A Survey of Trust and Risk Metrics for a BYOD Mobile Worker World

Jean-Marc Seigneur
University of Geneva
Switzerland
Jean-Marc.Seigneur@trustcomp.org

Petra Kölndorfer, Marc Busch, Christina Hochleitner
Center for Usability Research and Engineering
Vienna, Austria
koelndorfer@cure.at

***Abstract*—Users increasingly access corporate data from their own devices and public wireless networks such airports Wi-Fi or coworking offices. On one hand, more work is possible, but on the other hand, it is riskier because the devices and locations may be untrustworthy. However, the Bring-Your-Own-Device trend is a fact and it is the reason we survey in this paper how computational trust and risk metrics may help mitigating those new risks in a more dynamic way than in the past. An online survey that we have carried out confirms that users do not take care of security risks as they are communicated today and that new Human Computer Interfaces combined with opportunity-enabled risk management are needed to improve the situation.**

Keywords-trust; risk; Bring-Your-Own-Device

I. INTRODUCTION

Corporate users increasingly use computing environments in many other places than the corporate offices, accessing corporate information from homes, airports, conferences, etc. They are mobile workers who need to access remote corporate assets often from their own devices as part of the Bring-Your-Own-Device (BYOD) trend. Moreover, there are more and more projects where different companies and contractors have to collaboratively work together. Thus, the trustworthiness in both employees and external collaborators, who have no direct employment contract with the company of the Chief Security Officer (CSO), has to be taken into account in a more dynamic way. The computing environments are not fully controlled by the corporate IT administrators and new metrics to dynamically assess the trustworthiness of computing environments are needed.

It is the reason that we survey in this paper how computational trust management may be used to dynamically make access control decisions based on the level of trust and current risk. This work is part of an EU-funded FP7 project called MUSES [1], which aims at combining both the trust in requesting users and the trust in their current computing environments to decide whether or not the request should be granted. The survey has a section on Human Computer Interface (HCI) because reporting the results of those trust and risk metrics evaluations to the end-user in the most appropriate usable ways is very important to influence its future security behavior, especially as the result of an online questionnaire on Wi-Fi risks that we have carried out underlines that even security aware users do not care about the security risks they encounter.

This paper is organized as follows. In Section 2, an overview of computational trust and risk is given. Then, Section 3 explains why traditional risk management based only on threats is not suitable for BYOD mobile worker environments where work opportunities must also be taken into account even outside of the company. Section 4 discusses what kind of new HCI for risk and trust is needed. Section 5 concludes and underlines future work.

II. COMPUTATIONAL TRUST AND RISK OVERVIEW

This section first presents the computational models based on the human notion of trust and then describes the main components of a computational trust engine.

A. Computation Based on the Human Notion of Trust

In the human world, trust exists between two interacting entities and is very useful when there is uncertainty in result of the interaction. The requested entity uses the level of trust in the requesting entity as a mean to cope with uncertainty, to engage in an action in spite of the risk of a harmful outcome. There are many definitions of the human notion trust in a wide range of domains, with different approaches and methodologies: sociology, psychology, economics, pedagogy, etc. These definitions may even change when the application domain changes. However, it has been convincingly argued that these divergent trust definitions can fit together [2]. Romano's definition tries to encompass the previous work in all these domains: *"trust is a subjective assessment of another's influence in terms of the extent of one's perceptions about the quality and significance of another's impact over one's outcomes in a given situation, such that one's expectation of, openness to, and inclination toward such influence provide a sense of control over the potential outcomes of the situation"* [3].

Interactions with uncertain results between entities also happen in the online world. So, it would be useful to rely on trust in the online world as well. However, the terms trust, trusted, trustworthy and the like, which appear in the traditional computer science literature, have rarely been based on these comprehensive multi-disciplinary trust models and often correspond to an implicit element of trust – a limited view of the facetted human notion of trust. Trusted computing is important to try to better know if a computing platform is trustworthy. Krishna and Varadharajan [4] have proposed a model that encompasses the notions of 'hard' and 'soft' trust to determine whether a platform can be trusted for authorisation. Blaze et al. [5] coined the term "decentralized trust management" because their approach separates trust management from application: their PolicyMaker introduced

 ISBN: 978-1-61208-312-4

the fundamental concepts of policy, credential, and trust relationship. Terzis et al. [6] argued that this model of trust management still relies on an implicit notion of trust because it only describes *"a way of exploiting established trust relationships for distributed security policy management without determining how these relationships are formed"*.

A computational model of trust based on social research was first proposed by Marsh [7]. In social research, there are three main types of trust: interpersonal trust, based on past interactions with the trustee; dispositional trust, provided by the trustor's general disposition towards trust, independently of the trustee; and system trust, provided by external means such as insurance or laws [2]. Trust in a given situation is called the trust context. In Marsh's model, each trust context is assigned an importance value in the range [0,1] and utility value in the range [-1,1]. Any trust value is in the range [-1,1), from very untrustworthy to very trustworthy. In addition, each virtual identity is assigned a general trust value, which is based on all the trust values with this virtual identity in all the trust contexts. Dispositional trust appears in the model as the basic trust value: it is the total trust values in all contexts in all virtual identities with whom the trustor has interacted so far. Risk is used in a threshold for trusting decision making.

A number of other major trust models have followed Marsh's one [8]–[11]. Castelfranchi and Falcone [12] argue for a trust engine based on cognitive science where the main trust evidence type comes from the entity's belief and goals structure rather than probabilistic quantitative views, economics or game theory. Evidence encompasses outcome observations, recommendations and reputation. A trust metric consists of the different computations and communications, which are carried out by the trustor (and his/her network) to compute a trust value in the trustee. Sabater and Sierra [13] also remarked that *"direct experiences and witness information are the 'traditional' information sources used by computational trust and reputation models"*. Depending on the application domain, a few types of evidence may be more weighted in the computation than other types. When recommendations are used, a social network can be reconstructed. Reputation has been defined as follows : *"Reputation is the subjective aggregated value, as perceived by the requester, of the assessments by other people, who are not exactly identified, of some quality, character, characteristic or ability of a specific entity without taking into account direct previous interactions with the entity"* (adapted from [14]). However, to be able to perceive the reputation of an entity is only one aspect of reputation management. The other aspects of reputation management for an entity consist of:

- Monitoring the entity reputation as broadly as possible in a proactive way;
- Analysing the sources spreading the entity reputation;
- Influencing the number and content of these sources to spread an improved reputation.

Golbeck and Hendler [15] studied the problem of propagating trust value in social networks, by proposing an extension of the Friend-Of-A-Friend (FOAF) vocabulary and algorithms to propagate trust values estimated by users rather than computed based on a clear count of pieces of evidence. The propagation of trust in peer-to-peer networks has been studied by Despotovic and Aberer [16] who introduced a more efficient algorithm to propagate trust and recommendations in terms of computational overhead.

B. Evidence-Based Trust and Risk Engine

The EU-funded (SECURE) project [17] represents an example of a trust engine that uses evidence to compute trust values in entities and corresponds to evidence-based trust management systems. As depicted in Figure 1 below, the decision-making component can be called whenever a trusting decision has to be made. Most related work has focused on trust decision-making when a requested entity has to decide what action should be taken due to a request made by another entity, that is, the requesting entity. It is the reason that a specific module called Entity Recognition (ER) [18] is represented to recognise any entities and to deal with the requests from virtual identities. Relying on recognition rather than strong authentication is also better from a privacy point of view because there is no mandatory required link to the real-world identity of the user. Models to trade privacy for trust [19] have even been proposed.

It may happen that the trusting decision is not triggered by any requesting virtual identity, for example, when the user wants to select the most trustworthy used car dealer, or that other type of evidence, such as the level of system trust at time of decision, are more important than the involved virtual identities.

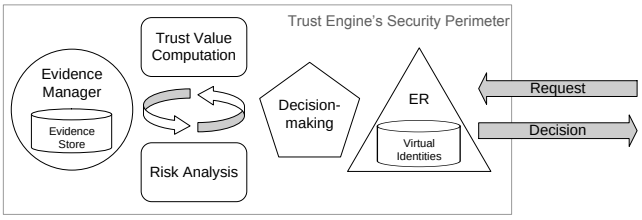

Figure 1. High-level View of a Trust Engine

The decision-making of the trust engine uses two sub-components:

- a trust module that can dynamically assess the trustworthiness of the requesting entity based on the trust evidence of any type stored in the evidence store;
- a risk module that can dynamically evaluate the risk involved in the interaction, again based on the available evidence in the evidence store.

A common decision-making policy is to choose (or suggest to the user) the action that would maintain the appropriate cost/benefit. In the background, the evidence manager component is in charge of gathering evidence (e.g., recommendations, comparisons between expected outcomes of the chosen actions and real outcomes, etc.) This evidence is used to update risk and trust evidence. Thus, trust and risk follow a managed life-cycle.

Dimmock, who took care of the risk module in the SECURE project, concludes in his PhD thesis that more

 ISBN: 978-1-61208-312-4

work with regard to the risk of the situation must be done and especially with regard to the time element of risk: *"one area that the framework does not currently address in great detail is the notion of time"* [20]. A recent survey of trust models for multi-agent systems still underlines that *"among these trust models, risk received the least attention. The element of risk is a very critical factor for each interaction; hence, there is a need to incorporate more consideration for risk in designing future trust models."* [21]

III. RISK AS PART OF THREAT MODELLING WITH OPPORTUNITIES IN MIND

Risk management is a broad field applied in many other application domains than Information Technology (IT), for example, nuclear power plants, with many different methodologies. Fortunately, in 2005 the European Network and Information Security Agency (ENISA) set up an ad hoc Working Group on "*Technical and Policy Aspects of Risk Assessment and Risk Management"* involving experts from eight Member States who cooperated through regular meetings within eight months. They produced an overview of existing risk methodologies and the relevant players in this field, and comparison of the different methodologies [22]. We have adapted below previous work for our BYOD mobile worker application domain.

A. Threat Modelling

ISO 27005 (information security risk management) underlines that risk management in the information security application domain relies on threat modelling. As Shostack [23] underlines there are three main types of threat modelling approaches:

- Asset-driven threat modelling focuses on the assets that attackers may attack include how they could attack them. Unfortunately digital data can be attacked in many different ways and any piece of software, network or hardware may become considered as assets.
- Attacker-driven threat modelling focuses on understanding the capabilities of the potential attackers would want to attack. It works well for *"a foreign army with a known strategic doctrine, physical world limits, and long-lead-time weapons systems development. This works less well when your adversary is a loosely organized group of anonymous hackers."* [23]
- Design-driven threat modelling is threat modelling based on where the security perimeter of software components where diagrams are drawn at design time to understand what can go wrong with each component following the STRIDE threat model (Spoofing, Tampering, Repudiation, Information disclosure, Denial of Service and Elevation of Privilege) [24] with two tools provided by Microsoft. Microsoft TAM (Threat Analysis and Modelling) is more dedicated to software applications than the more generic Microsoft Security Development Lifecycle (SDL) threat modelling tool (but that requires Visio). In TAM, risk is computed by multiplying the importance level by the probability level, whose levels go from low (1), medium (2) to high (3).

Although in this paper the assets are more related to corporate assets, we define an asset as anything that has value to the owner, which is an adaption of the definition of asset in ISO/IEC IS 13335-1 [25] where owner is replaced by organisation. An asset may be tangible or intangible, hardware, software, data, buildings, infrastructure, but also products, knowledge resources, customer relationships or reputation.

The ISO/IEC Guide 73 [26] defines an event as an occurrence of a particular set of circumstances. The event can be certain or uncertain. The event can be a single occurrence or a series of occurrences. Although this guide uses the term consequence rather than outcome that is the term used in the SECURE trust engine, the ISO/IEC Guide 73 [26] defines that there can be more than one outcome from one event. Outcomes can range from positive to negative and be expressed qualitatively or quantitatively.
According to ISO/IEC IS 13335-1 [25] where negative consequence is replaced by harm, a threat is any action or event with the potential to cause negative outcome(s). *"Sources of threats could be vandalism, espionage or just human mistakes and accidents. In the two first cases the strength of the threat can result from two major factors: the motivation of the threat and the attractiveness of the asset"* [25].

However, one report on the consumerisation of IT from the ENISA [27] underlines a major aspect that has not been taken into account in standard threat methodologies: *"As regards opportunities, due to missing standardised definitions"* [27]. There may be also positive consequences of an action or event and risk management tends to focus on negative outcomes and negative events, i.e., threats. Unfortunately, the BYOD trend is spreading in corporate environments because it brings many opportunities with beneficial outcomes: work from anywhere, fewer unproductive paid times, etc. Thus, based on the ENISA [27] report, we have defined opportunity as any action or event with the potential to cause positive outcome(s). However, this definition deviates from the definition of IT security risk of another ENISA report [22]: *"IT security risk is composed of an asset, a threat and vulnerability: if one of these items is irrelevant, then there is no IT security risk to encounter"* that does not take into account the positive outcomes and opportunities as underlined in the other ENISA report [27]. Concretely taking into account opportunities in addition to threats is a main innovative aspect of our work.

ISO/IEC IS 13335-1 [25] defines vulnerability as a weakness of an asset that can be exploited by one or more threats. *"Vulnerabilities can exist in all parts of an IT system, e.g., in hardware or software, in organizational structures, in the infrastructure or in personnel"* [25].

 ISBN: 978-1-61208-312-4

We use the ENISA [22] definition of probability: the extent to which an event is likely to occur.

B. Balancing Threats Costs and Benefits of Opportunities

Based on the above remark regarding the importance of allowing opportunities in the BYOD mobile worker application domain and above definitions, we have adapted the definition of risk from ISO/IEC 13335-1 [25] where probability is replaced by potential, owner by organization and opportunities are not taken into account. Hence, risk is the combination of the probability that a given threat will successfully exploit vulnerabilities of an asset or group of assets with the cost of the negative consequences to the owner balanced with the benefit of the positive consequence of an available opportunity.

Then, we have adapted the ENISA [22] definition of an incident: a security incident is an event that has been assessed as having an actual or potentially adverse effect on the security or performance of a system.

The ISO/IEC Guide 73 [26] defines the risk estimation process as the process to assign values to the probability and consequences of a risk. It can consider cost, benefits, the concerns of stakeholders and other variables, as appropriate for risk evaluation. In our MUSES project context, the probability that a user would like to access a company asset when the user makes the request to access such request is 1 because the user has already made the request. The benefit of letting the user accessing the asset could be computed based on the hourly cost of the user, who otherwise could not work, for example, because the user is at an airport without other opportunities to work if she has not access to this company asset. Regarding the value of the asset, it may also be estimated a priori, for example, the value of the confidential documents required for a patent proposal may be estimated a priori (although it may take some time to gather all information regarding how much benefits could be generated from this patent). Unfortunately, estimating the probability of putting in danger the company asset due to all the probable threats due to the vulnerabilities is much more difficult because the list of vulnerabilities and threats may be hard to collect and depending on the company more or less attackers may be trying to attack the current user device.

A second important paradigm shift that happens in MUSES application domain rather than in traditional risk management domains is that MUSES has specific modules that will compute in real-time the current context, including for a mobile device to detect being under attack, and store risk evidence both locally and with other MUSES peers, thus allowing real-time computation of the probabilities of a threat that would successfully exploit a vulnerability and compromise the asset. In traditional risk methodologies, after the risks have been estimated, the risk of a harmful outcome may be so low that it may be taken in order to reap the benefits with high probability or treatments to reduce risks may be considered such as mitigation with new security mechanisms or transfer to another context. For example, in MUSES, the phase of informing the user who is willing to access a company asset from a remote location may be informed that it should rather stop from the Starbucks airport Wi-Fi and go to the nearby airport business lounge, which is known to be more secure. The phase of informing the user is an important part and usually called *"risk communication"* [22]. It is the reason we adopt the two following remaining definitions from ISO/IEC Guide 73:

- Risk Communication: A process to exchange or share information about risk between the decision-maker and other stakeholders. The information can relate to the existence, nature, form, probability, severity, acceptability, treatment or other aspects of risk.
- Risk Treatment: Process of selection and implementation of measures to modify risk. Risk treatment measures can include avoiding, optimizing, transferring or retaining risk.

As our following users online survey about the specific risk of accessing corporate assets from public Wi-Fi shows, new HCI is needed to better communicate the risks to the users and the potential risk treatments they can try to apply.

IV. HUMAN COMPUTER INTERFACE TRUST AND RISK

In this section, we first show the result of our online survey and then give an overview of HCI aspects for trust and risk.

A. Wi-Fi Spoofing Users Online Survey and Weakest Link

During summer 2012, we created a short survey and sent it to a list of users who are subscribed to a marketing database and who are interested in computer programming and speak English or French. 1767 users answered, which is quite a large number of answers. We asked them the following question "Do you know that a Wi-Fi hotspot public access point name can be easily impersonated and that it can be a security risk for you?" They could reply one of the following answers "Yes; No; I don't care" and optionally add a textual comment. 5 of them used that comment option and answered: yes with the following comment "but it is possible to secure the link" ; yes with the following comment "VERY COMMON AND IT CAN CAUSE HAVOC!!!!!"; yes with the following comment "Obvious .. :P"; yes with the following comment "Honeypot :-)"; no with the following comment "Yes, Now i know. :P". Among the English speaking people, 540 replied "yes", 185 replied "no" and 1017 replied "I don't care". Figure 2 below indicates the percentages for each answer type.

 ISBN: 978-1-61208-312-4

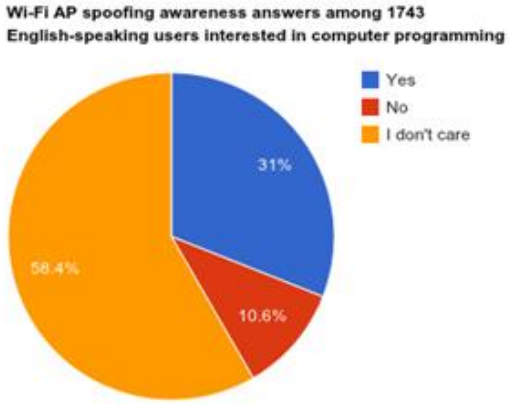

Figure 2. Wi-Fi Spoofing Awareness Results

Although these users are interested in computer programming, it is surprising to see that 58,4% of 1743 English-speaking users did not care about this issue and that 10,6% did not know it. Concerning the comment on securing the connection, few users would know how to really secure their connection. Furthermore, the fact that many of them answered that they do not care, leaves us to think that they would not take the time to secure it if it is not automated, which is not the case today with current Wi-Fi connections. The remaining security risk seems still quite important because even computer aware users do not know or do not bother about this issue although it is a real risk that current approaches do not solve.

Most researchers have come to the conclusion that it is not the security technology that is preventing the user to be safe when online, but the behaviour of the user itself that causes security breaches online. Investigators have gathered information on the behaviour of the user and concluded three main reasons as to why the user does not adhere to security applications.

The first one being that users do not necessarily do what they say they will do. For example, while users say that they will not give their password away or that they do use virus checking software regularly in reality their behaviour is different [28], [29]. Secondly, users perceive security and privacy issues differently than developers do as users do not have the background understanding issues [29]. People generally believe that they are at less risk than others. Likewise, they believe they are better than average drivers, live beyond the average age [30], etc. Therefore, many computer users have the belief that they are at less risk of computer vulnerability than others. Adams and Sasse [31] found out that users are much better at following security policies when they are given explanations on both the real security threats and the goals of the security policies. An immediate reward or instant gratification is seldom present when using security devices. Also, behaviour can also be shaped by negative reinforcement. However, in the case of security when the user does something bad the negative reinforcement can be delayed by days, weeks or even months [32]. Thirdly, the worst dilemma for users and the one that is the hardest to resolve is that from a user perspective, increases in security are most frequently accompanied by a reduction in convenience [29]. When security issues come in the way of the user completing a task, the user often chooses to let go of security to be able to complete the task.

B. Models for Trust and Risk User Interfaces

Latest psychological definitions of trust focusing on behavioural intentions define trust as an internal action similar to choosing, judging or preferring [33]. Hence, trust is a mechanism to reduce complexity since it helps reducing the number of options one has to consider in a given risky situation [34]–[37]: *"a psychological state comprising the intention to accept vulnerability based upon positive expectation of the intentions of behaviour of another."* [38]

Especially (perceived) trustworthiness is often used as synonym for trust and the differentiation of these two terms is not well defined [39]. Trustworthiness is evoked by characteristics of the trustee and therefore could be interpreted as antecedent for trust. Mayer et al. [34] specified these characteristics. They concluded that in fact perceived ability, benevolence and integrity are underlying factors of building up the impression of trustworthiness.

McKnight and Chevarny [40] developed and validated the model of system trust focusing on the user and his trust disposition, beliefs and intentions. Corritore et al. [41] focused on factors that evoke trust: external and situational factors which are located in the environment (e.g., reputation) and perceived factors (credibility, ease of use, risk) which are both hypothesized to lead to trust. Several other authors identified trust rising and influencing factors during a transaction with online services: usability and user satisfaction [42], reputation and size of the online shop [43], belief in integrity, competence and benevolence of the web vendor [44], as well as increased familiarity [45].

Schlosser et al. [46] provide a conceptual framework of the effect of online signals on trusting beliefs and intentions depicted in Figure 3 as well as operationalization to measure the identified factors. Regarding the trustworthiness of devices, Koien [47] notes that, compared to the ethical dimensions on which humans are more or less trustworthy, the trustworthiness of devices is based on the notion of intention and ability: the device intention to work as expected combined with its ability to actually do so. When trying to describe features, characteristics, experience of behaviour of people, there is a distinction of trait-parts of experience and behaviour and state-parts of experience and behaviour. Traits are personal variables that are supposed to be stable, consistent, invariant and dispositional across time and situations. States are situational variables that are supposed to be changing, discriminative, variable and dynamic across time and situations [40].

 ISBN: 978-1-61208-312-4

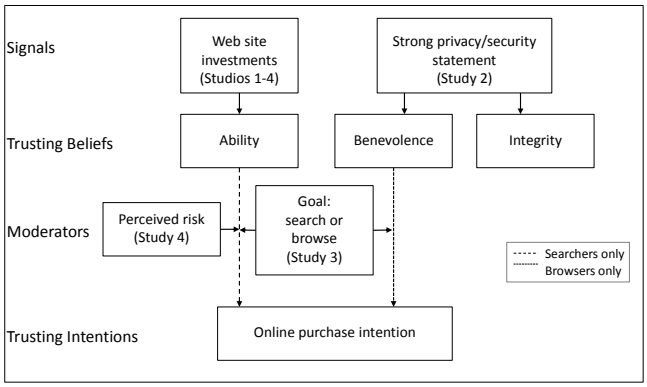

Figure 3. Schlosser's et al.'s Conceptual Framework of the Effect of Online Signals on Trusting Beliefs and Intentions [46]

There are currently no measurement approaches for the construct trust that consider a trait and a state-part of the construct. This leads to a critical psychometric issue: a measure of a (hypothesized) trait variable will always be influenced by the situation (for example: current mood of the participants induced by the surrounding) and also distorted by unsystematic measurement errors (for example: varying instructions or trust-inducing stimuli) [48]. Measuring trust and the related factor trustworthiness, which is seen as a technical property of a system, is hypothesized to evoke trust in a human. Therefore, trust is seen as a latent construct underlying behaviour and can only be assessed indirectly by certain empirical indicators [49].

Fogel and Nemad [50] investigated in their study risky behaviour in social networks. They used the risk averseness scale and the consumer trust scales, both by Pan & Zinkhan [51]. Additionally, they used the privacy behaviour scale [52], the time pressure scale [53], the privacy concerns scale and the perceived ability to control information scale, both by Dinev and Hart [54], the privacy attitude scale [52] and identity information disclosure scale [55]. Persons with social networks profile had significantly higher risk taking score than those without a social network profile. Men had greater risk taking scores than women, but there were no gender differences regarding privacy behaviour or privacy attitudes. Women had higher scores in privacy concerns.

C. User Interfaces Fostering the Sense of Trust and Risk

There are several user interface elements fostering trust in users. Users are used to some icons, e.g., the lock in the browser to show that it is a secure site. But there are no possibilities to show the user which data are shared with whom and if the data is sent to a trustworthy person, institution or website.

When a potential customer visits a Website, the first thing she encounters is the website user interface. This provides the consumer with a first impression about the site and its trustworthiness [56]. Three main targets of online trust are content, services, and people [57]. User interface designers should take care to provide a professional appearance of a vendor's Web site, in order to ease the customers' interaction with the Web site and hence increase the consumers' trust towards the merchant. The presence of some features, such as customization, user control capabilities, and customer support services has an important influence on the customer's perception and experience. In the event of a purchase or rental, the order fulfilment process will be the last and most crucial factor to satisfy the consumer's expectations about a vendor [56].

To increase the trustworthiness in e-commerce various technological tools have been developed to help the user to feel safer when exchanging personal information or buying online. During the PrimeLife project [58], user interfaces providing privacy and security feedback were evaluated. In this process the *"Send Data?"* dialog, an interface-element indicating what data was to be sent to whom for what purpose, was reviewed. The results of this study revealed that the test persons understood the meaning of this dialog, but test persons also said that they do not read the displayed information. They only look for familiar patterns or buttons and do not read the exact text. Although they did not understand some UI elements, the visualisation of the information, using color-coding worked very well [59]. Holtz et al. [60] also evaluated privacy-icons for the PrimeLife project. In order to do so, two icon sets were developed: one for general use and one for specific use in connection with access control functionalities. The outcome of this study reveals that users prefer clear icons with few details.

Icons were originally introduced to quickly and simply show facts, such as exits or fire distinguisher. They then found their way to the computer and some metaphors were used, e.g., icon for an e-Mail, icon for a bin, etc. For security and privacy reasons icons can show the privacy and security level of elements, such as a homepage or similar. A wide range of icon usage is described in [61]. Privacy icons were first introduced by Mary Rundle [62]. Other privacy icon sets are partially inspired by the Creative Commons licenses [63].

The following icons and pictures in Figure 4 should act as examples of different icons and icons set.

Figure 4. Security icons examples [61]

Different approaches to display information creating trust have been undertaken. One promising approach is the use of *"Nutrition Labels"* [64]. Using this approach known by users (also similar to energy labels), it is possible to display the privacy state of a system. Also, the uTRUSTit [65] project deals on how security and privacy information could be displayed to the user. An example of how to display icons and privacy information encountered in the uTRUSTit project follows in Figure 5:

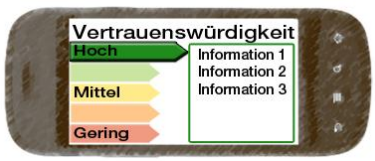

Figure 5. Nutrition labels [65]

 ISBN: 978-1-61208-312-4

D. Social Trust and Online Reputation User Interfaces

We finish the overview of trust and reputation user interfaces with the state-of-the-art of online reputation interfaces below.

Founded in 1995, eBay [14] has been a very successful online auction market place where buyers can search for products offered by sellers and buy them either directly or after an auction. After each transaction, the buyers can rate the transaction with the seller as *"positive"*, *"negative"* or *"neutral"*. Since May 2008, the sellers have only the choice to rate the buyer experience as *"positive"* or nothing else. Short comments of maximum 80 characters can be left with the rating. Their reputation is based on the number of positive and negative ratings that are aggregated in the Feedback Score as well as the comments if the user reads them. Buyers or sellers can affect each other's Feedback Score by only one point per week. Each positive rating counts for 1 point and each negative counts for -1 point. The balance of points is calculated at the end of the week and the Feedback Score is increased by 1 if the balance is positive or decreased by 1 if the balance is negative. Buyers can also leave anonymous *"Detailed Seller Ratings"* composed of different criteria, such as, *"Item as described"*, *"Communication"*, *"Shipping Time"*, etc. displayed as a number of stars from 0 to 5 stars. Different image icons are also displayed to quickly estimate the reputation of the user, for example, a star whose color depends on the Feedback Score, as depicted in Figure 6. After 90 days, detailed item information is removed. From a privacy point of view, on one hand, it is possible to use a pseudonym, on the other hand, a pretty exhaustive list of what has been bought is available, which is quite a privacy concern. There are different *"Insertion"* and *"Final Value"* fees depending on the item type.

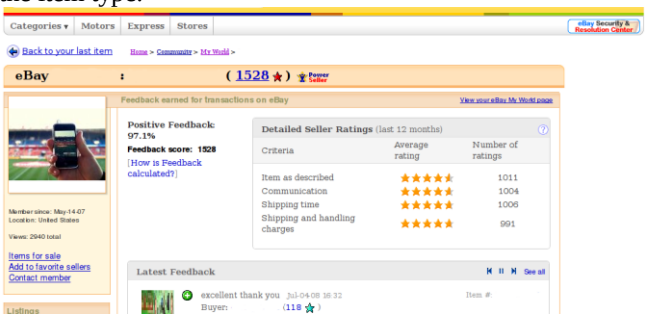

Figure 6. eBay online reputation visual representation [14]

Founded in 2006, Venyo [14] provided a worldwide people reputation index, called the Vindex, based on either direct ratings through the user profile on Venyo Web site or indirect ratings through contributions or profiles on partner Web sites. Venyo was very privacy-friendly because it was not asking the users for their external passwords and it did not crawl the Web to present a user reputation without his or her initial consent. Unfortunately, Venyo got fewer profiles than the other services that were more aggressive and less privacy friendly and was terminated in 2009. At time of rating, the rater specifies a value between 1 and 5 as well as keywords corresponding to the tags contextualizing the rating. The rating is also contextualized according to where the rating has been done. For example, if the rating is done from a GaultMillau restaurant blog article, the tag *"restaurant recommendation"* is automatically added to the list of tags. Venyo provides a reputation history chart as depicted in Figure 7 to help the users monitoring the evolution of their reputation on Venyo's and partner's Web sites. Venyo does not monitor external Web pages or information.

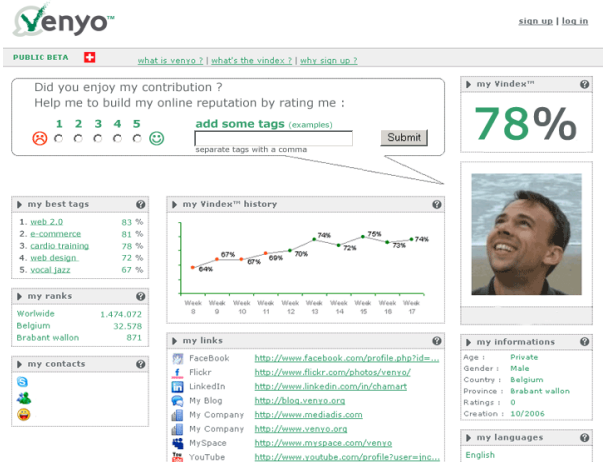

Figure 7. Venyo online reputation user interface [14]

TrustPlus [14] was another decentralized e-reputation calculation service that existed but unfortunately had also to close in April 2012 due to a business model that did not work. TrustPlus had partnered with a few other interesting e-services such as ZoomInfo. Founded in 1999, ZoomInfo is more a people (and company) search directory than a reputation services with more than 42 millions users, 3,8 millions companies and a partnership with Xing.com (a business social network similar to LinkedIn.com). Thanks to its partnership with SageFire, which is a trusted eBay Certified Solution Provider who has access to historical archives of eBay reputation data, TrustPlus was able to display and use eBay's reputation evidence when the users agreed to link their TrustPlus account with their eBay account. The main initial feature of TrustPlus was a Web browser plug-in that allowed the user to see the TrustPlus reputation of an online profile appearing on Web pages on different sites, such as, craiglist.org. At the identity layer, although it is not a recommended security practice, TrustPlus asked the users to type their external accounts passwords, for example, eBay's or Facebook's ones, to validate that they own these external accounts as well as to create their list of contacts. This list of contacts could be used to specify who among the contacts could see the detail of which transactions or ratings. As depicted in Figure 8, TrustPlus rating user interface was pretty complex but with interesting advanced trust features such as circles of trust to facilitate with whom some information would be shared. There were different contexts: a commercial transaction, a relationship and an interaction, for example, a chat or a date.

 ISBN: 978-1-61208-312-4

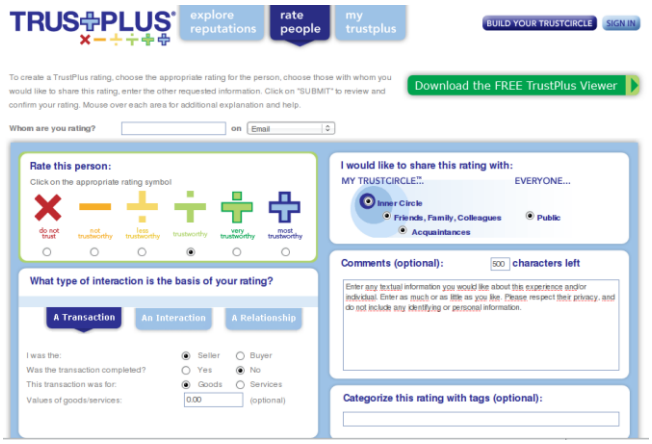

Figure 8. TrustPlus online reputation user interface [14]

Klout [14] was created in 2008 by Joé Fernandez. Instead of computing the reputation of a person mainly based on recommendations from other users, as we have seen above in previous reputation calculation services, Klout analyses the Twitter account of that person. Klout score is based on 3 main criterion:

- True Reach: the number of followers of the user's Twitter account and following the user's tweets
- Amplification: the number of people who share a post (who distribute it to other users)
- Network: the influence of the users composing the True Reach themselves

Klout may integrate other evidence such as posts on other social networks (such as Facebook) or other users who recommend the user by adding a +K to the user on specific topics, meaning that they click on a link provided by Klout saying that the user has influenced them regarding that topic. There are similar metrics that have been created since Klout, for example, Twitalizer (which is a very detailed one focusing on Twitter information), Peerindex, Kred, Identified, PROSkore, Jitterater (acquired by Meltwater), etc. Unfortunately most of those metrics are not open, i.e., it is not really clear how the results have been computed and based on which evidence. Klout initial business models is based on the fact that users with high Klout score in some topic would be rewarded by brands willing to influence that topic and would pay Klout to be able to do that. For example, Virgin Airline gave free airline tickets to users with high Klout score. At time of writing, it is still not possible to reward users outside the USA and its business model has still to prove its viability. Anyway, Klout has gained a decent level of visibility compared to earlier e-reputation calculation services, maybe because many more users use social networks than before, leading to a more viral effect, and e-reputation has become a hot product in traditional marketing companies. Once the Klout account is linked to a user's social network, it can detect automatically when the user sends a new post and check how much buzz it has generated. If another user gives the user a +K, she is informed by email or a notification on her social networks.

V. CONCLUSION

As part of the MUSES project, we are working towards a real time risk and trust engine that will better cope with the new challenges introduced by BYOD and mobile working including new HCI that will better explain the risks encountered by the mobile users especially because our online survey confirms that users do not take care of security risks.

This survey underlines that, from a corporate point of view, the BYOD and mobile working trend clearly challenges traditional IT risk management methodologies. They mainly focus on the negative outcomes where assets could be undermined due to probable threats that would successfully exploit vulnerabilities without taking into account that if the assets could be successful used and no threat would happen, the opportunity to use those assets would bring the benefits of the positive outcomes. There are some benefits in letting work being done in broader situations than the corporate environment and that if this work is not done there are direct loses. In addition, in traditional static threat modeling and risk management methodologies, threats and risks are manually assessed once for all and then either mitigated or accepted by corporate managers. Hence, those traditional approaches do not also fit where context can be evaluated in real time and more should be done if no risk is detected, i.e., the system is not under attack.

ACKNOWLEDGMENT

The research leading to these results has received funding from the EU IST Seventh Framework Programme (FP7) under grant agreement number 318508, project MUSES (Multiplatform Usable Endpoint Security).

REFERENCES

[1] "Multiplatform Usable Endpoint Security." [Online]. Available: http://www.musesproject.eu. [Accessed: 14-Jul-2013].

[2] D. McKnight and N. L. Chervany, "The Meanings of Trust." MISRC 96-04, University of Minnesota, Management Informations Systems Research Center, 1996.

[3] D. M. Romano, "The Nature of Trust: Conceptual and Operational Clarification," Louisiana State University, PhD Thesis, 2003.

[4] A. Krishna and V. Varadharajan, "A Hybrid Trust Model for Authorisation Using Trusted Platforms," in *Proceedings of the 2011IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications*, Washington, DC, USA, 2011, pp. 288–295.

[5] M. Blaze, J. Feigenbaum, and J. Lacy, "Decentralized Trust Management," in *the 17th IEEE Symposium on Security and Privacy*, 1996, pp. 164–173.

[6] S. Terzis, C. English, W. Wagealla, and P. Nixon, "Trust Formation Model," 2005.

[7] S. Marsh, "Formalising Trust as a Computational Concept," Department of Mathematics and Computer Science, University of Stirling, RP 1994.

[8] K. Govindan and P. Mohapatra, "Trust computations and trust dynamics in mobile adhoc networks: a survey,"

 ISBN: 978-1-61208-312-4

Commun. Surv. Tutorials IEEE, vol. 14, no. 2, pp. 279–298, 2012.

[9] T. Grandison and M. Sloman, "A Survey Of Trust In Internet Applications." 2000.

[10] D. Z. Kevin Hoffman and C. Nita-Rotaru, "A Survey of Attack and Defense Techniques for Reputation Systems," Purdue University, CSD TR #07-013, 2007.

[11] A. Medić, "Survey of Computer Trust and Reputation Models–The Literature Overview," *Int. J. Inf.*, vol. 2, no. 3, 2012.

[12] C. Castelfranchi and R. Falcone, "Trust is much more than subjective probability: Mental components and sources of trust," in *32nd Hawaii International Conference on System Sciences - Mini-Track on Software Agents*, 2000.

[13] J. Sabater and C. Sierra, "Review on Computational Trust and Reputation Models." Kluwer, 2005.

[14] J.-M. Seigneur, "Reputation Management," in *Computer and Information Security Handbook*, Morgan Kaufmann, 2009.

[15] J. Golbeck and J. Hendler, "Accuracy of Metrics for Inferring Trust and Reputation in Semantic Web-based Social Networks," in *the 14th International Conference on Knowledge Engineering and Knowledge Management*, 2004.

[16] Z. Despotovic and K. Aberer, "Maximum Likelihood Estimation of Peers' Performance in P2P Networks." 2004.

[17] V. Cahill, E. Gray, J.-M. Seigneur, C. Jensen, Y. Chen, B. Shand, N. Dimmock, A. Twigg, J. Bacon, C. English, W. Wagealla, S. Terzis, P. Nixon, G. di M. Serugendo, C. Bryce, M. Carbone, K. Krukow, and M. Nielsen, "Using Trust for Secure Collaboration in Uncertain Environments," *IEEE Pervasive Computing*, vol. July-September, 2003.

[18] J.-M. Seigneur, "Trust, Security and Privacy in Global Computing," Trinity College Dublin, Ph.D. Thesis, 2005.

[19] J.-M. Seigneur and C. D. Jensen, "Trading Privacy for Trust," in *the Second International Conference on Trust Management*, 2004, vol. LNCS 2995.

[20] N. Dimmock, "Using Trust and Risk for Access Control in Global Computing," University of Cambridge, 2005.

[21] V. Balakrishnan and E. Majd, "A Comparative Analysis of Trust Models for Multi-Agent Systems," *Lect. Notes Softw. Eng.*, vol. 1, no. 2, 2013.

[22] "Risk Assessment and Risk Management Methods: Information Packages for Small and Medium Sized Enterprises (SMEs)," ENISA, 2006.

[23] Adam, Shostack, "Reinvigorate your Threat Modeling Process," *MSDN Mag.*, vol. July, 2008.

[24] M. Howard and S. Lipner, "Inside the windows security push," *Secur. Priv. IEEE*, vol. 1, no. 1, pp. 57–61, 2003.

[25] "ISO/IEC 13335-1 Management of information and communications technology security."

[26] "ISO Guide 73 Risk management Vocabulary," ISO, 2009.

[27] J. Clarke, M. Gomez Hidalgo, A. Lioy, M. Petkovic, C. Vishik, and J. Ward, "Consumerization of IT: Top Risks and Opportunities," ENISA, 2012.

[28] A. Patrick, S. Marsh, and P. Briggs, "Designing systems that people will trust," 2005.

[29] C. Nodder, "Users and trust: A microsoft case study," *Secur. Usability*, pp. 589–606, 2005.

[30] P. Slovic, B. Fischhoff, and S. Lichtenstein, "Facts and fears: Understanding perceived risk," *Soc. Risk Assess. Safe Is Safe Enough*, vol. 4, pp. 181–214, 1980.

[31] A. Adams and M. A. Sasse, "Users are not the enemy," *Commun. ACM*, vol. 42, no. 12, pp. 40–46, 1999.

[32] R. West, "The psychology of security," *Commun. ACM*, vol. 51, no. 4, pp. 34–40, 2008.

[33] J. A. Colquitt, B. A. Scott, and J. A. LePine, "Trust, trustworthiness, and trust propensity: a meta-analytic test of their unique relationships with risk taking and job performance.," *J. Appl. Psychol.*, vol. 92, no. 4, p. 909, 2007.

[34] R. C. Mayer, J. H. Davis, and F. D. Schoorman, "An integrative model of organizational trust," *Acad. Manage. Rev.*, pp. 709–734, 1995.

[35] N. Luhmann, *Vertrauen: Ein Mechanismus der Reduktion sozialer Komplexitat*. F. Enke, 1968.

[36] B. Barber, *The logic and limits of trust*. Rutgers University Press New Brunswick, NJ, 1983.

[37] J. D. Lewis and A. Weigert, "Trust as a social reality," *Soc. Forces*, vol. 63, no. 4, pp. 967–985, 1985.

[38] D. M. Rousseau, S. B. Sitkin, R. S. Burt, and C. Camerer, "Not so different after all: A cross-discipline view of trust.," *Acad. Manage. Rev.*, vol. 23, no. 3, pp. 393–404, 1998.

[39] K. J. Blois, "Trust in business to business relationships: an evaluation of its status," *J. Manag. Stud.*, vol. 36, no. 2, pp. 197–215, 1999.

[40] D. H. McKnight and N. L. Chervany, "What trust means in e-commerce customer relationships: an interdisciplinary conceptual typology," *Int. J. Electron. Commer.*, vol. 6, pp. 35–60, 2002.

[41] C. L. Corritore, R. P. Marble, S. Wiedenbeck, B. Kracher, and A. Chandran, "Measuring online trust of websites: credibility, perceived ease of use, and risk," presented at the AMCIS, 2005.

[42] C. Flavián, M. Guinalíu, and R. Gurrea, "The role played by perceived usability, satisfaction and consumer trust on website loyalty," *Inf. Manage.*, vol. 43, no. 1, pp. 1–14, 2006.

[43] S. L. Jarvenpaa, N. Tractinsky, and L. Saarinen, "Consumer Trust in an Internet Store: A Cross-Cultural Validation," *J. Comput.-Mediat. Commun.*, vol. 5, no. 2, pp. 0–0, 1999.

[44] P. Palvia, "The role of trust in e-commerce relational exchange: A unified model," *Inf. Manage.*, vol. 46, no. 4, pp. 213–220, 2009.

[45] D. Gefen, "E-commerce: the role of familiarity and trust," *Omega*, vol. 28, no. 6, pp. 725–737, 2000.

[46] A. E. Schlosser, T. B. White, and S. M. Lloyd, "Converting web site visitors into buyers: how web site investment increases consumer trusting beliefs and online purchase intentions," *J. Mark.*, pp. 133–148, 2006.

[47] G. M. Køien, "Reflections on Trust in Devices: An Informal Survey of Human Trust in an Internet-of-Things Context," *Wirel. Pers. Commun.*, vol. 61, no. 3, pp. 495–510, 2011.

[48] D. Danner, D. Hagemann, A. Schankin, M. Hager, and J. Funke, "Beyond IQ: A latent state-trait analysis of general intelligence, dynamic decision making, and implicit learning," *Intelligence*, vol. 39, no. 5, pp. 323–334, 2011.

[49] E. L. Hamaker, J. R. Nesselroade, and P. Molenaar, "The integrated trait–state model," *J. Res. Pers.*, vol. 41, no. 2, pp. 295–315, 2007.

[50] J. Fogel and E. Nehmad, "Internet social network communities: Risk taking, trust, and privacy concerns," *Comput. Hum. Behav.*, vol. 25, no. 1, pp. 153–160, 2009.

[51] Y. Pan and G. M. Zinkhan, "Exploring the impact of online privacy disclosures on consumer trust," *J. Retail.*, vol. 82, no. 4, pp. 331–338, 2006.

[52] T. Buchanan, C. Paine, A. N. Joinson, and U.-D. Reips, "Development of measures of online privacy concern and

protection for use on the Internet," *J. Am. Soc. Inf. Sci. Technol.*, vol. 58, no. 2, pp. 157–165, 2007.
[53] B. Mittal, "An integrated framework for relating diverse consumer characteristics to supermarket coupon redemption," *J. Mark. Res.*, pp. 533–544, 1994.
[54] T. Dinev and P. Hart, "Internet privacy concerns and their antecedents-measurement validity and a regression model," *Behav. Inf. Technol.*, vol. 23, no. 6, pp. 413–422, 2004.
[55] F. Stutzman, "An evaluation of identity-sharing behavior in social network communities," *J. Int. Digit. Media Arts Assoc.*, vol. 3, no. 1, pp. 10–18, 2006.
[56] I. Araujo and I. Araujo, "Developing trust in internet commerce," in *Proceedings of the 2003 conference of the Centre for Advanced Studies on Collaborative research*, 2003, pp. 1–15.
[57] J. Golbeck, "Trust on the world wide web: a survey," *Found. Trends Web Sci.*, vol. 1, no. 2, pp. 131–197, 2006.
[58] J. Camenisch, *Privacy and identity management for life*. Springerverlag Berlin Heidelberg, 2011.
[59] J. Angulo, S. Fischer-Hübner, T. Pulls, and U. König, "HCI for policy display and administration," in *Privacy and Identity Management for Life*, Springer, 2011, pp. 261–277.
[60] L.-E. Holtz, H. Zwingelberg, and M. Hansen, "Privacy policy icons," in *Privacy and Identity Management for Life*, Springer, 2011, pp. 279–285.
[61] M. Hansen, "Putting privacy pictograms into practice-a european perspective," *GI Jahrestag.*, vol. 154, pp. 1–703, 2009.
[62] M. Rundle, "International data protection and digital identity management tools," in *IGF 2006: Privacy Workshop, Athens, at http://ssrn. com/abstract*, 2006, vol. 911607.
[63] A. Raskin, *Privacy Icons: Alpha Release*. 2010.
[64] P. G. Kelley, J. Bresee, L. F. Cranor, and R. W. Reeder, "A nutrition label for privacy," in *Proceedings of the 5th Symposium on Usable Privacy and Security*, 2009, p. 4.
[65] C. Hochleitner, C. Graf, D. Unger, M. Tscheligi, and I. Center, "Making Devices Trustworthy: Security and Trust Feedback in the Internet of Things," 2012.

 ISBN: 978-1-61208-312-4