Do graphical cues effectively inform users?
A socio-technical security study in accessing wifi networks

Ana Ferreira[1,2], Jean-Louis Huynen[1,2]
Vincent Koenig[1,2], Gabriele Lenzini[2], and Salvador Rivas[1] ⋆ ⋆⋆

[1] Institute of Cognitive Science and Assessment - Univ. of Luxembourg
[2] Interdisciplinary Centre for Security Reliability and Trust - Univ. of Luxembourg

Abstract. We study whether the padlock and the signal strength bars, two visual cues shown in network managers, convey their intended messages. Since users often choose insecure networks when they should not, finding the answer is not obvious; in our study we clarify whether the problem lies in uninformative and ambiguous cues or in the user who, despite understanding the cues, chooses otherwise. This paper describes experiments and comments the results that bring evidence to our study.

1 Introduction

In [1] we studied the human-computer interactions in hypothetical situations where users select one out of several hotspots offering access to Wi-Fi networks. Motivated to discover *where* security can fail, we highlighted the points in the user-interaction protocol where users opt for an open (insecure) network even for tasks that require security, and despite the presence of visual indicators (called *cues*) reminding the insecurity of the choice. However, to improve the security of those interactions one should rather understand *why* users decide insecurely when they should not and whether users consider or not in their decision making, the message carried by the security cues.

This paper's goal is to answer this "*why*" question, and clarify why Wi-Fi users select a certain network instead of others. There is little research on this question in relation to the security and to the understanding of symbols that network managers rely on. The closest is the research done by Jeske *et al.* who argue that the padlock and signal strength unintentionally nudge people to insecure choices [2]; however they do not explain *why* this happens: are these visual cues unclear and misleading the users? Are they ambiguous and leading users to ignore them? Or are they clear in their messages, but are users choosing insecurely for other reasons extraneous to the cues?

These three questions motivate the present paper. Generally speaking, we could think that users and interfaces are engaged into a sort of *visual conversation* and so it is legitimate to expect it to follow the same principles that rule a constructive and clear conversation. P. Grice, who studied this topic in

⋆ This research is supported by FNR Luxembourg, project I2R-APS-PFN-11STAS.
⋆⋆ In alphabetical order.

the philosophy of language, calls them *cooperative conversation* and lists those principles as follows [3]: *quantity* (state what is informative, no more and no less than that); *quality* (don't state what is false, don't state what lacks evidence); *relation* (be relevant); *manner* (avoid obscurity, ambiguity, verbosity, and be orderly).

To clarify whether cues are "cooperative" in the sense given above leads to an interesting approach to answer "*why* do users choose insecurely?" in the presence of cues. The approach consists of separating what can be explained in regard to "ineffective" cues from what instead is about an informed choice by the user.

Contribution. The paper describes the particular scenario where a user chooses a Wi-Fi network. We question whether the common visual cues employed in this task —the padlock and the bars that indicate the signal strength— succeed in communicating their intended message, and we contribute to understanding why. This study builds on observed behaviour of about 1000 participants.

Other authors have studied related questions. As noted earlier, Jeske *et al.* [2] observe that convenience-oriented students *behave* as if the padlock is a barrier to secure choices. They have however not investigated *why* users behave this way. Several key questions thus remain unanswered: does a user *behave* so because they *misunderstand* the padlock or rather because they overlook the padlock due to accompanying factors that force different meanings?

The difference between behaving and understanding is key for us. A user may (a) understand but ignore the cues, and this is after all an *informed* decision. Or they can (b) understand a different message and so take a *misinformed* decision, or they can (c) ignore completely the cue so prefer an *uninformed* decision.

Case (a) suggests that the cue works fine. But (b) suggests that the cue fails and needs a revision, whereas case (c) the cue is irrelevant, and thus useless. Moreover, in (a) one can still decide insecurely, as well as one can still behave securely in (b) or (c). But, in any of those situations, what nudges the user's behaviour should not only be searched for in the cue itself, but also in other factors, such as in the presence of other indicators, which influence a cue's message, or in the task a user is performing, or in the user.

Therefore, this work's main research questions are the following: Are the padlock and the signal strength and their relative importance responsible for a user's *informed*, *misinformed*, or *uninformed* decision? Which cues are the most influential in causing that difference, if any? Are the user's background and different Wi-fi scenarios also affecting the user's behaviour?

2 Methods

To distinguish the situations where people take *informed*, *misinformed*, and *uninformed* decisions, we need to compare people's understanding of the Wi-Fi networks' properties and visual cues relative to the choices they make. Therefore, we conduct a study where we ask participants the following: first, to read the description of a specific scenario setting, a given context and a specific task to

perform; second, to choose between different Wi-Fi networks to achieve the task; third, to answer questions about the meaning of the visual cues they encountered; and finally, to answer questions about their knowledge regarding Wi-Fi networks.

What we investigate is whether the choice of a Wi-Fi network depends on the properties of the Wi-Fi network itself and on the specific task to be undertaken. Thus, more precisely, the *dependent variable* we investigate is the participants' Wi-Fi choice, a dichotomous (i.e., 0/1, wrong/right) variable. As main *independent variables* we choose the presence/absence of the padlock sign (🔒) —supposed to indicate *secure communication*, technically the presence of encryption— and the presence of one of the two signal strength sign (📶 or 📶) —supposed to indicate *quality of connectivity*, technically the strength of the received Wi-Fi signal. These are in fact the properties of Wi-Fi networks typically communicated to the user. In our study we thus display one of the four possible combinations: '📶', '📶 🔒', '📶', or '📶 🔒'. In the remainder of this document, for sake of conciseness, we use the terms "Encryption" for *secure communication* and "QoS" for *good connectivity*.

"Encryption" (i.e., *secure communication*) and "QoS" (i.e., *good connectivity*) represent also the two meaning dimensions that we assess from our participants in relation to how they understand the cues. We measure how much the participants think a cue means "Encryption" or "QoS", and this is driven by the task a user is involved in; we consider four tasks designed to evoke a need for "Encryption" and "QoS" through context description.

Additional *independent variables* that we consider to be important factors to control for are the following: the order of the Wi-Fi network names; speed of appearance over time, i.e., how quickly or slowly the network is listed by the network manager; and the participant's social and personal background, i.e., tech-savvy *vs* non-tech-savvy users. Moreover, to ensure that participants do not avoid encrypted networks because they do not have a password, we provide a password to half of the sample, aleatorily.

To investigate those factors, while maximizing internal validity, we chose an in-between subject study design. Participants were presented only one scenario to avoid security priming of one scenario on the others. The study was conducted on-line: the flow of the study design comprised a socio-demographic questionnaire; the description of a scenario with instructions to select a Wi-Fi network from a given list; several rounds of network selections; an assessment of the meaning participants have for the given cues; and a follow-up questionnaire to assess further attitudes and beliefs about ICT security (e.g., misconceptions and beliefs regarding Wi-Fi networks). In each scenario, we describe for the participant a character they implicitly inhabit and ask him/her what network s/he would select given the context and task to be accomplished. Participants were assigned to respond to 1 scenario out of 4 possible ones; thus the probability of assignment was of .25. Each scenario differed in terms of the requirements the Wi-Fi network should have to complete the task (i.e., combination of "Encryption" and "QoS"). Participants had five rounds of choices; each round presented

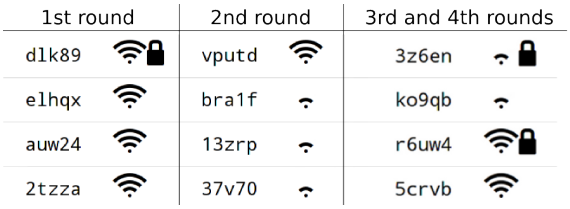

Fig. 1. Rounds of choices.

a list of 4 Wi-Fi networks, ordered randomly, each displaying a randomly generated name, a signal strength indicator (📶 or 📶), with or without a padlock sign (🔒). Figure 1 shows the Wi-Fi networks for the four rounds. To test for consistency we added a fifth round, not shown in the figure: it is one of the presented 4 rounds, randomly chosen. Due to space limitations, in this manuscript we focus and describe only the results associated with the third round of network choices. Either, we have no space to present and discuss how the delay, and/or the timing, of the listing of network names affects the Wi-Fi network choices; and also how the sequential order of the Wi-Fi networks makes a difference. This is left as future work.

To assess whether users associate the right intended meaning to the cues ("Encryption" for the padlock, and "QoS" for the signal strength bar) we ask the participants to express their understanding using a 4-points Likert scale (Not at all, Partially, Mostly, Completely) the extent to which they agree that each of the 2 visual cues (🔒 and 📶) corroborate in meaning with 4 words related to "Encryption" (confidential, protected, encrypted, and private), and 4 related to "QoS" (good signal strength, high-bandwidth, high-speed, and fast).

As mentioned above, we complement the study with additional attitude and belief questions regarding the participants' use of Wi-Fi networks. For instance we ask such things as their thoughts about whether the padlock sign 🔒 means "locked out", and whether they tend to make choices out of convenience. To be clear, our *convenience* variable is a composite of three questions (Cronbach's $\alpha = 0.76$) and is used as such in our analyses. Additional questions are used to measure ICT skills: these are split into 2 separate variables, *stated ICT skills* (s.ICT) reflecting the participants' stated ICT skills, and *measured ICT skills* (m.ICT) reflecting how well the participants answered the technical questions. We collected a host of other variables thought to be associated with the Wi-Fi network choice; for the sake of space we ought to omit these results as well.

Choosing the tool for our on-line survey. We aimed to have a large number of participants and among a population larger than the one we could reach if we had run our experiment within our University quarters. Therefore, we opted for Amazon Mechanical Turk (`mturk`), a market place for on-line work which however offers readily available and substantially large samples of participants. The use of `mturk` as a tool for social experiments is debated; we are aware of it and of `mturk`'s potential limitations (e.g., [4]) that can harm internal validity. For

this reason we took several countermeasures to maximise as much as we could the quality in the collected data. We implemented a great amount of quality checks to detect that participants provide answers simply by clicking randomly. Namely, we implemented attention checks, for instance we added choices like: "I answer randomly and I should not be paid: Yes or No"; we repeated questions several times and we presented them with different wording; we measured the time participants took to answer each question to test unusually fast answering which can potentially indicate a low quality data; we also prevented a participant from participating more than once.

On the positive side, however, `mturk` allows us to recruit participants worldwidely, and in the specific case of the US (and we admitted only participants from this country, see later in this paragraph) it is thought to be better representative of the general population than those commonly recruited via university settings [5]. Moreover, evidence suggests that self-reported behaviours gathered with `mturk` are comparable to observed behaviours in laboratory studies [6]. To make our analyses and interpretation of our results easier, we choose to recruit only participants located in the US, where the majority of `mturk` workers do not use the tool as their primary source of income. We ran the study by batch of 100 participants at different times of the day, during workdays and week-ends. Following the guide edited by a community [7] of `mturk` workers, we took great care to guarantee workers' rights of information and privacy, and we paid USD 0.90 for an average of 5 minutes of participation. We collect their age, gender, how comfortable they feel with ICT and their occupation. Occupation categories are organized following the US Bureau of labor statistic's classification major groups [8]. Optionally, participants can communicate ethnicity related information that follow the US census' interviewing manual guidelines [9].

The pilot study. Another issue, not related to `mturk`, but yet could potentially challenge the reliability of the data and the internal validity of the study is whether the participants in fact understand correctly what they are presented. In particular, because in theory there is an infinite number of scenarios we could have used to convey and illicit a need for certain Wi-Fi network properties, we had to take special care to pilot test several possible scenarios to identify the ones we ultimately used in our study. For instance, to evoke a task that does not need secure communications or good connectivity, we can ask the participants to picture themselves waiting at a bus stop (no time pressure) searching for a Wi-Fi network to browse the Internet (no need for security), but this scenario could be understood differently by men and women. To guarantee unambiguity in understanding the scenarios, we ran a pilot study using the same tools and settings as the main study that aimed at finding the most intelligible and less biased scenarios. We built 3 different "vignettes" [10], or candidates, for each scenario, and asked 156 participants to rate how much the task mentioned in the vignettes should comply with several properties. There were 6 properties related to "secure communications" (confidential, protected, encrypted, secret, masked, and private), and 6 related to the "good connectivity" (good signal strength, high-bandwidth, high-speed, first-class, responsive, and fast). We analysed the results

Table 1. Chosen vignettes to convey the need for "Encryption' or "QoS" and their limitations.

Scenario	Intended meaning		Displayed text	Limitations
	Encryp.	QoS		
S0-0	0	0	I am sitting in a coffee shop with some friends. As they want to go for dinner later, I use my smartphone to check for a good restaurant. Unfortunately, there is no 3G/4G network available, so I have to use an available Wi-Fi network instead.	QoS is not significantly perceived as needed or not needed, males significantly perceive it as not-needed.
S0-1	0	1	I am a graphic designer intending to show my latest work to some of my friends. Since the 3G/4G connection is failing to retrieve the files, which are rather big, I decide to try an available Wi-Fi network to get some connectivity.	No limitation.
S1-0	1	0	I am waiting at a bus stop and I need to verify whether the check I deposited yesterday has been cleared. I need to use the bank's application on my smartphone to check the bank account's balance, but unfortunately there is no 3G/4G. I thus decide to try an available Wi-Fi network to get some connectivity.	QoS significantly tends to be perceived as needed whereas we intend to convey the converse meaning.
S1-1	1	1	I am a government official staying at an hotel. I scheduled an international online meeting. I planned to use the hotel's Wi-Fi network but the hotelś Wi-Fi proved unreliable when I called my family earlier to test the connection. There is no 3G/4G network, so I decide to go somewhere else to find an available Wi-Fi network.	No limitation.

Table 2. Sociodemographics profile by scenario.

	S0-0	S0-1	S1-0	S1-1	Total
Gender: Female	41 %	43.4 %	36.1 %	41.2 %	40.4 %
Gender: Male	59 %	56.6 %	63.9 %	58.8 %	59.6 %
Highest ed: High-School	47 %	41 %	42.9 %	40.8 %	42.9 %
Highest ed: Bachelor Degree	41.7 %	48 %	46.4 %	44.6 %	45.2 %
Highest ed: Master Degree	7.9 %	8.2 %	8.7 %	12 %	9.2 %
Comfortable in IT: Not at all	3 %	6.2 %	2.8 %	3.9 %	4 %
Comfortable in IT: Not Very	18.8 %	13.7 %	16.7 %	18.5 %	16.9 %
Comfortable in IT: Somewhat	55.3 %	58.2 %	59.5 %	57.5 %	57.6 %
Comfortable in IT: Very	22.9 %	21.9 %	21 %	20.2 %	21.5 %
Total counts	266	256	252	233	1007

of the pilot study with the R statistical software [11] and performed Wilcoxon rank tests [12] to discriminate the vignettes with the best psychometrical discrimination while checking for gender, age, and other social background variable effects. Table 1 shows for each scenario: the technical property that it intends to convey ("Encryption" or "QoS"), the selected vignette, and the limitations we need to be aware of when using it.

In summary, we model the dichotomous outcome (dependent variable) using Logistic Regression [13]: we estimate the conditional probability of choosing the target response option "clicking on the network with a 🔒 and a 📶" net of important independent variables. Our statistical modelling approach is relatively straightforward: firstly, we investigate the effect of the password because we expect it to be an important and significant control; we in fact find evidence of this and thus include it in all subsequent models. Secondly, we investigate the question of whether participants make an informed decision relative to each scenario, and then whether the participants' answers reflect, in a consistent way, their expressed choice relative to the meaning they attribute to the 🔒 and 📶 cues. Finally, we investigate whether the respondents' choices vary significantly by several basic socio-demographic variables.

3 Results

A total of 1090 participants took part in our study. Of these 83 failed the post-hoc data quality and integrity checks, and we remained with 1007 consistent cases. As shown in Table 2 and Figure 2, our sample is rather balanced with regard to gender. The age distribution has a wide range (56 years). Table 3 shows the frequency of clicks (counts) and percentages for the round under investigation in this manuscript, the 3rd. Only 7 participants chose a network with a 📶; since this gives a too low variability, we excluded those 7 cases and proceeded with our statistical analysis on the 1000 remaining cases that display a 📶.

Varying "Encryption" and "QoS" (independent variables) in order to measure WiFi selection outcomes (dependent variable) may give biased results, because choosing or avoiding network selections marked with a 🔒 can occur as an effect of our independent variables or as an effect of simply having a password

Fig. 2. Age and Occupation distribution for Males and Females

available or not. In order to control this potential bias, we provided half of the sample with a password. Performing a logistic regression allows to determine if the password is a significant predictor of the outcome "clicking on the network with a 🔒" and to what extent it is an effect based on our independent variables. With a password, odds of clicking on the target are 2.1 times higher (exponentiated coefficient (expcoeff)=2.1 with $p < 0.001$). Tested in each scenario, the password effect is significant in S0-0 (expcoeff=3.22, $p < 0.001$), and S0-1 (expcoeff=4.7, $p < 0.001$). As the scenarios evoke the need for "Encryption" and/or

Table 3. Counts and frequencies for the third round of the study.

	counts	frequencies
📶	5	0.5 %
📶	688	68.3 %
📶 🔒	2	0.2 %
📶 🔒	312	31 %

Table 4. Trimmed results of the logistic regression of network selection on password + scenario. (S0-0 reference category)

	Password	S0-1	S1-0	S1-1
p	< 0.001	< 0.01	< 0.01	< 0.001
expcoeff	2.2	2.0	1.9	4.2

for "QoS", we first analyze if the scenario is a predictor of the outcome i.e. "clicking on the network with a 🔒" while adjusting for password. If people understand the meaning of the cues correctly, using S0-0 as intercept: S0-1 ("QoS" needed) should not increase the odds of clicking on the target, and S1-0 ("Encryption" needed) and S1-1 should increase the odds in the same proportion. The results shown in Table 4 prove that scenarios S0-0 and S1-1 increase the odds in the same proportion and that S1-1 nearly increases the odds twice as much. To

investigate this result further and to determine if the participants took an "informed" decision, we consider the meaning the respondents associated with their responses. That is to say, we include an interaction term (*meaning* × *scenario*) and checked the resulting model fit statistics (LR test). Table 5 shows that

Table 5. Exponentiated coefficients of the logistic regressions for the main effect of "Encryption" and "QoS" while controlling for password and scenario. LR tests compare models with and without interaction terms.

Cue	Dimension	Main effect		LR Tests
		expcoeff	p	p
🔒	Encryption	0.823	< 0.01	NS
	QoS	0.727	< 0.001	NS
📶	Encryption	0.860	NS	< 0.05
	QoS	0.826	< 0.01	NS

while the main effects of the meaning dimensions are by large significant, with the exception of the encryption for the 📶 symbol, the LR tests show lack of improvement in model fit by including the interaction terms. This suggests that the effects of the meaning dimensions do not vary significantly per scenario.

Then we turn our attention to the socio-demographic effects. Age has a significant effect ($p < .001$) as increasing age by 1 multiplies the odds of clicking on the target by expcoeff=1.026. Having good measured IT skills multiplies the odds of clicking on the target by expcoeff=1.389 ($p < 0.05$). Convenience-driven participants are expcoeff=0.104 ($p < 0.001$) times less likely of clicking on the target. Interactions of convenience with the scenarios are not significant. Gender, occupation, ethnicity and stated ICT skills don't have significant effects. To investigate the predictive power of the independent variables in our model, we conducted a series of logistical regressions in a stepwise fashion. We start with an adjusted model that includes password and scenario, then we add: the convenience, the measured ICT skills, the meaning dimensions, and the socio-demographic variables. Results are presented in Table 6 and discussed in the section below.

4 Discussion

Previous research shows that the 🔒 can act as a barrier for the user to choose a secure network [2]. This suggests that users are taking a "misinformed" decision, misunderstanding the meaning of that cue. This is actually the case because Table 6 shows that when 🔒 is misunderstood as meaning "QoS", users are less likely to choose the encrypted network.

Our results support that 📶 is the cue that interferes the most with the other cues. That is to say, we were unable to perform any substantive statistical analysis on this particular issue because only 7 participants out of 1007 chose a

Table 6. Logistic regression results. Tests are perfmormed between the current model and the previous one. AIC is evaluated as well. ($^{*} < .05$; $^{**} < .01$; $^{***} < .001$)

Variables	Step 1	Step 2	Step 3	Step 4	Model fit	
					LR Tests	AIC
Password	2.2 ***	2.4 ***	2.4 ***	2.4 ***	-	1171.88
S0-1	2.0 **	NS	NS	NS	-	1171.88
S1-0	1.9 **	1.8 *	1.8 *	1.8 *	-	1171.88
S1-1	4.2 ***	4.5 ***	4.6 ***	4.7 ***	-	1171.88
Convenience	-	0.10 ***	0.11 ***	0.11 ***	< 0.001	1000.87
m.ICT	Not significant, not added.					
🔒 = Enc.	Not significant, not added.					
🔒 = QoS	-	-	0.91 **	0.91 **	< 0.01	993.25
📶 = Enc.	Not significant, not added.					
📶 = QoS	Not significant, not added.					
age	-	-	-	1.0 **	< 0.01	986.72
gender	Not significant, not added.					
occupation	Not significant, not added.					
s.ICT	Not significant, not added.					
Ethicity	Not significant, not added.					
n = 1000						986.72

network with a 📶: participants avoided the 📶 sign without any regard for the other cues it was associated with or any other contextual factors. We can't discuss further the weight of its meaning in the decision without statistical evidences, but as participants massively rated 📶 as being the least related to "QoS" we can infer that they took "informed" decisions.

Table 6 lists the results of our regression modelling approach and shows the effect of adding other factors one by one. "Convenience" is the *most powerful predictor* of Wi-Fi network selection. We find that being convenience-driven lowers the probability of choosing the encrypted network by 89%. In fact, when we include "Convenience" in our model, it cancels-out the effect of scenario S0-1 ("QoS" needed); this effect suggests that the choices made for that scenario are explained by the convenience factor rather than the scenario itself.

"Scenario" is the *second most powerful predictor*. For instance, in the final model (Step 4), participants are 4.7 times more likely to choose the encrypted network in S1-1 ("Encryption" and "QoS" needed) than in the S0-0 scenario, which is the reference point. But the results also reveal an unexpected behaviour: participants are, almost equally, more likely to choose the encrypted network in both S0-1 ("QoS" needed) and S1-0 ("Encryption" needed). In S1-0 ("Encryption" needed), we can interpret that the participants seek for "Encryption" (still "QoS" can interfere because of the limitations, see Table 1), but in S0-1 ("QoS" needed) only the need for "QoS" can foster the choice of the encrypted network. Furthermore, still relatively to S0-0, change in odds in S1-1 are more than double than those for S1-0 ("Encryption" needed)– this difference suggests that participants confuse "QoS" and "Encryption"; and that needing "QoS" contribute to the choice of the encrypted network. Finally, we already observed that the introduction of "Convenience" in Step 2 cancels out the effect of S0-1 ("QoS" needed),

but this inclusion has a limited effect on S1-1 and S1-0 ("Encryption" needed). This suggests that the choice of an encrypted network that is only nudged by the need of "QoS" is fragile; the same choice performed in a scenario needing "Encryption" is stronger. That is to say, even convenience-driven people tend to adopt secure behavior when the situation calls for it.

We cannot say definitively whether or not the participants' understanding of the meaning of the cues is the cause of the discrepancies we observe in Step 1's odds of choosing the secure network for S1-0 ("Encryption" needed) and S1-1. As shown in Table 6 this is an important factor, but Table 5 shows that it does not interact with the scenario and therefore it is not the cause of those discrepancies.

The *third most powerful predictor* is the "Possession of a Password": participants with a password are 2.4 times more likely to choose the encrypted network (see final step in model). But the effect interacts with the scenario: in a scenario needing "Encryption" participants tend to choose the encrypted network, ignoring whether they have a password or not; but when the scenario does not require "Encryption" it appears that they do not look for an encrypted network, unless we provide them with a password.

The ICT skills that we asked our participants about did not result in significant effects as shown in Table 6. Furthermore, we found evidence that knowing what a cue means in terms of the dimensions we asked about, has very little impact on the participant' decisions. Thus, taking "informed" decisions does not foster a secure behavior and computer literacy seems to play little role in the decision process. The last significant factor is age, but its effect ends up being nonsignificant.

5 Conclusion

This paper explains *why* people choose Wi-Fi networks, and it does so by investigating how the cues (🔒, 📶 and 📶) displayed by Wi-Fi network managers affect Wi-Fi network selection. Using a sample of 1000 participants, collected through the Amazon mechanical turk, we analyzed through a series of logistic regressions the relative importance of the various factors associated with the participant's choice of Wi-Fi network.

We shed light on whether users understand and use the padlock and the signal strength visual cues to decide which Wi-Fi network to connect to: they blankly avoid the networks displaying 📶 because they understand that it is a sign of bad connectivity, but the decision is more subtle when 📶 🔒 and 📶 are competing. The choice of a network displaying a 🔒 is subject to more influences: users who are not convenience-driven tend to pick an encrypted network if they are provided a password or if the task undertaken calls for "QoS"; when needing "Encryption", all users tend to choose encrypted networks. But our analysis shows that the meaning our participants attribute to the cues and other socio-demographic variables do not explain why our participants choose encrypted networks when the task asks for "QoS", or even "Encryption". These results

suggest that beliefs and circumstances (i.e., context) are the real motivators behind our participants' choices, and that even if they that take ill-informed decisions regarding the meaning of the cues, they take "informed" decisions with regard to other factors.

In future work, we will seek to confirm our findings reported in this manuscript relative to the other rounds of data collected in our study. We will further investigate how the expressed beliefs of our participants regarding Wi-Fi networks affect their network choices. Moreover, we will investigate more closely the socio-demographic profiles of those who we have been identified as being convenience-driven.

References

1. Ferreira, A., Huynen, J.L., Koenig, V., Lenzini, G.: Socio-technical security analysis of wireless hotspots. In: Human Aspects of Information Security, Privacy, and Trust. Volume 8533 of Lecture Notes in Computer Science. Springer (2014) 306–317
2. Jeske, D., Coventry, L., Briggs, P.: Decision justifications for wireless network selection. In: Socio-Technical Aspects in Security and Trust (STAST), 2014 Workshop on. (July 2014) 1–7
3. Grice, P.: Studies in the Way of Words. Harvard University Press (1989)
4. Rand, D.G.: The promise of Mechanical Turk: How online labor markets can help theorists run behavioral experiments. Journal of Theoretical Biology **299** (2012) 172–179
5. Paolacci, G., Chandler, J., Ipeirotis, P.: Running experiments on amazon mechanical turk. Judgment and Decision making **5**(5) (2010) 411–419
6. Crump, M.J.C., McDonnell, J.V., Gureckis, T.M.: Evaluating Amazon's Mechanical Turk as a tool for experimental behavioral research. PloS one **8**(3) (January 2013) e57410
7. We Are Dynamo turker community: Guidelines for Academic Requesters
8. Bureau, U.S., Statistics, L.: Standard Occupational Classification and Coding Structure. Health (San Francisco) (February) (2010) 1–7
9. U.S. Department of the Census: Current Population Survey interviewing manual. (June 2013)
10. Finch, J.: The Vignette Technique in Survey Research. Sociology **21**(1) (feb 1987) 105–114
11. R Development Core Team: R: A Language and Environment for Statistical Computing. R Foundation for Statistical Computing, Vienna, Austria. (2008)
12. Wilcoxon, F.: Individual comparisons by ranking methods. Biometrics bulletin **1**(6) (1945) 80–83
13. McCullagh, P.: Generalized linear models. Chapman and Hall, London New York (1989)