How Can Personality Influence Perception on Security of Context-Aware Applications?

Nelly Condori-Fernandez[1,2(✉)], Franci Suni-Lopez[3], Denisse Muñante[4], and Maya Daneva[5]

[1] Universidade da Coruña, A Coruña, Spain
n.condori-fernandez@vu.nl, n.condori.fernandez@udc.es
[2] Vrije Universiteit Amsterdam, Amsterdam, The Netherlands
[3] Universidad Nacional de San Agustín, Arequipa, Peru
fsunilo@unsa.edu.pe
[4] SAMOVAR, Télécom SudParis, Institut Polytechnique de Paris, Paris, France
munante@telecom-sudparis.eu
[5] University of Twente, Enschede, The Netherlands
m.daneva@utwente.nl

Abstract. [**Context and Motivation**] Our lives are being transformed by context-aware software applications with important social, environmental, and economic implications. [**Question/Problem**] Experts recognized that quality attributes, e.g. security, are the cornerstone to get healthy social implications of these applications. However, do end-users (service consumers) perceive these attributes as so important? [**Methodology**] To answer this question, we designed a survey, to understand how end-users perceive security of context-aware software applications and how the users' personality traits might influence their perceptions. To this end, we did a web-based survey that embeds two animated-demonstration videos in order to present i) the functionality of a context-aware mobile app, and ii) some vulnerabilities of the mobile app. It involved 48 subjects divided in two groups: subjects with software engineering (SE) background (Group A) and subjects without any SE background (Group B). [**Results**] Our study found that the importance of *confidentiality* and *integrity* is more clearly perceived by subjects with SE backgrounds (Group A). *Accountability* is more difficult to be perceived by subjects. And this difficulty can be even more pronounced for subjects without any SE background (Group B). Our findings suggest that importance preferences on security are influenced by personality types. For instance, open-minded people have a higher propensity to perceive the importance of *confidentiality* and *integrity*. Whilst, people with a high level of agreeableness hold quite different perceptions regarding the importance of *authenticity* and *accountability*. Analyzing the level of association between personality and the perceived importance on security, we found that the importance perceptions on *confidentiality* are influenced by the personality of subjects from Group B. And, the changes (positive an negative) in the importance perception on confidentiality are very strongly influenced by personality, even more so by the personality of subjects from Group B.

T. Groß and L. Viganò (Eds.): STAST 2020, LNCS 12812, pp. 3–22, 2021.
https://doi.org/10.1007/978-3-030-79318-0_1

Keywords: Security · Users perception · Personality test · Survey · Context aware applications

1 Introduction

Context-aware software applications are transforming our daily lives with important social, environmental, and economic implications, for example, in domains such as transportation, health-care, telecommunication and banking. It is expected that in the near future software-intensive systems will behave autonomously thanks to the continuous sensing and monitoring.

Given the complexity of this kind of systems, and the social implications behind emerging wearable sensing technologies, Condori-Fernandez and Lago [10] investigated how quality attributes can contribute to the social, technical, economic and environmental sustainability dimensions from a developer perspective. These authors found that experts recognized that security quality attributes are the cornerstone to get healthy social implications of software-intensive systems. Even though the efforts made in conceiving secured software millions of dollars in losses are still the result of attacks on systems harming directly service consumers. Many security breaches occur in software due to errors in analysis, design and implementation [3,4]. Hence, security in software engineering (SE) is a critical issue that is clearly gaining more emphasis in the recent years [17,20]. However, to incorporate security in the software development is especially challenging because software designers/architects must consider not only security software mechanisms but also interactions among people, organizations, hardware, and other software systems, as it is described by Dalpiaz *et al.* in [13]. Despite the efforts made by the security engineers to consider both social and technical aspects, there is still a gap to be filled: we still understand relatively little about the end-user's behavior in adopting security, even more when software applications are used massively. Specifically, there is no published research on the possible relationships between personal attributes traceable to personality traits, and the ways in which end-users act and react when facing security issues in context-aware applications.

To address this gap of knowledge, it is necessary to investigate security from an end-user perspective, *i.e.,* how end-users perceive the importance on security of context-aware software applications. So, the present research makes a step in this direction. We start from the hypothesis that end-users perceive the importance of software functionalities in different ways due to their different profiles (e.g. educational backgrounds, ages, genders, personality traits) [9,21]. Furthermore, although there is a substantial evidence in the literature about factors such as personality traits that influence end-users perceptions on technology acceptance (e.g. [24,27]), there is not yet enough empirical research on how personality and certain contextual factors (e.g. educational background) of end-users can influence the perceived importance of security implementation (*i.e.,* security policies and security software technology) for context-aware software applications. Moreover, regarding to security, it becomes more challenging to be studied because, as West indicated [29], security is hard to be appreciated by end-users due to: *end-users do*

not think they are at risk, *safety is an abstract concept*, *security is considered as a secondary task* and *losses perceived disproportionately to gains*.

In this paper, we aim to investigate this phenomenon trough a survey questionnaire, by focusing on four specific quality attributes related to security such as confidentiality, authenticity, accountability and integrity. To this end, we did a web-based survey that embeds two animated-demonstration videos. Two experiments were conducted with SE experts who were attendees of REFSQ [11] and students from the Education department of the Universidad Nacional de San Agustin (Peru). In total, our study involved 48 subjects. Our study found that the importance of some security attributes (i.e. accountability) was more difficult to be perceived by end-users than others. And this difficulty was even more pronounced for end-users without any SE background, which is reflected in the variability of their answers (perceptions). Also our findings suggest that importance preferences on security are influenced by personality types and educational background. However our empirical results cannot be conclusive, therefore we call for more studies on this topic.

From a methodological perspective, our study highlights the importance of i) taking into account of personality tests for complementing the characterization of end-users and, in turn, get a better understanding on user perceptions about security, and ii) employing animated-demonstration videos as a medium to help in the importance recognition of security. Although the idea of using positive and negative scenarios in the user reactions assessment of interactive products was already considered in previous studies (i.e., [6,23]), as far we know, the use of these artifacts in the context of security is novel.

The remainder of this paper is organized as follows. Section 2 introduces our study design. Sections 3 and 4 present our results and threats to validity, respectively. Section 5 discusses some related empirical research publications. Finally, Sect. 6 describes our next steps and conclusion.

2 Study Design

This section first presents a realistic scenario which serves as a motivating example for our work. We then present our research questions and research goal. Next, we describe the participant selection, we then present the formulated hypothesis, variables and metrics. Finally we introduce the survey implementation and the survey validation and conduction[1].

2.1 Motivating Scenario Example

Frank lives in a city where the amount of parking spaces per motor vehicle is becoming scarce. Given the difficulty of finding a parking space, Frank uses a mobile application called happyParking. The application uses multiple input

[1] The artifacts used in this study were published in the following link: https://osf.io/wupd6/?view_only=30d712fee72243098fabd6bfee357567.

sources of i) external contextual information to provide a certain degree of probability of finding a parking spot in different locations; and ii) internal contextual information (i.e. emotional states) for assessing quality of User Experience (UX). happyParking is built based on a context-aware quality assurance framework.

For example, by knowing the current situation of other circulating cars, happyParking can recommend the fastest route by avoiding congested hot spots. However, despite the reduced time for finding a public parking space, sometimes Frank was not fully satisfied with happyParking because i) the navigation information was overloaded and difficult to interpret, or ii) space of the available parking spot was not large enough for Frank's car, or iii) the closest space recommended by happyParking was meanwhile taken.

In this situation, interacting with happyParking was annoying and stressful for Frank. This emotional information is derived from physiological data collected through wearable sensors of the E4-Wristband[2] device at runtime. Exploiting this emotional information, happyParking is able to measure the actual quality of UX, and consequently increase awareness of potential issues with the software services (e.g. finding a closest space), what could eventually lead to actions addressing the issue.

2.2 Goal and Research Questions

The goal of the study presented in this paper is to*understand* perceived importance with respect to security attributes *from the viewpoint of* service consumer[3], *in the context of* the smart parking happyParking. From this goal, the following research questions are derived:

RQ$_1$: *How do service consumers perceive the importance of security of a context-aware software intensive system?*
RQ$_2$: *Does the personality influence on the importance perceived of security of context-aware software applications?*

To answer these RQs we planned and executed a survey with volunteer participants as potential service consumers of happyParking. Our survey design draws on the methodological guidelines of Kitchenham and Pfleeger [16], and Molleri et al. [19].

2.3 Participant Selection

Considering the importance of modeling the diversity in users for identifying right subjects [26], we considered the educational background. This results in two groups: *Group A* consists of subjects at University education level, with background in SE. *Group B* includes subjects at University level with background in Education without an SE background.

[2] https://www.empatica.com/en-eu/research/e4/.
[3] We refer to end-users as to service consumers, as the applications usually provide services to their users.

2.4 Hypothesis, Variables and Metrics

We identify as a *hypothesis* that the personality influences the perceived importance of security attributes of software applications. From this hypothesis, we identified the following variables:

Response variables: the perceived importance of security, which is defined in terms of authenticity, confidentiality, accountability, and integrity attributes, is measured by means of i) four items formulated in 5-points ordinal scale (from "not at all important" to "extremely important"); ii) ranking ten domain-specific items, where at least five of them should be rated.

Factors: as the main functionality and some vulnerabilities of the happyParking app are illustrated through animated-demonstration videos. In this study, we identified the videos as a factor that could affect the response variables.
Personality is another important factor identified in our study. To measure it, we use the Big Five Inventory questionnaire (BFI) [14], which is a self-report inventory designed to measure the so-called Big Five dimensions: Extraversion, Agreeableness, Conscientiousness, Neuroticism, and Openness to experience.

2.5 Web-Based Survey Implementation

We implemented a web-based survey using the Qualtrics tool. Figure 1 presents the process of survey execution. The survey takes 35 min and it is composed of two parts:

A pre-questionnaire: aiming to collect demographic and personality information. The *demographic part* consists of nine questions (*e.g.,* sex, age, educational degree, domain expertise).

The *Personality test* based on "The BFI questionnaire" that consists of 44 items for measuring five dimensions: Extraversion, Agreeableness, Neuroticism,

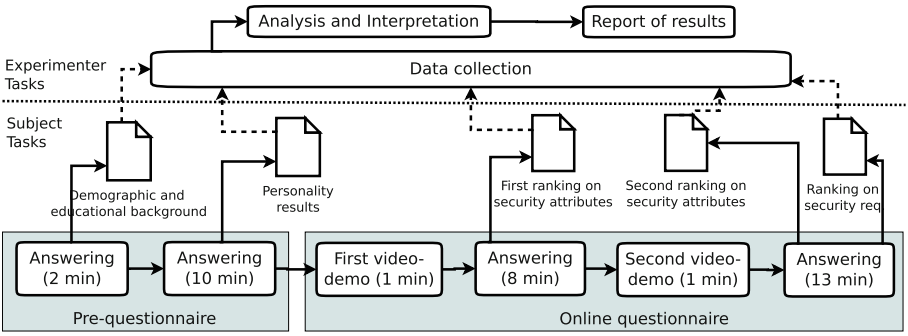

Fig. 1. An overview of the survey conduction

Openness, and Conscientiousness. However, for the purpose of reducing the average duration of the survey, we considered only those items related to the following dimensions:

i) Agreeableness: it refers to a person's tendency to be compassionate and cooperative toward others. Low Agreeableness is related to being suspicious, challenging, and antagonistic towards other people. Agreeableness is composed of the nine following items: *A1-Tends to find fault with others*, *A2-Is helpful and unselfish with others*, *A3-Starts quarrels with others*, *A4-Has a forgiving nature*, *A5-Is generally trusting*, *A6-Can be cold and aloof*, *A7-Is considerate and kind to almost everyone*, *A8-Is sometimes rude to others*, *A9-Likes to cooperate with others*.
ii) Neuroticism: it refers to the extent to which a person's emotions are sensitive to the environment, thus identifying individuals prone to psychological distress, anxiety or excessive urges. Those who have a low score in Neuroticism are calmer and more stable. Neuroticism is composed of the eight following items: *N1-Is depressed, blue*, *N2-Is relaxed, handles stress well*, *N3-Can be tense*, *N4-Worries a lot*, *N5-Is emotionally stable, not easily upset*, *N6-Can be moody*, *N7-Remains calm in tense situations*, *N8-Gets nervous easily*.
iii) Openness: it refers to the extent to which a person is open to experiencing a variety of activities. People low in Openness tend to be more conservative and close-minded. Openness is composed of the ten following items: *O1-Is original, comes up with new ideas*, *O2-Is curious about many different things*, *O3-Is ingenious, a deep thinker*, *O4-Has an active imagination*, *O5-Is inventive*, *O6-Values artistic, aesthetic experiences*, *O7-Prefers work that is routine*, *O8-Likes to reflect, play with ideas*, *O9-Has few artistic interests*, *O10-Is sophisticated in art, music, or literature*.

According to [22], these constructs (dimensions) were found as the most relevant for understanding the personality characteristics in the context of software technology. All of the scale items were in the Five-point Likert Response Format (where the lowest point of 1 means "strongly disagree" and the highest point of 5 means "strongly agree").

The online questionnaire: it gathers service consumer perceptions on security attributes of context-aware applications. To do that, two 1-minute animated demonstration videos were added to the survey. As shows in Fig. 1, the online questionnaire consists of two sub-parts:

i) First one: items (*i.e.,* definitions of security attributes) formulated to measure the first perceptions about the importance of security attributes according to the first video[4].

[4] happyparking.mp4 file in the OSF repository link (see Sect. 2).

ii) Second one: questions for re-evaluating the importance of security attributes (after watching the second video[5]) are formulated. Finally, a set of security requirements to keep quality of the case study high should be prioritized by subjects[6]. It helps us to confirm the importance provided in the second round, however the analysis of these requirements is not part of this paper.

2.6 Survey Validation and Conduction

Survey validation: a pilot study that used our survey design was performed in October 9, 2018 in the MEGSUS workshop at ESEM 2018 [18]. Therein, we collected feedback from seven subjects working on topics of software sustainability. Their feedback was used to improve the questionnaire design regarding: i) the clarity and relevance of the questions, and ii) the duration of the survey. The completing process of the survey took about 40–60 min. In this version, all items of the BFI dimensions were considered, which demanded more than 20 min. In order to reduce this time, we shortened the BFI questionnaire by considering items from three dimensions only (instead the total of five dimensions) as explained.

Survey Conduction

A. Data collection: considering the characteristics of our target audience, we planned our data collection in three stages. The first two collection stages were already conducted whilst the third one is planned for future work. They are described as follows:

First stage: the survey was conducted as part of the Live Study track of the International Working conference on Requirements Engineering: Foundations for Software Quality (REFSQ). Voluntary researchers and practitioners with background in Requirements Engineering completed this survey, which was opened from 18 March until 3th April 2019. General instructions were given during one of the plenary sessions of REFSQ [11].

Second stage: the survey was conducted with Students from the Education department of the Universidad Nacional de San Agustin (Peru) in June 18, 2019. With the purpose of avoiding some internet connection issues, the collection was carried out using the paper and electronic forms for the data collection. All subjects gave an informed consent before performing the study. The averaged actual time of executing the survey took about 35 min.

Regarding the ***third collection stage***, we plan to conduct the survey with teenagers and elderly people with basic educational background.

This new data will be independently analyzed and compared to our results obtained from the first two stages.

[5] happyparking-vulnerabilities.mp4 file in the OSF repository.

[6] SecurityRequirements.pdf file in the OSF repository link.

B. Data validation: it ensures that the survey questionnaire is completed and contains consistent data. In this paper, we focus on the analysis of the data collected from the two first stages of data collection described above. Overall, 20 subjects accepted to participate in Stage 1, whereas 33 Subjects participated in Stage 2. However, incomplete questionnaires were discarded (four were from the first stage, and only one from the second stage). Moreover, verifying the target group of all subjects involved in both stages, by means of some demographics (i.e., educational background), we identified four subjects involved in Stage 2 were categorized as Group A because of their mixed background in Education and SE. Therefore, we found that 20 subjects were categorized as Group A and 28 as Group B.

3 Results

As mentioned, data collected from a total of 48 subjects was used in our analysis. The demographics are presented in Table 1. We note that the subjects from Group B (with background in Education) are younger than the subjects in Group A (with Software Engineering background). We can also see that Group A tends to use the mobile phone with less frequency than Group B. The mobile feature most used were camera, and text messaging for Group A, whereas internet browsing/apps was for Group B. Moreover, Group A included men and women subjects, whereas over 90% of subjects from Group B were female.

Table 1. Demographics of subjects from Group A and B

Characteristics	Group A	Group B
Age	20–70 years old	20–28 years old
Sex	35% female, 65% male	93% female, 7% male
Background	Software engineering	Education
Frequency of mobile usage (per day)	15% <30 min	11% ≥30 min and <1 h
	20% ≥30 min and <1 h	18% ≥1 h and <2 h
	55% ≥1 h and <2 h	21% ≥2 h and ≤3 h
	10% ≥2 h and ≤3 h	50% >3 h
Mobile feature most used	Camera, text messaging (each <30 min)	Internet browsing/apps (>2 h)

In the following, we proceed to analyze the gathered data through the survey in order to answer our research questions.

3.1 RQ_1: How Do Service Consumers Perceive the Importance of Security of a Context-Aware Software Intensive System?

To answer RQ1, we analysed the frequency distribution per security attribute regarding the perceived importance, which is measured in a 5-points ordinal

Table 2. Comparison between answers on perceived importance of security attributes: 20 Subjects of Group A and 28 Subjects of Group B. Where: *1st Vid = first video, 2nd Vid = second video, NI = not at all important, SI = slightly important, MI = moderate important, VI = very important and EI = extremely important.*

		Confidentiality		Authenticity		Accountability		Integrity	
		1st Vid	2nd Vid	1st Vid	2nd Vid	1st Vid	2nd Vid	1st Vid	2nd Vid
Group A	NI	0	1	3	1	3	2	1	0
	SI	2	0	2	1	6	2	0	0
	MI	2	1	2	3	5	4	2	3
	VI	**5**	**6**	**8**	**6**	**4**	**6**	**8**	**4**
	EI	**11**	**12**	**5**	**9**	**2**	**6**	**9**	**13**
	% VI+EI	80%	90%	65%	75%	30%	60%	80%	85%
Group B	NI	0	5	0	4	0	6	0	4
	SI	3	3	4	6	2	2	3	4
	MI	10	5	7	5	12	6	11	6
	VI	**9**	**10**	**12**	**9**	**11**	**8**	**10**	**9**
	EI	**6**	**5**	**5**	**4**	**3**	**6**	**4**	**5**
	% VI+EI	54%	54%	61%	46%	50%	50%	50%	50%

scale. Table 2 presents the importance of security attributes perceived by subjects from Group A and B. As this measure was taken in two different moments, we added two columns to each security attribute: "1st Video" columns represent number of subject's answers about how a security attribute is perceived after watching the first video (main functionalities of happyParking), whereas "2nd Video" columns represent the number of answers to the same question but after watching the second video (happyParking with security breaches).

From this data, we can see that most of the security attributes were more clearly perceived as important by subjects from Group A than by subjects from Group B. Particularly, *Integrity* and *Confidentiality* were deemed extremely important security attributes by subjects from Group A. Interestingly, we noticed that the importance of both attributes could be perceived from the beginning (first video), whereas the importance for other security attributes, like *authenticity* or *accountability*, was most hardly perceived. For instance, most of the subjects from Group A realized the importance of accountability only after watching the second video. We can also observe that after watching the second video more subjects from Group A rate all security attributes as very and extremely important. It may also be the fact that the second video, which exhibits a scenario in which security breaches can damage service consumers, helps subjects to understand the value of keeping security attributes high.

The variation in the perceptions of the importance of security attributes seems to be even broader in case of subjects with non-technical background, i.e. different from SE, such as subjects from Group B. Another interesting observation was that subjects from Group B tend to perceive the importance of security attributes from the beginning but with not so much intensity such as it was with

the subjects of Group A. For example, as shown in Table 2 for Group B, about 35% of subjects perceived confidentiality, accountability, and integrity as security attributes with a moderate importance level. And, only around 50% of subjects from Group B perceived confidentiality and integrity as very or extremely important in contrast to the 80% of subjects from Group A.

Moreover, more or less 14% of subjects from Group B changed their perceptions after watching the second video, by considering the security attributes as not all important. This unexpected result may be due to the lack of adequate understanding on the security attributes definitions by subjects with a non-technical background. Another possible explanation for this may be related to the socio-cultural issues, e.g. vulnerabilities illustrated in the video could not have been considered as so critical in comparison with actual vulnerabilities experienced in real-life. Overall, we consider that this combination of results provides some support for the conceptual premise stated by West [29]: *"security is hard to be appreciated because end-users do not think they are at risk"* or *"losses perceived disproportionately to gains"*.

In response to RQ1: Confidentiality and integrity are more clearly perceived as important by service consumers with technical (SE) background. Whilst accountability is more difficult to be perceived as important by service consumers, even more pronounced for those without any SE background. Moreover, after watching a dangerous scenario in which security vulnerabilities were exploited, service consumers with SE background reassert their perception on the importance of security attributes (confidentiality, authenticity, accountability, integrity). Contrary to service consumers without SE background, where some of them (around 18%) perceived security attributes as not at all important.

In order to understand better these results, in the next sub-section, we will investigate how personality traits influence subjects' answers in this study.

3.2 RQ_2: Do the Personality Influence on the Importance Perceived of Security of Context-Aware Software Applications?

To answer RQ2, our analysis consists of three steps: 1) characterizing each subject by means of three personality dimensions; 2) analyzing the influence of personality on the perceived importance of security attributes; 3) analyzing the personality's influence on change in security perceptions.

Step1: characterizing each subject by means of three personality dimensions. To characterize each subject through the three personality dimensions (i.e. agreeableness, neuroticism, openness), we have first calculated the scores self-reported by means of the personality test. To do this, for each dimension (construct), the scores of the corresponding items were added. Then, in order to make comparable our dimensions, each result was normalized to a common ratio scale with values between 0 and 1. Next, for each subject, we chose

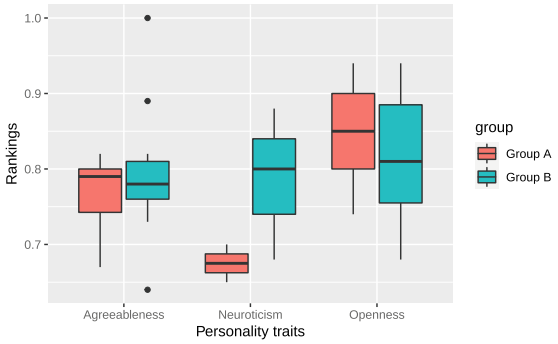

Fig. 2. Personality distributions of subjects from Group A and B

the maximum value of these normalized values. If this value was greater than 0.75 we labeled it as high level of the personality. Otherwise, if this value was greater than 0.5 we labeled it as a moderate level, else the subject will not be characterized by any personality trait studied in this paper. Analysing our data set we found that all subjects were characterized by high or moderate levels of personalities. Notice that two subjects from Group B presented the same maximum value for two different dimensions. To analyse both personality dimensions, we have duplicated the entries related to these subjects. This is the reason why we have 50 Subjects in total (instead of 48) for the analysis of RQ_2.

Figure 2 depicts the personality distributions of the subjects from Group A and B. We observe that Group A tends to have a greater level of *openness* and a lower level of *neuroticism* than Group B. Both groups seem to have a similar level of *agreeableness*, however Group B contains three subjects who are outside of the range. On the other hand, Table 3 introduces the percentages of subjects from Group A and B who are characterized by a personality in two levels: high and moderate values. From this table we notice that both groups have equivalent percentages of subjects characterized by the *Neuroticism* personality. Moreover, Group B has a slightly greater percentage of subjects who were characterized by

Table 3. Percentages of subjects characterized by a personality trait

Groups	Values	Personality traits		
		Agreeableness	Neuroticism	Openness
A	High	20	0	45
	Moderate	10	10	15
	% Total	30	10	60
B	High	30	6.67	40
	Moderate	6.67	3.33	13.33
	% Total	36.67	10	53.33

the *agreeableness* personality than Group A, but a lower percentage of subjects characterized by the *openness* personality. In general, we can say that the subjects of our study tend to be more open-minded (Columns 5) and cooperative toward others (Columns 3).

For the rest of our analysis, we do not differentiate between subjects characterized by high or moderate levels of personality types. However, we should keep in mind that the characterization of subjects using personality test is not trivial. For instance, from Table 3, we notice that 35% of subjects from Group A were characterized as a certain personality type using moderate values. In the case of Group B, this percentage is around 23%. It reflects the variability of personality tendencies presented by service consumers. Moreover, the fact that people could present different combinations of personality types increases the difficulty of characterization. As mentioned, we considered only the type of personality with highest value. However for future work, a deep analysis of users characterization will be needed.

Step2: analyzing the influence of personality on the perceived importance of security attributes. To investigate whether personality types influence on the perceived importance of security attributes, we firstly analyzed the distribution of our data set[7] (see Table 4). From this table, we can see that subjects with a high level of *openness* have a higher propensity to perceive the importance of certain security attributes like *confidentiality* and *integrity*. However, subjects hold quite different perceptions regarding the importance of *authenticity* and *accountability*.

This variability is even greater for those subjects with a high level of *agreeableness* (who are assumed to be kind, considerate, likable, helpful, and cooperative). It is interesting to note that most of these kind of respondents from Group B considered security attributes like *confidentiality*, *accountability* and *integrity* as not at all important (see Table 4, Column 9, on the right). It is somewhat surprising since this perception was after watching the second video (scenarios with vulnerabilities of the mobile app). A possible explanation for this might be that the mobile app such as happyParking could have been perceived as so useful that security was not considered as important. The first part of this observation seems to be consistent with other research which found that *"individuals with a high level of agreeableness have a higher propensity to perceive smart phone technology as more useful"* [22]. However, further research needs to be carried out in order to get a better understanding whether the importance of security can be more difficult perceived by people with a high level in agreeableness.

The relationships between our categorical variables (personality type in a nominal scale and perceived importance in a ordinal scale) were analyzed by means of cross-tabulation. Then, in order to determine the strength of association between both variables, we used the Cramer's V measure[8], whose value

[7] You can find the data set (SecurityPerception.csv file) in the OSF repository.

[8] According to [1], the strength of association is interpreted as follows: >0.25 very strong; >0.15 strong; >0.10 moderate; >0.05 weak; >0 to 0.05 no relationship.

Table 4. Frequency distribution about the perceived importance of security attributes. Where: *NI = not at all important, SI = slightly important, MI = moderate important, VI = very important and EI = extremely important.*

	Personality dimension	Group	First video					Second video				
			NI	SI	MI	VI	EI	NI	SI	MI	VI	EI
Confident.	Agreeableness	A	0	0	1	1	4	0	0	0	2	4
		B	0	1	5	4	1	4	0	3	1	3
	Neuroticism	A	0	0	0	1	1	0	0	0	1	1
		B	0	2	0	1	0	1	1	0	1	0
	Openness	A	0	2	1	3	6	1	0	1	3	7
		B	0	1	6	4	5	1	3	2	8	2
Authent.	Agreeableness	A	0	0	1	3	2	0	0	0	2	4
		B	0	2	4	4	1	2	4	2	2	1
	Neuroticism	A	0	0	1	1	0	0	0	1	0	1
		B	0	1	0	2	0	1	1	1	0	0
	Openness	A	3	2	0	4	3	1	1	2	4	4
		B	0	3	3	6	4	2	2	2	7	3
Account.	Agreeableness	A	0	0	3	2	1	0	0	0	3	3
		B	0	1	5	5	0	4	1	2	2	2
	Neuroticism	A	0	2	0	0	0	0	1	1	4	5
		B	0	1	1	1	0	1	1	0	0	1
	Openness	A	3	4	2	2	1	2	1	3	3	3
		B	0	1	7	5	3	2	1	4	6	3
Integrity	Agreeableness	A	0	0	0	4	2	0	0	1	1	4
		B	0	2	6	3	0	3	2	2	3	1
	Neuroticism	A	0	0	1	1	0	0	0	0	1	1
		B	0	0	1	1	1	1	1	0	1	0
	Openness	A	1	0	1	3	7	0	0	2	2	8
		B	0	2	4	6	4	1	2	4	5	4

varies between 0 and 1. The Cramer's V values calculated from our data set are presented in Table 5. As we can notice from this table, the *p-values* suggest non-significant results to reject the null hypothesis (*i.e.,* that variables are independent). According to our first descriptive data analysis (Fig. 2), three data points were located outside the whiskers of the box plot. Considering these data points as outliers, we recalculated the Cramer's V values. For this, we obtained one significant result, which is related to personality types of Group B and the *confidentiality* attribute (first video). We obtained 0.04 as *p-value* and 0.5 as Cramers'V value, so it suggests a very strong association between service consumers' personality types and the importance perception on confidentiality. The complete results are not shown for space limitation reasons.

Table 5. Cramer's V measure to evaluate the association between personality traits and security attributes

		First video				Second video			
		Conf.	Authent.	Account.	Integr.	Conf.	Authent.	Account.	Integr.
Total	p-value	0.35	0.56	0.15	0.60	0.43	0.63	0.40	0.66
	Chi-square	6.69	6.76	12.10	6.42	8.01	6.19	8.36	5.87
	Cramer's V	0.26	0.26	0.35	0.25	0.28	0.25	0.29	0.24
GrpA	p-value	0.84	0.34	0.20	0.25	0.94	0.70	0.24	0.84
	Chi-square	2.71	9.00	10.94	7.85	1.81	5.56	10.42	1.41
	Cramer's V	0.26	0.47	0.52	0.44	0.21	0.37	0.51	0.19
GrpB	p-value	0.09	0.67	0.55	0.50	0.15	0.60	0.59	0.72
	Chi-square	11.05	4.08	4.94	5.37	12.06	6.42	6.52	5.38
	Cramer's V	0.43	0.26	0.29	0.30	0.45	0.33	0.33	0.30

Step3: analyzing the personality's influence on change in security perceptions. To investigate whether personality type influence on changes in the importance perceived by service consumers, we firstly calculated the delta values (*i.e., perception_value*$_{second\_video}$ − *perception_value*$_{first\_video}$). Then, the Cramer's V values were calculated to analyze the level of association between the different (positive and negative) delta values and personality types (see Table 6). From this table, we notice that the positive and negative delta values of the importance on *confidentiality* are very strongly influenced by the subjects' personality traits (the *p-values* are 0.02 and 0.05, and the *Cramer's values* are 0.84 and 0.54, see Column 3 and 7). It does not depend on the subjects' education background. This result is even more clear for the positive delta values whose *p-values* is 0.02 and the *Cramer's V value* is = 0.84 (see Column 3).

Table 6. Cramer's V measure to evaluate the association between personality traits and changes in security perceptions (delta)

		Positive delta				Negative delta			
		Conf.	Authent.	Account.	Integr.	Conf.	Authent.	Account.	Integr.
Total	p-value	0.02	0.74	0.87	0.51	0.05	0.25	0.29	0.33
	Chi-square	7.76	0.61	1.23	1.33	9.48	5.40	4.99	4.62
	Cramer's V	0.84	0.21	0.19	0.33	0.54	0.42	0.46	0.42
GrpA	p-value	0.32	0.55	0.69	0.30				
	Chi-square	1.00	1.20	2.25	2.40				
	Cramer's V	0.50	0.39	0.34	0.63				
GrpB	p-value	0.03	1.00	0.46	1.00	0.07	0.32	0.29	0.36
	Chi-square	7.00	0.00	1.56	0.00	8.61	4.67	4.99	4.37
	Cramer's V	1.00	0.00	0.47	0.00	0.54	0.41	0.46	0.43

Analysing each group, we notice that Group A does not have enough negative variations to calculate the chi-square and Cramer's V values. It could be

explained by the fact of the subjects from Group A, having a SE background, understand better the importance of security attributes. So, their perceptions could not be changed in a negative way. Regarding Group B, we note that the positive variations of perceptions on confidentiality are perfectly associated to the subjects personality types (the *p-value* is 0.03 and the *Cramer's V value* is 1.0). And, the negative variations of perceptions on confidentiality could be very strongly associated to the subjects personality types if we accept the *p-value* = 0.07 (the *Cramer's V value* is = 0.54). For the rest of the calculated Cramer's V values, we obtained non-significant results to reject the null hypothesis.

In response to RQ2: Open-minded service consumers have a higher propensity to perceive the importance of confidentiality and integrity. Whilst, service consumers with levels of openness or agreeableness hold quite different importance perceptions on authenticity and accountability. Moreover, according to Cramers'V values, the importance perceptions on confidentiality are influenced by the personality of service consumers without SE background. And, the (positive or negative) changes in the importance perception on confidentiality are also very strongly influenced by the personality of service consumers without SE background.

4 Threats to Validity

Internal validity: As the survey was conducted with two different target audiences, we translated the original instruments (questionnaires, personality test and videos) from English to Spanish. To mitigate any error in the translation, Spanish native speakers reviewed the instruments used in our study. Another potential threat is regarding the unequally sized gender groups, which can impact on our results.

Construct validity: We mitigated the threat related to the following two social factors by implementing specific actions: (i) regarding *Hypothesis guessing*, we did not reveal the research goal before conducting the survey, and (ii) regarding *Evaluation apprehension*, we made the completion of both personality test and online questionnaire anonymous as some people are afraid of being evaluated. Regarding the threats related to the design of the study: the most important is *mono-operation bias*; as we included only one treatment (happyParking app), the study could be under-representing the identified constructs (perceived importance on security). To mitigate this threat, we carefully selected the software domain (IoT systems for the smart parking sector in which security and privacy are crucial [2]), which we think it is representative enough for measuring our response variables. Also we considered other relevant factors as personality, which was measured by means of the BFI questionnaire, defined and validated in the psychology field [14]. Moreover, the BFI model has been widely used in the SE field (*e.g.,* the analysis of developers' personalities in the Apache ecosystem pre-sented by Calefato *et al.* [8]). For our analysis, we focused especially on a

sub set of constructs that have an effect on the Technology acceptance [22] (i.e. agreeableness, neuroticism, openness). However, our current analysis is limited in considering only one personality type by subject (the maximum value of the three personality dimensions). Further work is needed to characterize individuals by considering other levels of personality dimensions. For example, a subject can be high in openness, but moderate in agreeableness, and low in neuroticism.

Regarding the questions in ordinal scale (importance level) we added the option: "No opinion" to avoid forcing respondents in choosing one of the other levels of importance.

External validity: concerns the *generalization* of the findings beyond the validation settings. As our sample corresponds to a selective proportion of end-users (48 subjects) of a context-aware software application (*i.e.,* happyParking mobile app), our results can not be generalized. This threat is partly reduced by the fact that the survey was first conducted with volunteer attendees from REFSQ 2019, then replicated in Peru with volunteer education students.

5 Related Work

The 2015 mapping study of Cruz *et al.* [12] on empirical research on personality types in SE, indicated a broad array of contexts in which SE researchers analyzed the role and the effect of personality, e.g. pair programming, individual performance team process, team effectiveness, leadership performance, software process allocation, and SE education. Although this mapping study covers a 40 years long period of research publication activity, very few papers were found on the topic of linkages between personality types and security engineering.

For instance, Shropshire *et al.* [25] propose a method for identifying those individuals in an organization that are most likely to commit IT security infractions, based on some dimensions of their personality. However, the authors just motivate and propose an empirical research design, without reporting how it is executed in a study with real-world subjects. Furthermore, Uffen *et al.* [28] empirically investigated the relationship between personality traits and attitudes towards security risks of security executives. These authors hypothesized relationships between the construct of the five-factor model (FFM) and technical and non-technical dimensions (e.g. culture, compliance, organization, strategic management) of information security management. Next, Bansal empirically examined the relation of the FFM constructs and concerns of security and privacy on websites [5]. This study found that neuroticism, conscientiousness and extraversion are positively related with concerns for security. Personality traits of agreeableness and openness are significantly associated with concern for privacy. Moreover, Junglas et al. [15] used protection motivation theory to look into any possible relationship between privacy concerns and agreeableness, conscientiousness, and openness. These authors found that personality traits affect the concern for privacy in location-based services. Finally, Bulgurcu *et al.* [7] investigated how personality influences employees' intention to comply with the requirements of an organization's security policies. The authors's empirical design is grounded

on the theory of planned behavior and the rational choice theory and investigates the possible relationships between the constructs of these theories and individual intention to comply with the requirements of the information security policies. Using data of 110 practitioners in a company, this study shows that the individual intention to comply is significantly influenced by attitude, normative beliefs, and self-efficacy to comply.

To the best of our knowledge, our approach is the first designed to analyse empirically end-users (*i.e.,* service consumers who are outside of a company) perception on security attributes of context-aware software applications. Moreover, our approach differs from previous works on the methodology employed to collect end-users perceptions on the importance of security attributes. In particular, none of these approaches used contra-version scenarios to analyse users profile (user's personality types and educational background) in perceiving security.

6 Conclusions and Further Work

In this paper we studied how end-users perceive security attributes of context-aware software applications. To do that, we performed a survey in two stages: firstly, it was with voluntary participants of the REFSQ conference. Secondly, it as with volunteers of education students of the Universidad Nacional San Agustin (Peru). The survey allowed us to understand how a selective proportion of end-users (48 subjects) perceives security in two different scenarios of a mobile app (with and without security vulnerabilities), and how the users personality types affect these perceptions and changes in them.

From this sample of potential service consumers, the results showed that subjects' educational background influenced their perception on security. After watching the second video, Group A (subjects with SE background) considered security attributes more important, whilst Group B (subjects with education background) deemed them less important. This phenomenon could be traceable to the use of technical terms in security, which were probably better understood by software engineers than educators.

The research has also shown that subjects with a higher level of openness would have a much better perception on the importance of confidentiality and integrity. However, the importance of security attributes like accountability and authenticity was not appreciated by subjects from Group B with a highest level of agreeableness. Considering the Cramer's V values, we found a significant very strong association between personality traits of subjects from Group B and the importance perception on confidentiality. We also obtained that users personality types is very strongly associated to the changes in the importance perception on confidentiality. This conclusion is even more clear for subjects from Group B.

For the next step of our study we plan to replicate the survey with a broader group of participants, and consider other variables such as gender and the frequency of mobile apps usage.

Acknowledgment. We thank the participants of the study. N. Condori-Fernandez and F. Suni-Lopez acknowledge the financial support of the KUSISQA Project - World Bank, through Fondo Nacional de Desarrollo Cientfico, Tecnolgico y de Innovacin Tecnolgica (FONDECYT). Also, this work has been partially supported by Datos 4.0 (TIN2016-78011-C4-1-R) funded by MINECO-AEI/FEDER-UE.

References

1. Akoglu, H.: User's guide to correlation coefficients. Turk. J. Emerg. Med. **18**(3), 91–93 (2018)
2. Al-Turjman, F., Malekloo, A.: Smart parking in IoT-enabled cities: a survey. Sustain. Cities Soc. **49**, 101608 (2019)
3. Anderson, R.J.: Security Engineering: A Guide to Building Dependable Distributed Systems, 2nd edn. Wiley, Hoboken (2008)
4. Anderson, R., et al.: Measuring the cost of cybercrime. In: Böhme, R. (ed.) The Economics of Information Security and Privacy, pp. 265–300. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-39498-0_12
5. Bansal, G.: Security concerns in the nomological network of trust and big 5: first order vs. second order. In: Galletta, D.F., Liang, T. (eds.) Proceedings of the International Conference on Information Systems, ICIS 2011, Shanghai, China, 4–7 December 2011. Association for Information Systems (2011). http://aisel.aisnet.org/icis2011/proceedings/ISsecurity/9
6. Bødker, S.: Scenarios in user-centred design setting the stage for reflection and action. Interact. Comput. **13**(1), 61–75 (2000). https://doi.org/10.1016/S0953-5438(00)00024-2
7. Bulgurcu, B., Cavusoglu, H., Benbasat, I.: Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Q. **34**(3), 523–548 (2010)
8. Calefato, F., Lanubile, F., Vasilescu, B.: A large-scale, in-depth analysis of developers' personalities in the apache ecosystem. Inf. Softw. Technol. **114**, 1–20 (2019). https://doi.org/10.1016/j.infsof.2019.05.012
9. Condori-Fernández, N.: HAPPYNESS: an emotion-aware QoS assurance framework for enhancing user experience. In: Uchitel, S., Orso, A., Robillard, M.P. (eds.) Proceedings of the 39th International Conference on Software Engineering, ICSE 2017, Buenos Aires, Argentina, 20–28 May 2017 - Companion Volume, pp. 235–237. IEEE Computer Society (2017). https://doi.org/10.1109/ICSE-C.2017.137
10. Condori-Fernández, N., Lago, P.: Characterizing the contribution of quality requirements to software sustainability. J. Syst. Softw. **137**, 289–305 (2018). https://doi.org/10.1016/j.jss.2017.12.005
11. Condori-Fernández, N., Muñante, D., Lopez, F.S.: Exploring users perception on security and satisfaction requirements of context-aware applications: an online survey. In: Spoletini, P., et al. (eds.) Joint Proceedings of REFSQ-2019 Workshops, Doctoral Symposium, Live Studies Track, and Poster Track Co-Located with the 25th International Conference on Requirements Engineering: Foundation for Software Quality (REFSQ 2019). CEUR Workshop Proceedings, Essen, Germany, 18 March 2019, vol. 2376. CEUR-WS.org (2019). http://ceur-ws.org/Vol-2376/LS_paper1.pdf
12. Cruz, S.S.J.O., da Silva, F.Q.B., Capretz, L.F.: Forty years of research on personality in software engineering: a mapping study. Comput. Hum. Behav. **46**, 94–113 (2015). https://doi.org/10.1016/j.chb.2014.12.008

13. Dalpiaz, F., Paja, E., Giorgini, P.: Security Requirements Engineering: Designing Secure Socio-Technical Systems. MIT Press, Cambridge (2016)
14. John, O.P., Srivastava, S.: The big five trait taxonomy: history, measurement, and theoretical perspectives. In: Pervin, L.A., John, O.P. (eds.) Handbook of Personality: Theory and Research, 2nd edn, pp. 102–138. Guilford Press, New York (1999)
15. Junglas, I.A., Johnson, N.A., Spitzmüller, C.: Personality traits and concern for privacy: an empirical study in the context of location-based services. Eur. J. Inf. Syst. **17**(4), 387–402 (2008). https://doi.org/10.1057/ejis.2008.29
16. Kitchenham, B.A., Pfleeger, S.L.: Principles of survey research part 2: designing a survey. ACM SIGSOFT Softw. Eng. Notes **27**(1), 18–20 (2002). https://doi.org/10.1145/566493.566495
17. Laverdière, M., Mourad, A., Hanna, A., Debbabi, M.: Security design patterns: survey and evaluation. In: Proceedings of the Canadian Conference on Electrical and Computer Engineering, CCECE 2006, Ottawa Congress Centre, Ottawa, Canada, 7–10 May 2006, pp. 1605–1608. IEEE (2006). https://doi.org/10.1109/CCECE.2006.277727
18. Lopez, F.S., Condori-Fernández, N., Muñante, D.: End-user perceptions on social sustainability in context-aware applications: validation of an experiment design. In: Condori-Fernández, N., Bagnato, A., Kern, E. (eds.) Proceedings of the 4th International Workshop on Measurement and Metrics for Green and Sustainable Software Systems Co-Located with Empirical Software Engineering International Week (ESEIW 2018). CEUR Workshop Proceedings, Oulu, Finland, 9 October 2018, vol. 2286, p. 31. CEUR-WS.org (2018). http://ceur-ws.org/Vol-2286/paper_4.pdf
19. Molléri, J.S., Petersen, K., Mendes, E.: Survey guidelines in software engineering: an annotated review. In: Proceedings of the 10th ACM/IEEE International Symposium on Empirical Software Engineering and Measurement, ESEM 2016, Ciudad Real, Spain, 8–9 September 2016, pp. 58:1–58:6. ACM (2016). https://doi.org/10.1145/2961111.2962619
20. Muñante, D., Chiprianov, V., Gallon, L., Aniorté, P.: A review of security requirements engineering methods with respect to risk analysis and model-driven engineering. In: Teufel, S., Min, T.A., You, I., Weippl, E. (eds.) CD-ARES 2014. LNCS, vol. 8708, pp. 79–93. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-10975-6_6
21. Muñante, D., Siena, A., Kifetew, F.M., Susi, A., Stade, M.J.C., Seyff, N.: Gathering requirements for software configuration from the crowd. In: IEEE 25th International Requirements Engineering Conference Workshops, RE 2017 Workshops, Lisbon, Portugal, 4–8 September 2017, pp. 176–181. IEEE Computer Society (2017). https://doi.org/10.1109/REW.2017.74
22. Özbek, V., Alnıaçık, Ü., Koc, F., Akkılıç, M.E., Kaş, E.: The impact of personality on technology acceptance: a study on smart phone users. Procedia. Soc. Behav. Sci. **150**, 541–551 (2014)
23. Price, B.A., et al.: Contravision: presenting contrasting visions of future technology. In: Mynatt, E.D., Schoner, D., Fitzpatrick, G., Hudson, S.E., Edwards, W.K., Rodden, T. (eds.) Proceedings of the 28th International Conference on Human Factors in Computing Systems, CHI 2010, Extended Abstracts Volume, Atlanta, Georgia, USA, 10–15 April 2010, pp. 4759–4764. ACM (2010). https://doi.org/10.1145/1753846.1754227
24. Rad, M.S., Nilashi, M., Dahlan, H.M.: Information technology adoption: a review of the literature and classification. Univ. Access Inf. Soc. **17**(2), 361–390 (2018). https://doi.org/10.1007/s10209-017-0534-z

25. Shropshire, J., Warkentin, M., Johnston, A.C., Schmidt, M.B.: Personality and IT security: an application of the five-factor model. In: Rodríguez-Abitia, G., B., I.A. (eds.) Connecting the Americas. 12th Americas Conference on Information Systems, AMCIS 2006, Acapulco, Mexico, 4–6 August 2006, p. 415. Association for Information Systems (2006). http://aisel.aisnet.org/amcis2006/415
26. Soikkeli, T., Karikoski, J., Hämmäinen, H.: Diversity and end user context in smartphone usage sessions. In: Al-Begain, K., Belimpasakis, P., Balakrishna, C. (eds.) 5th International Conference on Next Generation Mobile Applications, Services and Technologies, NGMAST 2011, Cardiff, United Kingdom, 14–16 September 2011, pp. 7–12. IEEE (2011). https://doi.org/10.1109/NGMAST.2011.12
27. Svendsen, G.B., Johnsen, J.K., Almås-Sørensen, L., Vittersø, J.: Personality and technology acceptance: the influence of personality factors on the core constructs of the technology acceptance model. Behav. Inf. Technol. **32**(4), 323–334 (2013). https://doi.org/10.1080/0144929X.2011.553740
28. Uffen, J., Kaemmerer, N., Breitner, M.H.: Personality traits and cognitive determinants—an empirical investigation of the use of smartphone security measures. J. Inf. Secur. **04**(04), 203–212 (2013)
29. West, R.: The psychology of security. Commun. ACM **51**(4), 34–40 (2008). https://doi.org/10.1145/1330311.1330320