were still going in and out were mainly DNS-requests, UDP, TCP and HTTP packages. Most of the TCP packets were empty but sometimes they contained encrypted data. The HTTP packages were most of the time requests, but sometimes they also contained data. When looking at "everything allowed except for WhatsApp" the difference between measurement 1 and measurement 2 is remarkable. With measurement 1, packets are still coming through, but few packets are sent to IP addresses owned by T-Systems International, Vodafone NL.

3.3.5 ProtWall

Noticeable is that with measurement 1 in Table 2 more packages are going out when everything is blocked except WhatsApp than when nothing is blocked. Even though the number of Facebook (WhatsApp) packages is about equal. When you compare "disable all applications" with "Allow everything" it is noticeable that when all data is blocked the size of the packages is about equal. However, when only WhatsApp is blocked Facebook packages contain less bytes. Outgoing packets were generally using TCP and UDP as protocols and were sent to IP addresses owned by (among others) T-Systems International, Google and Facebook.

3.3.6 Comparative analysis

InternetGuard Data Saver and Protwall are based on Netguard, but the results do not match each other. InternetGuard Data Saver is the only application that was able to block most of the packages (Table 2). No firewalls other than NoRoot Firewall, InternetGuard Data Saver and Droid Firewall showed zero packets related to Facebook at least in one measurement. Amounts and sizes among different measurements and firewalls differed.

4. DISCUSSION

The impact of the work on society and scientific community of this research is that people are going to reconsider which firewall they are going to use and that they are aware that the apps are not as protecting as they claim to be. Despite the fact that this research provides some clear answers, is it good to say that a follow-up research must be done to make the answers more reliable.

A question that is still not answered after the research is: “Is an external firewall application able to block incoming data?”. This question could not be answered through the research because it was measured exclusively from the laptop, not from the phone which contained the firewall application, so that means that it is not possible to see if the incoming data went through the firewall.

Within this work, it was not possible to perform more than two network analysis tests. This makes the results less reliable because there were big differences in the results of the two measurements. This also made it difficult to compare the firewalls, which in term made it difficult to draw strong conclusions. For a subsequent research it is important to perform more network analysis tests. Another limitation was the variation in internet connection speed, which may have influenced the results.

One of the problems that came through during the research was that it was difficult to distinguish which Facebook package contained data from WhatsApp. When everything was blocked and there were still packages going around from Facebook it was hard to prove that the packages that were going around were linked to WhatsApp. Another problem in the research is that there was a lot of DNS-traffic. The DNS packages, were most of the time, requests. Without these packages the total amount of the packages would be much lower. It is still unclear if this should be seen as data or not.

In the future it would be interesting to perform the test from a phone with a clean Android install. In this way there will be less external factors that can influence the results. It is interesting whether there is a difference between the results of the two cases. For a subsequent research it would be relevant to measure the baseline before the test without a connected firewall. The research lacks this information because this was only measured before the first test, but it was not done in the second test, so it cannot be checked whether the baseline is accurate. However, it is important to measure whether there is a difference between in and outgoing data with and without a firewall.

5. CONCLUSION

In this paper, we studied the user friendliness and the effectiveness of the five best rated firewall applications. By two lines of research, usability testing and network traffic capturing testing, we obtained important insights in the performance of Android firewall applications and proposed some methodology for evaluating such apps.

We tested the user friendliness with a heuristic evaluation and a usability test. From the heuristic evaluation, problems have come up from the five applications. The most user-friendly application according to heuristic evaluation is "NetGuard". This application has a clear visibility of system status by using red and green indicators, no room for errors, needs confirmation if you change settings and has helpful tooltips.

The usability test has revealed that NetGuard has the best average grading from the 25 participants. The least scoring applications is NoRoot Firewall.

In addition to user friendliness, effectiveness was also an important aspect of the research. From the network capturing test we can conclude that the firewall applications do not do what the user expects; blocking in and outgoing data. Although no application blocked all data during each test, the most effective application is "NoRoot Firewall”.

6. Acknowledgments

The researchers would like to thank Daniël Meinsma for his guidance through this research. We also like to thank the Hague University of Applied Sciences for sponsoring this research at the Dutch Innovation Factory in Zoetermeer, The Netherlands.

BIBLIOGRAPHY

[1] Statista. 2016. “Number of smartphone users worldwide from 2014 to 2020 (in billions)”. https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide

[2] Shih, Dong-Her, et al. 2008 "Security aspects of mobile phone virus: a critical survey." *Industrial Management & Data Systems* 108.4: 478-494. https://www.emerald.com/insight/content/doi/10.1108/02635570810868344/full/html

[3] Muhammad, Nooh Bany. 2018. "A study on cell phone security: Authentication techniques." *2018 International Conference on Information and Computer Technologies (ICICT)*. IEEE, 2018. https://doi.org/10.1109/INFOCT.2018.8356847

[4] Nielsen, Jakob, and Rolf Molich. 1990. "Heuristic evaluation of user interfaces." *Proceedings of the SIGCHI conference on Human factors in computing systems*. ACM, 1990.

[5] Lessard, Jeff, and Gary Kessler. 2010 "Android Forensics: Simplifying Cell Phone Examinations." . http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=7480&context=ecuworks

[6] Wireshark. Wireshark - Go Deep. Retrieved from www.wireshark.org

[7] Google. 2019. Google Play. Retrieved from https://play.google.com/store

[8] mxttoolbox.com. 2019. Supertool. Retrieved from https://mxtoolbox.com/SuperTool.aspx

*Title can be chosen from: master student, Phd candidate, assistant professor, lecture, senior lecture, associate professor, full professor

Your Name	Position*	Email	Research Field	Personal website
Wouter Louman	Bachelor Student	16071670@student.hhs.nl	Mobile Security	
Mitchell Vernee	Bachelor Student	16099567@student.hhs.nl	Mobile Security	
Danique de Bruijn	Bachelor Student	17100992@student.hhs.nl	Mobile Security	
Babette van 't Riet	Bachelor Student	17064953@student.hhs.nl	Mobile Security	
Hani Alers	Lecturer	HAL@HHS.NL	Man-Machine Interaction	