# To Trust or Not to Trust

Alexander Mirnig, Sandra Troesterer, Elke Beck, Manfred Tscheligi



# To Trust or not to Trust

## Six Recommendations for System Feedback in a Dynamic Environment

Alexander G. Mirnig, Sandra Troesterer, Elke Beck, and Manfred Tscheligi

University of Salzburg, Salzburg, Austria,
firstname.lastname@sbg.ac.at,
WWW home page: http://icts.sbg.ac.at

**Abstract.** In today's rapidly developing Internet, the web sites and services end users see are more and more composed of multiple services, originating from many different providers in a dynamic way. This means that it can be difficult for the user to single out individual web services or service providers and consequently judge them regarding how much they trust them. So the question is how to communicate indicators of trustworthiness and provide adequate security feedback to the user in such a situation. Contemporary literature on trust design and security feedback is mostly focused on static web services and, therefore, only partially applicable to dynamic composite web services. We conducted two consecutive studies (a qualitative and a quantitative one) to answer the questions of how and when security feedback in dynamic web service environments should be provided and how it influences the user's trust in the system. The findings from the studies were then analyzed with regards to Riegelsberger and Sasse's ten principles for trust design [24]. The outcome we present in this paper is an adapted list of trust principles for dynamic systems.

**Keywords:** trust, automation, dynamic web services, feedback design

## 1 Introduction: The User in A Dynamic Environment

As technology advances, the status quo of static web services is increasingly on the verge of being replaced by more dynamic solutions (e.g., Facebook's dynamic targeted advertising based on likes, etc. is probably one of the most well-known examples for this). The additional flexibility and convenience such a dynamic context can provide comes at the price of new privacy and security issues. These have to be tackled before a truly dynamic web can be regarded as a realistic alternative to today' still majorly static web services. A dynamic web platform is a framework for a multitude of web services which are presented to the web service end user, who comes into contact with only a very small part of the whole platform (see Figure 1 – service end users), in a dynamic way. The ANIKETOS project[1], which our research is based on, is one such attempt at providing a

[1] ANIKETOS (www.aniketos.eu) is an EU-funded project about ensuring trustworthiness and security in composite web services

platform for secure and trustworthy Internet services. The number of services presented to the user depends not only on the user's requirements, but also on whether or not the service is regarded as trustworthy by the platform. This is where the dynamic component comes into play, as the status of a certain web service might change due to an attack, a change of policies, etc. In such a case, the platform can adapt to these changes as they happen and replace the service with a different, more trusted one. Being in a dynamic environment means that service consumers will be interacting with applications based on a multitude of exchangeable service components that can adapt in an instant to changes in service availability, price, and security attributes. The security attributes and how well the system can handle them is ultimately what determines the success of such a system. With static and disconnected web services, a user might lose trust in the one web service they had a bad experience with. But if that one web service is part of a service platform, then the user might not only lose trust in the web service, but in the entire service platform the web service is part of. Thus, one bad apple could quite easily spoil the whole digital fruit basket, making it all the more important to ensure trust in the system at all times.

Currently it is not intended that the service end user is notified about any changes (recompositions) taking place "behind the user interface" by the platform developers, i.e., the replacement of a service component with a similar, but more secure and trustworthy one (see Figure 1 for an illustration of such a dynamic web service recomposition) is intended to occur without the end user ever noticing it. On one hand, this way of shaping what the user perceives has many benefits, e.g., to avoid annoying the users with uninteresting system in-

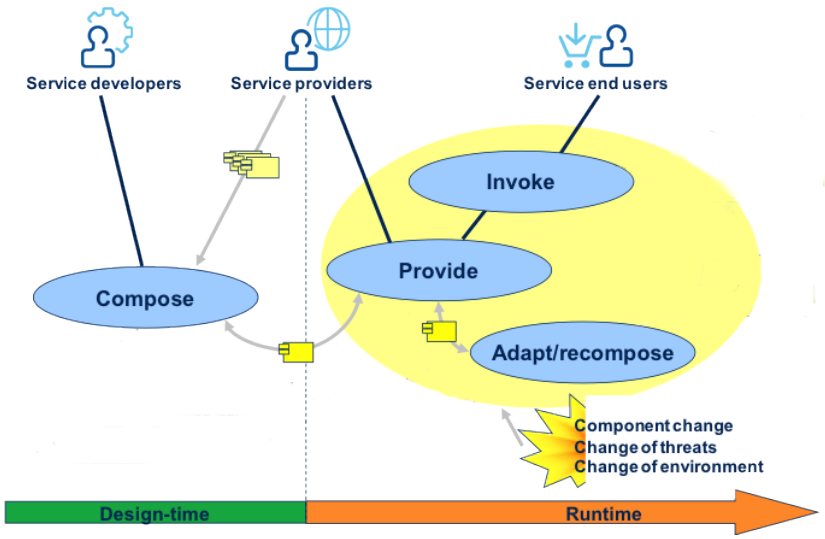


**Fig. 1.** The user in a dynamic composite web service environment (Image ©Per Håkon Meland)

formation. On the other hand, the system remains a black box for the user and it is difficult for them to judge whether or not to trust it (e.g., to provide sensitive personal data). But even with such a system a complete secure internet experience cannot be guaranteed. So how should one deal with dynamic systems and their process (in)transparency for users and how does this affect the user's trust in the system? It needs to be clarified, which *parts* of the black box should be made visible to the user, so that they can make informed decisions whenever necessary, while still benefitting from the added convenience of automatic web service supply.

## 2 Trustworthy User Feedback Design

System transparency is an important topic in user interface design in general. In Johnston et al.'s [15] proposal of criteria for a positive HCI (Human Computer Interaction) and user experience applied in the area of security, "visibility of system status" is among these criteria. It is understood as "it is important for the user to be able to observe the security status of the internal operations." Studies have shown that system transparency affects how much trust a user puts into a system. For instance, the model for trust in automated systems of Hoff and Bashir [14] stresses the importance of design features for the user's perception of a system's performance, such as ease-of-use, transparency, and appearance. Therefore, designing for trust is an important issue ([26], [25]). Patrick et al. [21] define trust as "a positive expectation regarding the behaviour of someone or something in a situation that entails risk to the trusting party". Specifically for on-line trust, Corritore et al. [6] provide the following definition. Online-trust is "an attitude of confident expectation in an online situation of risk that one's vulnerabilities will not be exploited". Therefore, by this definition, trust is necessary only in situations of vulnerability and risk. Trust can be considered as a process with the goal of risk reduction, which is dynamic and develops over time ([7], [6]). Risk is "the likelihood of an undesirable outcome" (Deutsch, 1958, c.f. [6]), p.751). From that point of view, the higher the user's perception of being in control, the less the user has a need to trust.

Closely related to trust is trustworthiness, i.e., a characteristic of someone or something that is the object of trust [6]. Generally, there exist several hints in literature (e.g., [6], [7], [2], [11]) that the *perception* of the trustworthiness of a website is determined by numerous factors such as e.g., ease of navigation or freedom from grammatical and typographical errors. A further reason for different perceptions of the trustworthiness and security of a website is that there is a variety of different attitudes about privacy among Internet users. Ackerman et al. [1] differentiate between privacy fundamentalists, pragmatists, and marginally concerned Internet users. Further categorizations are provided by Sheehan et al. [27] and Berendt et al. [3]. Another important factor is acceptance, with the Technology Acceptance Model (TAM) [22] being one of the most influential and widely used explanatory models for explaining and measuring user/computer/technology acceptance.

All of these system- and user-related factors finally point towards the central problem of user feedback design, i.e., how to provide users with security-related information in an adequate way. Which *feedback* does the user require in order to be able to reasonably judge whether a certain service or website is trustworthy or not? Existing approaches on risk communication and security alert dialogs are manifold (e.g., [9], [4], [23], [29]). But their success is not undisputed – Raja et al. [23] summarize the situation well by stating that users do not pay attention to risk communications, that they do not read or simply ignore security warning texts, as the users often do not understand the messages, nor the options provided to them for responding to the warning. They are unaware of the risks or have an incorrect mental model of the risks. So a truly successful and widely applicable way to communicate trust-relevant information is still not an easy task with a uniform solution. Maurer et al. [17] have recently shown a very promising attempt at what they call a "semi-blocking" approach to help users identify fraudulent websites. Another interesting approach towards facilitating secure and trustworthy design is the work of Riegelsberger and Sasse [24]. They have put forward a comprehensive set of principles for trustworthy and usable design, that builds on a vast pool of research and puts it into a concise and comprehensible format.

To date, HCI research on system transparency and trust has mostly focused on automated systems (e.g., [14], [31]), recommender systems (e.g., [28]), and e-commerce systems (e.g., [6], [12]). Contemporary research on automation is mostly focused robotics and social computing (e.g., [13], [20]). In the *blinded* project, however, we were confronted with a different kind of system, namely a dynamic system of composite web services. A composite web service consists of several sub-services, and any of these services could be exchanged for another one at any time. So while the individual sub-services are more or less static individuals, the composite web service is the complete opposite and may change rapidly in composition in irregular intervals. Services in the *blinded* framework are modeled in a goal-oriented language [10] which depicts threats as their own entities. As Patrick et al. [21] state, "Any security system is only as secure as its weakest link. Invariably, because of their social nature (and because of their human nature), the weakest links are often humans." Therefore, it is not enough to design systems that are theoretically secure without taking the end users into account. It needs to be investigated, how end user feedback has to be implemented in such a framework, so that an appropriate level of security can be provided and communicated, while at the same time not inconveniencing the user.

It can be assumed that what is known about (static) trust design or trust design for automation of a different nature (recommender systems, anthropomorphic robots) might not completely hold for composite web services as well. Therefore, we decided to investigate this issue further and expand the status quo on security and trust design, both in general as well as for dynamic web services. Our goal was to expand what is known about trust and trustworthy design in familiar contexts, with the final aim of being able to derive recommen-

dations for trust design in dynamic web systems that are grounded in an actual application Starting from the assumption that automated processes should not be completely invisible to the end user [14], we focused on the following areas in our research:

- Means of feedback provision about automated processes (behind the web interface) of a dynamic system to users
- Conditions under which such user feedback should be provided
- The effect of appropriate user feedback on the user's trust in and acceptance of a web service that is part of a dynamic system

We started with the first two of these and conducted an initial, qualitative interview study to collect information on user's needs and priorities regarding trust and system feedback in a web environment with dynamic composite services. Based on these findings we designed feedback prototypes along with concrete use scenarios for a final quantitative questionnaire study. There, we investigated trust and acceptance in both prototypes. As final step, we contrasted our findings regarding acceptance and trust influence of the feedback solutions in the scenarios with Riegelsberger and Sasse's principles for trust design.

## 3 Interview Study

In order to find out what information should be presented to the end-user and how it should be presented, we conducted an interview study with 8 participants (4 male, 4 female), aged between 24 and 40 (mean age 30 years). The subjects were recruited at our institution in Austria, out of a pool of about 45 possible subjects and all of them were external to the project. Each subject had a different professional background, to ensure a diversity of viewpoints. They were all frequent Internet users, i.e., seven participants used the Internet several times a day, and one several times a week for private purposes. Only one participant reported that they are always aware whether the website they are visiting is safe when surfing the Internet, and one participant that they do not care at all. All other participants reported that they only took care in specific cases, such as online banking, online shopping, entering contact data, entering credit card information, transmission of private data in general, when no choice is available concerning a specific website, or when information is only available on an insecure website. None of the participants were familiar with dynamic web services or details of the *blinded* project.

Each interview lasted between half an hour and an hour, was audio-recorded, conducted individually, and in German. The interview was set up in a way that the interviewee got an oral description of a possible scenario at the beginning of the interview, and the questions were posed in conjunction with this scenario. The participant had to imagine a vacation planning website, consisting of different web services, e.g., weather information, flight booking, hotel booking, and payment services. They were told that the website was controlled by a platform

in the background that made sure that the services were trustworthy and secure, and that in case a threat was detected, the service would be substituted by another service that fulfilled the security requirements. This was illustrated with an example concerning credit card payment. Questions posed during the interview focused on how the subjects would want to be informed about such a service substitution, followed by questions about whether they would need that information and why they would need it. For the analysis the interviews were first transcribed. Then the individual statements were paraphrased in English and further summarized for each question.

### 3.1 Study Results

In the following we present the most relevant the results from the larger preliminary interview study, together with a summary of the overall implications for our further research at the end.

**How should the information be provided?** Whereas two participants suggested something like a pop-up window, other participants suggested a less obtrusive way, with the motivation that something like a pop-up window would probably scare them, or that they would think they have done something wrong. The message should not appear as a warning, but could be, e.g., a field at the bottom of the website which nicely explains the issue. One participant suggested to have no message at all, but that the website generally provides a statement in the sense "It is ensured that the most secure service is provided" and in case a change happens, it should be added that a new service is available or has been changed because it is ensured that the safest service is always available. Further information should be not provided directly, "only when one clicks on the message or a part of the message". Also the opportunity to click the window/field away if one is not interested should be given. All interviewees suggested visual feedback, expect for one participant who said they wanted to be informed, e.g., via telephone if there were harmful consequences (high financial damage) for them. The participants preferring a dynamic, situated information provision, e.g., a pop-up window, said that this should be shown to point out the urgency, or that it should show up before logging in, informing that there have been changes of services due to this and that, and whether one agrees to use it.

**Which information should be provided?** There was a general agreement among interviewees that information about which service was changed, and why it was changed, is relevant. However, the message should be kept short, and further information could be provided when clicking on a link for further information. Such further information could include a list of web services to choose from, or information about whether a web service was changed very often. Additionally, it was suggested that the message should contain information whether the user has been already affected in some way by the insecurity. One participant, however, mentioned that the feedback should not happen while they were in the middle of doing something, because this would disturb their workflow.

**Which information do the users require in order to trust the platform the web service is part of?** One important issue which was raised in this regard is the reputation and popularity of the platform itself. It has to be made sure, that the platform is a certified platform and is secure and safe against phishing threats. Interviewees mentioned that the platform needs to gather reputation over time, and, therefore, information about which websites use the platform, and how this impacts their security, is relevant. Additionally, having the "big players", e.g., Amazon, or bank websites, visibly use the platform would increase user trust in it (or not, in case these big players themselves are untrustworthy in the user's eyes). Two interviewees also mentioned that the platform should provide a "seal of quality" that should be displayed on a protected website.

### Conditions for (not) notifying users about web service changes

*Kind of web service (security relevance):* Services that are related to the provision of personal data (credit card data, log-in data, personal email addresses) were generally seen as very security relevant and in case of an exchange of such services, end users prefer to be notified about the change. For less security relevant web services (e.g., weather information service), users do not seem to want further information about any related changes.

*Visibility of changes for users:* In case that any changes of web services cause additional changes that are visible for users, then users would like to be informed, because if another service appeared without information, they could get the impression that the website is not alright or has been hacked. Thus, in case of a "something is different" experience, users should be provided with an explanation for the change. In case of a change being unnoticeable to the user, one interviewee explicitly stated to prefer to not be informed about the change.

*General trust or distrust in website:* The general impression the website conveys to a user (trust or distrust in the website) also seems to affect their need for information about web service changes. If they generally trusted the website, they did not wish to be informed about service exchanges, whereas the opposite was true for websites they did not trust.

*Change of data policy, contact person, web service functionality:* Being informed about what happens to personal data once provided to the service, e.g., in case, when data are disclosed to 3rd parties, was of general importance to the interviewees. For some users it is also important to know who the contact person is in case something goes wrong during the use of a service. Finally, an exchange of web services may also lead to changed functionality, which affects the use of the service by the user. In such cases, the interviewees preferred to be informed about any changes regarding data policy, contact person, or web service functionality.

*Existing negative consequences for users:* In case of existing negative consequences for users due to a security flaw, users want to be informed about this flaw and any related security incidents with the web service(s) in question. One interviewee, for instance, mentioned that if there had been a security problem when they used a service, and the problem affected them personally, they wanted to get informed about it and about what they could do, e.g., to carefully check their credit card bills. Participants mentioned that when loosing confidence in one of the web services, this will also have a trust-reducing effect for any related web service within the application.

*User contribution to security:* Finally, some users are willing to contribute to security and want to be informed of opportunities to do so. One interviewee explained that when they can actively do something to improve the security of a service, e.g., to update their browser, then they want to be informed about these possibilities.

Overall, our primary finding was that, even in a dynamic environment, the users expect to receive feedback in the traditional and established ways. So as the logical next step in our research, we wanted to know whether this preference of traditional feedback still held true when actually put into practice. The interviews showed a clear tendency towards the need for feedback in cases where a change directly affected the user and potentially put them at risk. Risk and its influence on the desire for feedback is not a strictly binary affair [7], we wanted to take closer look at the *extent* to which risk influences the need for feedback. Based on our findings, we decided to examine two cases of risk for our follow-up research: (a) cases in which both the user's personal data and their money are at risk; and (b) cases in which only a user's personal data is at risk. Considering the dynamic environment and its high feedback potential, it was quite surprising to still see so many non-feedback related factors being mentioned. So It seems that appropriate and well-designed feedback might not be enough to ensure trust on its own. Although it can certainly maintain a certain level of trust, that trust likely has to be built up beforehand via other means.

Building on the results of the interview study, we decided to conduct a workshop involving only HCI and usability experts (all external to the project) to create low fidelity feedback design prototypes as examples for how feedback about dynamic web service recompositions might look like in practice. With these we would then prepare a final, quantitative study focused primarily on trust and acceptance. In the workshop, our general approach was to put the designers into the shoes of a particular user type via a persona[5]-like user description, and have them experience a certain scenario of an interaction with dynamically exchanged web services. To achieve this we decided to develop and make use of a user type description, more specifically a description of a privacy pragmatist (which is likely the numerically broadest user group [1]) according to Westin's General Privacy Concern Index [16]. To avoid characterising only a particular subgroup of security pragmatists and to keep the characterisation as broad as possible, we described the user type such that it could not be classified as a purely circumspect/wary [27] or identity concerned/profile averse [3] user re-

spectively. The workshop participants, six in total, were divided into two groups, and each group was given the aforementioned user type description as well as a scenario. Both scenarios (an online payment and a forum post scenario) were designed in a way so that the recomposition component was initially invisible to the user. The outcome of the workshop were two paper prototypes designed to provide adequate feedback for both scenarios. These would then serve as the basis for the follow-up questionnaire study, in which we wanted to investigate, how the users would react to these scenarios and the prototype designs (i.e., whether these feedback solutions were perceived as adequate by them as well).

## 4 Questionnaire Study

The aim of the questionnaire[2] was to evaluate on a broader basis whether website users wanted feedback regarding service recomposition in scenarios of different risk (personal data vs. payment credentials) whether the provided feedback solutions are helpful in terms of acceptance of and trust in the website. Therefore, participants were given the textual description of the two scenarios in randomized order, followed by questions regarding the general use of the described website, general need for information about the occurring service recomposition, and items regarding acceptance of and overall trust in the website (based on existing questionnaires ([22], [18], [19]) and adapted for our purposes). In addition, participants were provided with an image of the corresponding feedback prototype for one of the scenarios developed in the workshop (see Figure 2 and Figure 3) with textual explanations of each step, before being asked to answer the questions. The scenarios were chosen randomly, so that each participant saw one scenario with the feedback solution, and the other one without in random order.The participants were then asked whether they would like to be informed about the service recomposition in the proposed manner. After that, they answered the 30 adapted trust and acceptance items (e.g., "The website is deceptive.", "I could imagine using this website", "The website is reliable", to name a few). We chose this approach in order to be able to compare acceptance and trust in the website when (1) no feedback about the service recomposition is given to cases in which (2) feedback about the service composition is provided. Our assumption was that providing feedback to the website user should raise the acceptance of and trust in the website, compared to the no-feedback condition.

The questionnaire contained 38 questions in total, including demographic questions (age, gender, education), which were asked at the beginning. The items had to be answered on a 5-point Likert scale. Answering the questionnaire took about 10-15 minutes, and participants could win one of five Amazon vouchers worth 20 Euro as incentive. The questionnaire was distributed via several channels (student distribution list, Facebook, online portal of the Austrian National Student Union). In total, we received 101 completed questionnaires. The mean age of the participants was 26 years (SD=8.59); the youngest person was 18 and the oldest 65 years old. Female participants comprised 75%, while 25% were

[2] available at http://aniketos.icts.sbg.ac.at/questionnaire.html

male. Some of the results that were gained from the online payment scenario questionnaire were discussed at a workshop at SOUPS 2013[30]. In the following sections we describe the scenarios and prototypes that were created in the design workshop, followed by the questionnaire results for each scenario.

### 4.1 Scenario 1: Online Payment

*Data at risk: payment credentials.* A web shop offers its customers the possibility to add several payment options as well as all the necessary information to complete a financial transaction to their customer profile. The user must then choose one as the default payment option and rank the remaining options according to his/her preference. At the time a purchase is made the system will automatically attempt to conclude the transaction via the default payment method. If this fails for any reason, the system will try again with the next in the list and so on, until it is either successful or has exhausted all available payment methods, all without any additional user input. In the case of a successful transaction, the user is not immediately notified of any failed attempts the system might have encountered internally. The reasons for failed payment attempts range from harmless (e.g., temporarily busy server) to severe (e.g., stolen credit card or malware infection). In this particular case, a payment is made and, after payment via the default option fails, successfully concluded via the second option. The prototype for the online payment scenario (see Figure 2) displays multiple animated progress bars (one for each payment method) upon the user confirming their purchase. If one payment method fails, the prototype would halt its respective progress bar, grey it out, and shift focus to the next method's progress bar, until payment succeeded. Once that happened, another window opens that informs the user of the successful transaction as well as any unsuccessful attempts. Each mention of an unsuccessful attempt would contain a link to wherever the user could find out more about the details as to why that particular attempt had been unsuccessful (e.g., to the credit card company's website).


**Fig. 2.** Online payment scenario prototype excerpt

### 4.2 Scenario 1 Questionnaire Results

Generally, 14% of participants confirmed that they would use a website with automated payment transposition, whereas 37% indicated that they would rather not use such a website and 48% stated that they would not use it by any means. This high rejection seemed to further suggest that trust in such a system would have to be built in advance, as opposed to more traditional static services. In general, 78% of participants replied that they want to be informed in all cases about the payment transposition, 17% would prefer to be informed, and only 5% did not wish to be informed. This confirms our initial assumption that there is indeed a need for adequate feedback among a significant majority of all participants (i.e., the black box should not remain completely invisible to the user, even in a dynamic system).

Half of the participants were presented the feedback solution as described above and shown in figure 2 (the others did not receive this feedback). These participants were further asked whether they would want to be informed about the payment transposition in the presented way. More than a half of the participants (60% ) replied that they wanted to be informed in this way while 40% would prefer another way. Comparing the feedback and the no-feedback condition, we could not find any significant differences regarding the acceptance of the website, independent of whether the participants were happy with the feedback solution ($t(76)=1.569$, n.s.) or not ($t(68)=-.420$, n.s.). For trust, we found different results. Participants who were satisfied with the feedback solution did indeed show significantly higher trust in the website when feedback was provided ($t(77)=2.546$, $p<.05$).

However, 40% would have preferred a different feedback solution. Here we also found no difference regarding trust in the website compared to the no-feedback condition ($t(68)=-.146$, n.s.). To account for that possibility we had included the possibility to comment on which feedback the participants would prefer. Approximately 40% were dissatisfied with the overly passive nature of the feedback solution. They wanted to be able to choose whether the system should try again with the second credit card or cancel the payment as a whole. Another 20% expressed that the red warning box at the end (see Figure 2) had frightened them too much. They had automatically associated it with errors, danger, and money loss – regardless of the fact that payment was eventually successful.

So while we can conclude that, even in dynamic systems, the need to keep the user informed *at all times* takes priority over convenience, the discrepancy between effective feedback and convenience is not to be underestimated and can potentially devastating effects, considering the low initial trust users seem to put in such systems.

### 4.3 Scenario 2: Forum Post

*Data at risk: personal data.* An Internet Forum is split into a private and a public section. The private section is visible only to registered members, the public section to everyone. In this particular scenario, a posting is made in the

private section, containing personal details such as name, mailing address and phone number. During the time the post is written, but before it is submitted, owing to unfortunate circumstances the private section is switched to be visible to the public as well, so that at the time the user clicks "submit", the message is visible to everyone. The user notices this only a day later upon noticing that all sections of the forum are accessible without having logged in beforehand. We consciously chose a scenario in which the default configuration was sub-optimal in order to elicit when and how the user would want to be informed about and deal with such cases. The prototype from the forum post scenario (see Figure 3) notifies the user of the change in forum visibility directly via private message as well as via a notification in the system and privacy settings menu. Links to both sections are visible all the time (envelope and lightning bolt in the top frame) and superimposed with an exclamation mark whenever an important change occurs. In addition, the prototype featured a real-time warning system that worked similarly to an autocorrect function: It scans the text typed in for strings that look like addresses, telephone numbers, etc., highlights them and gives the user a brief warning that the information will be posted in a public section. In addition, the user also receives a brief recommendation on how to handle potentially sensitive data (e.g., "You might want to send this as a personal message instead."). Upon trying to send the message, the user receives another warning and is prompted to confirm that they want to send the message. They are presented with three options: send the message, delete it, or edit it. The button to edit the message is highlighted by default.

### 4.4 Scenario 2 Questionnaire Results

After being given the textual description of the scenario, participants were asked whether they would use the described website to post their contact details. Only 18% replied that they would use it, whereas 49% expressed that would rather not use it, and 33% that they would definitely not use it. An overwhelming majority (84%) wanted to be informed by all means if a change in the privacy

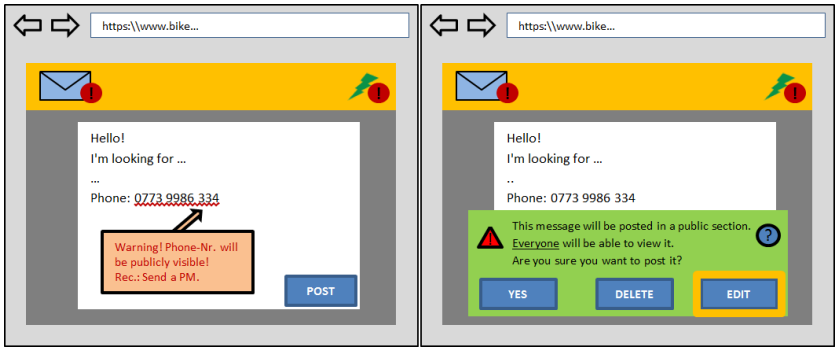


**Fig. 3.** Forum post scenario prototype excerpt

settings occurred, whereas 11% would rather be informed and only 3% were not interested in being informed at all. Once again, half of the participants were presented the feedback solution as described above and shown in figure 3, while the other half did not. Almost all of the participants (92%) presented with the feedback solution for this scenario, replied that they want to be informed in this way, while only 8% would have preferred another way. Here it was mentioned that some general hints and tips at the end with the possibility to confirm, cancel, or change would be better as it could be "exaggerated and disturbing if a warning appears at every underlined word". As opposed to scenario 1 we could find highly significant differences regarding acceptance ($t(99)=-3.67$, $p<.001$) and trust ($t(99)=-9.20$, $p<.001$) in the website depending on whether feedback was provided or not. Acceptance ($M=3.31$, $SD=.60$) and trust ($M=3.40$, $SD=.65$) were higher when feedback was given compared to when no feedback was given (acceptance: $M=2.90$, $SD=.53$; trust: $M=2.34$, $SD=.50$). We believe that this is due to the much higher satisfaction with the provided feedback solution as compared to scenario 1.

**Summary** Regarding feedback modality, it seems that established ways of providing user feedback work and are understandable as well as acceptable in cases of dynamic web service exchanges. Furthermore, we can confirm that when high or medium risk is involved, the need for adequate and frequent feedback is higher than the desire for convenience, even in a dynamic system. Even so, a solution like the one in scenario 2 (potentially underlining every word was considered to be too much) shows that there is a fine line that separates what is necessary from what is too much.

It should be noted at this point, that when we designed the scenarios, we wanted to simulate a world in which dynamic web service systems were already part of a user's everyday web experience. We did this in order to gain more natural reactions and results that are less influenced by any sense of novelty of dynamic service transposition. So we took interactions we assumed everyone would be mostly familiar with (online payment and forum posting) and included a dynamic component. This also meant that the scenarios were only similar *in principle* to how a dynamic web platform would operate. While we succeeded in eliciting familiarity from the workshop participants, the dynamic component seemed weird and alienating to some. We received comments like "I would never use a service that works in such a strange way." or "But why does it work exactly like *this*? That seems very strange to me". Scenario 2 (forum post) seemed particularly unrealistic in this regard. It could furthermore be assumed that the high rejection rates (14% and 18%, respectively) of the feedback solution in the questionnaire study is at least somewhat due to the scenario description not being entirely adequate. In retrospect, it might have been better to put less emphasis on the user's familiarity with a given scenario and to focus more on making it work exactly as it would in a dynamic system instead.

The feedback solution for scenario 1 had a significantly positive effect on the user's trust in the system as opposed to when no feedback was given, but

only when the way feedback was provided was accepted by the user. The same was true for scenario 2, except that we could not find a significant difference for participants who did not accept the feedback solution, due to the low number of participants who were dissatisfied with the feedback from scenario 2. Our finding, that adequate feedback does indeed increase trust in the platform, might not be very surprising on its own. However, automatisation and convenience are two of the main benefits of dynamic systems. So it is interesting to see a clear priority of feedback over convenience even here.

## 5 Discussion

In the following we discuss and analyze our results from the interview and questionnaire study, contrasting them (if applicable) with the principles for trust design developed by Riegelsberger and Sasse [24]. Our aim is to derive recommendations for security feedback and trust in dynamic websites and to point out, which particularities have to be considered in this specific context.

**Trust assessment:** According to Riegelsberger and Sasse [24], a user's assessment of the trustworthiness of a website is always a secondary task to their primary goal, whichever that might be. The whole point of automation in a dynamic web system is to let the users focus on their primary tasks. The interviewee's preferences expressed during the interview studies seemed to emphasize that as soon as a user has to devote more effort to trust assessment than to their initial primary goal, the automated system loses its purpose and advantage over traditional systems. So establishing trust as well as providing adequate security becomes an even more difficult balancing act in the case of dynamic systems, as inadequate trustbuilding strategies and/or feedback solutions might lead to the system losing its main advantage. Hence, it should be kept in mind at all times when designing for a dynamic systems, that *trust assessment is a secondary task of primary importance.*

**Risk:** A dynamic service platform cannot remain a completely invisible black box once risk for the user is involved, or the user's uncertainty will increase, and their trust in the platform decrease as a consequence [8]. The results from the interview study showed a clear influence of risk on the desire for feedback among users, i.e., while our interviewees wanted to be informed, e.g., when financial risk was involved, they did not care about changes of weather services. The high rejection rates of both scenarios from the questionnaire study further suggest, that the benefits of dynamic services do not counteract the potential risk of personal data or even money loss. Although we also have to point out here, that the participants did not get any further information about the underlying system responsible for the web service recomposition, i.e., information in terms of a trust seal (as wished by some participants in the interview study) or information about its reputation was missing. Hence, we certainly had the worst case scenario here with the website user knowing nothing about the "security guard in the background", i.e., the trustee was "opaque" to the trustor. Furthermore, a problem lies in the fact that a potential risk for the user might not always

perceived as such. It is, therefore, further recommended that *feedback messages should contain information on the type of risk involved, in order to gain the user's understanding and their trust, but only if it is really warranted.* This goes hand in hand with the principle of "Trust requires risk and uncertainty" by Riegelsberger and Sasse.

**Reliance:** From both the interview and questionnaire studies we found that users have very low initial trust in a dynamic web service platform. This is certainly in part due to the fact that such services are not yet very widespread in today's Internet. Another factor that is likely a great influence here is what we like to call the "opaque trustee" phenomenon, as mentioned above. The interview study showed a desire of users to know who they are interacting with. So the users know of the fact that they are interacting with a multitude of services, but it cannot be expected of them to separately assess every single of these services with regard to its trustworthiness. However, if the user has had successful interactions with the system and its services, then the resulting reliance should take precedence over the unrealistic expectation of having to assess each potential web service's trustworthiness individually. So we suggest to go even further than Riegelsberger and Sasse's original principle "Support reliance, as well as trust", and argue that in dynamic systems, *reliance is fundamental for trust and reliance-fostering measures should be treated as important as (or perhaps even more important than) traditional trust building strategies.*

**Feedback density:** Security feedback is a difficult balancing act of giving the user all the information necessary without annoying or frightening them. A high density of warning messages or similarly alarming feedback might easily intimidate a user and scare them off from using a certain web service. Nevertheless, the emphasis the design prototypes put on frequent and dense feedback, together with the relative success these feedback solutions had in the questionnaire study, suggests that in risk-involving cases the emphasis should clearly be put on informing and warning the user, with less regard for potential side effects. In dynamic systems *the user needs to be able to act immediately on any potential security issues.* This is only possible if these issues *are clearly perceived as such* by the user. However, one question remains at this point. Although most participants indicated in the questionnaire study that they wanted to be informed about the service recomposition by all means, further focus should be put on the active perception of such feedback over a longer period of time. As pointed out in section 2, after some time website users might get annoyed by these messages or just click them away without reading them. Furthermore, it still needs to be investigated how frequent web service recompositions, and with it frequent security feedback, would impact the overall trust in the website.

**Choice and control:** When using a dynamic platform, the user is already delegating many of their choices to the platform. It is therefore very important that, when any event occurs that is important enough so that the user needs to know about it, the user is able to make a choice. The results of the questionnaire study clearly showed, that the feedback solution for the payment scenario was less preferred than the feedback solution for the posting scenario. In the former

scenario, the users complained about not being given a choice (as opposed to the posting scenario) when the feedback was given, even though the scenario had allowed a multitude of choices via a user preference menu. This means that *the user needs to be able to make an active choice right as the feedback happens*, regardless of any other choices made by the user before that time. If the user perceives that they have no control at all even when risk is involved, they will not trust the platform. This goes hand in hand with the previous recommendation regarding the security feedback, in that a user will appreciate feedback that offers them to make a choice over being railroaded. From our findings we can only confirm this for cases in which risk is involved and, as a consequence, recommend this strategy to be applied only in such cases and not overload the user with information in low or no risk cases.

**Color coding:** The perception of trust signals also depends on the situation the user is in at the time of interacting with the system. So if there is a multitude of situations a user of the system could potentially be in (e.g., using a payment service vs. reading a news site), then these differences must be accounted for. In our research we found that a high feedback density, with an emphasis of clearly warning the user, was acceptable over a more passive approach in risk-involving cases. However, a large number of participants from the questionnaire study was not satisfied with the feedback provided for the payment scenario. Apart from the problem of no choice mentioned above, many users had expressed dissatisfaction with the color coding, which had mainly adhered to common practices (red to warn the user, green to express everything works normally, etc.). However, when a web service recomposition happens, conflicting information has to be provided to the website user, i.e., that one service is secure and working, while the other is not. We conclude, that *it is better to avoid signal colors that connote danger or peril in cases of feedback in dynamic systems. In such cases, the warning should be communicated via the feedback text and not via its color.*

## 6 Conclusion and Future Work

We wanted to know how and under which conditions security feedback in dynamic web systems should be given and what its influence on user trust is. After a qualitative study, in which we explored these questions from a user perspective, we refined our findings in a final quantitative study. We matched our findings to the trust design principles laid out by Riegelsberger and Sasse [24] and were able to generate a concise list of recommendations for security feedback design in dynamic systems. This list shall serve as a reference for user-system trust design in HCI. There are still some unanswered issues that need to be investigated in the future. In our investigations, we focused on scenarios involving financial risk and the risk of losing personal data. While these rather medium to high risk cases are certainly the most important ones, we only gathered preliminary insights for low or no risk cases in the interview study and did not examine long-term security feedback effects in the subsequent study. More research with actual high-fidelity prototypes is needed for a more decisive answer

on how feedback should be given in such cases. In the workshop for developing the feedback prototypes, we were working with a security pragmatist persona in order to cover the majority of Internet users. Although this is a good starting point, we believe that further research is needed on other (more extreme) user types. A one-for-all approach would be desirable, and we believe that shedding more light on the different particularities of certain user types, would help to refine and adapt security feedback in dynamic systems.

## 7 Acknowledgments

This work was funded by the European Union Seventh Framework Programme (FP7/2007-2013) under grant 257930 (ANIKETOS; see http://www.aniketos.eu/).

## References

1. Ackerman, M.S., Cranor, L.F., Reagle, Jr., J.: Privacy in E-Commerce: Examining User Scenarios and Privacy Preferences. In: Proc. 1st ACM Conf. on Electronic Commerce, ACM (1999) 1–8
2. Belanche, D., Casaló, L.V., Guinalíu, M.: How to make online public services trustworthy. Electronic Government, an International Journal 9(3) (01 2012) 291–308
3. Berendt, B., Günther, O., Spiekermann, S.: Privacy in e-commerce: stated preferences vs. actual behavior. Commun. ACM 48(4) (April 2005) 101–106
4. Bravo-Lillo, C., Cranor, L.F., Downs, J., Komanduri, S., Sleeper, M.: Improving computer security dialogs. In: Human-Computer Interaction–INTERACT 2011. Springer (2011) 18–35
5. Cooper, A., Reimann, R., Cronin, D.: About Face 3: CoThe Essentials of Interaction Design John Wiley & Sons, Inc., New York, NY, USA (2007) 75–108
6. Corritore, C.L., Kracher, B., Wiedenbeck, S.: On-line trust: concepts, evolving themes, a model. Int. Journal of Human-Computer Studies 58(6) (2003) 737–758
7. Diller, S., Lin, L., Tashjian, V.: The human-computer interaction handbook. L. Erlbaum Associates Inc., Hillsdale, NJ, USA (2003) 1213–1225
8. Dzindolet, M., Peterson, S., Plmranky, R., Pierce, L., Beck, H. The role of trust in automation reliance. Int J. Hum.-Comput. Stud. 58(6) (June 2003) 697-718
9. Egelman, S., Cranor, L.F., Hong, J.: You've been warned: an empirical study of the effectiveness of web browser phishing warnings. In: Proc. SIGCHI Conf. on Human Factors in Computing Systems. CHI '08, New York, NY, USA, ACM (2008) 1065–1074
10. Elahi, G., Yu, E.: A Goal Oriented Approach for Modeling and Analyzing Security Trade-Offs In: Proc. 26th Int. Conf. on Conceptual modeling. ER '07, volume 4801 of LNCS, Springer (2007) 375–390
11. Flavián, C., Guinalíu, M., Gurrea, R.: The role played by perceived usability, satisfaction and consumer trust on website loyalty. Information & Management 43(1) (2006) 1 – 14
12. Friedman, B., Khan, Jr., P.H., Howe, D.C.: Trust online. Commun. ACM 43(12) (December 2000) 34–40
13. Glass, A., McGuinness, D.L., Wolverton, M.: Toward establishing trust in adaptive agents. In: Proc. 13th Int. Conf. on Intelligent User Interfaces. IUI '08, New York, NY, USA, ACM (2008) 227–236

14. Hoff, K., Bashir, M.: A theoretical model for trust in automated systems. In: CHI '13 Extended Abstracts on Human Factors in Computing Systems. CHI EA '13, New York, NY, USA, ACM (2013) 115–120
15. Johnston, J., Eloff, J., Labuschagne, L.: Security and human computer interfaces. Computers & Security 22(8) (2003) 675 – 684
16. Kumaraguru, P., and Cranor, L. F. Privacy indexes: A survey of Westin's studies. ISRI Technical Report (2005).
17. Maurer, M.E., De Luca, A., Kempe, S.: Using data type based security alert dialogs to raise online security awareness. In: Proc. SOUPS '11, NY, USA, ACM (2011) 2:1–2:13
18. Master, R., Jiang, X., Khasawneh, M. T., Bowling, S. R., Grimes, L., Gramopadhye, A. K., and Melloy, B. J. Measurement of trust over time in hybrid inspection systems: Research articles. Hum. Factor. Ergon. Manuf. 15, 2 (Mar. 2005), 177–196.
19. McKnight, D.H., Carter, M., Thatcher, J.B., Clay, P.F.: Trust in a specific technology: An investigation of its components and measures. ACM Trans. Manage. Inf. Syst. 2(2) (July 2011) 12:1–12:25
20. Pak, R., Fink, N., Price, M., Bass, B., and Sturre, L. Decision support aids with anthropomorphic characteristics influence trust and performance in younger and older adults. Ergonomics 55, 9 (2012), 1059–1072. PMID: 22799560.
21. Patrick, Andrew S., B.P., Marsh, S.: Designing systems that people will trust. In: Security and Usability. O'Reilly Media, Inc. (2005)
22. Pavlou, P.A.: Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. Int. J. Electron. Commerce 7(3) (April 2003) 101–134
23. Raja, F., Hawkey, K., Hsu, S., Wang, K.L.C., Beznosov, K.: A brick wall, a locked door, and a bandit: a physical security metaphor for firewall warnings. In: Proc. SOUPS '11, NY, USA, ACM (2011) 1:1–1:20
24. Riegelsberger, J., Sasse, M.A.: Ignore these at your peril: Ten principles for trust design. In: Trust 2010. 3rd International Conference on Trust and Trustworthy Computing. (2010)
25. Riegelsberger, J., Sasse, M., McCarthy, J.: The mechanics of trust: A framework for research and design. International Journal of Human-Computer Studies 62(3) (2005) 381–422
26. Riegelsberger, J., Sasse, M., McCarthy, J.: The researcher's dilemma: evaluating trust in computer-mediated communication. International Journal of Human-Computer Studies 58(6) (2003) 759–781
27. Sheehan, K.B.: Toward a typology of internet users and online privacy concerns. The Information Society (2002) 21–32
28. Sinha, R., Swearingen, K.: The role of transparency in recommender systems. In: CHI '02 Extended Abstracts on Human Factors in Computing Systems. CHI EA '02, NY, USA, ACM (2002) 830–831
29. Stoll, J., Tashman, C.S., Edwards, W.K., Spafford, K.: Sesame: informing user security decisions with system visualization. In: Proc. SIGCHI Conf. on Human Factors in Computing Systems. CHI '08, NY, USA, ACM (2008) 1045–1054
30. Raja, F., Hawkey, K., Hsu, S., Wang, K.L.C., Beznosov, K.: No choice, no trust? A Turn for the Worse: Trustbusters for User Interfaces Workshop (SOUPS '13). http://cups.cs.cmu.edu/soups/2013/trustbusters2013/No_Choice_no_Trust_Troesterer.pdf (2013)
31. Wang, L., Jamieson, G.A., Hollands, J.G.: Trust and reliance on an automated combat identification system. Human Factors: The Journal of the Human Factors and Ergonomics Society 51(3) (2009) 281–291