Socio-Technical Study On the Effect of Trust and Context when Choosing WiFi Names

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

email:{firstname.lastname}@uni.lu

[1] Educational Measurement and Applied Cognitive Science
[2] Interdisciplinary Centre for Security Reliability and Trust
Univ. of Luxembourg, Luxembourg (LU)

Abstract. We study trust and context as factors influencing how people choose wireless network names. Our approach imagines the mindset of a hypothetical attacker whose goal is to ensnare unsuspecting victims into accessing dishonest WiFi access points. For this purpose, we conducted an online survey. We used two separate forms. The first form asked a random group of participants to rate a list of wireless names according to their preferences (some real and others purposely made-up) and afterwards with implied trust in mind. The second form was designed to assess the effect of context and it asked a different set of respondents to rate the same list of wireless names in relation to four different contexts. Our results provide some evidence confirming the idea that trust and context can be exploited by an attacker by purposely, or strategically, naming WiFi access points with reference to trust or within certain contexts. We suggest, in certain cases, possible defence strategies.

1 Introduction

Even "secure" systems can turn out to be vulnerable when attackers target not the system and its security mechanisms but the people interacting with it. In such situations, security is not a purely technical property but rather a socio-technical quality stemming from factors such as people's behaviours with regard to technology and the underline cognitive and psychological factors.

Can we protect systems whose weaknesses lay in the behaviours and minds of users? Likely we can, but not without better understanding how the "user component" works. A few general behavioural and cognitive principles have been identified (see [1–7]), but socio-technical security is mostly newly evolving research.

While security experts are just starting to explore this new field, hackers already master the art. They usually know the "user component" more deeply than do average security engineers. They also have an advantage: finding one vulnerability is easier than protecting the whole system, which requires finding and fixing all vulnerabilities. However, this duality offers us an interesting perspective: we can take the intruder's viewpoint, plan and assess socio-technical attacks, then change hats and take the security engineering side, this time trying to patch the discovered vulnerabilities.

To illustrate this, we imagine the mind-set of an attacker who intends to set-up a fake WiFi access point and who speculates on the best strategy to name it to "phish" people. A good strategy could be to choose names that relate to trust and/or context.

Trust is a catalyst factor in many indirect/remote interactions as the ones daily happening over the Internet ([8,9]). By addressing this element, we are interested in understanding whether people think spontaneously of trust when choosing names or whether instead they need to be hinted before the idea of trust triggers in their mind. If trust is feeble in people's minds, an attacker could easily deviate people's trust onto something that can be controlled, but if it is strong, the attacker could still plan to gain people's trust, as it is usually done, by impersonating the object of trust (cf. Section 4).

Context, at least in this paper, is the physical or the social space where actions and decisions occur (in a laboratory, at work, at home). By addressing context we are interested in understanding whether this factor has an effect on people's choices of names. If that is true, an attacker can be more effective by contextualising his/her attack or by fooling users to be in a context favourable to him/her. However, this brings new ideas on how to contain these context-exploiting attacks, for example by securing the access to the context (cf. Section 4).

In summary, the aim of this paper is to present a study that investigates the effect that trust and context have on users when choosing wireless network names. Our study relates to decisions that do not require complex probabilities, balancing risks, or evaluating security with respect to goals: in such complex scenarios, user choices are ruled by principles of mental economics [3, 4], out-of-scope here.

1.1 Use-Case Scenario

Our hypothetical use-case scenario consists of a set of wireless network names (SSIDs), various locations, and a user. The user is expected to scan and choose an SSID from a list of names that his/her device detects to get Internet access. This can happen in four different well known locations: the university, a shopping mall (a specific one), the city centre, and a hospital (a specific one).

On the other hand, our scenario imagines an attacker whose intent is to deploy a dishonest WiFi base station. This station's name will appear in the list of available SSIDs that the user can browse from its device. The attacker seeks to maximize the number of victims, so s/he looks for alluring names that inspire security, convenience, or trustworthiness with names such as 'secured_hotspot', or takes advantage of the location to inspire legitimacy with names such as 'wifi_unilu'. Table 1 shows a comprehensive view of the 12 SSIDs used in this study, including those existing and those made up. The SSIDs have been carefully compiled: they may or may not exist in the region where the study was conducted, evoke security or freeness, or be location-specific.

Research Questions. We intend to answer two research questions about preferences in wireless network names:
(RQ1): *Does thinking about trust affect participants' preferences*?
(RQ2): *Does context affect participants' preferences*?

2 The Survey

For reasons of feasibility and ethics we opted for a survey rather than an experimental setup, the latter being the setup of a"malicious" access point airing different SSIDs. Our survey asks respondents to rate a list of SSIDs according to their preferences while excluding technical aspects such as signal strength or protected access. We also question them about their sense of trust or in relation to specific contexts. Our survey relies on an online questionnaire rather than a paper-pencil version that would have required a large logistical effort to field and to encode, while not offering the same level of convenience to the respondent. The questionnaire was structured into

Table 1. Existing/nonexistent wireless names and their grouping in relation to security and context. Security: (G1-existing; G2-nonexistent; G3-nonexistent and related to security; G4-nonexistent and not related to security). Context: (L1-existing and expected in the context; L2-existing and not expected in the context; L3-nonexistent and expected in the context; L4-nonexistent and not expected in the context).

					University				City Center				Shopping				Hospital			
	G1	G2	G3	G4	L1	L2	L3	L4	L1	L2	L3	L4	L1	L2	L3	L4	L1	L2	L3	L4
eduroam	■				■				■					■				■		
uni-visitor	■				■					■				■				■		
uni-student		■		■			■									■				■
wifi_unilu		■		■			■									■				■
hotcity	■					■			■				■				■			
Hotel_le_Place_D'Armes	■					■			■					■				■		
Cafe_de_Paris	■					■			■					■				■		
secured_hotspot		■	■	■				■				■				■				■
secure_wifi_BelleEtoile		■	■	■				■				■			■					■
free_wifi_BelleEtoile		■		■				■				■			■					■
Maroquinerie_Kirchberg		■		■				■				■				■			■	
free_AP		■		■				■				■				■				■

four parts: (1) the socio-demographics part that surveys respondents about their age, gender, education, IT skills and comfort using IT; (2) the "general preferences" part that lists 12 SSIDs the respondents are asked to rate with regard to their general preferences based on a 5 point Likert scale (1-Not at all preferred, 2-Not very preferred, 3-Neutral, 4-Preferred, 5-Most preferred), respectively; (3) the "trust" part lists the same 12 SSIDs and asks respondents to rate them with special regard to trust when connecting/avoiding them (1-Not at all trusted, 2-Not very trusted, 3-Neutral, 4-Trusted, 5-Highly trusted); (4) the "context" part consists of 4 specific and familiar locations, each of these locations listing the same 12 SSIDs, asking respondents to rate them regarding specific contexts when connecting/avoiding them (same Likert scale as for the general preferences).

The instructions provided to the respondents have been translated from English to German and French in order to accommodate the multilingual population of Luxembourg and surrounding areas. The respondents were randomly associated with one of two conditions. Condition 1 is designed to assess the effect of trust by administering the following questionnaire parts to each assigned respondent: socio-demographic $\rightarrow$ general preference $\rightarrow$ trust. Condition 2 is designed to assess the effect of context with respondents answering the following parts: socio-demographic $\rightarrow$ general preference $\rightarrow$ con-

Table 2. Sociodemographics for the population of the survey for conditions 1 and 2.

Demographics	Condition 1 (n=59)	Condition 2 (n=40)	Total (n=99)
Female	36%	58%	**45%**
Male	64%	42%	**55%**
Age (average)	27%	25%	**26%**
High School	19%	28%	**22%**
Bachelor Degree	49%	50%	**49%**
Master Degree	20%	7%	**15%**
PhD	10%	13%	**11%**
Very comfortable using IT	69%	73%	**70%**
Somewhat comfortable using IT	27%	25%	**26%**
Very good IT skills	34%	23%	**29%**
Good IT skills	37%	60%	**46%**
Average IT skills	25%	15%	**21%**

text. We recruited participants by sending an invitation via email to students and staff from the University of Luxembourg.

Data were collected within a MySql database and exported to a CSV file format. Statistical analyses were done using the R statistical analysis software [10]. The collected data were analysed using basic descriptive statistics, followed by specific analysis of variance tests (t-tests [11] and Wilcoxon rank [12] tests) in order to assess the significant differences between general preferences and the trust condition (cf. condition 1, RQ1) and between general preferences and the context condition (cf. condition 2, RQ2). In order to apply t-tests on data derived from Likert scales, we systematically verified its normal distribution and also employed the Wilcoxon signed-rank test to further support t-test results. We also included open questions (analysed manually) that allowed respondents to provide the rationale for their ratings.

3 Results

A total of 235 participants took part in our study; however our analysis focuses on the 99 completed cases (136 cases have not been fully completed and thus have not been considered for analysis). As shown in Table 2 our sample is rather balanced with regard to gender. On average our respondents are rather young (age 26), mostly highly educated (over 75% have a bachelor degree or higher), very IT literate and highly skilled (75%).

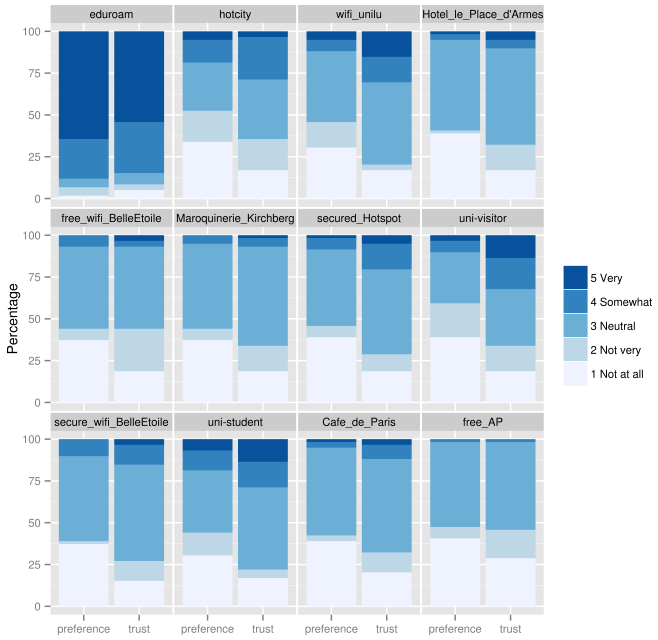

Fig. 1. General preferences vs. trust. in condition 1 for each SSID.

Next, we present the results obtained for conditions 1 and 2. Whenever possible, we proceed by first describing general tendencies as visualized through graphical representations, followed by more specific analyses whose results are presented as tables. Differences between repeated measures have systematically been computed as follows: measure 2 − measure 1. Negative differences suggest than on average measure 1 > measure 2 and positive values suggest measure 2 > measure 1. More precisely, a negative value indicates a decrease in trust/preferences and conversely a positive value suggests an increase in trust/preference. The statistical tests inform us on the significance of these differences.

3.1 Trust

Fig. 1 displays general preference and trust results side-by-side for all 12 SSIDs in condition 1. In general we find a tendency towards higher preference ratings (except for eduroam) when invoking trust. This is illustrated by a systematic change in the extremes of the Likert scores, shown in Fig. 1 (cf. RQ1), change that happens regardless

of the name's properties (existing, open, secure, etc.). A large proportion of the respondents report a neutral preference for each of the wireless network names.

Table 3. Statistical significance for the differences between: (a) general preferences and trust; (b) general preferences and trust but for groups G1-G4.

	Diff. (trust pref.)
Whole sample	$0.38^{**\sharp}$
Male	$0.32^{*\sharp}$
$\leq$ 24 years old	$0.49^{**\sharp}$
$>$ 24 years old	-
$\leq$ Bachelor Degree	$0.40^{*\sharp}$
$>$ Bachelor Degree	-
$\leq$ Good IT skills	$0.50^{**\sharp}$

(a)

	Diff. (trust pref. Gx)			
	G1	**G2**	**G3**	**G4**
Whole sample	$0.32^{***\sharp\sharp\sharp}$	0.45^{*}	0.47^{*}	0.44^{*}
Males	$0.30^{**\sharp\sharp\sharp}$	-	-	-
$\leq$ 24 years old	$0.40^{**\sharp\sharp}$	0.59^{*}	0.70^{*}	0.53^{*}
$>$ 24 years old	0.23^{*}	-	-	-
$\leq$ Bachelor Degree	$0.31^{**\sharp\sharp}$	0.49^{*}	-	0.47^{*}
$>$ Bachelor Degree	$0.34^{*\sharp\sharp}$	-	-	-
$\leq$ Good IT skills	$0.40^{**\sharp\sharp}$	0.59^{*}	0.62^{*}	0.58^{*}

(b)

Legend: For all tables superscripts have the following meaning: t-test result: $^{*}p < 0.05$; $^{**}p < 0.01$; $^{***}p < 0.001$. Wilcoxon result: $^{\sharp}p < 0.05$; $^{\sharp\sharp}p < 0.01$; $^{\sharp\sharp\sharp}p < 0.001$.

Table 3.(a) shows the significant results for the whole sample, indicating that on average the shift from general preferences to trust was towards a more discerning preference (higher positive values).

A similar pattern is shown for the other socio-demographic subgroups. We also studied more specifically what subgroups of our sample might be particularly affected by this effect. Test results indicate this is true for male participants, for those who are aged 24 years or less, for those who have successfully finished a bachelor degree or less, and for those who consider themselves not very IT literate. Conversely, this means that participants who are not part of these subgroups tend to be more cautious with their ratings in the condition of trust-awareness; our results suggest that age, general education and IT skills contribute to shaping these attitudes.

In addition to the preceding person-centric analysis, we analysed the data more closely under the perspective of wireless network names, allowing us to better understand whether the formerly described effects apply to all SSIDs or to subsets only. To this end, we grouped wireless network names with regard to our objectives of including them in our study.

Fig. 2 presents the results between general preferences and trust for the four groups G1-G4 (cf. Table 1). Table 3.(b) shows the t-test results for the difference in ratings between general preferences and trust, for each of the 4 groups.

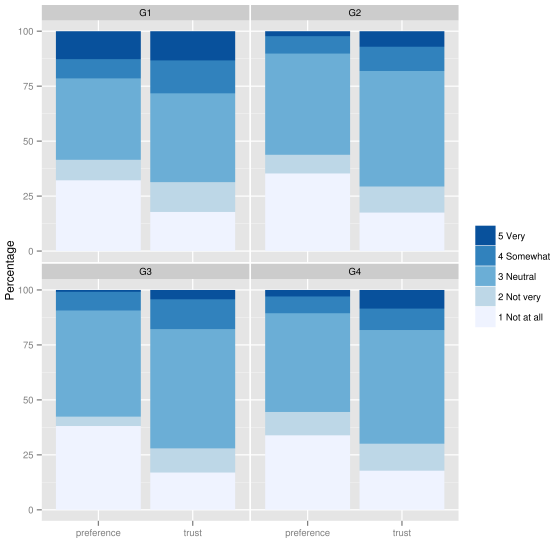

Fig. 2. General preferences vs. trust for groups G1-G4.

The results suggest a strong and systematic effect of trust for G1, for the entire sample, except those participants who describe themselves to be very IT literate. Regarding fake SSIDs (G2), there is still an effect noticeable both for the entire sample and more specifically for subgroups of lower age, lower education and lower IT literacy. This pattern is almost identical for G3 (fake names related to security) and G4 (fake names not related to security). The effects demonstrated for G2, G3 and G4 require further attention as they especially indicate potentially unsafe user behaviour. It should be noted that participants who think themselves very IT literate do not demonstrate any effect of trust awareness and it might well be that these participants are aware of trust issues already when considering SSIDs.

Table 4 shows the results of the analysis of the open questions. The two most common reasons for participants' preferences are the

Table 4. Most common reasons related to general preferences (G) and trust (T) for all choices, choices that change to nonexistent names (CPTUN), or to nonexistent names related to security (CPTSN), and that do not change from general preferences to trust.

	All choices (n =53)		**CPTUN (n =11)**		**CPTSN (n =10)**		**No change (n =18)**	
	G	T	G	T	G	T	G	T
Do not use other networks	30	6	4	–	3	–	7	2
Do not know other networks	22	26	2	1	4	1	5	1
Security	13	3	3	1	-	-	2	2
Easy Access	8	-	-	-	-	-	2	-
Trust	3	10	-	3	-	1	-	1

fact that they use the networks or they know them, not necessarily because they consider them trusted or secured.

3.2 Context

Fig. 3 displays the SSID preference ratings for only 4 of the 12 names that show some change throughout the contexts (i.e., University, City Center, Shopping Mall and Hospital) as compared to the general and non-context dependent situation, which is labeled "generic" in the figure.

Table 5 shows the significant results about the effect that context awareness has on respondent's names preference ratings.

In contrast to the findings for condition 1, significant results in the context condition indicate a decrease in preference ratings when respondents are made aware of specific contexts. This applies to the University context where the effect is demonstrated for the entire sample of respondents and, only for specific sample groups in the shopping mall and hospital context. The shopping mall indeed seems to demonstrate an effect specifically for female respondents and for

Table 5. Statistical significance for the differences between general preferences and the contexts (in this case, there is no statistical significance for the context "city center").

	Difference (Context preference-generic preference)		
	University	**Shopping Mall**	**Hospital**
Whole sample	-0.15*♯	-	-
Females	-	-0.23*♯	-0.33*♯
> 24 years old	-	-	-0.27*♯
> bachelor degree	-	-0.32*	-0.37*♯

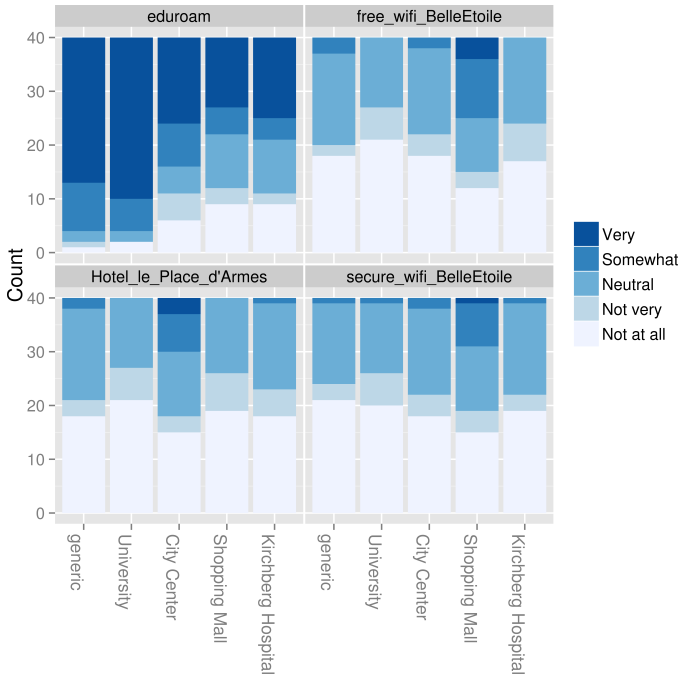

Fig. 3. Selection made for eduroam, Hotel_le_Place_d'Armes, secure_wifi_BelleEtoile and free-wifi_BelleEtoile within the four contexts by all participants of condition 2.

those who are more educated. This is also true for the hospital context, the results indicate an effect for respondents aged more than 24 years old. These effects indicate that these respondents may be more aware when choosing a name for those three contexts.

Similar to our analysis for condition 1, we completed our analysis for condition 2 by a specific name grouping, illustrated in Table 1.

Fig. 4 compares between general preferences and the four groups (L1-L4) for all the contexts. Participants rate higher the SSIDs for L1 - existing and are expected within the university and the city center while in the other two contexts (shopping mall and the hospital) participants rate higher the names for L2 - existing but are not expected in that context. The figure also shows a tendency for participants to rate higher nonexistent wireless network names but which may be expected in the context (L3) (for the university, shopping mall and hospital contexts).

Table 6 provides an overview of the effects that the University context has on user's preferences. Group L1 of "existing names and

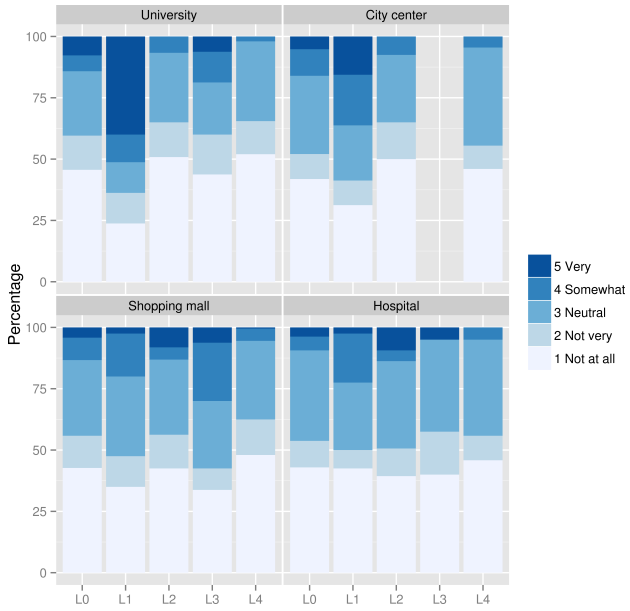

Fig. 4. General preferences in the 4 groups (L1-L4) for all the contexts.

expected in the context", are all affected by the university context in the sense that these names are rated higher, respondents thus being more cautious when context-aware. In contrast, group L2 of "existing names but not expected in the context", have been rated lower when awareness about the context was included, except for male respondents. The "nonexistent and not expected names in the context" (L4) have systematically been rated lower. Finally, the "nonexistent and expected" names (L3) show a weaker effect on the entire sample and higher effects for subgroups of respondents younger than 24 years, with less than a bachelor degree, or proficient with IT.

Table 7.(a) provides an overview of the effects that the shopping mall context has on user's preferences. This context seems to be associated with a less pronounced effect on user response patterns as there is no significant difference for groups L1 and L2. However, there is a series of effects indicating a rating increase in subgroup L3 and a general decrease in ratings for L4.

Table 7(b) provides an overview of the effects that the hospital context has on user's preferences. This context is associated with few significant effects. Results for L1 indicate positive ratings for males while the opposite for female respondents. There is also a decrease in

Table 6. Statistical significance for the differences between general preferences and the context of the University.

	Differences (L* − generic)			
	L1	**L2**	**L3**	**L4**
Whole sample	1.00$^{***\sharp\sharp\sharp}$	-0.40$^{***\sharp\sharp\sharp}$	-0.10$^{\sharp}$	-0.47$^{***\sharp\sharp\sharp}$
Males	0.86$^{***\sharp\sharp\sharp}$	-	-	-0.48$^{**\sharp\sharp\sharp}$
Females	1.10$^{***\sharp\sharp\sharp}$	-0.50$^{***\sharp\sharp\sharp}$	-	-0.46$^{***\sharp\sharp\sharp}$
$\leq$ 24 years old	0.99$^{***\sharp\sharp\sharp}$	-0.37$^{**\sharp\sharp}$	-0.22$^{\sharp}$	-0.43$^{***\sharp\sharp\sharp}$
$>$ 24 years old	1.03$^{***\sharp\sharp\sharp}$	-0.47$^{**\sharp\sharp}$	-	-0.55$^{**\sharp\sharp}$
$\leq$ Bachelor Degree	1.01$^{***\sharp\sharp\sharp}$	-0.35$^{**\sharp\sharp}$	-0.18$^{\sharp}$	-0.40$^{***\sharp\sharp\sharp}$
$>$ Bachelor Degree	0.95$^{**\sharp}$	-0.60$^{**\sharp}$	-	-0.71$^{*\sharp}$
$\leq$ Good IT skills	1.02$^{***\sharp\sharp\sharp}$	-1.41$^{***\sharp\sharp\sharp}$	-	-0.46$^{***\sharp\sharp\sharp}$
$>$ Good IT skills	0.94$^{***\sharp\sharp}$	-0.39$^{*\sharp}$	-0.22$^{***\sharp}$	-0.50$^{*\sharp}$

Table 7. Statistical significance for the differences between general preferences and the context for: (a) Shopping Mall, and (b) the Hospital.

	Differences (L* − generic)	
	L3	**L4**
Whole sample	0.29*	-0.36$^{**\sharp\sharp\sharp}$
Male	0.43$^{*\sharp}$	-0.48$^{***\sharp\sharp\sharp}$
Female		
$\leq$ 24 years old	0.43$^{**\sharp}$	-0.32$^{*\sharp}$
$>$ 24 years old	-	-0.44$^{**\sharp\sharp}$
$\leq$ Bachelor Degree	0.38$^{**\sharp}$	-0.30$^{*\sharp\sharp}$
$>$ Bachelor Degree	-	-0.56$^{**\sharp}$
$\leq$ Good IT skills	0.40$^{**\sharp}$	-0.43$^{**\sharp\sharp\sharp}$

(a)

	Differences (L* − generic)		
	L1	**L3**	**L4**
Whole sample	-	-0.19$^{\sharp}$	-0.28$^{*\sharp}$
Males	0.69*	-	-
Females	-0.49$^{**\sharp\sharp}$	-	-0.44$^{***\sharp\sharp\sharp}$
$\leq$ 24 years old	-	-	-0.22$^{\sharp}$
$>$ 24 years old	-	-	-0.40$^{**\sharp\sharp}$
$\leq$ Bachelor Degree	-	-	-0.22$^{\sharp}$
$>$ Bachelor Degree	-	-	-0.49$^{**\sharp}$
$\leq$ Good IT skills	-	-	-0.32$^{*\sharp\sharp}$

(b)

ratings for the whole respondent sample in L3. And finally, consistent with results in Table 7(a), L4 names are systematically rated lower, except for male respondents.

Table 8 shows the results for the open questions relating to context. Again, the most common reasons relate to the use and knowledge of the network names, and that they provide easy access. To note that outside the University context, the most common reason states clearly that the place where the participants are, can greatly influence their choices.

Table 8. Most common reasons for general preferences and each context.

	General pref.	University	City Centre	Shopping Mall	Hospital
Do not use other networks	34	11	7	3	2
Do not know other networks	15	8	7	-	-
Easy Access	9	7	5	2	3
Security	5	1	3	3	1
Place where I am	-	-	9	10	2

4 Security Discussion

In our scenario the attacker pondered the best strategy for naming his malicious SSID to "hook" the most people to choose it when accessing the Internet. The results of our survey show three main elements that could make our attacker more successful.

Trust. Let us look at Fig. 1. It compares the preferences before and after for the entire sample. Let us focus on the two highest ratings, "very preferred" and "somewhat preferred": when taken together they indicate a positive preference.

For all network names, with the puzzling exception of "eduroam'' (commented in the next paragraph) the preference of a network has increased after people have been asked to think about trust. This seems to indicate that an attacker can gain people's trust by suggesting trust in the name, at least if he uses names similar to the ones we use in our study. Fig. 2 shows, in fact, that the increment in preference is almost the same regardless whether the network name exists or not. We therefore conclude that an attacker would be more effective by suggesting or including the word "trust" in the network name itself. If this hypothesis were true, names that hint "trust" should rate better than those suggesting "security" or "freeness"; proving or disproving this claim is left as future work.

We comment now the small drop in trust regarding 'eduroam'. From the analysis of the open answers it emerges that people said to prefer 'eduroam' because they know the network (= have been told to use it); however they said to trust 'eduroam' only indirectly (or better comparatively), that is they do not know whether to trust the other networks. Therefore there is reason to believe that people chose 'eduroam' by habit, which is a known principle of mental economics. It would be interesting to test whether people would still use

'eduroam' (by habit) in contexts outside the University (the Shopping Mall), where this network has no reason to exist. This would be an attack to implement with little effort.

Context. The discussion about context is less straightforward. Fig. 3 shows that people prefer a network that communicates a context-specific meaning. For example, the made-up 'free_wifi_BelleEtoile' rated higher in the shopping mall context than in general (Belle Etoile is an existing shopping mall, where there is no existing SSID reminding that name). This can appear obvious, but Fig. 4, which shows the results for groups gives more useful insights. In the context "Shopping Mall" the increment is positive for all the made-up networks that refer to it (cf. Table 7.(a) first row, first column); but in context "University" this does not happen. Here, made-up names referring to the context (group $L3$, which includes 'wifi_unilu' for example) rated less on average (cf. Table 6 first row, third column)[3].

Our sample, mostly students and employees of the university, know better what network is available at the university. They do not expect networks to appear without notice. Thus, the strategy of contextualizing names has less impact at the university, at least for the possible victims who regularly frequent the university, as our population. However, it may work for guests or visitors, who may not be so aware of what access point exists.

In fact, in contexts like the shopping mall, the same strategy of contextualizing made-up names works nicely: those names outrate the existing ones. An attacker targeting public places can thus increase odds by including the context in the name of a dishonest base station. Conferences, for example, are sites where such an attack could work very well.

What could be a recommendation to prevent such kinds of attacks? One suggestion, which could be tested for efficacy, would be to advertise the names of legitimate networks, for example by deploying stickers informing visitors about the legitimate access points. (An attacker can do the same, but this requires him to work and

[3] We got a similar despite weaker result for the context "Hospital" but with a different explanation. The contextualized name 'maroquinerie_Kirchberg' is ambiguous because Kirchberg is also the name of a large zone of the city where the hospital and many other offices stand, while Maroquinerie is out-of-context.

expose himself more). Another defence consists in avoiding to leave unused names which are related to the context. For example, a hotel should re-name SSID with the hotel's name. Such simple action is usually disregarded: it is common to see WiFi with the name of the router ('linksys01') or with that of the network provider ('Numericable_6A85').

5 Conclusion and Future Work

In this paper we tested a few hypothesis about how people are biased to choose WiFi access point names when we offer them a pool of names among which there are names of real WiFi networks, names that remind security and trust and names that relate with the current location (context).

Our result shows that, in familiar contexts, adding security or freeness in the names does not bias user's preferences; however, in unfamiliar contexts the choice of even expert people is biased towards names reminding the context. These results devise sever socio-technical attacks that can be easily launched by interfering with user's knowledge of the context. To contain those attacks we have suggested a few simple socio-technical defences. Testing whether these are effective in preventing people from falling victims of attacks was not in the scope of this paper, but needs to be proved and will be done as future work.

The study carried on in this paper has some limitations. We did not have a larger and more diversified population, as we had permission to broadcast our survey only within the university. The small sample size did not allow for more complex multivariate statistical analyses and we had less participants for condition 2 of the survey, as they had to fill more information. Also, not many participants filled the open questions. In addition to the experiment we plan to do, we would like to improve our survey and include more effective ways to characterize the participants (student - area of study, not student - area of work or research) so that we can identify specific characteristics that may help us better understand their different behaviours. We think it would also be useful to analyse in more detail each wireless network name separately and verify its statistical significance. It may be that one or two names have more meaning

than others and can in themselves be used to improve or mitigate socio-technical attacks.

We would have liked to set up attacks with real WiFi access points in real places; however launching such actions and harvesting the data for the analysis requires an authorization from an ethical committee and a compliance with our legal framework, assurances that were not ready for this paper. We plan it as future work.

Acknowledgments

We thank E. François for helping with the on-line questionnaire and K. Weinerth and S. Doublet for the translations. This research is supported by FNR Luxembourg, project I2R-APS-PFN-11STAS.

References

1. B. E. and N. R. E., "The Differential Impact of Abstract vs. Concrete Information on Decisions," *J. of Applied Social Phychology*, pp. 258–271, 1977.
2. A. Tversky and D. Kahneman, "Rational Choice and The Framining of Decisions," *J. Business*, vol. 59, pp. 251–278, 1986.
3. R. Anderson and T. Moore, "Information Security Economics - and Beyond," in *DEON '08: Proceedings of the 9th international conference on Deontic Logic in Computer Science*, vol. 5076. Springer-Verlag, July, 15-18 2008, pp. 1–26.
4. A. Adams and A. Sasse, "Users Are Not the Enemy," *Comm. ACM*, vol. 42, pp. 40–46, 1999.
5. R. West, "The Psychology of Security," *Communication of the ACM*, vol. 51, no. 4, pp. 34–38, April 2008.
6. R. Dhamija, J. D. Tygar, and M. Hearst, "Why phishing works," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ser. CHI '06. New York, NY, USA: ACM, 2006, pp. 581–590.
7. J. Sunshine, S. Egelman, H. Almuhimedi, N. Atri, and L. F. Cranor, "Crying wolf: An empirical study of SSL warning effectiveness," in *Proc. of USENIX'09*, 2009.
8. D. Gambetta, "Can We Trust Trust?" in *Trust: Making and Breaking Cooperative Relatioins*, D. Gambetta, Ed. Basil Blackwell, 2000, ch. 13, pp. 213–237.
9. C. Castelfranchi and R. Falcone, *Trust Theory: A Socio-Cognitive and Computational Model*. Wiley, 2010.
10. R Development Core Team, *R: A Language and Environment for Statistical Computing*, R Foundation for Statistical Computing, Vienna, Austria, 2008, ISBN 3-900051-07-0. [Online]. Available: http://www.R-project.org
11. E. L. Lehmann, "'student' and small-sample theory," *STATISTICAL SCIENCE*, vol. 14, pp. 418–426, 1999.
12. F. Wilcoxon, "Individual comparisons by ranking methods," *Biometrics bulletin*, vol. 1, no. 6, pp. 80–83, 1945.