On-line trust perception: what really matters

Citation for published version (APA):

Costante, E., Hartog, den, J. I., & Petkovic, M. (2011). On-line trust perception: what really matters. In *Proceedings of the First Workshop on Socio-Technical Aspects in Security and Trust (STAST'11, Milan, Italy, September 8, 2011)* (pp. 52-59). Institute of Electrical and Electronics Engineers.
<https://doi.org/10.1109/STAST.2011.6059256>

DOI:

[10.1109/STAST.2011.6059256](https://doi.org/10.1109/STAST.2011.6059256)

Document status and date:

Published: 01/01/2011

Document Version:

Publisher's PDF, also known as Version of Record (includes final page, issue and volume numbers)

Please check the document version of this publication:

- A submitted manuscript is the version of the article upon submission and before peer-review. There can be important differences between the submitted version and the official published version of record. People interested in the research are advised to contact the author for the final version of the publication, or visit the DOI to the publisher's website.
- The final author version and the galley proof are versions of the publication after peer review.
- The final published version features the final layout of the paper including the volume, issue and page numbers.

[Link to publication](#)

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal.

If the publication is distributed under the terms of Article 25fa of the Dutch Copyright Act, indicated by the "Taverne" license above, please follow below link for the End User Agreement:

www.tue.nl/taverne

Take down policy

If you believe that this document breaches copyright please contact us at:

openaccess@tue.nl

providing details and we will investigate your claim.

On-line Trust Perception: What Really Matters

Elisa Costante
Eindhoven University of Technology
The Netherlands
Email: e.costante@tue.nl

Jerry den Hartog
Eindhoven University of Technology
The Netherlands
Email: j.d.hartog@tue.nl

Milan Petkovic
Eindhoven University of Technology
Philips Research Europe
The Netherlands
Email: m.petkovic@tue.nl

Abstract—Trust is an essential ingredient in our daily activities. The fact that these activities are increasingly carried out using the large number of available services on the Internet makes it necessary to understand how users perceive trust in the online environment. A wide body of literature concerning trust perception and ways to model it already exists. A trust perception model generally lists a set of factors influencing a person trusting another person, a computer, or a website. Different models define different set of factors, but a single unifying model, applicable to multiple scenarios in different settings, is still missing. Moreover, there are no conclusions on the importance each factor has on trust perception. In this paper, we review the existing literature and provide a general trust perception model, which is able to measure the trustworthiness of a website. Such a model takes into account a comprehensive set of trust factors, ranking them based on their importance, and can be easily adapted to different application domains. A user study has been used to determine the importance, or weight, of each factor. The results of the study show evidence that such weight differs from one application domain (e.g. e-banking or e-health) to another. We also demonstrate that the weight of certain factors is related to the users knowledge in the IT Security field. This paper constitutes a first step towards the ability to measure the trustworthiness of a website, helping developers to create more trustworthy websites, and users to make their trust decisions when using on-line services.

I. INTRODUCTION

An increasing number of users adopt e-services to manage their daily activities: on-line they can declare taxes (e-government), check their account balance (e-banking), purchase holidays (e-commerce), or renew their periodical prescriptions (e-health). Unfortunately, the use of such services, although of great benefit to the end user, also exposes him to cyber risks like on-line frauds, phishing attacks, or identity theft, resulting in the user's loss of personal data or money. Because of these threats, there is the need for mechanisms able to protect the user, and to help him to assess the trustworthiness of an e-service.

Trust governs most *human-to-human relationships*: we trust our family, our friends, the butcher at the corner shop, or our bank. When it comes to the use of e-services, trust is even more critical, because it is more difficult to establish. This is mostly due to the fact that the signals of trust generally used to establish human-to-human relationships, such as physical aspect or body language, are missing in the on-line world. To understand and establish trust on-line, we need to find

the analogous signals of trust and learn in which way they influence the users' perception of trust. In this paper, we refer to the on-line signals of trust as *factors of trust*, and they represent peculiar characteristics of a website such as its look and feel, its quality, its privacy management, or its security.

Understanding the on-line user's perception of trust can help us to: i) develop services that better meet user's requirements for trust; ii) provide tools able to assist the user in assessing the trustworthiness of a given service; and iii) create *ad hoc* training programs to increase the user's trust awareness. For example, an outcome of our study indicates that the privacy policies stated by a service provider do not influence the user's trust perception, mainly because users do not read them; this suggests that one should i) develop tools to show the user how good or bad a privacy policy is; ii) improve the way privacy policies are expressed to make them more user-friendly; and iii) raise the user's awareness not only concerning the presence of privacy policies, but also on the importance of their contents, explaining that policies can actually state malicious usage of personal data.

To succeed in understanding the on-line user's perception of trust, we need a deep understanding of what trust means (can trust be formally defined?), of the way it is established (which are the factors of trust?), and whether (and if so how) trust perception changes according to different application domains (does Bob assess the trustworthiness of his e-banking in the same way he does for an e-commerce website?).

Trust has been defined in different ways: as expectation [1]–[3], as vulnerability to the actions of others [4], as probability [5], and as risk [6]. Ermisch observes that “(trust) *someone doing X does not necessarily extend to trust in that same person doing Y*” [7]. This leads us to consider trust as a multi-dimensional, context-dependent concept. In this paper we investigate the different dimensions (factors) of on-line trust perception, their importance for the end-user, and if and how they change according to the application domain.

Studies on trust perception aim to understand the mechanisms adopted by humans to trust other humans, machines or e-services. Generally, they are based on a theoretical *trust perception model* (TPM), accounting for several factors of trust. Such a model is usually validated by means of a user study, used to understand which of the factors present in the model, are actually considered by the user. Every trust model generally applies to specific application domains and categories of users. Trust models for human-to-human [4],

This work has been supported by European Commission FP7 TAS3 project, nr. 216287.

human-to-aid systems [8], [9], human-to-computer [10], and human-to-e-services [11] relationships can be found in the literature. In the field of human-to-e-services, specific trust perception models about e-commerce [12]–[18], e-banking [19], [20], and e-health services [21]–[23] can be found.

We observed that existing TPMs share a significant number of factors of trust: these factors can be aggregated to form a generic trust perception model (GTPM), accounting for the shared factors and adaptable to different application domains. No matter what the domain is, such a model should be able to describe the trust perception of an e-service by giving the right importance to each factor: for example, privacy should be much more important in domains where sensitive data is collected (as in e-health systems) than in those where only an e-mail address is requested (as in mailing lists).

The main contributions of this paper are the following:

- A General Trust Perception Model (GTPM), based on literature study, and accounting for a comprehensive list of factors of trust is provided. An importance value (also called *weight*) is associated with each factor: changing this value allows the model to adapt to different application domains;
- Evidence that factors have different weights, according to the application domain;
- Evidence that the weight of a factor depends on the user and on some of his characteristics, especially on his level of knowledge in Information Technology (IT) Security field. Particularly, we believe that users with little or no knowledge about security or privacy mechanisms and technologies, attach less importance to technical factors (as *security*), and more importance to aspect-related factors (as *Look&Feel*). On the other hand, users with expert IT Security knowledge rank security as one of the most important factors of trust.

The afore mentioned evidence is provided using the results of a user study, carried out with a questionnaire. The questionnaire was developed to investigate the user's perception of trust within different application domains: e-banking, e-commerce, e-health and e-portfolio (services for the on-line management of curricula and job opportunities).

To the best of our knowledge, this is the first study to associate a specific numeric weight distribution to the factors of trust, and to analyze the relationship existing between this distribution and the user's IT Security knowledge. This brings two major benefits to the state of the art: first, assuming that each factor can be objectively measured, a trustworthiness value for an e-service in a given domain can be computed; second, developers in a given domain, where users have a specific IT Security knowledge profile, have guidance on which factors should focus the most to make their website more trustworthy.

Note that trust evolves with time and use of an e-service. In this study, we focus on the factors of trust important at a very early stage, when the user approaches a website for the first time. Also, it is important to mention that trust is not

trustworthiness: trust is an action (someone trusting, someone, or something else), while trustworthiness is a property of someone or something [11]. In this paper we focus on *trust perception*, i.e. the user's perceived trustworthiness of a website. The remaining part of this paper is organized as follows. In Section II we present the related works, in Section III we show the GTPM and the way we obtained it, while in Section IV we explain the trust perception questionnaire design and validation process. In Section V the results of the questionnaire are presented and discussed, while, finally, in Section VI, conclusions are provided.

II. RELATED WORK & FACTORS OF TRUST

Trust has been studied at different levels: individual, interpersonal, relational and societal [24]. This paper focuses on the interpersonal trust ([2], [3], [5], [6]) that has been defined as the "generalized expectancy held by an individual that the word, promise, oral or written statement can be relied on" [25].

Despite claims such as "people trust people, not technology" [26], several human-to-computer trust perception models have been proposed over time [8]–[10], [27]. Muir asserted that trusting computer systems is crucial to use them [9], while Mayer et al. [4] started to look at trust as a multi-dimensional concept, where context and risk represented important dimensions. Atoyan et al. [8] demonstrated that usability is a relevant dimension of trust and that, if it is improved, that also improves trust in the system. Madsen and Gregor divided trust dimensions in two categories: cognition-based (as technical competencies, reliability, and understandability), and affect-based (as personal affinity to the system) [10]. According to Hoffman, security, together with privacy and usability, are amongst the most decisive factors of trust; also, he suggested the importance of finding metrics able to measure the trust level of a system [28].

The recent explosion in the provision of e-service moved the interest of researchers towards on-line transactional systems (websites). According to Camp [29] such systems, to be trusted, need to be 'designed for trust', i.e. accounting for factors such as privacy, security and reliability from the very beginning. Corritore detected reputation, usability and risk as determinant factors of trust in websites [11], while McKnight, focusing on trust in e-commerce services, affirmed that users go through two different stages before using an e-commerce service: an introductory stage, where they decide whether risk to explore the website, and an exploratory stage, where they have to decide whether to make any transaction using it [30]. The quality of a website, such as the absence of presentation flaws, also seems to influence the trust and the willingness to buy in the e-commerce setting [17].

Another factor that seems to be related with trust is the user's knowledge [28]: studies revealed that misconceptions about the technologies used for security and privacy on-line, can lead to a false perception of trust [31]. The influence that such knowledge has on trust is still not clear; some authors assert that having expert knowledge on security mechanisms

decrease the general trust in e-services [32], while others [33] believe that the higher the knowledge, the higher the trust.

Table I shows the results of our literature review: each row represents a TPM and each column a factor of trust; a cross indicates that the factor has been considered by the model. Authors use different terms to refer to the factors of trust, which we try to unify as follows in Table I. The last row of the table indicates the percentage of analyzed TPMs accounting for each factor. We can observe that some of the listed factors refers to properties of the website (e.g. reputation, privacy, security), while others refers to properties of the user (e.g. user's knowledge and disposition to trust).

TABLE I
TRUST PERCEPTION MODELS, LITERATURE REVIEW

Reference	Risk	Reliability & Availability	Third Party Seals	Privacy	User's Knowledge	Security	Disposition to Trust	Quality and Look & Feel	Reputation	Brand Name	Usability
[9]	x	x								x	
[4]	x						x			x	
[8]											x
[10]										x	x
[11]	x		x				x	x	x		
[28]		x		x	x	x			x		x
[29]		x		x		x					
[34]		x					x	x		x	x
[22]					x			x			x
[23]			x					x	x	x	
[14]	x		x		x		x	x	x		
[35]	x	x				x	x	x		x	x
[17]								x			
[36]			x			x					x
[37]	x			x		x	x			x	
[38]			x					x			
[18]			x	x	x	x	x	x	x		
[20]	x			x		x				x	
Rate (%)	39	28	33	28	22	39	39	50	28	44	39

Let us give a brief explanation of the meaning of each factor. *Risk* is expressed as the probability that damages or loss can happen due to the use of a website; *reputation* represents the others' experiences with the website; *privacy* regards the safeguards of the user's personal data; *security* has to do with protection mechanisms such as login or encryption procedures used by the website; and the *usability* assesses how easy is, for the end-user, to accomplish his goals using the website. *Reliability & availability* is a factor representing the probability that the website will perform and maintain its functionalities; *third party seals* refers to the presence of trusted third party logos on the pages of the website; *quality and Look&Feel* is the summation of characteristics such as an overall pleasant aspect of the website, and the absence of spelling and grammatical errors; finally *brand name* says how well the brand behind the website is known. We need to

Fig. 1. General Trust Perception Model (GTPM). Trust Perception (TP) is influenced by the user's characteristics, such as his knowledge (UK) and his disposition to trust (TD), and characteristics of the website, referred as factors of trust.

mention that the *brand name* factor has been obtained merging the factors *competence*, *integrity* and *benevolence*, since these characteristics are often associated to well know brands.

As concerns the factors representing user's characteristics (light gray in the table), the *disposition to trust* is a subjective factor representing the user's general predisposition to trust the world [13], while the *user's knowledge* refers to the expertise the user has about web, risk and security matters (e.g. level of knowledge about internet security, https, digital certificates, reputation system).

III. THE GENERAL TRUST PERCEPTION MODEL

Observing Table I, we can notice how the analyzed TPMs share several factors of trust: *disposition to trust*, for example, is present in half of the models. The aggregation of these factors in a generic trust perception model (GTPM) is important for several reasons [39], amongst them the fact that it provides a single model adaptable to different situations, and that it unifies the work carried out by different studies in different areas. Our GTPM, able to measure $TP(u)$, the user's (u) perception of the trustworthiness (TP) of a website (WB), is presented in Figure 1. Measuring $TP(u)$ can help the user to choose a website based on its trustworthiness, seen as a numerical value, and developers to verify whether their website is trustworthy enough (the user in that case would be a profile of the website's target users). $TP(u)$ can be formalized as follows:

$$TP(u) = \alpha * TD(u) + (1 - \alpha) * T_{WB}(u) \quad (1)$$

$TP(u)$ is built as a weighted ($\alpha \in [0,1]$) average of two components: the user's independent disposition to trust $TD(u)$, and the user's view of the website trustworthiness $T_{WB}(u)$. Several scales are available to measure TD ([3], [40]), while to measure $T_{WB}(u)$ we need to refer to the factors of trust highlighted by our model.

Let FS be the set of factors of trust (the ones above the website block in Figure 1), and $f \in FS$ a specific factor: if

w_f is the weight of the factor f and v_f is its value, then we can define T_{WB} as:

$$T_{WB}(u) = \sum_{f \in FS} w_f(u) * v_f \quad (2)$$

Combining equation (1) and (2) we obtain the following expression to quantify trust perception:

$$TP(u) = \alpha * TD(u) + (1 - \alpha) * \sum_{f \in FS} w_f(u) * v_f \quad (3)$$

To measure T_{WB} we need to know the value and the weight of each factor of our model. Finding metrics able to give values to such factors is part of emerging research topics. Here, the focus is on understanding the factors' weight distribution, which we believe depends on the user's knowledge (hence the notation $w_f(u)$).

Different from others [28], [33] we do not think that knowledge influences trust in a direct (positive or negative) way. We believe, instead, that it determines the higher or lower weight associated to a factor of trust. Essentially, the more the user knows about privacy and security technologies, the more importance he will give to such factors. We expect that users with expert knowledge will give higher weight to factors such as *privacy*, *security* and *reputation* than users with limited knowledge, that will be more interested in factors such as *quality* and *Look&Feel*, *reliability* & *availability* and *usability*. To validate this expectations, in our study we tested the following hypotheses:

Hypothesis 1: The weight of a factor w_f is not the same in every application domain.

Hypothesis 2: The weight of a factor w_f is correlated to the user's knowledge in the IT security field (UK);

IV. METHODS

To empirically verify our hypotheses, an on-line trust perception questionnaire was developed, which addresses the following research questions:

- What level of knowledge in the IT Security field (UK), does a potential user of e-services possess?
- What is the weight the user gives to the different factors of trust? Is it the same for each factor? Is it the same for different application domains (such as e-banking, e-commerce, e-portfolio and e-health)?
- Is the user's IT Security knowledge correlated to the weight given to the factors of trust?

The questionnaire¹ is composed by a total number of 10 questions, divided in three sections: one to gather demographic information about the respondent, one to measure the weight he associates to each factor of trust, and one to evaluate his IT Security knowledge.

The validity of the questionnaire has been shown applying the content validity method [41]. We asked a panel of experts from the TAS³ Consortium to review and rate each item

(question) of the survey. The items rated as *relevant* remained untouched while the others were deleted or adjusted according to reviewers' feedback. A pilot study, monitoring five respondents while answering the questionnaire, was also performed. This helped in rephrasing unclear questions, verifying and eliminating the presence of bias, and adding details to terms seen as vague (e.g. quantifying *very often* to mean *at least once a month*). In the remainder of this section, we discuss the three different parts of the questionnaire, named the *sample frame*, the *factors' importance*, and the *users' knowledge*.

A. The Sample Frame

The population of our survey is represented by users of e-services such as e-banking, e-commerce, e-portfolio and e-health. The "Digital Report 2009" [42] reveals that 89% of Dutch internet users, aged 25-44, use e-banking services; that the typical on-line shopper is high-educated, aged 25-44; that 19% (aged 12-74) use the Internet to look for a job; and that 30%, aged 55-64, surf the web to look for health-related information. This let us to believe that employees and students of the Eindhoven University Technology (TU/e), chosen as sampling frame for our survey, well represent the population of *e-users*. Moreover, they cover the spectrum of knowledge since both, people with low and high IT Security expertise, are part of the sample. The TU/e has about 6000 students and 4000 employees (PhD students are considered as employees). To obtain enough responses, statistically significant results, and to account for lost e-mails and uncooperative subjects, 1600 e-mails were sent to addresses randomly selected from the TU/e internal mailing list. During the sample selection the percentage of students (about 60% of the whole) and staff (about 40% of the whole) has been maintained. The first part of the survey contains questions about gender, age, educational level, and job position of the respondents to help us in verifying whether the respondents group reflects the sampling frame of our study.

B. Factors' Importance

Another part of the questionnaire is the one aiming at measuring the weight the users give to each factor of trust. This is done by verifying how much attention users dedicate to each of them. Respondents were presented with a service usage scenario in each of the settings (e-banking, e-commerce, e-portfolio and e-health) and asked to answer questions assuming it was the first time they used the specific service.

Questions were formulated in such a way as to verify the influence each factor has on trust perception. To test the importance of the factor *quality* and *Look&Feel*, for example, we ask to the user whether the design aspects of the website (e.g. attractive colors), or professional icons, influence his trust in it. Let Q_f be the set of questions used to measure the weight of the factor f . For each question $q \in Q_f$, respondents were allowed to choose amongst four optional answers: *never*, *almost never*, *very often*, and *always*; to each option is associated a numerical value: (in the order) 0.00, 0.33, 0.66, 1.00. The value of the answer to the question q

¹A copy of the questionnaire is available on-line at http://security1.win.tue.nl/~ecostant/Trustworthiness_Perception.pdf

is denoted as v_q . To compute the weight w_f of each factor $f \in FS$, we first compute its score, as an average of the answers given to each question q in Q_f ; then, the score is scaled to sum up to 1. In formulas:

$$score_f = \frac{1}{|Q_f|} \sum_{q \in Q_f} v_q \quad (4)$$

$$w_f = \frac{score_f}{\sum_{f \in FS} score_f} \quad (5)$$

C. The User's Knowledge (UK)

Questions in this part of the questionnaire aim to understand the user's knowledge in the IT Security field. Users are asked to judge their own knowledge and ability on IT security-related topics, such as computer and internet usage, privacy policies, https, pki, reputation, and digital certificates. A four-item scale is used for the answers (each item has a numerical value associated): *no knowledge* (0.00), *limited Knowledge* (0.33), *good knowledge* (0.66), and *expert knowledge* (1.00). The global UK is computed as average of the values associated to the answers.

V. RESULTS

A web interview methodology was chosen for our survey: respondents, selected by our random procedure, received an e-mail, and a reminder one week later, explaining the scope of our research and inviting them to participate to our on-line questionnaire. In the e-mail, they were informed of the anonymous nature of the questionnaire.

A total of 335 valid responses were collected. Responses presenting missing values were ignored since their percentage was below the 20% and this, as indicated in [43], does not effect our final results. To check the presence of CMV (Common Method Variance), i.e. the "variance attributable to the measurement method rather than to the constructs the measures represents" [44]), Harman's one-factor test was conducted. No single factor with covariance bigger than 50% emerged from the test, indicating that CMV does not constitute a problem for our study.

A. The Sample

Our respondents group is composed of 76% male and 24% female, which reflects the overall population at TU/e. The age distribution, divided for gender, is the one presented in Figure 2: the graph shows the percentage of the male component (respectively the female) falling in each of the age categories. In each category men and women are more or less equally represented but there is a lack of respondents aged 65 or older: this is mostly due to the fact that retired people were not invited to fill the questionnaire.

Figure 3 shows the education level accomplished by our respondents: assuming that persons who already got a master degree are employees at the TU/e, we can say that 60% of our sample is formed by students and 40% by employees, matching the sample frame.

Fig. 2. Respondents age distribution. The graph shows the percentage of male and female for each age range.

Fig. 3. Education level accomplished by the respondents.

B. Factors' Importance

Results of our experiment confirm that the weight of a factor of trust is not the same in different application domains (hyp. 1). The graph in Figure 4 represents the factors ranking in two of the different scenarios we considered: e-banking (Figure 4(a)) and e-commerce (Figure 4(b)). Below we describe notable results, and provide possible explanations.

In the e-banking domain, the factor that influences the perception of trust the most is the *brand name*: this supports the theory that trust in traditional banking influences trust in the online bank [19]. As expected, another factor of trust is represented by the presence of *security* mechanisms: 89% of our respondents asserted they verify (always or very often) that the online banking transactions are carried out through the HTTPS protocol. Furthermore, *reliability and availability* appears to be essential for e-banking environment: frequent error messages and crashes influence the feeling of trust towards the online bank. The presence of *trusted seals* and the *risk* associated to the use of the website, have the same importance, exceeded by the *Look&Feel* of the bank's website that is considered more important.

Surprisingly, the factors *reputation* and *privacy* do not seem to considerably influence user's perception of trust. It appears that users do not look for third party opinions about their online bank: 59% of our respondents said they never (or almost never) verify the reputation of the e-banking service provider and 45% does not bother to ask their friends about what kind of experience they had with the on-line bank. This can be explained by the fact that users do not like to manually collect and evaluate feedback on their own, but not necessary that they

Fig. 4. Factors ranking in the e-banking (a) and e-commerce (b) settings.

would not like to use automatic systems providing them with the reputation of the service (a fact confirmed by the success of reputation systems such as Tripadvisor ²). Another reason for the low importance given to *reputation* in e-banking can be that users trust the brand and, then, the on-line version too, so that they do not have to check *reputation*.

The *privacy* factor needs special attention: in all the scenarios we analyzed, its weight is never higher than 0.05. This result can be misleading, letting us think that users do not care about privacy. Actually, most of the respondents said they never read the privacy policy stated by a website. This does not necessarily mean users are not interested in their privacy but, most probably, that mechanisms currently used to address the privacy issue (privacy policies above all) are not usable enough. Privacy policies, indeed, are too long, written in a complex language, which is difficult to understand, and for this reason they are just ignored by the users. This result suggests that new mechanisms, easy to use and allowing the user to understand how good or bad a privacy policy is, are necessary.

In the e-commerce settings, the factors' ranking is different from the one presented in the e-banking scenario, with a slightly more uniform weight distribution. The most important factor is the *reliability and availability*, followed by *brand name*. It is interesting to note how users care more about the aspects of a website (*Look&Feel*) than about its *security* mechanisms: their trust is influenced by a good-looking web site from a well known firm that works good. The *risk* factor is a bit more important than in the e-banking, and *third party seals* is almost as important as in the e-banking environment. *Privacy* and *reputation* are still at the bottom of the list.

A comparative graph, showing the factors' ranking differences amongst the domains we analyzed is presented in Figure 5. The graph is divided into three bands of equal width, defining the importance of a factor as low, medium or high. We can observe that the *brand name* is especially high in the e-banking scenario, maybe because a strong connection between on-line and off-line organizations mainly exists with banks. *Usability* gains importance in the e-portfolio and e-health, we think because users expect more usability for this

kind of services, that are still not so popular. E-banking and e-commerce, indeed, have almost *de facto standard* features (e.g. wish-lists or carts) that help users in understanding how a website works even if they never used it before. This is not true with the newborns e-health and e-portfolio services.

The *quality and Look&Feel* is considered very important in the e-portfolio, at cost of *risk* and *third party seals*, slightly lower for the e-portfolio but almost constant elsewhere. The factor *reputation*, is also almost uniform in all the domains we considered, but in the e-commerce, where it is more important probably because it is the domain with the highest presence of automatic reputation systems (e.g. eBay, Tripadvisors). For the reasons explained before, *privacy* is the only factor occupying the low band in each scenario, while *reliability and availability* is always in the high band, suggesting that, to get the user's trust, it is very important to have an always-available, error-free service.

Although *security* is one of the most important factors in e-banking and e-commerce, its weight drops in the e-health and e-portfolio domains. This is counterintuitive since both the domains, especially the e-health, manage extremely sensitive data. In these domains, users should require much stronger security mechanisms. The following observations might help in explaining this phenomenon: i) e-health and e-portfolio are still not well known services, and, although our respondents have been provided with an example of use, only a low percentage of them (1.5% for e-health and 15.8% for e-portfolio) had previously used, at least one time, such services (versus the 96.7% of e-banking and 71.9% of e-commerce); ii) since sensitive data are collected in such domains, users may assume that the service providers will be specialist of the sector in which they have a pre-built trust (e.g. hospitals or government institution). However, further analysis are required to clarify why *security* is not considered as important as expected in these domains.

C. The User's Knowledge

To measure the user's knowledge we considered the ten questions on the IT Security topics, as explained in Section IV-C. The Cronbach's alpha test was conducted to calculate the reliability of the scale. The item-total correlation is above 0.5 for each item (values above 0.3 are acceptable) and the

³<http://www.tripadvisor.com/>

Fig. 5. Factors' ranking in the different application domains (e-banking, e-commerce, e-health and e-portfolio).

Cronbach's alpha value, for all the items we used to build UK, is 0.9, proving the reliability of our scale.

UK has been computed summing the value associated to each answer, and then dividing the sum by the number of items. The minimum registered value for UK (ranging in [0,1]) was 0.07, and the maximum 0.87. A correlation analysis between the weight of the factors and the user's class of knowledge, was carried out and the results are presented in Table II. We used the Sperman's non-parametric correlation test since the normal distribution assumption was not verified by our sample.

TABLE II
SPEARMAN'S CORRELATION TEST

	e-banking	e-commerce	e-health	e-portfolio
Brand Name	0.093	0.065	0.022	0.063
Usability	-0.169*	-0.184*	-0.114*	-0.127*
Look & Feel	-0.158**	-0.156**	-0.051	-0.119**
Privacy	0.119*	0.120*	0.177**	0.210**
Rel. & Avail.	-0.164**	-0.224**	-0.183**	-0.185**
Reputation	-0.072	0.043	0.078	0.047
Risk	0.088	0.125*	0.008	0.087
Security	0.183*	0.249**	0.116*	0.197**
Third Party Seals	0.110*	0.043	0.021	0.019

* = Correlation is significant with $p < 0.05$
** = Correlation is significant with $p < 0.01$

Table II shows that a correlation amongst the weight of each factor and UK, does exist for *usability*, *quality and Look&Feel* (excluding the e-health context), *privacy*, *reliability & availability*, and *security*, while this has not been confirmed for *brand name*, *reputation*, *risk* (excluding the e-commerce context) and *third party seals* (excluding the e-banking context). Note that *risk*, *reputation* and *third party seals*, constant over domains, are also constant over knowledge, showing no correlation.

Observing the graphs in Figure 6, obtained using a clustering technique to classify the user according to his knowledge, we can conclude that users with no or limited knowledge tend to put more attention on factors such as *reliability & availability*, *Look&Feel*, *usability*, and *brand name*. At the increasing of the knowledge level, also the importance associate to factors such as *security*, *risk* and *privacy* increases.

The fact that the weight of privacy increases with knowledge support the idea that current privacy mechanisms are not easy to be understood and therefore require much knowledge. The graph shows the results for the e-commerce domain but the trend is the same for the other domains according to the correlation coefficients shown in Table II.

Fig. 6. The weight distribution of the factors of trust, clustered for class of knowledge, in the e-commerce domain.

VI. CONCLUSIONS

In this paper we analyzed the user's perception of trust. Based on the existing trust perception models (TPMs) taken from Literature, we developed a general trust perception model (GTPM) that contains a comprehensive set of trust factors. The GTPM can be used to measure the user's perception of the trustworthiness of a website, in different application domains. Also, we argued that trust perception is influenced by the user's knowledge in the IT Security field and, specifically, we hypothesized that such knowledge influences the importance users give to the different factors of trust. The results of a user study, aiming at investigating the main hypotheses of our research, have been presented, confirming that the weight of a factor changes according to the application domain (hyp. 1) and to the user's knowledge (hyp. 2). Particularly, the weight of *privacy* and *security* increases with the knowledge, while for *reliability & availability*, *usability*, and *Look&Feel* the weight decreases where the knowledge increases.

To the best of our knowledge this is the first attempt to quantify the user's perception of trust; while previous studies are limited to identify the set of factors influencing trust, we focused on quantifying the importance associated to each factor in a given application domain. The results of our study can be useful to website developers, to focus on the elements that need to be addressed to make a site trustworthy. Moreover, this work can be considered as a first step towards a trustworthiness evaluation process: once detected the important factors and their weight, researchers can look at ways to find metrics to measure the factors and to quantify the trustworthiness of a website.

Note that in our questionnaire, we did not account for the *disposition to trust*. This has mainly been done to keep the questionnaire short enough to avoid a big drop in responses. Measuring the user's disposition to trust, e.g. using Rotter's scale [3], and investigating its relationships with the ranking

of the trust factors, would represent an interesting future work. A limitation of our work regards the question used to assess the privacy's weight: we asked the users whether they read the privacy policy stated by a service provider. To get a real view on the privacy one should reformulate this question and ask, for example, whether the way service providers address users privacy influences his trust in the website. Finally, we want to observe that users were provided with a scenario of the e-services they were supposed to use and not with real on-line services; we are considering to compare the results we obtained in this way with those that can be obtained after users experienced a real e-service in each of these domains.

REFERENCES

- [1] L. Mui, M. Mohtashemi, and A. Halberstadt, "A computational model of trust and reputation," in *System Sciences, 2002. HICSS. Proceedings of the 35th Annual Hawaii International Conference on System Sciences*. IEEE, 2002, pp. 2431–2439.
- [2] M. Deutsch, *Cooperation and trust: Some theoretical notes*. Lincoln: Univer. Nebraska Press, 1962, pp. pp. 275–320.
- [3] J. Rotter, "Generalized expectancies for interpersonal trust," *American psychologist*, vol. 26, no. 5, p. 443, 1971.
- [4] R. Mayer, J. Davis, and F. Schoorman, "An integrative model of organizational trust," *The Academy of Management Review*, vol. 20, no. 3, pp. 709–734, 1995.
- [5] D. Gambetta, "Can we trust trust," *Trust: Making and Breaking Cooperative Relations, electronic edition, Department of Sociology, University of Oxford*, pp. 213–237, 2000.
- [6] C. Johnson-George and W. Swap, "Measurement of specific interpersonal trust: Construction and validation of a scale to assess trust in a specific other," *Journal of Personality and Social Psychology*, vol. 43, no. 6, p. 1306, 1982.
- [7] J. Ermisch, D. Gambetta, H. Laurie, T. Siedler, and S. Noah Uhrig, "Measuring people's trust," *Journal of the Royal Statistical Society: Series A (Statistics in Society)*, vol. 172, no. 4, pp. 749–769, Oct. 2009.
- [8] H. Atoyian and J. Duquet, "Trust in new decision aid systems," in *Proceedings of the 18th Francophone Conference on Human Computer Interaction*. ACM Press, 2006, pp. 115–122.
- [9] B. Muir, "Trust between humans and machines, and the design of decision aids," *International Journal of Man-Machine Studies*, vol. 27, no. 5-6, pp. 527–539, Nov. 1987.
- [10] M. Madsen and S. Gregor, "Measuring human-computer trust," in *Proceedings of the 11th Australasian Conference on Information Systems*, 2000, pp. 6–8.
- [11] C. Corritore, B. Kracher, and S. Wiedenbeck, "On-line trust: concepts, evolving themes, a model," *International Journal of Human-Computer Studies*, vol. 58, no. 6, pp. 737–758, Jun. 2003.
- [12] D. McKnight, V. Choudhury, and C. Kacmar, "Developing and validating trust measures for e-commerce: An integrative typology," *Information systems research*, vol. 13, no. 3, pp. 334–359, Sep. 2003.
- [13] D. McKnight and N. Chervany, "What trust means in e-commerce customer relationships: an interdisciplinary conceptual typology," *International Journal of Electronic Commerce*, vol. 6, no. 2, pp. 35–59, 2001.
- [14] D. McKnight, V. Choudhury, and C. Kacmar, "Trust in e-commerce vendors: a two-stage model," in *Proceedings of the twenty first international conference on Information systems*. Association for Information Systems, 2000, pp. 532–536.
- [15] D. McKnight, L. Cummings, and N. Chervany, "Initial trust formation in new organizational relationships," *The Academy of Management Review*, vol. 23, no. 3, pp. 473–490, Jul. 1998.
- [16] A. Kini and J. Choobineh, "Trust in electronic commerce: definition and theoretical considerations," in *HICSS (4)'98*. Published by the IEEE Computer Society, 1998, pp. 51–61.
- [17] A. Everard and D. Galletta, "Effect of Presentation Flaws on Users Perception of Quality of On-Line Stores Web Sites: Is it Perception that Really Counts?" *Second Annual Workshop on HCI Research*, p. 60, 2003.
- [18] C. Hsu, "Dominant Factors for Online Trust," in *International Conference on Cyberworlds 2008*. IEEE, Sep. 2008, pp. 165–172.
- [19] K. Lee, I. Kang, and D. McKnight, "Transfer from offline trust to key online perceptions: an empirical study," *IEEE Transactions on Engineering Management*, vol. 54, no. 4, pp. 729–741, Nov. 2007.
- [20] S. Yousafzai, J. Pallister, and G. Foxall, "A proposed model of e-trust for electronic banking," *Technovation*, vol. 23, no. 11, pp. 847–860, Nov. 2003.
- [21] A. Fruhling and S. Lee, "The influence of user interface usability on rural consumers' trust of e-health services," *International journal of electronic healthcare*, vol. 2, no. 4, pp. 305–321, 2006.
- [22] S. Faja and A. Likcani, "E-Health: An Exploratory Study of Trust Building Elements in Behavioral Health Web Sites," *Journal of Information Science and Technology*, vol. 3, no. 1, 2006.
- [23] E. Silience, P. Briggs, P. Harris, and L. Fishwick, *Developing trust practices for e-health*. London: IGI Global, 2007, ch. X, pp. 235–258.
- [24] K. Kelton, K. Fleischmann, and W. Wallace, "Trust in digital information," *Journal of the American Society for Information Science and Technology*, vol. 59, no. 3, pp. 363–374, 2008.
- [25] J. B. Rotter, "Interpersonal trust, trustworthiness, and gullibility," *American Psychologist*, vol. 35, no. 1, pp. 1–7, 1980.
- [26] B. Friedman, P. H. Khan, and D. C. Howe, "Trust online," *Communications of the ACM*, vol. 43, no. 12, pp. 34–40, Dec. 2000.
- [27] J. D. Lee and K. a. See, "Trust in automation: designing for appropriate reliance," *Human factors*, vol. 46, no. 1, pp. 50–80, Jan. 2004.
- [28] L. J. Hoffman, K. Lawson-Jenkins, and J. Blum, "Trust beyond security," *Communications of the ACM*, vol. 49, no. 7, pp. 94–101, Jul. 2006.
- [29] L. Camp, "Designing for trust," *Trust, Reputation, and Security: Theories and Practice*, vol. 35, no. 3, pp. 239–251, Apr. 2003.
- [30] D. H. McKnight, C. J. Kacmar, and V. Choudhury, "Shifting Factors and the Ineffectiveness of Third Party Assurance Seals: A Two-Stage Model of Initial Trust in a Web Business," *Electronic Markets*, vol. 14, no. 3, pp. 252–266, Sep. 2004.
- [31] S. Flinn and J. Lumsden, "User perceptions of privacy and security on the web," in *The Third Annual Conference on Privacy, Security and Trust (PST 2005)*, 2005.
- [32] D. Hoffman, T. Novak, and M. Peralta, "Building consumer trust online," *Communications of the ACM*, vol. 42, no. 4, pp. 80–85, 1999.
- [33] J.-C. Jiang, C.-A. Chen, and C.-C. Wang, "Knowledge and Trust in E-consumers' Online Shopping Behavior," in *2008 International Symposium on Electronic Commerce and Security*. IEEE, 2008, pp. 652–656.
- [34] A. L. Fruhling and Sang M. Lee, "The influence of user interface usability on rural consumers' trust of e-health services," *International Journal of Electronic Healthcare*, 2006.
- [35] A. Kini and J. Choobineh, "An Empirical evaluation of the factors affecting trust in web banking systems," in *Americas Conference on Information System*, 2000, pp. 185–191.
- [36] B. Suh and I. Han, "The Impact of Customer Trust and Perception of Security Control on the Acceptance of Electronic Commerce," *International Journal of Electronic Commerce*, vol. 7, no. 3, pp. 135–161, 2003.
- [37] C. M. K. Cheung and M. K. O. Lee, "An integrative model of consumer trust in internet shopping," in *European Conference on Information Systems*, 2003.
- [38] K. Jones, "Trust in consumer-to-consumer electronic commerce," *Information & Management*, vol. 45, no. 2, pp. 88–95, Mar. 2008.
- [39] F. Li, D. Piekowski, A. van Moorsel, and C. Smith, "The Establishment of End-user Trust in Web Information Management Systems," in *2010 Second International Conference on MultiMedia and Information Technology*. IEEE, 2010, pp. 314–317.
- [40] R. Christie and F. Geis, *Studies in machiavellianism*. Academic Pr, 1970.
- [41] M. Lynn, "Determination and quantification of content validity," *Nursing Research*, vol. 35, no. 6, p. 382, 1986.
- [42] Statistics Netherlands, "The digital economy 2009," 2009. [Online]. Available: <http://www.cbs.nl/NR/rdonlyres/E4311D6B-6BE6-4996-A4AB-804FC0A07A4C/0/2009p38pub.pdf>
- [43] R. a. Mcdonald, P. W. Thurston, and M. R. Nelson, "A Monte Carlo Study of Missing Item Methods," *Organizational Research Methods*, vol. 3, no. 1, pp. 71–92, Jan. 2000.
- [44] P. M. Podsakoff, S. B. MacKenzie, J.-Y. Lee, and N. P. Podsakoff, "Common method biases in behavioral research: a critical review of the literature and recommended remedies," *Journal of Applied Psychology*, vol. 88, no. 5, pp. 879–903, 2003.