Johnny in Internet Café:
User Study and Exploration of Password Autocomplete in Web Browsers

Kemal Bicakci
TOBB University of Economics and Technology
Ankara, Turkey
bicakci@etu.edu.tr

Nart Bedin Atalay
Selcuk University
Konya, Turkey
nartbedin@gmail.com

Hakan Ezgi Kiziloz
TOBB University of Economics and Technology
Ankara, Turkey
hakanezgi@etu.edu.tr

ABSTRACT

One of the most popular aids adopted by users to reduce the pain suffered from the use of passwords is browsers' autocomplete feature. This feature, caching username and password after getting the user consent and using them later for automatic completion, is available in all modern browsers but communication with the user asking consent is implemented in different ways. In this paper, we report on user studies comparing active communication with a blocking dialog box and passive communication with a non-intrusive toolbar. We found that a dialog box misled users to save passwords in public computers. Conversely, no security problem was observed with passive communication. Our exploration provides empirical evidence for the risks of preferring active communication for password autocomplete and other similar interactions and sheds light on many other aspects of password autocomplete.

Categories and Subject Descriptors

C.2.0 [**Computer-Communication Networks**]: General-Security and Protection; H.5.2 [**User Interfaces**]: Evaluation/methodology.

General Terms

Experimentation, Security, Human Factors.

Keywords

Usable security, passwords, user study.

1. INTRODUCTION

Given the growing number of accounts users have passwords for [4], password management incurs an overwhelming cognitive load and becomes a herculean task not easily be succeeded without any aid. One popular aid adopted by users to reduce the pain suffered is browsers' autocomplete feature [7].

While many aspects of the password problem have been studied in the literature (e.g., [4][5][7]), despite its wide adoption up to our best knowledge no previous study on password autocomplete has been reported. In this paper, we make a first attempt towards having a better understanding for the security risks and usability benefits of this feature. Specifically, the emphasis in this work is on user interfaces for password autocomplete and the risks when public computers are in use.

Today, all modern web browsers support password autocomplete; caching username and password after getting the user consent and filling fields automatically thereafter. In all of these browsers, input from the user is asked before the password is stored because it is not secure to save the password in a computer not owned by the user. Users are supposed to make the correct decision. They should choose not to store when the computer they use is not solely under their control (e.g., public or borrowed machines), whereas they are free to use this useful feature when there is no security consequence or when security risks are relatively smaller (e.g., their own laptop).

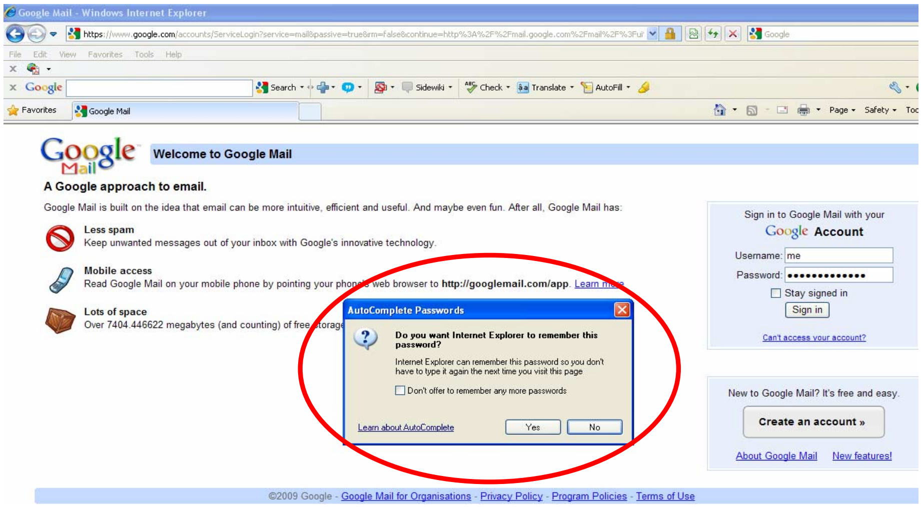
Different types and versions of web browsers implement the password autocomplete feature in different ways. Specifically, version 8 of Internet Explorer communicate users with a dialog box which blocks them continuing (Figure 1). On the other hand, Firefox version 3 applies the non-intrusive toolbar approach (Figure 2). The main research question we investigate in this paper is whether the aforementioned implementation choice has an impact on taking the right decision of not saving passwords on public computers. Besides this central focus, our study pursues a number of other usability issues surrounding the password autocomplete feature. For these purposes, we conducted a series of user studies and reported on the results. In summary, we found that non-intrusive toolbar approach provides a significantly more secure user experience. We argue that our results can be generalized to similar interface problems, and hence we conclude that secure interaction designers should think twice before choosing active type of communication if simply neglecting the message does not pose any security threat.

The rest of our paper is organized as follows: Section 2 summarizes related work. Section 3 provides more information on password autocomplete feature. Section 4 presents the method and results of our usability studies. Section 5 provides a general discussion of the results. Section 6 concludes the paper.

2. RELATED WORK

Being a weak link in the security chain and becoming a real nuisance for users, passwords have always been an important

DIM'11, October 21, 2011, Chicago, Illinois, USA.


Google Mail - Windows Internet Explorer
https://www.google.com/accounts/ServiceLogin?service=mail&passive=true&rm=false&continue=http%3A%2F%2Fmail.google.com%2Fmail%2F%3Fui
File Edit View Favorites Tools Help
Google Search Sidewiki Check Translate AutoFill
Favorites Google Mail
Page Safety Too
Yes
No
Sign in
Create an account »

Welcome to Google Mail

A Google approach to email.

Google Mail is built on the idea that email can be more intuitive, efficient and useful. And maybe even fun. After all, Google Mail has:

Less spam
Keep unwanted messages out of your inbox with Google's innovative technology.

Mobile access
Read Google Mail on your mobile phone by pointing your phone's web browser to **http://googlemail.com/app**. Learn more

Lots of space
Over 7404.446622 megabytes (and counting) of free storage

AutoComplete Passwords

Do you want Internet Explorer to remember this password?

Internet Explorer can remember this password so you don't have to type it again the next time you visit this page

□ Don't offer to remember any more passwords

Learn about AutoComplete

Sign in to Google Mail with your Google Account

Username: me

Password: •••••••••••••

□ Stay signed in

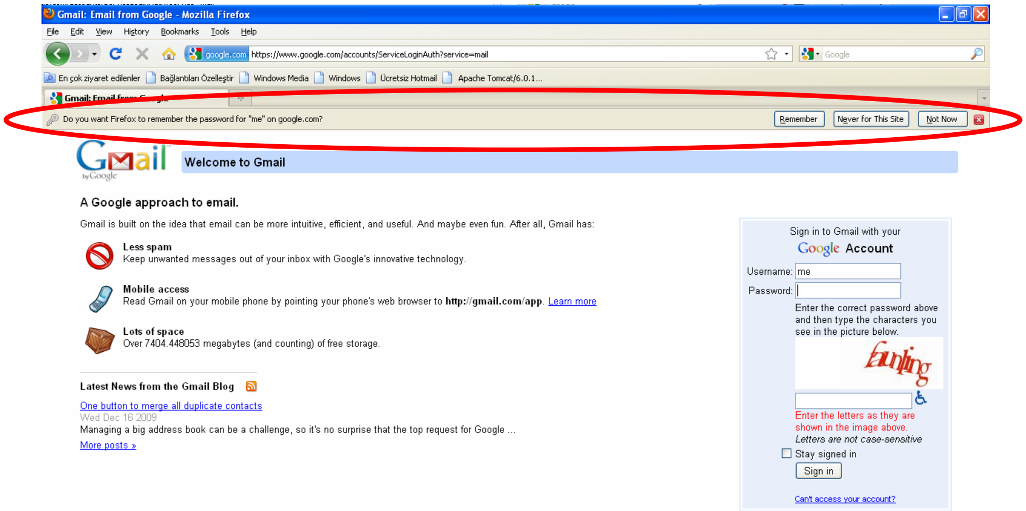
Can't access your account?

New to Google Mail? It's free and easy.

About Google Mail New features!

©2009 Google - Google Mail for Organisations - Privacy Policy - Program Policies - Terms of Use

Figure 1. User is expected to click on "AutoComplete Passwords" dialog box to be able to continue with his task in Internet Explorer 8.



Do you want Firefox to remember the password for "me" on google.com?

Welcome to Gmail

A Google approach to email.

Gmail is built on the idea that email can be more intuitive, efficient, and useful. And maybe even fun. After all, Gmail has:

Less spam
Keep unwanted messages out of your inbox with Google's innovative technology.

Mobile access
Read Gmail on your mobile phone by pointing your phone's web browser to **http://gmail.com/app**. Learn more

Lots of space
Over 7404.448053 megabytes (and counting) of free storage.

Latest News from the Gmail Blog

One button to merge all duplicate contacts
Wed Dec 16 2009
Managing a big address book can be a challenge, so it's no surprise that the top request for Google ...
More posts »

Sign in to Gmail with your Google Account

Username: me

Password:

Enter the correct password above and then type the characters you see in the picture below.

Enter the letters as they are shown in the image above.
Letters are not case-sensitive

□ Stay signed in

Can't access your account?

Figure 2. Password Autocomplete does not interrupt user's task with "Remember the Password" toolbar in Firefox 3.5 (in this example login attempt failed).

target for security research [10]. Fueled by the usability and security problems of passwords, a recent surge of research on this area has also been triggered (e.g., [9]). Today, we know many things about passwords; users generally choose weak passwords [4], they reuse their passwords over several accounts [5], etc. However we have not found any prior work on password autocomplete feature despite its common use in practice [7]. Below, we provide a summary of previous work related to this topic in a more general context.

The conceptual framework proposed by Cranor [2] is useful to identify problems when secure systems rely on a "human in the loop" to perform security-critical functions. Cranor argued that security decisions should be made by the system automatically whenever possible so that error-prone users are taken out of the security loop. However cases do exist for which this recommended best practice is not applicable [2] [19]. When a system should rely on user decisions to perform a security-critical function, communication with the user can be placed anywhere on a spectrum, ranging from active i.e., by interrupting user's primary task to passive i.e., available to users but can easily be ignored.

Less intrusive approaches are already considered to be more suitable in a number of situations. To exemplify; asking users to install a software in Firefox [15] and pop-up blocking in Internet Explorer (with Windows XP service pack 2) [11] is preferred to be presented to users in a non-intrusive toolbar. This is accepted as a good compromise and right balance between security and convenience [15]. It was acknowledged that if an intrusive dialog box is used instead to notify users, being conditioned to ignore such messages [6] [11] users want to dismiss the message in the quickest way possible [15]. Consequently, this habituation may lead to security breaches. On the other hand, the investigation on password autocomplete feature in this paper clearly shows that this user interface design principle has not been applied consistently throughout all browsers types and all relevant security interactions.

Guttman provides a nice overview of usability problems in security domain [6]. Particularly, the section on user conditioning (pages 70-75) is provoking. According to him, “Like Pavlov’s dogs, users quickly learn that clicking the close or cancel button allows them to continue doing what they want to do”.

On the other hand, passive communication is not appropriate in a number of situations. For instance, Dhamija et al. showed that passive security indicators are ineffective against phishing websites hence not recommended [3].

3. PASSWORD AUTOCOMPLETE

Password autocomplete feature would be the answer to all usability problems of passwords and free of security problems under ideal circumstances. In an ideal world where every Internet user has a single computer they always carry with them and that computer is reliable (not break down) and secure (no other person can have an access and there is no malware inside), then all problems that passwords bring for the Internet would suddenly go away. Strong passwords could be assigned to users while they are registering to web sites, these passwords are stored in browser cache and then the browser automatically completes all logins thereafter. We note that password autocomplete feature could even be a solution to phishing attacks in this ideal world because users become victim of these attacks mostly because they are being conditioned into constantly entering passwords [6]. In this ideal world, browser does not need any user input to give a decision, it simply caches all passwords by default.

However the real world is far from being ideal. We list some of the usability concerns in the above scenario in today’s world as follows:

1. Occasionally, we buy new computers or format hard drives hence passwords are not always in the cache.
2. Sometimes, we require to login from other computers hence enter passwords manually (unless we use a portable browser e.g., Portable Firefox [13]).
3. On the new computer we login, our passwords could be available to next users unless we took necessary countermeasures (e.g., manually erasing the password.).

First two items in the above list are practical usability problems. Last issue is even more problematic because obviously it also brings security issues.

One may argue that regardless of password autocomplete entering passwords on another computer is always dangerous. In a sense that is true; all needed to capture the password is a simple keylogger program. However we believe that storing passwords in browser’s cache significantly increases the security risk. For instance a small Javascript code executed on the browser (e.g., Figure 3) is sufficient to view passwords stored with password autocomplete feature [8].

To deal with the security problems autocomplete brings for public computers, disabling autocomplete entirely in public computers (for instance by the system admin of public computers) is an option but this secure practice is not common and not always applicable. To mitigate the security risks, “Private Browsing” mode, available in most browsers, could also be useful. Password autocomplete is disabled in a “Private Browsing” mode however our anecdotal observation is that this mode of operation is also not widely used. Another secure but not widely adopted practice is the protection of saved passwords with a master password.

```
javascript:
var x=document.getElementsByTagName('input');
myVals='';
for(var i=0;i<x.length;i++){z=x[i].getAttribute('type');
if(z=='password')myVals=myVals+'The password value is:
'+x.item(i).value+('\n\n')};
alert(myVals);
```

Figure 3. Javascript code to view a password in browser’s cache [8].

In the web application developer community, the risks of password autocomplete feature are well-understood. For instance, Yahoo mail and some Internet banking web sites set off password autocomplete by putting the command *<FORM autocomplete = "off">* on their web pages[1] [16] (some browser extensions offer a solution to this inconvenience! e.g., [12]).

The short discussion above explains why all browsers enable password autocomplete only after communicating with the user and getting consent. But browsers have different types of implementation for this communication. If we look specifically at two most used browsers [1] [17], we see that Internet Explorer implements blocking dialog box[2] (Figure 1) whereas Firefox adopts nonintrusive widget (toolbar) approach (Figure 2).

As a summary for this section; password autocomplete is a useful feature implemented in all modern web browsers but we should give a consideration of its security risks due to careless use especially in public computers.

4. USER STUDY

In this study, our main objective is to compare active (intrusive) and passive (non-intrusive) types of communication for password autocomplete in web browsers when public computers are in use. We proposed that blocking users’ action for asking them question about password autocomplete might lead to inadvertent storage of passwords whereas non-intrusive communication does not have such vulnerability. Even though disadvantage of active (intrusive) communication is evident, at least for us, there was no empirical study which has investigated security vulnerabilities of intrusive type of communication for security decisions.

[1] We note that cookie based password avoidance techniques some of these sites implement have also security implications [16].

[2] The latest version of Internet Explorer (version 9) was released on March 14, 2011. This new version which replaces active (intrusive) communication with passive one for password autocomplete was not available while we were conducting our user studies. Version 9 is not supported in Windows XP, which is still the most popular version of Windows operating system based on user base [20] and earlier Windows versions. An additional note is that dialog box approach for password autocomplete is still preferred in the latest versions of some browsers (e.g., Safari, fourth most widely used browser [17], version 5).

We have chosen Internet Explorer and Firefox as the browsers to investigate in our study and compared users' choices of saving passwords with Internet Explorer version 6 and Firefox version 3. Internet Explorer version 6 (henceforth IE) is no different than other versions up to 8 in the sense that it communicates with a dialog box which blocks users continuing with their login. Firefox version 3 (henceforth FF) and newer versions communicate with a non-intrusive toolbar. We observed users' behavior to see whether and when password autocomplete feature creates security vulnerability in public computers. We hypothesized that more users would save their password with IE (when an active - intrusive communication is prompted) compared to FF.

To test our hypothesis, three different but similar experiments were performed. We looked at each experiment and its results with a critical eye and designed the next experiment with some necessary modifications to address ecological validity concerns and to explore new arising questions. These experiments are presented in order under the following subheadings. A general discussion is provided at the next section.

4.1 Experiment 1

4.1.1 Method

4.1.1.1 Lab and Participants

Our study was conducted in the student-computer lab of Selcuk University. There were 10 personal computers in the lab, and each was running Turkish Windows XP (with service pack 2). IE and FF were already installed on all computers.

Students had been using lab computers for the course named Introduction to Information Technologies and Applications. Login to computers was with a generic account requiring no authentication. Restarting a computer kept all information of the previous session intact. Every student was aware of the fact that recording personal information on a computer would make it available to anybody using that computer. At the time of the study, participants had been using the computer lab at least for 3 months.

We consulted non-technical students in this study in order to be able to generalize our results to Internet users who are not computer experts,. Participants were 27 (16 male and 11 female) students of Selcuk University, Konya, Turkey. 22 of them were between 20-30 years old and 5 of them were in a younger age.

The second author (NBA) teaches the 'Introduction to Information Technologies and Applications' course in this lab. The aim of the course is to introduce basic computer skills, such as using Windows operating system, browsers, ftp software, office programs, etc. Before the execution of the study, no lecture on security and passwords was given.

4.1.1.2 Procedure

The data were collected with a semi-controlled lab experiment. Before the experiment, any password saved on IE and FF was deleted and the password autocomplete feature was checked and set it active if not. Participants were invited to the experiment in groups (min. 2 and max. 10). Each participant used a computer in the lab individually. In order to conceal the true aim of Experiment 1, participants were told that the study investigates the speed of IE and FF. They were instructed to login to the student registration web page of Selcuk University, with IE and FF. The web page contains personal and private information, such as home address, telephone, cumulative GPA, etc. The order of browser use was counterbalanced across participants. To collect their habitual responses, participants were instructed to finish the task as fast as possible.

After completing the login tasks, participants answered questions regarding their choices for password autocomplete options and their knowledge about deletion of saved passwords on browsers. At the end of the experiment, they were instructed about the nature of the study. They filled a second questionnaire on their computer skills and attitudes towards the password autocomplete feature. Following that, they were given a lecture on password security.

Experimenter (NBA) checked whether a user saved his/her password of student registration web page using password autocomplete feature on IE and FF. Then, saved passwords were deleted and password autocomplete was set to active in both browsers to test next group of participants.

4.1.2 Results

4.1.2.1 User Profile and User Knowledge on Password Autocomplete

Most of the participants rated their computer skills as average or below average (21 participants, 78%). Most of them were using Internet on daily basis (18 participants, 67%). Majority of participants in Experiment 1 prefer using IE in their daily life (20 participants, 77%). About half of our participants (15 participants, 55%) reported that they knew about password autocomplete. Among these participants most of them (10 out of 15 participants, 66%) were using it for more than one account. When we asked whether they knew how to delete saved password from browsers, only small number of participants responded affirmatively (7 participants, 26%, for IE; 4 participants, 15%, for FF). On the other hand, only one of them were able to correctly describe how (i.e., with the Delete button). Some of the participants believed that deleting browser history and cookies also erases the saved passwords on a browser. Another one believed saved passwords are erased automatically after some time. One participant confused autocomplete feature with cookie based "Remember me" option on web pages.

In summary, participants of Experiment 1 were non-expert computer users. About half of them were actively using

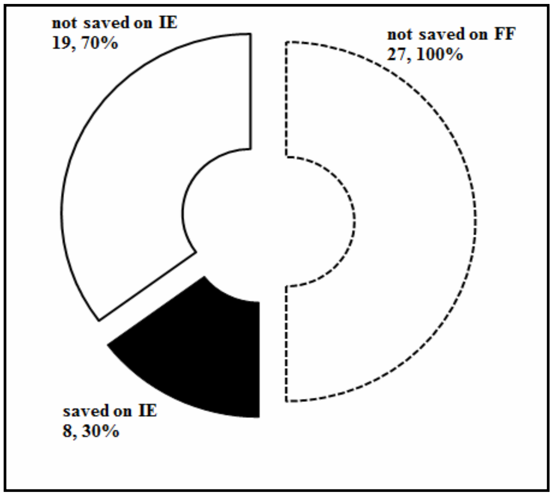


Figure 4. Number of participants who saved a password on IE and FF in Experiment 1.

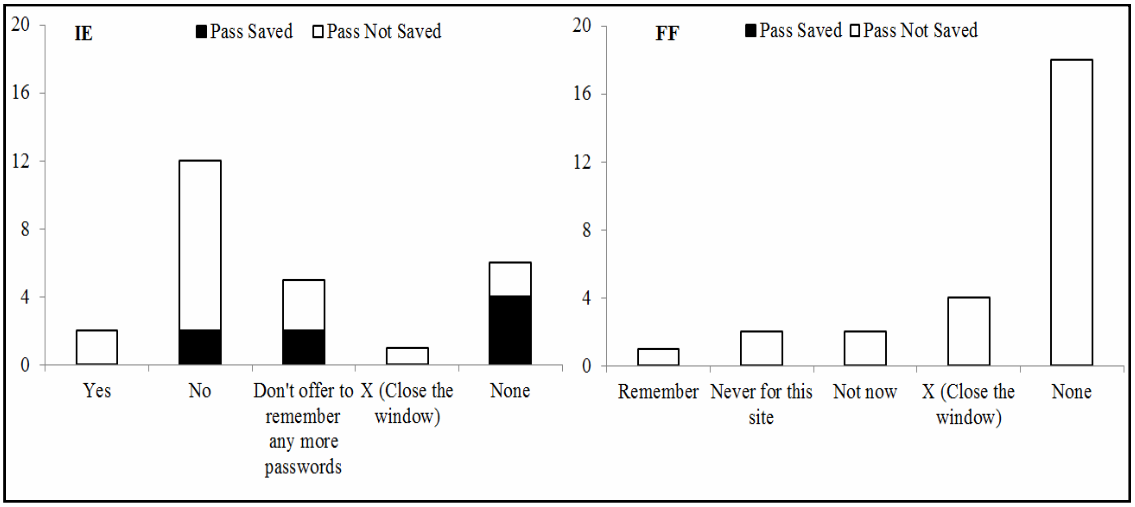


Figure 5. Number of clicks made for each option as seen in Figure 1 and Figure 2 for password autocomplete on IE (left) and FF (right) based on participants' memory in Experiment 1. (x-axis and y-axis represents click options and number of clicks respectively.) (e.g., for IE, 12 users reported they clicked on "No", but 2 out of 12 actually saved their passwords.)

password autocomplete while the other half were not aware of it. Almost all of them did not know how to delete stored passwords on browsers.

4.1.2.2 Saving Passwords

None of 27 participants saved password on FF, but 8 of them (~30%) saved their passwords on IE (See Figure 4). The association between browser type and saving password was significant [$\chi^2(1)=9.39$, $p < 0.05$]. These results showed that the tendency to save password on a browser increases with the active (intrusive) dialog box.

We also investigated another important issue, participants' memory about the option they clicked for password autocomplete. Among the 8 participants who saved their password on IE, none of them reported that they clicked to the option for saving the password (See Figure 5). In other words, none of the participants who saved password on IE correctly remembered his/her action. Among the 19 participants who did not save password on IE, 14 (77%) of them remembered correctly that they clicked to the one of the options that did not save password. Interestingly, 2 participants reported that they saved their password, actually they did not and another 2 participants reported that they did not remember their action. (One participant did not answer this question.) For FF, among 27 participants, 18 (66%) of them reported that they either did not recollect their response or they took no action (Response “None” in Figure 5 covers both options in Experiment 1). Interestingly, one participant reported that he saved his password on FF, but actually he did not. These results showed that regarding the option that they clicked for password autocomplete participants' memory was poor and this was especially so when they actually saved it.

4.1.3 Discussion and Limitations

In Experiment 1, we observed that with non-expert computer users active communication increases the rate of saving password on a public computer. Users should not save their passwords on public computers however, 8 out of 27 participants did so in our study when they were confronted with a pop-up dialog box. This was in contrast to FF on which nobody stored his/her password with the nonintrusive toolbar. The significant association between communication type and password saving behavior confirmed our hypothesis that more users would save their password on a public computer with active (intrusive) communication.

In Experiment 1, participants who saved passwords on IE were not able to remember their actions correctly. Some of them even claimed that they did not save passwords. We think this was an important finding because it eliminated other explanations for password saving. For instance, if participants had made a deliberate choice, we could have speculated that participants behaved so since they trusted other students using the same lab or they thought that university environment is not as risky as an Internet café, etc.

Our results also showed that almost all participants did not have an idea about how to erase saved passwords. Even if they had known, this would not have helped much since some participants could not recall their choice of saving passwords in the first place. Being conditioned to respond such pop-up boxes quickly, participants’ responses to intrusive toolbars were reflexive.

There may be concerns regarding ecological validity of Experiment 1 since we instructed participants to finish tasks (login to web pages) as fast as possible. It might be the case that participants randomly clicked to an option on the active (intrusive) communication to achieve the task demanded quickly. In addition, it might be the case that participants did not see the non-intrusive toolbar when using FF. We did not explicitly explore whether participants did not save their password because of not seeing the toolbar or not. Furthermore, given that most of our participants were unfamiliar with password autocomplete, they might have difficulties in understanding questions about their memory. In Experiment 2, these methodological problems were addressed.

4.2 Experiment 2

In Experiment 2, participants finished the task at their own pace (we did not ask them to finish the tasks as soon as possible). To measure the visibility of dialog box and toolbar used for password autocomplete, we explicitly asked participants whether they had seen them during browsing. We also asked for

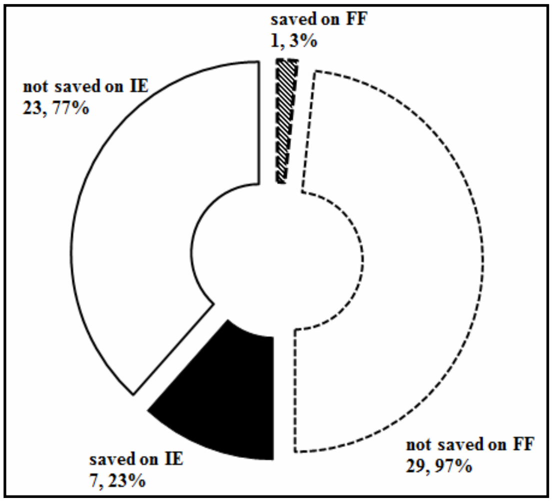


Figure 6. Number of participants who saved a password on IE and FF in Experiment 2.

the confidence levels in their answers. We added the pictures of IE dialog box and FF toolbar to the questionnaire and slightly changed the wording of questions to clarify the meaning.

4.2.1 Method

Experiment 2 was conducted in the same laboratory. Procedure was same as in Experiment 1 except the above mentioned methodological differences. In order to conceal the true aim of the study, participants were asked to check and confirm their address information on the student registration page of Selcuk University using IE and FF. The order of browser use was again counterbalanced across participants. There were 30 participants (10 of them were female, and mean age = 22.5), who were students of Selcuk University. None of them participated in Experiment 1.

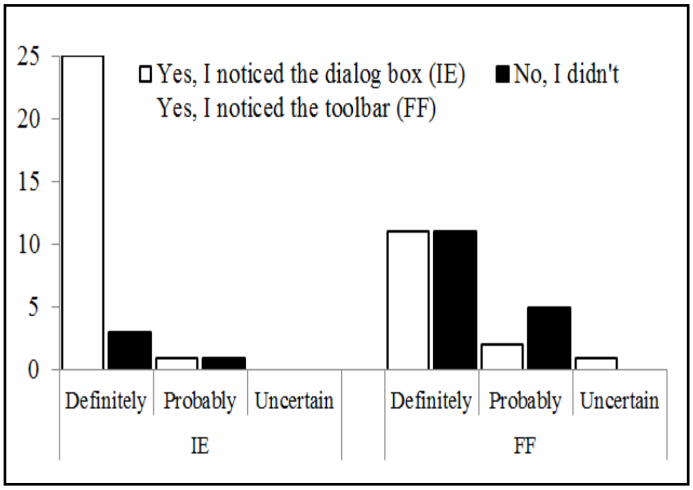


Figure 7. Number of different responses to the question "Did you notice the dialog box / toolbar?" and "How confident are you?"

4.2.2 Results

4.2.2.1 User Profile and User Knowledge on Password Autocomplete

Approximately, half of the participants in Experiment 2 rated their computer skills as average or below average (14 participants, 47%). Most of the participants of Experiment 2 were using Internet on daily basis (26 participants, 87%). About half of them reported that they were using IE (14 participants, 47%), most of others were using either FF (6 participants, 20%) or Google Chrome (7 participants, 23%). In Experiment 2, most of the participants (23 participants, 85%) reported that they knew about password autocomplete feature. Among these participants almost all of them (21 out of 23 participants, 66%) were using it for at least one account. 6 participants for both IE and FF (25%) reported that they knew how to delete password from browsers, but most of them could not correctly describe how.

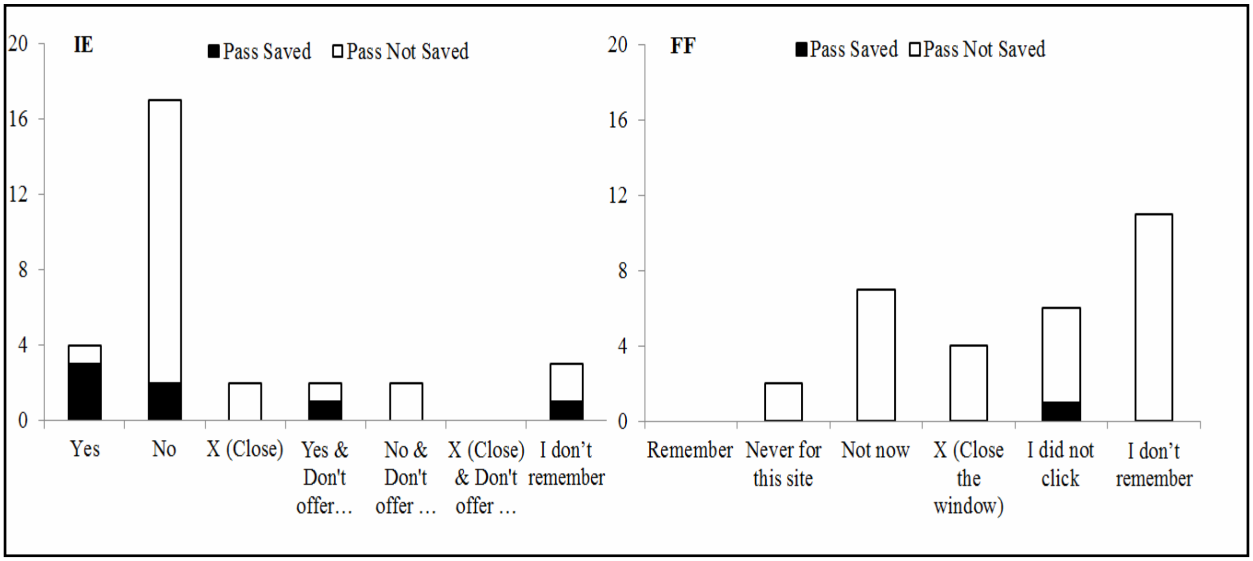


Figure 8. Number of clicks made for each option for password autocomplete on IE (left) and FF (right) based on participants' memory in Experiment 2 (x-axis and y-axis represents click options and number of clicks, respectively).

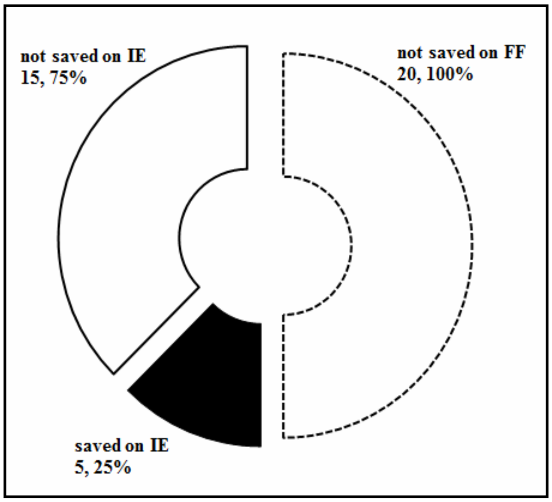


Figure 9. Number of participants who saved a password on IE and FF in Experiment 3.

In summary, participants of Experiment 2 were non-expert computer users. Most of them were actively using password autocomplete unlike to the participants of Experiment 1. However, similar to Experiment 1, most of the participants in Experiment 2 did not know how to delete stored password on a browser.

4.2.2.2 Saving Passwords

In Experiment 2, 7 participants (23%) saved passwords on IE, but only one participant (3.3%) saved password on FF (see Figure 6). The association between browser type and saving password was significant [$\chi^2(1)=4.97$, $p < 0.05$]. These results, which replicated results of Experiment 1, confirmed that (intrusive) dialog box increases the tendency to save password on a browser. Furthermore, these results could not be attributed completely for the invisibility of FF's non-intrusive toolbar since around half of participants (14 participants, 46%) reported that they had seen FF's passive (non-intrusive) toolbar (see Figure 7). Most of them were pretty sure about their answers.

In Experiment 2, among 7 participants who saved their password on IE, half of them (3 participants, 43%) did not remember that they clicked one of the options that saves the password. For FF, one participant who saved password did not remember his/her action correctly (see Figure 8).

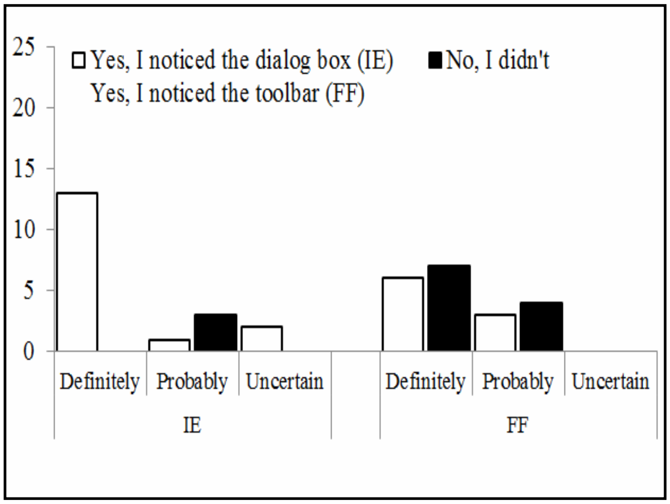


Figure 10. Number of responses to the question "Did you notice the dialog box / toolbar?" and "How confident are you?"

4.2.3 Discussion

In Experiment 2, we replicated the result that active communication increases the rate of saving password on a browser. 7 participants out of 30 saved their passwords on a public computer, when they were confronted with pop-up dialog box. Contrarily, only one participant saved his/her password with the non-intrusive toolbar. The significant association between communication type and password saving behavior in Experiment 2 confirmed our hypothesis with a different group of participants. Furthermore, most of the participants in Experiment 2 knew about and have been using password autocomplete unlike to the participants of Experiment 1. The similarity of results in Experiments 1 and 2 showed that saving password with an active dialog box on a public computer is not a direct consequence of unfamiliarity with password autocomplete feature.

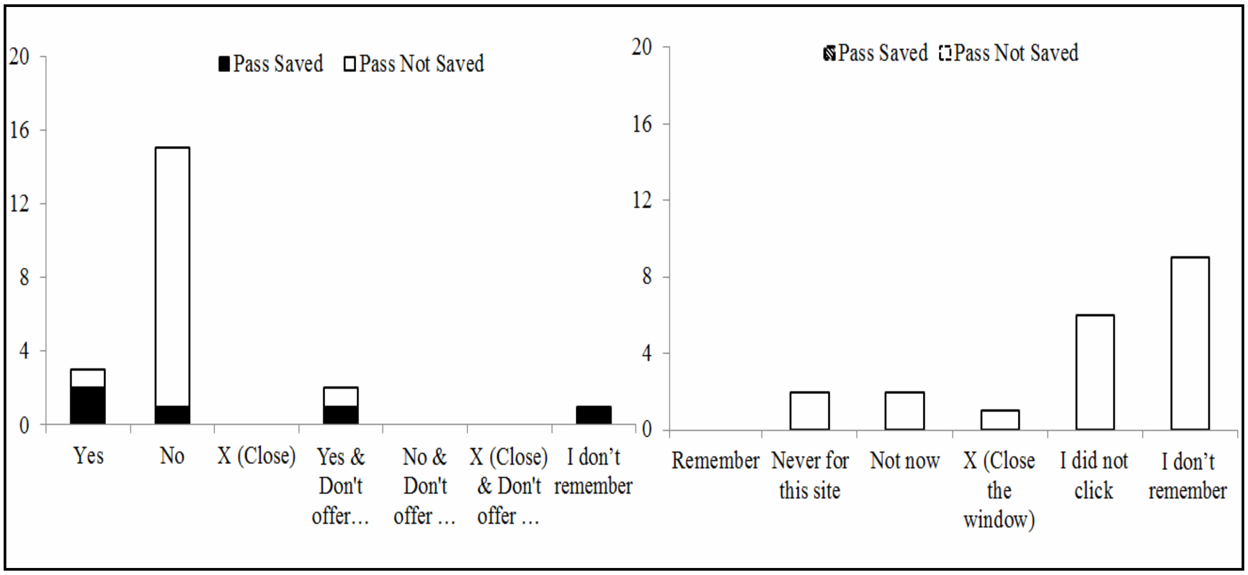


Figure 11. Number of clicks made for each option for password autocomplete on IE (left) and FF (right) based on participants' memory in Experiment 3 (x-axis and y-axis represents click options and number of clicks, respectively).

Although IE's dialog box is more visible than FF's toolbar, not saving passwords in public computers is not a direct result of not seeing the non-intrusive toolbar because half of our participants in Experiment 2 reported that they remember seeing the toolbar and most of them were very confident about their answers.

For participants who saved their passwords on lab computers, it might be the case that they did so because they were unaware of the risks of saving passwords on public computers. We tested this assumption in Experiment 3.

4.3 Experiment 3

In Experiment 3 we investigated whether having knowledge on password security has an effect on saving passwords on public computers. In order to test this, we re-invited participants of Experiment 1 for a new experiment. Participants of Experiment 1 were already given a lecture on password security and risks of saving passwords on public computers. These participants would be less likely to save passwords on a public computer if they had saved it in Experiment 1 due to lack of knowledge on password security. On the other hand, if participants' responses to intrusive dialog boxes had been reflexive, we would observe that some participants save their password on IE in Experiment 3 as well.

4.3.1 Method

The procedure of Experiment 3 was identical to Experiment 2. There were twenty participants all of whom had participated in Experiment 1. Experiment 3 was conducted about seven months later than Experiments 1.

4.3.2 Results

4.3.2.1 Saving Passwords

In Experiment 3, 5 out of 20 participants (25%) saved their password on IE, but none of them saved on FF (Figure 9). This pattern of results revealed a significant relation between browser type and saving password [$\chi^2(1)=5.71$, $p < 0.05$], which replicated Experiments 1 and 2. Similar to Experiment 2, about half of the participants (9 participants, 45%) reported that they had seen the toolbar of FF (Figure 10). Among the participants who saved their password on IE, 2 of them remembered reported that they did not save it (Figure 11).

4.3.3 Discussion

Experiment 3 replicated results of Experiment 2. We observed that the tendency to save password with intrusive dialog box exists among participants even if they had participated in the same study previously and knew about the risks of saving passwords on a public computer. About half of the participants reported that they had seen the nonintrusive toolbar of Firefox. This result confirmed that nonintrusive toolbar is not completely invisible.

5. GENERAL DISCUSSION

In this study we showed with repeated experiments that active (intrusive) communication for password autocomplete increases significantly the risk of inadvertent saving of passwords on public computers (there is a significant association between saving passwords on a public computer and type of communication). Our last experiment also shows that some participants saved their passwords with active type of communication even if they were previously informed about the security risks of saving passwords on public computers. Furthermore, we observed that passive communication was not completely invisible to the participants. In both Experiment 2 and Experiment 3 half of the participants reported that they had seen the password autocomplete toolbar.

In our study we observed that among the participants who saved their passwords, some of them remembered their choice correctly while some did not. Surprisingly, this pattern of results was observed even in Experiment 3 in which participants were aware of the risks of saving passwords. It was interesting to point out the numbers who self reported their savings incorrectly. Not definite in any sense, but this data reminds how tenuous it is to get self reported information.

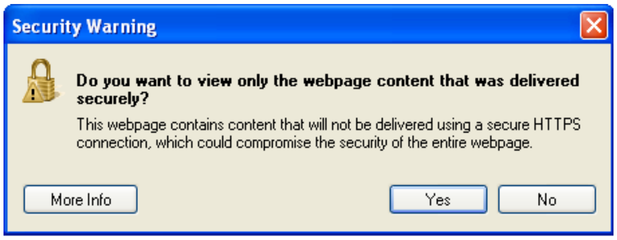
In the lab experiments described above, we observed behavior of users while they were using public computers. Another important issue under our on-going investigation is the behavior of users when they are using their own computers. We performed a large survey study completed by 686 users to understand the usage of password autocomplete feature in users' own computers and the relationship between usage pattern and the type of browser used. Due to space limitations, we cannot discuss the results of this survey in detail in this paper. However a snapshot of our results is provided in the Appendix for the interested readers.

Based on our results, as a security recommendation we suggest browser developers to choose passive communication for password autocomplete. In this sense, we think it was a considerate action to prefer passive communication in the latest version of Internet Explorer (i.e., version 9) (We recommend a similar change for password autocomplete in the Safari browser which still uses dialog boxes in its latest version). However since Internet Explorer version 9 is not compatible with Windows XP, still the most popular version of Windows [20], older versions of Internet Explorer are still widely used. Hence average users might be more likely to continue saving their passwords on public computers with Internet Explorer unless another action (e.g., releasing an update for older versions of Internet Explorer) is taken by Microsoft. We conjecture that our results can be generalized to other security interactions in which simply ignoring the communication does not pose any security threat. This hypothesis may be of interest to test in a separate study. As an example, consider the dialog box in Internet Explorer version 8 for warning about the content not secured with SSL protocol (Figure 12). In our opinion, active communication is not appropriate for this warning message about mixed content, either. Providing only the secure content without blocking user's primary task and presenting the option of viewing additional content not delivered with HTTPS in a nonintrusive toolbar could be a better option[3]. Users are not conditioned to react poorly to warnings and become more effective to produce the appropriate behavior if active communication is used only when it is really needed.

6. CONCLUSION

Passwords are an easy target for attackers. In this paper, we address an important aspect of password protection problem previously untouched in the literature. We performed a number of user studies which provide empirical evidence for the risks of using intrusive dialog boxes to ask users input for password autocomplete. In all three experiments we repeatedly observed

[3] Developers of Internet Explorer have not preferred passive communication because they worry about the web layout problems when only secure content is displayed [18].



Do you want to view only the webpage content that was delivered securely?

This webpage contains content that will not be delivered using a secure HTTPS connection, which could compromise the security of the entire webpage.

Figure 12. Intrusive dialog for warning about the content not delivered using secure connection in Internet Explorer version 8.

that participants may click on the "Yes" button reflexively and store their passwords on a public computer when prompted with a pop-up dialog box.

We suggest users to consult private browsing when they are using public computers. With private browsing, password autocomplete is disabled and no question is asked for user input. This simple strategy prevents not only the problems due to careless password savings but also mitigates privacy related problems. We suggest secure interaction designers to think twice before preferring an active communication over nonintrusive alternatives. Unless active communication starts to be used less, the market size would be increasing for commercial applications such as PTFB (Push the Freaking Button) that automatically responds to pop-up boxes on behalf of the user [6] [14].

7. ACKNOWLEDGEMENTS

We thank Paul C. van Oorschot and anonymous referees for comments that considerably improved the paper. This research is supported by TUBITAK (The Scientific and Technological Research Council of Turkey) under project number 107E227.

8. REFERENCES

[1] Browser Market Share, http://marketshare.hitslink.com/report.aspx?qprid=0, last accessed on 02/July/2011.

[2] L.F.Cranor: A framework for reasoning about the human in the loop. In Proceedings of the 1st Conference on Usability, Psychology, and Security, pages 1-15, Berkeley, CA, USA, 2008.

[3] R. Dhamija, J.D. Tygar, and M. Hearst. Why phishing works. In Proc. of the SIGCHI Conference on Human Factors in Computing Systems, pp. 581-590, New York, NY, USA, 2006, ACM.

[4] D. Florencio and C. Herley. A large-scale study of web password habits. In Proc. of WWW (2007).

[5] S. Gaw, E.W. Felten, Password management strategies for online accounts, in: SOUPS '06, ACM Press, 2006, pp. 44–55.

[6] Peter Gutmann: Security usability, http://www.cs.auckland.ac.nz/~pgut001/pubs/usability.pdf, February 2008. Draft. Last accessed on 02/July/2011.

[7] E. Hayashi and J.I. Hong. A diary study of password usage in daily life, In Proc. of CHI 2011.

[8] C. Heilman. Web Security: Are you part of the problem. White paper, http://coding.smashingmagazine.com/2010/01/14/web-security-primer-are-you-part-of-the-problem/, last accessed on 02/July/2011.

[9] C. Herley, P.C. van Oorschot and A.S. Patrick. Passwords: If We're So Smart Why Are We Still Using Them? Proc. Financial Crypto 2009.

[10] R. Morris and K. Thompson. Password security: a case history. Communications of the ACM, 22:594-597, 1979.

[11] C. Nodder: Users and trust: A microsoft case study. In L. F. Cranor and S. Garfinkel, editors, Security and Usability: Designing Secure Systems that People Can Use, August 2005.

[12] Kevin Purdy, post to lifehacker.com, Available at http://lifehacker.com/5431466/autocomplete-extension-makes-chrome-save-nearly-any-password, last accessed on 02/July/2011.

[13] Portable Firefox project, available at http://portablefirefox.mozdev.org/, last accessed on 02/July/2011.

[14] PTFB Pro Mouse AutoClicker and Macro Recorder, http://www.ptfbpro.com, last accessed on 02/July/2011.

[15] B.Ross: Firefox and the worry free web. In L.F. Cranor and S.Garfinkel, editors, Security and Usability: Designing Secure Systems that People Can Use, August 2005.

[16] Brent Strange, Password harvesting with AutoComplete, available at http://www.testingreflections.com/node/view/3482, last accessed on 02/July/2011.

[17] Usage share of web browsers, http://en.wikipedia.org/wiki/Usage_share_of_web_browsers

[18] Walker News, Why IE8 Displays Security Warning When Loading HTTPS Page?, http://www.walkernews.net/2009/10/19/why-ie8-displays-security-warning-when-loading-https-page/.

[19] Alma Whitten and J. D. Tygar. Why Johnny can't encrypt: A usability evaluation of PGP 5.0. In 8th USENIX Security Symposium, pages 169 – 184. Usenix, 1999.

[20] Windows XP, http://en.wikipedia.org/wiki/Windows_XP

APPENDIX: Survey Study

Methodology and Results

With the aim of collecting information for the use of password autocomplete in participants' own computers, we conducted an online web-based survey in June 2011 (three months after version 9 of Internet Explorer is made publicly available) with students and employees of TOBB University of Economics and Technology. There were 686 participants in total (242 of them were female, and mean age = 22.68). They gave subjective ratings about their knowledge on computers on a Likert scale (1-5). The average rating was 3.73 (with standard deviation of 0.82). Majority of our participants rated themselves as average, and above-average computer users. Among 686 participants 305 of them (44.5%) were using Google Chrome (GC), 37 of them (5.4%) were using Firefox (FF) 3.x or a lower version, 237 of them (34.5%) were using FF 4.x, 49 of them (7.1%) were using Internet Explorer (IE) 8.x or a lower version, 39 of them (5.7%) were using IE 9.x, 7 participants (1.0%) were using Safari, and remaining 12 participants (1.7%) were using other browsers (see Figure 13).

GC, FF and IE 9.x have non-intrusive toolbars for the password autocomplete feature whereas IE 8.x (and lower versions) and Safari implement intrusive dialog boxes. On their own computers, majority of our participants (630, 91.8%) were using browsers implementing password autocomplete with nonintrusive type of communication. We divide participants into two groups (non-intrusive vs. intrusive) and in the following analysis we compare these two groups with respect to the information they reported about password autocomplete.

We asked our participants whether they knew about the password autocomplete feature. We compared the proportion of participants who reported knowing it with respect to the group they belong to. While 87% (548 of 630) of users in the non-intrusive group reported that they knew about the feature, this proportion drops to 77% (42 of 56) for the other group, which was a statistically significant difference [$\chi^2(1)=4.48$, $p<0.05$] (see Figure 14).

We asked participants the ratio of their passwords saved on browser with the password autocomplete feature. Based on the information reported, 106 participants (15%) saved none of their passwords on browser. 191 (27%) reported that they saved up to

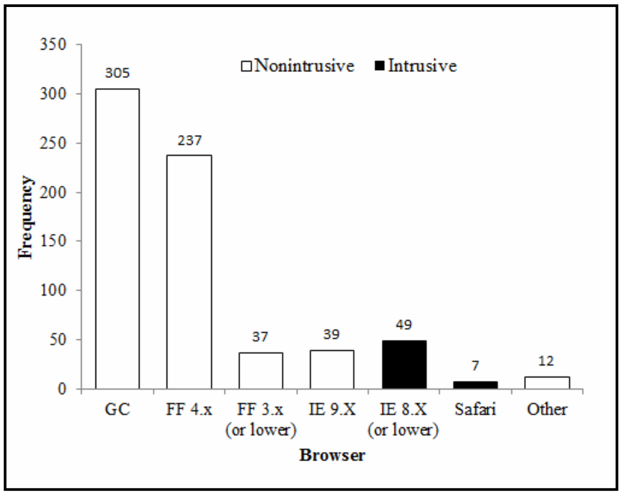


Figure 13. Usage share of browsers in the survey study

25% of their passwords. 160 of them (23%) saved 25-75% of their passwords, and 229 (33%) saved 75-100% of their passwords. We observed significant differences between the groups of non-intrusive and intrusive [$\chi^2(3)=10$, $p<0.05$] (see Figure 15). Significantly more users (35%, 219 of 630) in the nonintrusive group save majority (i.e., 76-100%) of their passwords. On the other hand, significantly more participants (39%, 22 of 56) in the intrusive group save only 1-25% of their passwords with the password autocomplete feature.

Discussion

In the lab studies, we have shown that active communication for password autocomplete brings security risks when public computers are in use. An additional important finding obtained in the survey study is that with active dialog boxes the ratio of passwords saved on users' own computers is less than the passwords saved with the passive toolbar. Similarly, significantly a smaller proportion of participants in the intrusive group reported that they knew about password autocomplete feature as compared to non-intrusive group. With the assumption that knowing password autocomplete and ratio of passwords saved are indicators of usability of the implementation of password autocomplete feature, we can say that passive communication does not have any usability disadvantage in the environment of users' own computers (due to its less visibility or for other reasons). This result confirms our conclusion that active communication for password autocomplete should be avoided in web browsers.

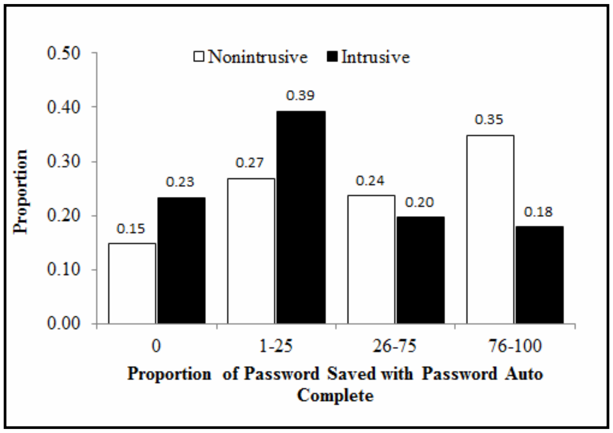


Figure 15. Proportion of participants as a function of ratio of passwords saved on their browsers in intrusive and nonintrusive groups.

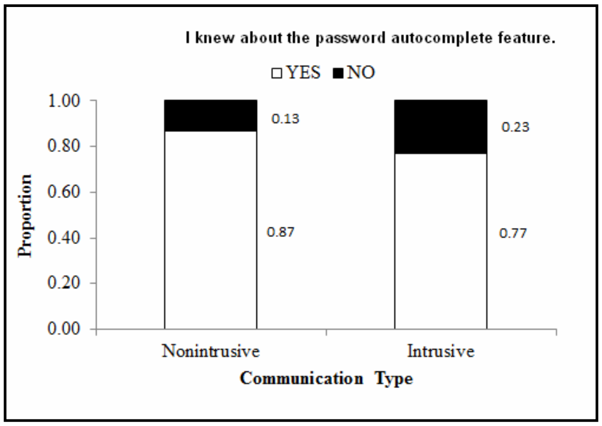


Figure 14. Proportion of participants who knew about password autocomplete feature as a function of communication type implemented in their browsers.

In the survey study usage share of browsers is substantially different than the share in our lab studies (i.e., IE is the most popular browser among the participants of lab study in contrast to the survey study). We note that user bases are different in these two studies. In addition, this difference may be partially attributed to the rise of new browsers.

It is interesting to note that in the survey study more than half of IE users still reported that they did not use the latest version (version 9) three months after its release. On the other hand, older versions were reported to be less used among Firefox users.