Changing People's Behaviour towards Unsecured Wi-Fi Hotspots

W. Noort
University of Twente

W.J.B. Beukema
University of Twente

S.H.S. de Vries
University of Twente

There are serious risks attached to the use of public Wi-Fi hotspots. As most people are not aware of these risks, an experiment was conducted where users were actively warned about the dangers of public Wi-Fi hotspots. The result of the experiment is that 40% of the people who have seen no warning will connect to another hotspot, while 43% of the people who have seen the warning will connect to another insecure network. Therefore, increasing awareness to this problem by actively warning people upon connecting to wireless networks is ineffective and other solutions should be found.

1 Introduction

As of 2014, it is estimated that there are 47.7 milion public Wi-Fi hotspots deployed worldwide (iPass Inc., 2014). Public hotspots are often used in businesses to provide an extra service to customers, but public hotspots can also be found in trains, buses, planes, or even city-wide. Thus, customers have a lot of opportunities to access these public Wi-Fi networks.

However, there are serious risks attached to the use of public Wi-Fi hotspots. As the data is transmitted over the air, Wi-Fi is more vulnerable to interception attacks compared to the traditional wired connections and private (i.e. encrypted) Wi-Fi connections. Criminals could setup fake Wi-Fi hotspots or even clone existing Wi-Fi hotspots in order to intercept data from victims, without the victims even knowing they are being eavesdropped. Personal information can be stolen and abused. Therefore, the people should be aware of the dangers that public Wi-Fi hotspots impose.

As research shows, about seven out of ten US consumers frequently connect to a public Wi-Fi hotspot, regardless whether it is a secured network or not (Taylor & Christensen, 2013). Despite several campaigns by organisations such as the FBI and Europol stressing the dangers of using public Wi-Fi hotspots, it can be concluded from research that over the last three years, the number of people using public Wi-Fi hotspots has been increasing (Taylor & Christensen, 2013).

Therefore, the current awareness campaigns are not effective when it comes to decreasing the number of people using public Wi-Fi hotspots. This research intends to investigate whether actively warning people against the dangers is a more effective approach. We establish this by setting up our own public Wi-Fi hotspots that serve warning pages about the dangers of public Wi-Fi hotspots when a user connects instead of providing internet connectivity.

Hence, our research question is: *How can people's awareness regarding unsecured Wi-Fi hotspots be increased?* Our hypothesis is that informing people using a warning page that is shown upon connecting is a successful approach to increase people's conscience on this issue.

1.1 Related literature

In this section we will review several papers about different security risks that exists in the Wi-Fi protocol for hotspots. These papers demonstrate the need for improving wireless security. Some papers about technical solutions and the behaviour of people towards network will also be reviewed.

Park et al. (2014) focuses on the dangers of connecting to unsecured Wi-Fi hotspots with a smartphone. The authors emphasise that most of the time smartphones contain personal information, which increases the possible impact of an attack. In this work, an attack is demonstrated in which a rogue Wi-Fi hotspot seems to serve a normal Internet connection, though it injects malicious code using DNS spoofing. Another issue regarding fake Wi-Fi hotspots is addressed by Dondyk et al. (2013), which the authors call a *denial-of-convenience attack*. In this attack, a fake Wi-Fi hotspot that does not provide an Internet connection might deprive users from any Internet connetion, as devices that also have a cellular connection often terminate this connection and try to use the Wi-Fi connection instead. As, according to the authors, most devices do not detect the lack of Internet connection, users have to manually turn off Wi-Fi in order to be able to use their cellular connection instead. An even more dangerous attack is presented by Lanze et al. (2014), using an *evil twin*. An evil twin is a rogue Wi-Fi network that clones the broadcast details of a genuine, unsecured Wi-Fi hotspot. As devices cannot verify the validity of a Wi-Fi hotspot, most

devices will automatically connect to the evil twin if the device has been connected to the original network before. The fact that devices connect automatically to the rogue hotspots makes it even easier for attackers to find victims.

Lanze et al. (2014) suggests a solution for the problems described above by authenticating known wireless hotspots similar to the way authentication is done in SSH. This approach would improve confidentiality because is allows traffic to be encrypted for open hotspots. Also, integrity and availability will be improved because clients will not automatically connect to a rogue network with a known name that manipulates network traffic, because the public key would be different. However, even with this method some problems persist. The first time a user connects to a wireless network no authentication can be performed, or a manual authentication at best. There are also practical difficulties which prevent a wide-scale implementation of this technique: it would require changes in the protocol and thus changes in existing Wi-Fi hardware.

Other technical solutions would also require changes in the Wi-Fi protocol and have the same practical limitations. Therefore, we also consider improving awareness among users of Wi-Fi networks as a solution. Research has been performed to measure the security awareness regarding unsecured access points amongst people with different backgrounds, such as social sciences students and science students (Lorente et al., 2014). Additionally, users were warned by means of flyers and banners. However, no significant difference in levels of awareness has been found.

When it comes to changing people's behaviour regarding a certain 'crime', Clarke (1997) introduces a number of techniques on situational crime prevention. These techniques can be divided into five categories: increasing the effort, increasing the risks, reducing the rewards, reducing the provocations and removing the excuses. This last category is based on the fact that offenders often try to rationalise their behaviour by neutralising the outcomes of their actions. By removing the ability to make such excuses, people's behaviour can be changed, according to the author. One of the solutions to remove excuses is to alert conscience, by means of displaying warning signs.

As can be seen from the discussed literature, there are serious risks attached to the use of unsecured Wi-Fi hotspots and technical solutions to this problem require major changes. Hence, our approach aims, similar to Lorente et al. (2014), also at improving awareness, but in a more direct way. We set up fake Wi-Fi hotspots in order to warn people about the dangers that are attached to connecting to unknown wireless networks, and investigate whether educating the end users with this approach is an effective method. The main difference is that users receive direct feedback on 'bad' behaviour, as our warning page is visible immediately upon connecting. This is in line with the the work of Clarke (1997), as our approach intends to stimulate conscience and hence removes excuses for people to use public Wi-Fi hotspots.

2 Method

For this research, we create two public Wi-Fi networks where people could be looking for internet access[1]. Based on research earlier mentioned in this paper, we assume that people who are looking for free Internet access will connect to one of our networks (Taylor & Christensen, 2013). The hotspots are configured in such a way that each network has a 50% probability of showing a warning page upon connecting. Showing the warning page on the user's device is established by resolving all domain names to our local IP address, which serves the warning page. This so-called *Captive Portal*

[1] A code repository with the source code of the pages, scripts to create the hotspots and the raw results can be found here `https://bitbucket.org/tux4life/team-314-pub`

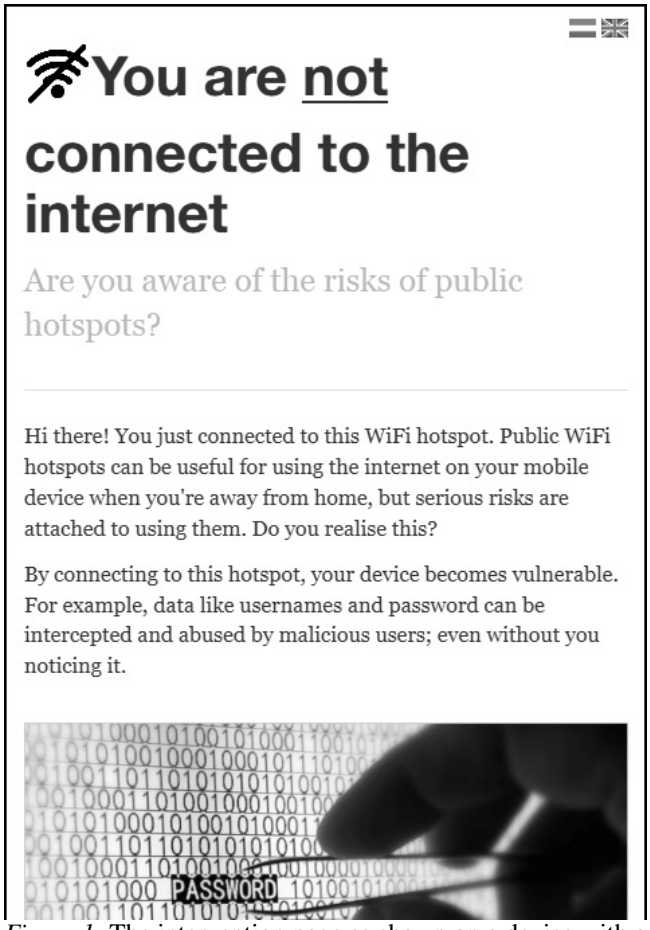

Figure 1. The intervention page as shown on a device with a display resolution of 480x800.

is often used by Wi-Fi hotspots that require user input, such as log in credentials or a payment, before Internet access is provided. Most devices will automatically detect the redirection and will notify the user. Devices running on iOS or Windows Phone even immediately show a pop up with the portal after connecting.

2.1 Intervention

The intervention page that is shown to about 50% of the users, warns the user about the dangers that are attached to the use of public Wi-Fi hotspots. It consists of a title, a small introduction paragraph, a paragraph about the risks of using public Wi-Fi hotspots, and a small list of *do's and don'ts* when using hotspots. The web page is designed to display well on devices with small screens (such as smartphones and tablets) as well as devices with larger screens (such as laptops) using a responsive design. Based on the language preferences the user's browser sends when trying to access the warning page, the page is shown either in English or Dutch. On the warning page itself it is also possible to switch between these two languages.

The other 50% of the devices that connect will just receive a page that states 'No Internet connection'.

Both hotspots do not provides actual Internet access, but rather just serve our own pages.

We assume that someone who is looking for Internet access will normally connect to our other network in order to get Internet access, after finding out that the network he connected to does not provide Internet access, However, our hypothesis is that those who have seen the intervention page, are less likely to connect to the other network because they are supposedly more aware of the dangers connecting to an open Wi-Fi network imposes.

In order to let our access points look like common hotspots, we use general broadcast names. The SSIDs we used were *Hotspot* and *WiFi*.

2.2 Data collection

For our experiment, we use a laptop with a built-in Wi-Fi adapter and an extra external Wi-Fi adapter. The laptop runs a script that sets up two Wi-Fi networks, starts a web server that hosts our intervention page and starts the DNS server that redirects the incoming traffic to this web server.

Of every device that connected to one of the networks, we collected its MAC address[2], whether or not the warning page has been served, whether or not the the warning page was actually shown, and whether or not they have tried to access the other Wi-Fi network afterwards.

In order to determine whether or not the device has actually showed the warning page to the user, we included a JavaScript script that sends an HTTP request after the web page has been visible for two seconds. Determining this is necessary to verify the effectiveness of the intervention: people might not actually have seen the page, e.g. because someone's device has automatically connected to one of our networks because it has a network with the same SSID in its 'saved networks' list.

We have constructed a hash function for the MAC-addresses by taking the last 24 bits (3 bytes) of the SHA-1 hash. This way, when we hash up to 100 different MAC-addresses, the hashes will be all different with a $p \geq .999$ [3].

2.3 Data analysis

Based on the collected data, we determine whether people who have connected to our hotspot and have actually seen the warning page are less likely to connect to our second network. The people who connect to our hotspot and do not get the warning page, form our control group. We expect our intervention to be effective, thus our hypothesis is that people who have seen the intervention first are significantly less likely to connect to the other network, compared to the people who have not seen the intervention the first time. If this is true, we might conclude that our intervention indeed is effective.

To calculate whether the test results are significant, we postulate two populations of people who either have or haven't seen our intervention page. We take random samples from both populations and test the following variable: subject connecting to both networks. The proportions of subjects connecting to both networks are expressed as p_t and p_c for both groups respectively. We now state two hypotheses:

h_0: $p_t = p_c$. This means the intervention page has no effect.

h_1: $p_t < p_c$. This means the intervention page has a positive effect.

To test whether we can reject h_0, we use the *one tailed paired Z-test for proportions* with $\alpha = 0.05$:

$$Z = \frac{\hat{p}_t - \hat{p}_c}{\sqrt{\hat{p}(1-\hat{p})\left(\frac{1}{n_t} + \frac{1}{n_c}\right)}} \tag{1}$$

where $\hat{p}_i$ is the proportion of group i, $\hat{p}$ is proportion of the groups combined and n_i is the sample size of group i.

Because $\alpha = 0.05$ and a one tailed test is performed, we obtain $z_{\text{critical}} = -1.645$ (from z-table). The means the computed value for Z should be lower than z_{critical} to reject h_0.

[2]Because MAC-addresses are considered personally identifiable information(Engelfriet, 2014), we will only store an irreversible hash of MAC addresses instead of the MAC address itself

[3]Due to the Birthday paradox, we have to keep quite a large entropy for a sufficiently high p.

Table 1
Results of the test group and the control group

	Control group		Intervention group			
	1 pageview	2 pageviews	1 pageview	2 pageviews	total pageviews	total connected devices
Total	10	4	14	6	34	71
iOS	5	1	10	1	17	24
Android	2	2	2	4	10	15
Windows Phone	1	0	0	0	1	2
Other / Unknown	2	1	2	1	6	30
6:00 - 9:00 (3 sessions)	1	1	2	1	5	16
9:01 - 12:00 (4 sessions)	5	2	6	1	14	20
12:01 - 15:00 (5 sessions)	3	1	4	2	10	20
15:01 - 18:00 (2 sessions)	1	0	2	2	5	14
18:01 - 0:00 (1 session)	0	0	0	0	0	1
Enschede - Zwolle	4	1	3	1	9	24
Zwolle - Enschede	4	3	11	5	23	43
Amersfoort - Ede-Wageningen	2	0	0	0	2	4
AR (Arabic)	0	0	1	0	1	1
DU (German)	0	0	1	0	1	1
EN (English)	1	1	1	0	3	4
NL (Dutch)	9	3	11	6	29	29
None	0	0	0	0	0	36

2.4 Locations

In order to get reliable results, it is important that there are no other public Wi-Fi networks available at the place the experiment is conducted. If there were, the measured data would possibly be inaccurate, as we cannot determine whether users connected to the hotspot(s) we do not control. To achieve this, we conduct the experiment on train lines Enschede-Zwolle, Enschede-Apeldoorn and Amersfoort-Ede-Wageningen during both peak and off times. On these train lines, no hotspot is provided by the train operator; therefore, our networks are the only ones available. Train passengers are an interesting group, as it is a very diverse group of people who might be checking for open Wi-Fi networks in order to kill the time they have to wait to get at their destinations.

3 Results

Our control group consists of 14 people. Of these 14 people, 10 connected to one network and 4 people connected to both networks. Our test group consists of 20 people. Of this group, 14 connected to only one network. These 14 people can be regarded as successful interventions. 6 people in the test group connected to both networks, which can be regarded as unsuccessful interventions. This is summarised in Table 1. These results were obtained during 15 measurement sessions, of which the details can be found in Table 2.

The results in Table 1 are also split according to operating system, time of the first connection attempt, train line and the preferred language of the browser. The last column of Table 1 contains the amount of raw connects, whereas the other columns contain the verified amount of pageviews (of either the intervention page or the no-internet-available page). Because the measurement sessions are not evenly distributed amongst the time slots, the amount of sessions for each time slot are added to the table (see Table 2 for more details).

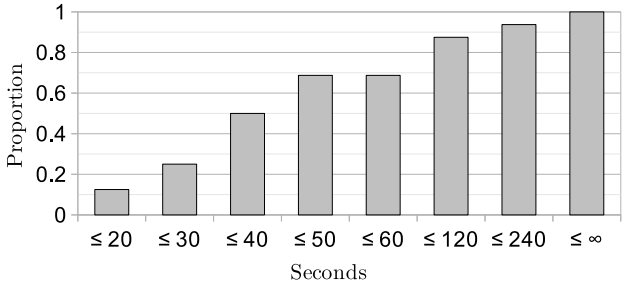

Figure 2. Time between first connect to the first network and first connect to the second network

Furthermore, Figure 2 contains the time elapsted between a connection to both networks (if this actually happened).

4 Discussion

Using the gathered data and formula (1), we find $z = 0.3792$. Based on this, we conclude $z \not\leq z_{\text{critical}}$. Therefore,

Table 2
Measurement sessions

Date	Begin time	End time	Route
November 26th 2014	8:08	9:11	Enschede Drienerlo – Zwolle
November 26th 2014	9:19	10:22	Zwolle – Enschede Drienerlo
November 28th 2014	13:08	14:11	Enschede Drienerlo – Zwolle
December 1st 2014	11:49	12:52	Enschede Drienerlo – Zwolle
December 2nd 2014	8:08	9:11	Enschede Drienerlo – Zwolle
December 2nd 2014	9:19	10:22	Zwolle – Enschede Drienerlo
December 2nd 2014	15:08	16:11	Enschede Drienerlo – Zwolle
December 2nd 2014	16:19	17:22	Zwolle – Enschede Drienerlo
December 3rd 2014	8:08	9:11	Enschede Drienerlo – Zwolle
December 3rd 2014	9:19	10:22	Zwolle – Enschede Drienerlo
December 3nd 2014	22:19	23:27	Zwolle – Enschede
December 5th 2014	12:11	12:48	Amersfoort – Ede-Wageningen
December 8th 2014	9:19	10:22	Zwolle – Enschede Drienerlo
December 17th 2014	12:08	13:11	Enschede Drienerlo – Zwolle
December 17th 2014	13:19	14:52	Zwolle – Enschede Drienerlo

we do not reject h_0. In other words, we do not have statistically significant evidence at $\alpha = 0.05$ to show that our intervention was effective.

According to Otto (2014) Android has a market share of 54.22% in The Netherlands and iOS 44.30%. However, we have found iOS users viewing a page more often ($n_{\text{iOS}} = 17$) than Android users ($n_{\text{Android}} = 10$). When compared to the market share of both operating systems, we have found that iOS users connect more often to our networks. This can possibly be explained by a feature of iOS that informs the user of newly available Wi-Fi networks. If this is the case, iOS users are encouraged towards unsave behaviour (connecting to unknown / unexpected / unsecured Wi-Fi networks). Although the intervention is more effective for iOS users than for all operating systems, a significant effect of the intervention can still not be proved ($z = -0.4635$, $p = 0.05$).

When looking at the different time periods, we were expecting more results per session during peak hours (6:00 - 9:00 and 15:01 - 18:00), because the trains are busier during those periods compared to off hours. However, this assumption is contradicted by the results. This could be explained as follows: during peak hours the trains are filled with commuters who have tried to connect to the Wi-Fi hotspot of the train operator and concluded there is no internet service in the specific train. These subjects are less likely to search for a hotspot again. During off hours however, less frequent travellers occupy the train, expecting internet access like in most other trains. The most promising time slot for a successful intervention seems to be 9:01 - 12:00. Unfortunately this result is also not significant ($z = -0.6515$, $p = 0.05$).

When we compare the different train lines and preffered language, no significant results can be obtained either.

A remarkable observation from the data is that some devices connected to the hotspot while the page was presumably (see Limitations) not shown to the user. The most credible explanation for this is that some devices have connected to networks with the same SSID before (and as a result be stored in the device's stored networks list). This may result in their devices automatically connecting to one of our hotspots, even without the user noticing this. As the user may be not actively using his phone when this happens, our page will not be shown. Therefore, we only counted devices for which we could verify that the page was shown in order to measure the effectiveness.

4.1 Limitations

There are some limitations in the methodology as used in this research. First of all, a possible limitation could be people who see two open networks and have seen the warning page get curious to what happens when they connect to the other network. This might cause them to connect to the other network.

As we performed the experiment in trains, our subjects were train passengers. Although this is a diverse group, it might not be a completely representative group. For instance, people who commute by train every day might not check for open hotspots because they know the train operator does not provide Internet access.

Another limitation is our use of a JavaScript AJAX-call to measure whether the intervention was actually seen by the users, and not just automatically requested by the device. Two problems may arise: firstly, JavaScript may be disabled. This means people who have read the page are not being taken into account in the results. Secondly, the warning page may have been visible, but this does not mean that the user has actually read the page. These problems have only a limited impact, because the problems apply to both the test

group and the control group.

Finally, we performed the experiment using the same warning page. The design of the warning page affects the effectiveness of the experiment; a different design might have been more successful. In future research, the effectiveness of different types and designs of warning pages could be investigated.

Nevertheless, we are still able to conclude that showing a warning page is an ineffective method to prevent people from connecting to unsecured wireless networks.

4.2 Other mitigations

There are other possible solutions to the problem of unsecured Wi-Fi hotspots. Besides increasing awareness, as our research proposes, another option would be to make changes in the design of Wi-Fi or Wi-Fi compatible devices. For instance, SSL combined with DNSSec could provide a solution. If implemented on a large scale, devices would be able to detect when DNS records are altered or when there is a man-in-the-middle active. However, we do not expect this to be implemented on a large scale in short term as it requires massive changes to the Internet infrastructure.

Another solution would be to implement an SSH-like authentication mechanism for Wi-Fi access point, as suggested by Lanze et al. (2014). This approach prevents Wi-Fi devices from automatically connecting to an access point with the same SSID. However, this is not a solution for the short term either, as both Wi-Fi access points and Wi-Fi client devices should be updated. Besides that, this mitigation only prevents SSID cloning, whereas it does not solve the problem of man-in-the-middle attacks.

Nevertheless, as raising awareness for the problem does not seem to solve this problem, a technical solution is needed. Although this might require radical changes to the Internet infrastructure and/or to Wi-Fi devices, it is another reason to speed up the adaption of these new technologies as they address a serious problem. As we have seen, rogue Wi-Fi hotspots can be set up easily while they can cause serious damage; therefore, to completely solve this issue, we need technical solutions.

4.3 Conclusion

This research has shown that our approach of actively warning people about the dangers of connecting to open wireless networks using warning pages is ineffective. Hence, the problem of unsecured wireless networks remains unsolved. As we have seen, the extent of the problem points towards a technical solution rather than a solution aiming for increased awareness amongst end users.

5 References

Clarke, R. V. G. (1997). *Situational crime prevention*. Criminal Justice Press.

Dondyk, E., Rivera, L., & Zou, C. C. (2013, November). Wi-Fi Access Denial of Service Attack to Smartphones. *Int. J. Secur. Netw.*, *8*(3), 117–129. doi: 10.1504/IJSN.2013.057698

Engelfriet, A. (2014, January). *Wifi-tracking: winkels volgen je voetsporen.* Retrieved from `http://blog.iusmentis.com/2014/01/24/wifi-tracking-winkels-volgen-je-voetsporen/`

iPass Inc. (2014, November). *iPass Wi-Fi Growth Map Shows 1 Public Hotspot for Every 20 people on Earth by 2018.* Retrieved from `http://www.ipass.com/press-releases/ipass-wi-fi-growth-map-shows-one-public-hotspot-for-every-20-people-on-earth-by-2018/`

Lanze, F., Panchenko, A., Ponce-Alcaide, I., & Engel, T. (2014). Undesired Relatives: Protection Mechanisms Against the Evil Twin Attack in IEEE 802.11. In *Proceedings of the 10th acm symposium on qos and security for wireless and mobile networks* (pp. 87–94). New York, NY, USA: ACM. doi: 10.1145/2642687.2642691

Lorente, E. N., Meijer, C., & Verbruggen, R. (2014). *Removing SSL using man in the middle on a wireless access point.* University of Twente.

Otto, R. (2014, July). *iOS en Samsung hebben 84% marktaandeel in Nederland.* Retrieved from `http://www.adformatie.nl/artikel/ios-en-samsung-hebben-84-marktaandeel-nederland`

Park, M.-W., Choi, Y.-H., Eom, J.-H., & Chung, T.-M. (2014, August). Dangerous Wi-Fi Access Point: Attacks to Benign Smartphone Applications. *Personal Ubiquitous Comput.*, *18*(6), 1373–1386. doi: 10.1007/s00779-013-0739-y

Taylor, S., & Christensen, T. (2013). *What Do Consumers Want from Public Wi-Fi? Gain Insights from Cisco's Mobile Consumer Research.* Retrieved from `http://www.cisco.com/c/en/us/solutions/collateral/service-provider/service-provider-wi-fi/white-paper-c11-729797.pdf`