# An Analysis of User Interface Factors Influencing the Acceptance of Code Download

Gianluca Dini
Pierfrancesco Foglia
Cosimo Antonio Prete
*Information Engineering Department*
*Engineering Faculty, University of Pisa,*
*V. Diotisalvi, 2 – 56126 Pisa (Italy)*
*{dini, foglia, prete}@iet.unipi.it*

Michele Zanda
*Computer Science and Engineering*
*IMT Institute for Advanced Studies*
*V. S. Micheletto, 3 – 55100 Lucca (Italy)*
*michele.zanda@imtlucca.it*

**Abstract**. *In this paper we analyze how the elements in the Microsoft Authenticode interface influence final users' decisions about downloading code from the Internet. Results show that the users' behavior appears to be mostly driven from the code publisher name, without considering other information provided by the interface. A proposal to improve the user interface is currently under evaluation.*

**Keywords.** Usability, authentication, user tests, security.

## 1. Introduction

Internet authentication procedures and related user interfaces allow providers to offer their services to remote users. In such environment, the design of the user interface is critical both for users and service providers. In fact, users can be exposed to unacceptable risks and damages if interfaces are hard to learn and use, don't allowing aware decisions [2, 8]. Software providers can become unable to distribute their services on the Internet, if risks and damages reduce users' trust in the procedures. As of our knowledge, there are no guidelines for designing such critical interfaces.

In this paper, we present a usability analysis of the Microsoft Authenticode [11] interface for code download on the Internet. We analyze which elements in the Security Warning dialog box (Fig. 1) influence the users when they have to decide whether to accept or refuse the download of regularly certified code. We adopted the Authenticode technology due to its wide diffusion in the Internet.

In our tests we changed some elements of the Security Warning dialog box and we tested the effects of these changes on the users' behavior. In particular, we investigated the following factors: how the elements in the Security Warning dialog box influence the user attention; and how the elements in the Security Warning dialog box influence the acceptance of code download or its refusal.

Starting from our results, we propose an alternative interaction model, which is currently under evaluation.

The rest of the paper is organized as follows: the next section briefly describes the Microsoft Authenticode technology. Then, we describe the experiment methodology and discuss the obtained results. Finally, we describe our on-going research work.

## 2. The Authenticode technology

We analyzed the Authenticode version released with Internet Explorer 6 SP-1. A software publisher signs the code and publishes a package containing the signed code together with the publisher's certificate released by a given Certification Authority (CA). Upon downloading the code, a user's browser verifies the signature on the code. If the verification is successful, the browser shows a Security Warning dialog box (Fig. 1).

If the signature cannot be verified, this is a security problem and the user is notified with a different dialog box.

The dialog box reports information that is supposed to be useful for the end user's decision to accept or refuse the code download: it encloses the name of the CA, the name of the software publisher, the software name, its price. The Microsoft Authenticode technology only binds the software publisher and the code. It does not give any guarantee about the code quality.

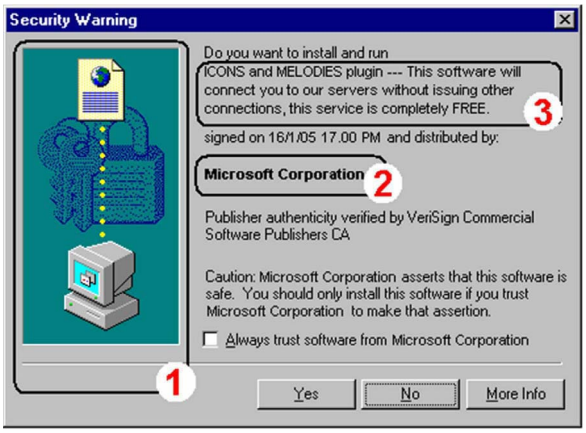


**Figure 1. The Security Warning dialog box with the parameters that have been tested: (1) the image, (2) the software publisher name, (3) the information about the code to be downloaded. This is a layout without link.**

## 3. The experiments

Our goal was to evaluate how the users' attention and behavior were influenced by the information provided in the Security Warning dialog box. In particular, we tested the influence of the type of the image, of the publisher name, of the presence of either code information or a link to an external web page conveying that information (Fig. 1). In order to test the influence of each parameter, we arranged a set of Internet pages and corresponding Security Warning dialog boxes. Such dialog boxes included the usual image or an impressive one (Fig. 2). Software publishers were varied according to the following: names of famous companies, names of unknown companies, deceptive names of companies, and names of companies that provide adult contents. The link, whether present, was pointing to a web page with the cost information of the code. If the link was not present, the cost information appeared in the dialog box.

### 3.1 Method

*Control* windows guided participants in the experiments. Such windows included a short tutorial at the beginning of each experiment and *information* windows. The *information* windows included: a *start*, a *end* and an *interest* window. The *start* and *end* windows were shown respectively at the beginning and at the end of each test session. The *interest* window, shown four seconds after a participant visits an Internet page, consists of three radio buttons to assess the level of interest of the participant in the page content (Fig. 3).

To avoid that results were influenced by a lack of interest, we considered only the tests that had the users' interest (first radio button in Fig. 3).

The Internet pages and the corresponding dialog boxes were prepared to include different combinations of the tests parameters. Each participant completed three separate test sessions, of about 5 minutes each, and answered a questionnaire in the end.

The results of the tests have been logged on text files for later analyses. In total, the overall tests were more than 1300.

Our methodology is similar to other usability studies [3, 6], in particular the reader can check [6] for a detailed description of the methodology we adopted.

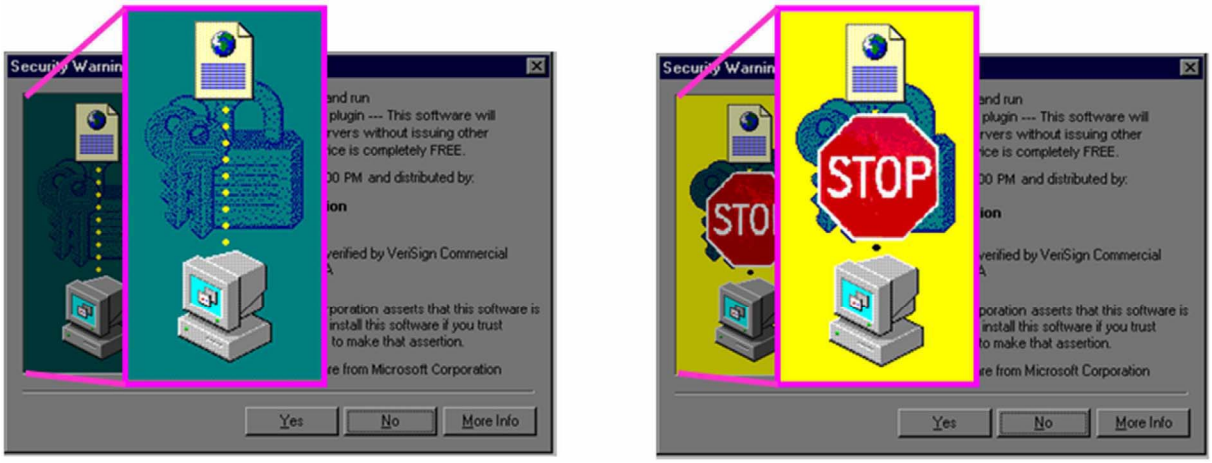


**Figure 2. The two images that have been used during our tests: the usual image (on the left) and an impressive one (on the right).**

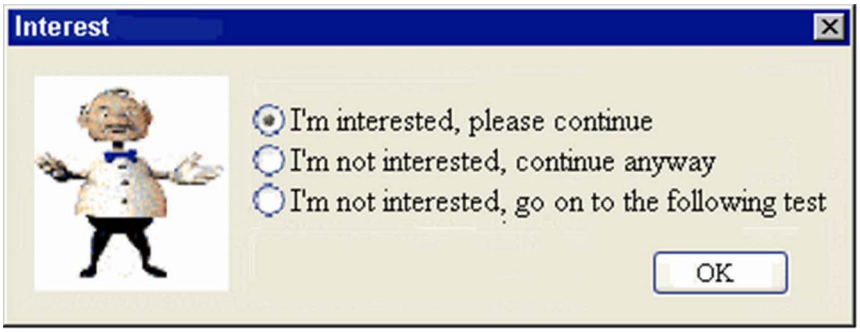


**Figure 3. The feedback window with three radio-buttons assessing the interest level of the participant.**

### 3.2 Participants

The tests were performed by undergraduate students at our Information Engineering Department, and by high school students in a local job fair. The participants were 43, with ages ranging from 17 to 28 years (mean age 20), and the group was gender balanced. This is a good age range for usability tests, as research suggests that older adults perform worse than young people (for the errors made [9] and mouse usage [14]). Besides, choosing too young participants is another problem, since they can have difficulties in performing tasks without assistance [3, 4]. The participants were not rewarded for their time, but they were told that "they were participating to the design of the next user interface for e-government web sites".

### 3.3 Tests classification and questionnaire

Before showing our results we need to introduce a few basic definitions. The code that is proposed to the users is said to be *free* if its use doesn't imply added costs to the normal Internet connection, and it is said to be *costly* if its use implies added costs to the Internet connection (e.g.: dialers). Moreover, the code is defined as *accepted* if the user clicks *yes* in the security warning dialog box, otherwise it is *refused*.

At the beginning of a test session, a start window told each participant: *"try to download the maximum quantity of software minimizing the risks, whatever this means to you"*. Participants were aware that the shown information was true (not fraudulent), since we wanted to evaluate the awareness degree of the information shown in the dialog box. At the end of the tests, the participants answered a usability questionnaire [10] containing 20 questions. The answers to the questionnaire helped us to identify the concept of risk for our participants. The risks identification phase drove the classification of the tests between *correct* and *wrong* ones. Since our participants did not want to download costly software (table 2), a costly code download acceptance was considered a *wrong* behavior. Furthermore, since participants were interested in the software, refusing free software was considered *wrong*, because they didn't consider it a risk. Conversely, accepting free software, or refusing costly software, was considered *correct*. Note that this classification among *correct* and *wrong* tests is an ad-hoc classification, which is useful to summarize the results and classify the users' behaviors. It is related to the users' intentions with respect to their actual actions. In an absolute way, downloading free or costly code can hardly be considered correct or wrong.

### 3.4 Analysis techniques

The results are reported with the ANOVA analysis [5] or simply reporting percentage data.

## 4. Results

The overall wrong ratio resulted to be rather high: 38%, and only one participant completed the test with an error rate below 15%.

### 4.1 Image type effect

No significant effect of the image type was observed on participants' behavior while dealing with a normal or impressive image. ANOVA results: $F(1,84)=1.02$, $p=0.315$ (Table 1). Roughly, p-values estimate the likelihood that observed differences are due to chance. Group cardinalities and degrees of freedom can be derived by the formulas.

### 4.2 Link presence and publisher name effect

Table 1 shows the outcome of the tests about the link parameter. Such results show that the link presence influenced the participants' behavior. ANOVA results: $F(1,84)=5.13$, $p=0.026$.

Participants, when the link was present, did not use it in the 97% of the cases. Despite this fact, the prevalence has still been of correct answers. This result is a consequence of the fact that most of our tests were designed to replicate real browsing scenarios. Thus, the Security Warning dialog box with link has been included in pages of well-known companies (Macromedia Inc., Microsoft Corporation) that offered free software, and in pages of companies providing adult contents that offered costly software (Table 3).

The results of the former scenarios show that participants are very willing to accept downloading software from well-known companies (Table 3), even if they cannot know the cost of the software because they do not use the link (in 97% of the cases it has not been used). Participants strongly refused to download the code published by adult contents providers.

Users tend to trust well-known software houses and tend to accept their software (Table 3). In contrast, users do not trust companies providing adult contents and refuse to download from them even without reading the actual costs. Note that the users were interested in the page, and that they considered added value connections a risk (Table 2): but the adult content was proposed with no value added connection. It follows that the correctness of the results is not due to the information shown in the dialog box, but rather to the participants' previous knowledge and feelings about the company name.

During the test sessions we also proposed costly code by a well-known publishing company (Table 3) with cost information immediately readable in the dialog box. Despite this fact, the wrong ratio of such scenario resulted to be very high (49%), since participants tend to accept in any case the download of code published by a well-known company. Note again that for the users, costly software is a risk in any case, as appears in Table 2.

The same tendency has been confirmed in further tests with deceptive names of companies. In these tests, we prepared some web pages almost identical to the real ones, and we changed slightly the names of the code publishers. The dialog boxes that appeared had the same deceptive publisher names, with a link pointing to an external web page with cost information (no cost information in the dialog box text area). This configuration misled participants (Table 4).

When the dialog box presented a link, it was accessed very rarely (3% of the cases). In this aspect, the Security Warning dialog box doesn't respect the basic criteria of computer human interaction with regards to security [7]: it doesn't have a minimalist design. Participants, answering the questionnaire, told us that: 33% of them believed that the link led to a web page containing information about the software (but they didn't use it), 38% of them believed that it was a link to the publisher's home page, and the remaining 29% had other opinions (an executable file, a web page not checked by the CA) or had no idea.

**Table 1. Statistical evaluation of image type effect and link presence effect.**

| Hypothesis | ANOVA | Significance | Correct tests |
|---|---|---|---|
| An impressive image provides more correct tests than a normal image | $F = 1.02$ | Not significant | 61.73 % (normal image)<br>58.27 % (impressive image) |
| A dialog box with link provides more correct tests than a link-less dialog box | $F = 5.13$ | Significant | 55.52 % (no link)<br>64.19 % (with link) |

**Table 2. Some major questions asked at the end of the tests. The questionnaire did not suggest the answers to the participants.**

| Question | Yes | No | Don't know |
|---|---|---|---|
| Is it a risk for you that software download implies other costs? | 93 % | 7 % | 0 % |
| Is it a risk for you that software usage implies an added value connection? | 93 % | 7 % | 0 % |
| Do you think that the image in the dialog box increases your attention? | 67 % | 12 % | 21 % |
| Was the image in the dialog box always the same? | 16 % | 40 % | 44 % |

**Table 3. Tests results with well-known software publishers, unknown publishers and publishers providing adult contents, respectively.**

| Code Publisher | Code type | Code info | Correct tests |
|---|---|---|---|
| Well-known | Free | In an external page | 89 % (major accepted) |
| | Costly | In the text area | 51 % |
| Unknown | Free | In the text area | 49 % |
| | Costly | In an external page | 70 % (major refused) |
| Adult contents | Free | In the text area | 18 % (major refused) |
| | Costly | In an external page | 71 % (major refused) |

**Table 4. Tests results with publishers whose name is deceptive.**

| Code Publisher | Code type | Code info | Correct tests |
|---|---|---|---|
| Deceptive name | Costly | In an external page | 23 % (major accepted) |

## 5. Discussion and future work

In summary, participants tend to accept code download if it is provided by a well-known company (Table 3) or one believed so, even if it is costly software (Table 4). According to our experiments, such results indicate that the Security Warning dialog box doesn't ensure a high awareness level in the participants.

The dialog box doesn't succeed in communicating to users important features to accomplish their tasks. So, as users don't get the required information from the interface, they decide on the basis of their trust in the information source. This result accords with the Elaboration Likelihood Model of persuasion: if a decision is not of vital personal importance, then source characteristics, such as trustworthiness and likableness of the source of information, have a significant influence on the decision [1, 13].

In this aspect, the code download procedure does not respect the usability principle: *recognition rather than recall* [12]. Users only recall the code publisher name, without understanding the other information shown in the dialog boxes.

Furthermore, changing the appearance (type of image, link presence) of the Security Warning dialog box during the experiments did not change the tests' results significantly. In particular, the use of an impressive image instead of the usual one did not influence the tests results (Table 1).

The observed behaviors indicate that users find the dialog box hard to use as they do not understand the shown information. Our tests suggest that some objects of the user interface have little impact since they do not increase the user attention (at least concerning the tested impressive image) or are used very rarely (the link).

We think that forcing the users to read and understand the whole text in the dialog box can change the analyzed behaviors, since all the information needed to take aware decisions is in the text.

Our proposal to solve the above problems is to have an installation wizard, organized with three steps (Fig. 4). In the second step the wizard has to ask for some user feedback in order to check the user's awareness level about the presented information. Only when the user feedback matches with the given information, the procedure goes on, permitting to download or refuse the software. Currently, we are conducting user tests to validate this approach.

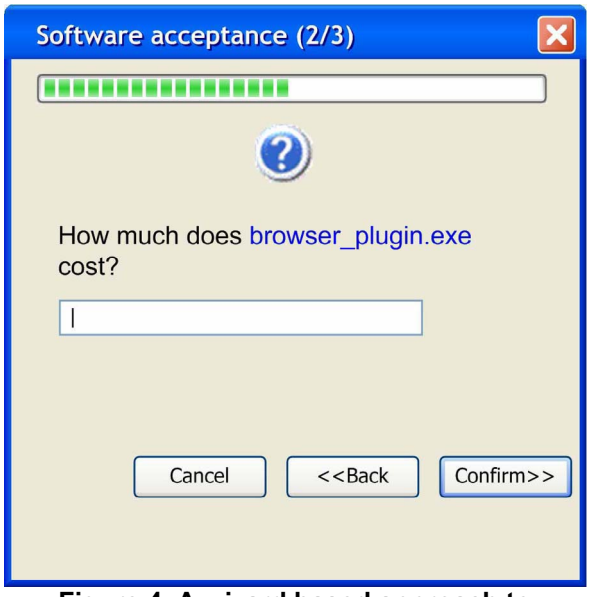


**Figure 4. A wizard based approach to increase the users' awareness level**

## 6. Conclusions

When dealing with procedures for code download from the Internet, usability issues are

as much important as the protocol security aspects, since users can perform unaware actions with a safe security protocol.

We tested the usability of the Microsoft Authenticode technology, used to download code from the Internet. Results indicate that the related Security Warning dialog box is not fully usable. Users do not fully understand the information that the dialog box is showing them, and the major influencing factor is the name of the code publisher. If the user knows the publisher name (or believes knowing it), he is more willing to accept the code download. The tests results show that the image type in the Security Warning dialog box does not influence the users' attention and that the link is almost unused.

Starting from our results, we propose a wizard-based approach to increase the users' awareness level. The effectiveness of such approach is currently under evaluation.

## 7. Acknowledgments

This work has been supported by the "Fondazione Cassa di Risparmio di Pisa", in the framework of the *Easy.Gov* project, for the development of usable e-government websites. Participants were aware of this fact while performing the experiments.

## 8. References

[1] Bickmore T-W, Picard R-W. Establishing and Maintaining Long-Term Human-Computer Relationships. Transactions on Computer Human Interaction; 12(2): 293–327; ACM Press (2005).

[2] Brustoloni X, Brustoloni J-C. Hardening Web browsers against man-in-the-middle and eavesdropping attacks. In Proc. of the 14th Int. Conf. on World Wide Web; ACM Press (2005); Chiba, Japan; 489-498.

[3] Hourcade J-P, Bederson B-B, Druin A, Guimbretière F. Differences in pointing task performance between preschool children and adults using mice. Transactions on Computer Human Interaction; 11(4): 357-386 ACM Press (2004).

[4] Inkpen K-M. Drag-and-drop versus point-and-click mouse interaction styles for children. Transactions on Computer Human Interaction; 8(1): 1-33; ACM Press (2001).

[5] Glantz S-A. Primer of Biostatistics. McGraw-Hill Medical Publishing, New York; 2005.

[6] Hornbaek K, Bederson B-B, Plaisant C. Navigation patterns and usability of zoomable user interfaces with and without an overview. Transactions on Computer Human Interaction; 9(4): 362-389; ACM Press (2002).

[7] Johnston J, Eloff J-H-P, Labuschagne L. Security and human computer interfaces. Computers & Security; 22(8):675-684; Elsevier (2003).

[8] Kormann D-P, Rubin A-D. Risks of the Passport single sign-on protocol. Computer Networks; Elsevier (2000); 33(1-6): 51-58.

[9] Kubeck J-E, Delp N-D, Haslett T-K, McDaniel M-A. Does Job-Related Training Performance Decline With Age? Psychology and Aging; 11: 92-107; APA (1996).

[10] Lewis J-R. IBM Computer Usability Satisfaction Questionnaires: Psychometric Evaluation and Instruction for Use. International Journal of Human-Computer Interaction; 7(1): 57–78; LEA (1995).

[11] Microsoft Authenticode; 2005. http://msdn.microsoft.com/library/default.asp?url=/workshop/security/authcode/authenticode_ovw_entry.asp.

[12] Nielsen J. Enhancing the explanatory power of usability heuristics. In Proc. of Int. Conf. on Computer Human Interaction, ACM Press (1994); 152-158.

[13] Petty R-E, Wegener D-T. Attitude change: Multiple roles for persuasion variables. In The Handbook of Social Psychology. 323–390; McGraw-Hill, New York, 1998.

[14] Riviere C-N, Thakor N-V. Effects of Age and Disability on Tracking Tasks with a Computer Mouse: Accuracy and Linearity. Journal of Rehabilitation Research and Development; 33: 6-16; (1996).

[15] Thomas B-H, Calder P. Applying cartoon animation techniques to graphical user interfaces. Transactions on Computer Human Interaction, ACM Press (2001); 8(3): 198-222.