Decision justifications for wireless network selection

Debora Jeske, Lynne Coventry, Pam Briggs
PaCT Lab, Psychology Department
Northumbria University
Newcastle-upon-Tyne, UK
debora.jeske@northumbria.ac.uk
lynne.coventry@northumbria.ac.uk
p.briggs@northumbria.ac.uk

Abstract— **A number of security risks are associated with the selection of wireless networks. We examined wireless network choices in a study involving 104 undergraduate social science students. One research goal was to examine the extent to which features (such as padlocks) and colours could be used to 'nudge' individuals towards more secure network and away from open (unsecured) network options. Another goal was to better understand the basis for their decision-making. Using qualitative as well as quantitative data, we were able to differentiate groups whose decision were driven by security concerns, those who made convenience-based decisions, and those whose motives were unclear or undefined. These groups made different network choices, in part due to different perceived functionality of the padlock. We further observed significant effects for the use of colour when nudging participants towards more secure choices. We also wanted to examine the role of individual differences in relation to the choices individuals make. Perceived controllability of risk played a role in terms of the extent to which participants would make more secure vs. unsecure choices, although we obtained no significant group differences when we examined these variables in relation to the different decision justification groups. This indicates that perceived risk perceptions and reasons for decisions may relate differently to the actual behavioural choices individuals make, with perceptions of risk not necessarily relating to the reasons that participants consider when making security decisions.**

Keywords—user perception; security; padlock; usability

I. Introduction

The focus of our research was to examine what information people utilize when making security-related decisions. Given the prevalence and known security risks of public wireless networks [1], we decided to examine decision making in relation to the selection of public wireless networks. At present, public wireless networks pose a significant risk to data security as they provide a clear opportunity for many cyber-attacks (snooping or mac spoofing, man in the middle, see [2] or [3]). Public networks are often unsecured and unmonitored, leaving the network vulnerable to various attacks aimed at the network itself or on individuals using the network [4]. Using encryption via a password, as indicated by a padlock, can help to limit access. However, even if the network is encrypted, users are still not completely safe. Using encryption methods is helpful, but again some methods are better than others.

Reports about the insecurity of public wireless networks may decrease user confidence and results in people avoiding their use. But as more people use them, and their use does not appear to result in any negative consequence (as far as the average user can tell), the sense of risks associated with the use of the "hotspots" and the internet is reduced [5]. In other words, we may be aware of the risks associated with using mobile devices and wireless network options, but we are also becoming rather blasé about the need to mediate our behaviour and reduce known risks. Various attempts have been made to engage users to adopt more secure behaviours, for instance issuing guidelines [6] and personalized messages [7]. It is also possible for a company to set up a list of trusted networks – i.e. networks the company have evaluated and would prefer their staff to utilise. Unfortunately, these approaches are not always likely to be followed through in practice.

Another approach is to help the users make the best security decisions they can by making it easier for them to locate and identify the most secure option amongst those presented to them at any one time. Given the prolific use and associated risks of public wireless networks, we wished to examine whether the design of the interface used to present network options can influence the choices made. That is, we wanted to see if we can 'nudge' novice users to select more secure network options by changing the choice architecture of options presented [8]. Past evidence suggests that *forcing* users to adopt higher security can result in a high false alarm rate. It may also lead to lower compliance and reduce their willingness to follow subsequent advice provided by the system [9]. If users retain the ability to choose security levels – with choice architecture – they can then find their own balance between usability and security. They are more likely to trust the system, comply with suggested behaviours and find the associated effort acceptable [9]. There are important implications here for designing choice architecture for wireless network selection, including allowing the user to decide on the security versus productivity balance for their particular context.

However, it is unclear which designs are most effective. As a result, we also wanted to examine the effect of alternative nudge designs when attempting to influence users towards making more 'secure' and 'trusted' network decisions as opposed to 'open' network choices. The presence of different security labels for different networks was also of interest as a nudging mechanism, such as the use of labels such as 'secure' to show that a network is using a password to encrypt the data transmitted. The presence of a padlock is indicative of a secure

This research is supported by EPSRC Grant EP/K006568 Choice Architecture for Information Security, part of the GCHQ/EPSRC Research Institute in Science of Cyber Security, London, United Kingdom.

network and can therefore be important in influencing the choice of networks. Past research suggests that designers can improve the perceived trustworthiness of web browsers by adding padlocks into the address bar [10]. Mozilla provides a Site Identity Button which allows users to assess whether or not the visited websites are encrypted, if it is verified, and by whom [11], a feature that is similar to other site advisors frequently offered by various virus scanning software programmes. Padlocks are also included as a feature elsewhere, including transactions, wireless network options, and software [12]. We explored these issues by manipulating the presence and absence of padlocks and by logging choices but also by examining the *decision justifications* users made for particular network selection.

II. NETWORK CHOICE AND PADLOCKS

A. *Research questions*

Using information about the reasons for specific network choices may improve our understanding how users justify their decisions and what types of information they tend to consider. In addition, knowing more about user differences may help us gain another perspective on user behaviour.

The research questions we hoped to answer were as follows:

(1) Do padlocks act as a barrier or facilitator of secure network use?

(2) Can menu order and colour (that is, the presentation of network options) act as nudges to influence network choice?

(3) How do individual differences such as technical self-efficacy, perceived controllability and vulnerability to risk influence security decisions?

(4) Do individual differences such as technical self-efficacy, perceived controllability and vulnerability predict the security of the networks participants will select?

Essentially, we wanted to conduct an investigation of the efficacy of different nudges on wireless network security decisions, taking into account a range of individual differences and user perceptions in relation to risk and rationale. Our exploratory stance considers the user as a rational (if not a secure) decision-maker. In this instance, we are therefore taking a user-centric perspective.

The answers to the research questions will provide some preliminary evidence to support educational awareness campaigns on university campuses or other public spaces where public wireless networks are frequently available and utilized by the general public.

B. *Study materials*

We developed a series of 6 screen shots to explore our research questions. The screenshots were based on the Android default display.

TABLE 1. FEATURES OF THE DIFFERENT SCREENSHOTS

	Screenshot characteristics
(1)	random, white, padlock present (android default)
(2)	ordered, white, padlock present
(3)	random, coloured, padlock present
(4)	ordered, coloured, padlock present
(5)	random, white*, no padlock
(6)	ordered, coloured*, no padlock

The six different screenshots each presented six network options, four of which were secure network choices (labelled 'secure' or 'trusted') and two of which were labelled 'open' and excluded padlocks (unsecure options).

We used randomly generated network names to avoid biasing the results due to perceived familiarity with the network (see work on this by [13].)

The different screen shots varied in terms of presentation of networks. Three design features were manipulated. Firstly the order of the networks was manipulated: networks were presented in alphabetical ordering (with an open network appearing in the first position) or ordered in terms of security of networks (listing first 'trusted', then 'secure' and lastly 'open' network options). Secondly, colour was used. Some screenshots listed all available networks in white (no colour coding). Others used a colour coding scheme (using a traffic light system with trusted being green, secure being orange and open being the red). And third, networks were presented with or without a padlock symbol being present. The signal strength indicator was also present on the screen. Screen 1 represents the original android display. An overview is presented in Table 1.

We were also interested in the influence of individual differences such as technological self-efficacy, perceived controllability of risk and perceived vulnerability to risk, and IT proficiency. We used a number of self-report measures; self-efficacy [14]; perceived controllability [15]; perceived vulnerability [14] and IT proficiency. In addition, we collected general information about participant's age, gender, use of computers in home and work.

C. *Procedure and participants*

Our preliminary evaluation was conducted with 104 university students. We recruited non-computing students that were familiar with using wireless networks on campus at Northumbria University. All participants could earn research credits for their respective programs.

Participants were given the following scenario (see [4]): They have an hour to submit some urgent work and decide to go to a public café to connect to the Internet. In this context, they are presented with a screen of networks available. Screenshot images were randomly presented to reduce order effects. Participants were then asked to indicate their first choice from the available networks on the six screen shots and to explain the reasons for their choice. These explanations suggested that trusted implied secure for almost all participants.

Participants who were colour-blind were excluded from the study as the displays included red and green colour coding that might have been less compelling to these participants. Part-way through the study, we added a sixth screen shot was to the set of displays (listed as option (5) in Table 1). This meant that we had a more limited dataset for performance on the task that included this screenshot (38 participants out of 104 participants tested overall).

In order to examine which variables were relevant to their network choices, all participants were asked – after making their selection - to select those features they felt had most influenced their choice (i.e. name of the network, signal strength, padlock, colour, or position on screen). In addition, we presented all participants with an option to add their own comments.

Following the completion of the choice task, we asked our participants to complete a follow-up questionnaire that included all the individual difference measures (technical self-efficacy, perceived controllability of risk and perceived vulnerability to risk, IT proficiency) and demographic characteristics (age, gender) as well as generic use of computers at home and at work.

D. Data preparation and participant characteristics

Upon completion of the survey, we examined the open responses as well as features that the participants selected when explaining their choice of networks. Three categories of explanations were identified and the most frequently occurring explanation (mode) was used to categorize participants into groups based on their tendency to subscribe to any of these four explanations across all screens. We use the label *decision justification* to describe this new grouping measure.

In the first group, participants selected their networks because they considered them to be ‘safe’ or ‘secure’. Several individuals also picked up on the fact they were ‘trusted’ which included the secure networks labelled green. The padlock represented security to this group. These two groups were combined in one category called *security-driven* (n=29).

The second category included all those participants who explained their choice of network in terms of this network being ‘accessible’ or ‘unlocked’ (n=21). This means this group included all participants who associated the padlock with restricted access. Participants in this group appeared to make more *convenience-based* decisions. In the open response options, these participants would write brief explanations such as “no password needed,” “not locked,” or “open, easy access.”

The third group included all those participants who had given various different reasons or none at all. We therefore labelled these the *unknown* group. We considered this group in our analysis in order to examine what network choices this group of participants made compared to those who explained the reasons for their choices more clearly (the first two categories).

TABLE 2. NETWORK CHOICE AND DECISION JUSTIFICATIONS

Reasons for network choice [a.]	**Security driven** (n=29)	**Convenience driven** (n=21)	**Unknown** (n=54)
Signal strength	96.55%	100.00%	98.15%
Padlock	93.10%	76.19%	79.63%
Colour	51.72%	28.57%	25.93%
Order	13.79%	28.57%	37.04%
Network name	13.79%	4.76%	16.67%

[a.] We utilized the information from five screenshots (n=104) as we did not have sufficient data for the sixth screenshots. Colour was featured in three screenshots only. All results represent percentage of individuals within each selecting these reasons.

When we examined the reasons for participants’ choices, we noted that signal strength followed by the padlock were the two option selected most frequently (Table 2). As we had randomly generated non-meaningful network names, the network name was selected least often and did not seem to affect choice (but even then we had a handful of candidates believing that they recognised the network names). Signal strength seemed to be an important factor in decision-making, however, our data does not allow us to discriminate if signal strength is more influential than the other features. Note, however, that in our study, each level of security had two signal strengths available (2 or 4 bars indicating low or high signal strength respectively).

An overview of decision justification in relation to the network choices made by participant is presented in Table 3. As can be seen when comparing the columns for *security-driven*, *convenience-based* and the *unknown* decision groups, they show different tendencies to select secure and trusted vs. open (and unsecure) network options. When comparing the *security-driven* vs. *convenience-based* group, we see a greater tendency for the security-driven group to select secure and trusted networks across the first five options (the sixth screen shot produced identical results).

TABLE 3. DECISION JUSTIFICATIONS FOR THEIR NETWORK CHOICES

	Decision justifications					
	security-driven		***convenience-based***		***unknown***	
Network presentation [a.]	*secure/ trusted*	*open*	*secure/ trusted*	*open*	*secure/ trusted*	*open*
(1) Random, white	15 (51.7%)	14 (48.3%)	0 (0.0%)	21 (100%)	13 (21.1%)	41 (75.9%)
(2) Ordered, white	18 (62.1%)	11 (37.9%)	0 (0.0%)	21 (100%)	17 (31.5%)	37 (68.5%)
(3) Random, coloured	27 (93.1%)	2 (6.9%)	3 (14.3%)	18 (85.7%)	28 (51.9%)	26 (48.1%)
(4) Ordered, coloured	28 (96.6%)	1 (3.4%)	5 (23.8%)	16 (76.2)	32 (59.3%)	22 (40.7%)
(5) Random, white*	4 (100%)	0 (0.0%)	4 (80.0%)	1 (20.0%)	25 (86.2%)	4 (13.8%)
(6) Ordered, coloured*	29 (100%)	0 (0.0%)	21 (100%)	0 (0.0%)	53 (98.1%)	1 (1.9%)

[a.] N=104 except for option (5) (here n=38). Percentage represents percent of individuals who within that category (decision justification) a specific type of network

To prepare further analyses, we also computed reliability and created composites for all additional scales (except for IT proficiency). All scales performed adequately (self-efficacy α=.86; perceived vulnerability α=.83; perceived controllability r=.355, p<.001). We also computed a score for the number of open networks selected (sum of all choices across all five screen shots presented to all 104 participants). We did the same for the number of secure networks selected (sum of all choices across all five screen shots presented to all 104 participants). Both scores had a range of 0 to 5.

IT proficiency varied as expected, with participants believing themselves to be predominantly in the intermediate category (n=71), rather than novices (n=21) or professionals (n=8) and 4 missing variables.

III. RESULTS

We present the results of each analysis in a separate section below.

A. Network selection and decision justifications

To answer our first research question (1), we wanted to know whether or not security decisions when selecting the preferred wireless networks were influenced by the extent to which individuals' decision-making was driven by security concerns or convenience-based. To examine this, we used the new categorical variable we introduced in the previous section (decision justifications). The dependent variables captured the overall number of open and secure wireless network options that participants selected (the composites).

We examined group differences using analysis of variance, also controlling for a variety of covariates, such as age, gender, IT proficiency and use of computers at home and at work (n=98, 6 missing values). The results were significant for the selection of open wireless networks across the five screenshots (*F*(2,91)=22.08, *p*<.001; partial η^2=.327). All groups differed significantly from one another in terms of the degree to which they selected open wireless networks (post-hoc analysis, all *p*≤.003). The results indicate that those individuals in the *convenience-based group* who based their decision on the extent to which a network was available or 'unlocked' (open, absence of padlock) would be more likely to select the open and unsecure wireless option (3.60 on average in terms of frequency on a scale ranging from 0 to 5). Those who made their decisions based on the network being considered 'secure' – *the security-driven group* - would select the lowest number of open networks (1.00 on average). As to be expected, the category including all participants from whom we had little information had an average (2.34) – those whose reasons were *unknown* or unclear – had an average located between the two aforementioned categories (Table 4).

The results were also significant for the selection of secure (and trusted) networks across the five screenshots (*F*(2,91)=18.856, *p*<.001; partial η^2=.293). All groups differed significantly from one another in terms of the degree to which they selected secure wireless networks (post-hoc analysis, all *p*≤.006; Table 5).

TABLE 4. SELECTION OF OPEN NETWORKS.

Network access (open)	**M**	**SD**	**n**
Security-driven	1.00	1.05	28
Unknown	2.34	1.62	50
Convenience-based	3.60	0.75	20

TABLE 5. SELECTION OF SECURE NETWORKS

Network access (secure/trusted)	**M**	**SD**	**n**
Security-driven	3.03	0.96	28
Unknown	2.06	1.22	50
Convenience-based	1.15	0.37	20

These results provide support for the suggestion that the basis on which our participants made decisions had a significant effect on the type of networks they selected.

What this does not answer, of course, is how much effort the convenience-based group would go to get a password rather than just use an open but unsecure wireless work option.

B. Additional verification of results on padlock perception

To understand the influence of having a readily available password, we reran our experiment with a second small group of 34 participants. This time we told our participants that they also had the password to access any of the networks on the list on each screen shot. These participants in this second follow-up study tended to be slightly older (range 14-67, MN=32.39, SD=11.42). Unfortunately, in terms of decision justifications, this new group tended to be of a similar mind (security-based justifications were important to 30 out of 34 participants). This meant we did not have the appropriate group sizes to run additional statistics. Descriptive statistics indicated that the results were in line with those obtained for the previous sample (those who emphasized security tended to select significantly more secure and trusted options and fewer open networks options; *p*<.05).

Similar to the previous section, we wanted to examine if providing a password had a significant influence on the decision of our participants overall. We combined the two datasets and analysed whether or not the selection of options between the two groups (those without a password, n=104, compared to those with a password, n=34) would be significantly different from one another. We also controlled for age, gender, and decision justifications. As expected, the group that did not have the password (MN=2.21, SD=1.61, n=98) selected open networks significantly more often than the group who had access (MN=.32, SD=.91, n=34) to all networks (*F*(1,127)=26.530, *p*<.001).

In other words, the group that did not have the password (MN=2.15, SD=1.21, n=98) also selected significantly fewer secure or trusted networks than the group who had access (MN=3.73, SD=.79, n=34) to all networks (*F*(1,127) =29.940, *p*<.001). This provides support for the idea that having password access will enable and encourage users to select more secure options.

C. *Network presentation and decision justifications*

We also wanted to find out to what extent does the presentation of network options (in terms of order and colour) influence individuals' selection. In order to answer research question (2), we first looked at the percentages representing the frequencies with which individuals selected open vs. secure choices. Table 6 show what type of network options were selected (in percentage, across all participants).

TABLE 6. CHOICES ACROSS ALL SIX SCREENS

	Networks selected	
Network presentation [a.]	*open/unsecure*	*secure/trusted*
(1) Random, white	73.1%	26.9%
(2) Ordered, white	66.3%	33.7%
(3) Random, colour	44.2%	55.8%
(4) Ordered, coloured	37.5%	62.5%
(5) Random, white*	13.2%	86.8%
(6) Ordered, coloured*	1.0%	99.0%

[a.] *No padlock. N=104 for options (1) to (4) and (6). N=38 for option (5).

This table is a simplification of Table 3. The descriptive statistics indicate that nudging by design (colour and menu order) works. This can be seen in terms of the increasing trend towards secure network selection when examining selection for options (1) to (4).

When we look at options (5) and (6), the two screen shots without padlocks, we can observe a significant shift towards more secure network selection. This means the absence of padlocks has an impact on participant choices, shifting more participants over to secure network selection.

Again, the choice design of networks makes a significant difference. We assessed selection of networks for the last two options without padlock using chi-square (p=.001). When available public network options are listed based on security order and colour (option 6), participants were more likely to select secure networks than when the networks were not ordered or coloured (option 5)[1].

The next step involved an examination of the relationship between the padlock and the tendencies of participants to select open or secure/trusted networks using likelihood ratio (χ^2). We utilized all screenshots that featured a padlock (options (1) to (4). We excluded the last two screenshots as the explanation of being 'locked' out from a network could not be assessed in the absence of a padlock.

The results for all four options indicated a significant effect of the decision justifications selected by our participants (security-driven, convenience-based, und unknown). For option (1) presenting networks randomly and in white, the *convenience-driven* group was observed to select a significantly a higher number of open networks than would have been expected (χ^2(2)=21.38, p<.001; ratio observed to expected = 21/15.3). The same applied for option (2) where networks were ordered based on security but still in white (χ^2(2)=27.08, p<.001; ratio observed to expected = 21/13.9). Option (3) presented options randomly, but now colouring the trusted networks in green, secure networks in yellow, and open in red. Unfortunately, the issue of greater selection of open networks continued to be a problem, although the frequency vs. expected count changed slightly (χ^2(2)=36.22, p<.001; ratio observed to expected = 18/9.3). Option (4) presented networks reordered based their security status (secure first) and in colour. While the observed frequency further declined, it was still significantly higher than would have been expected for the category encompassing participants who had made *convenience-based* decision justifications (χ^2(2)=32.85, p<.001; ratio observed to expected = 16/7.9).

These ratios provide further support for the evidence observed in the previous section: the likelihood of people selecting an open (unsecure) network was significantly higher when they prioritised finding an unlocked network over finding a secure network, that is, they make *convenience-based* decisions. People who focused on making *security-driven* decision were significantly more likely to select secure options. Moreover, while ordering of networks and colour labels seem to have a positive effect of moving individuals to more secure choices, the evidence clearly suggests that it is more difficult to influence the decisions of those whose decision is biased towards the convenience of finding an unlocked network.

D. *Decision justifications in relation to other variables*

We were also interested to learn about the extent to which the decision justifications (for N=104) were associated with individual differences (3), particularly in terms of technical self-efficacy, perceived controllability and vulnerability to risk. We utilized ANCOVA again, controlling for the same covariates as before.

Decision justifications were not associated with different levels of technical self-efficacy (F(2,91)=.254, p=ns). It is possible that since self-efficacy measures perceived capability rather than knowledge, that decision justifications would not be associated with different levels of self-efficacy. We also obtained no support for the suggestion that the different type of decision justifications were associated with different levels of perceived controllability of risk (F(2,91)=.240, p=ns).

We did obtain a marginally significant group difference in relation to perceived vulnerability (F(2,92)=2.899, p=.060, partial η^2=.061). However, this difference reflected differences in means for those whose reasons were *unknown* (MN=2.91, SD=.75) and the other two categories representing participants who made *security-driven* (MN=3.17, SD=.77) vs. *convenience-based* network decisions (MN=3.20, SD=.70). The last two groups had very similar levels of perceived vulnerability.

As a result, we found no evidence indicating that the *security-based* or *convenience-based* decision-makers were significantly influenced by their technical self-efficacy, the self-reported perceived controllability or vulnerability to risk.

E. *Network selection in relation to other variables*

Next we examined the extent to which the aforementioned individual differences (technical self-efficacy, perceived

[1] We do need to acknowledge, however, that one cell size was smaller than 5 (recommended for chi-square).

controllability and vulnerability) predict which networks participants will select. This research question (4) required regression to examine the extent to which the selection of open networks (on five screenshots, excluding option (5) due to missing values, n=104) could be predicted by individual's self-efficacy and perceptions. We included the same covariates as in the previous analyses in the first step of the analysis.

The results suggest a marginally significant prediction of open network choice in relation to perceived controllability of risk (*b*=.415, *β*=.191, *t*=1.88, *p*=.067). Open network choice was positively predicted by perceived controllability of risk, controlling for age, gender, use of computers in home and work, and IT proficiency. No other significant results were obtained in relation to technical self-efficacy or perceived vulnerability the open network score.

Secure network choice was negatively predicted by perceived controllability of risk, controlling for age, gender, use of computers in home and work, and IT proficiency (*b*=-.358, *β*=-.218, *t*=-2.14, *p*=.035). In other words: Even when we take various participant demographics and experience with and access to computers into account, participants made more unsecure decisions if they felt that they were better able to control risk (controllability). Participants made more secure decisions (less likely to select open networks) when they were more cautious regarding the perceived controllability of risk.

Despite these findings, we observed no significant differences regarding controllability of risk in relation to the explanations given by participants (e.g., security-based, convenience-based or mixed explanations). This suggests that the reasons for selecting networks were not associated with different levels of perceived controllability of risk (in terms of security threats). Participants in the group making security-based choices did not report lower or higher perceived controllability of risk compared to other groups.

IV. Conclusions

Several conclusions can be drawn from these results. First, we could see a clear relationship between the stated rationale for making a decision and the type of wireless networks selected. In other words, our participants based their network selection on specific pieces of information. There is a clear trend indicating that security decisions were influenced by participant perceptions and beliefs. Group comparison showed that participants who tended to make *convenience-based* decisions also tended to make significantly more insecure decisions (that is, they would select a greater number of open and a smaller number of secure networks from the screenshots). This suggests that all those who tend to select networks out of convenience make the poorest security decisions initially and are harder to nudge. These results continued to be significant even after considering the various participant characteristics that might influence user decision-making (IT proficiency, age and gender).

Second, it appears that when we add colour-coded security levels to our networks decision making improves. At the same time, the absence or presence of the padlock appears to be an important consideration for decision-making – according to the decision justifications recorded by our participants. While some participant groups are amenable to nudging, those who seem to perceive padlocks as restricting access (*convenience-based* category) continue to make significantly worse decisions regardless of how the networks are presented (with only slight improvements to security performance when we include colour labels). One possibility is that for these participants, the padlock presents a barrier when they are left uncertain about whether or not they have access (via a password) to the network.

Third, we obtained no evidence participants in the three groups (based on decision justifications) expressed significantly different levels of perceived vulnerability and perceived controllability of risk. This suggests that either their decisions did not align with different risk perceptions or that they lacked awareness of their vulnerability to risks.

V. Limitations

We would be amiss to not point out a number of small limitations to the study.

First, we did not provide all participants with the passwords. We did so intentionally to analyse the influence of such uncertainty. At the same time, we gave them a very specific scenario which had them focused on getting the job done (submitting an assignment within one hour). This may have implied an urgency that fostered a greater productivity than security focus when our participants made their choices.

However, this is a productivity scenario, familiar to people who work away from the office. We did not have an alternative scenario where time pressure was not implied. It is therefore possible that when our participants had the passwords to access any of the presented networks and no time pressure, they would have made better choices.

One related caveat in our research regards the fact that we did not consider the potential role of other security measures that our participants might normally use to secure wireless information traffic (e.g., VPN or encryption devices). When employing these additional measures, the user may not necessarily evaluate open networks as a security risk. Future research should therefore consider potential other variables that could shape user decisions.

It is our belief that most individuals using public wireless networks will face comparable amount of uncertainty about the situation and networks, thus giving some external validity to our scenario. In addition, time pressure is a frequent determinant of satisficing behaviour, i.e. simply selecting the most reasonable option given the constraints. Research by [16] has already shown that usability and convenience are often predominant concerns, unless there is a much stronger perceived threat which might then increase their willingness to go to extra lengths (such as obtaining a password for a secure network).

VI. Implications

Our results suggest that the padlock appears to function as both barrier and facilitator in wireless network selection, depending on whether or not their selection is *security-driven* vs. *convenience-based*. Previous research has suggested that when we increase security measures that participants may then perceive the increased effort required to adhere to these measures as a barrier [17]. We believe that this also applies to some of our participants whose decision-making was more convenience-based.

In addition, the presentation of a padlock also has another meaning. It designates a wireless network as secure. This is only partially accurate. Passwords are meant to prevent the unauthorized use of wireless connections. However, at the same time that does not mean these connections are more secure as evidenced in the emergence of rogue hotspots [18]. This means while it is reassuring that the security of a wireless network is something a number of participants consider in their choices, their perception of padlock-designated wireless networks as more secure is nevertheless a concern as this belief may then be more readily exploited by malicious users of the network.

This then suggests two threats. The presence of the padlock may actually 'nudge' legitimate users towards insecure behaviour if they interpret the presence of a padlock as a barrier which requires extra effort to overcome. Furthermore, if the rogue network also presents the user with a stronger signal, they will appear even more attractive to a user.

The ubiquitous use of padlocks may be misleading as they do not necessarily represent reliable security is indeed present. At the same time, it is easy to manipulate user perceptions using such symbols. The current overuse of padlocks may explain why our participants adopted different decision justifications – many of which may not just be the results of encountering different issues when using such sites, resulting in user uncertainty about the reliability of such symbols and their meaning. Examining how users relate to and interpret such symbols in relation to network choices represents an important contribution to understanding user decision-making and the influence of user uncertainty on behaviour.

Acknowledgment

We would like to acknowledge and thank James Turland and other colleagues from Computing Science at Newcastle University for their support and contributions. James developed the application for Android phones and played an important role in helping us identify issues and solutions.

References

[1] Simmons, D. Free wiifi hotspots pose data risk, Europol warns. BBC News, 7 March. Available from http://www.bbc.co.uk/news/technology-26469598 (2014).

[2] Callegati, F., Cerroni, W., Ramilli, M. Man-in-the-middle attack to the HTTPS protocol. Security & Privacy, Jan/Feb, 78-81. IEEE. (2009).

[3] Gelenbe, E., Gorbil, G., Tzovaras, D., Liebergeld, S., Garcia, D., Baltatu, M., & Lyberopoulos, G. Security for smart mobile networks: The NEMESYS approach. *CoRR*, abs/1307.0687. (2013).

[4] Williams, P. Cappuccino, muffin, Wifi – but what about the security? Network Security, October, 13-17. (2006).

[5] Ferreira, A., Huynen, J.-L., Koenig, V., Lenzini, G. Socio-technical security analysis of wireless hotspots. Lecture notes, 22-27 June, HCI International, Heraklion, Greece. (2014).

[6] Clonts, M. Security methodologies for wireless networks. Available at: cs.uccs.edu/~cs591/studentproj/projF2010/mclonts/doc/report.pdf (2010).

[7] Davinson, N., & Sillence, E. It won't happen to me: Promoting secure behaviour among internet users. Computers in Human Behavior, 26, 1739-1747. (2010).

[8] Thaler, R.H., & Sunstein, C.R. Nudge. Improving Decisions About Health, Wealth and Happiness. Penguin. (2008).

[9] Merkel, C., & Wiczorek, R. In D. de Waard, K. Brookhuis, F. Dehais, C. Weikert, S. Röttger, D. Manzey, S. Biede, F. Reuzeau, and P. Terrier (Eds.) Human Factors: a view from an integrative perspective. Proceedings HFES Europe Chapter Conference Toulouse. Available from http://hfes-europe.org (2012).

[10] Hoffmann, H., & Söllner, M. Incorporating behavioral trust theory into system development for ubiquitous applications. Personal and Ubiquitous Computing, 18, 117-128. (2014).

[11] Mozilla. How do I tell if my connection to a website is secure? Retrieved March 18. Available from https://support.mozilla.org/en-US/kb/how-do-i-tell-if-my-connection-is-secure (2014).

[12] SSL. Q10068 - FAQ: How can I tell if a web page is secure? Accessed March 18, 2014. Available from http://info.ssl.com/article.aspx?id=10068 (2013).

[13] Ferreira, A., Huynen, J.-L., Koenig, V., Lenzini, G., & Rivas, S. Socio-technical study on the effect of trust and context when choosing wifi names. Security and Trust Management - Lecture Notes in Computer Science, Vol. 8203, 131-143. (2013).

[14] Ifinedo, P. Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. Computers & Security, 31, 83-95. (2012).

[15] Al-Omari, A., El-Gayar, O., & Deokar, A. Security policy compliance: User acceptance perspective. 45th Hawaii International Conference on System Sciences, 3317-326. (2012).

[16] Weir, C.S., Douglas, G., Carruthers, M., & Jack, M. User Perceptions of Security, Convenience and Usability for ebanking Authentication Tokens. (2009).

[17] Dourish, P., Grinter, R.E., Delgado de la Flor, J.,& Joseph, M. Security in the wild: user strategies for managing security as an everyday, practicalproblem. Personal and Ubiquitous Computing, 8,391–401. (2004).

[18] Cracknell, P. Why 'phish' when you can trawl? Information Security Technical Report 10, 236-239. (2005).