Chapter 3  Survey of User Perceptions

Online service providers require a method to identify users on the web. This is critical to force different levels of access rights on individuals. Legitimate members must gain access with the appropriate privileges smoothly whilst malicious login attempts must be banned from the system.

Text passwords are used for authentication and end users are familiar with them because they have been employed in computers since 1960 when Corbato designed the first access control solution for time sharing systems based on passwords and usernames login (Smith, 2001). However, these are not the only ways to electronically verify that people are who they say they are; various methods have been suggested and developed based on different factors. This chapter introduces a survey of user perceptions to measure and analyze the acceptance of different VP categories. The concept of continuous monitoring is also presented as a new security enhancement technique.

The survey proposed solutions within the scope of this thesis. VPs for example do not require any additional hardware text passwords do not use. As such, a successful candidate to replace text passwords must be cost-effective and suitable to cover a wide area of application. In addition, it is critical for any proposed scheme to maintain usability by enhancing user memorability through simplifying password entry and providing cues to trigger user LTM. In theory, a method with these characteristics should gain user acceptance and be described as a user-friendly solution.

Up-to-date information about users’ awareness of, and attitudes towards, text password security practices is also presented and discussed because the password problem covered in Chapter 2 remains an issue despite all policies and guidelines being taught to end users. For example, the survey studies the demand for more password-protected accounts in people’s lives which encourage insecure password practices. Further, a question to investigate is whether people’s demographic information such as
a knee, major or being a student affects the number of these accounts. Studying these practices with up-to-date information helps research in this area with evidence.

3.1. The survey

The survey aims to assess the following issues to achieve the first objective of this thesis:

- Public awareness of, and attitudes toward, password security and usability.
- Public attitudes toward different forms of initial user authentication for web applications.
- Public attitudes toward the concept of continuous monitoring.

The assumptions before performing the survey were:

- System administrators and security consultants encourage policies and guidelines such as the ones presented in Section 2.2.2 to resist insecure behaviours and control the text password problem. However, a minority of users succeed in following all these guidelines while the majority fail.
- The number of frequently used password-protected systems is continually increasing.

There are 46 questions in this survey presented in five groups, many of them were presented as multiple-choice and the rest employed a Likert scale. Some questions were answered using a comment box.

Responses were date stamped and IP Addresses were logged because participants were required to complete the survey online (Appendix A includes snapshots for the survey) and this helped to put restrictions on how many times a survey can be accepted from a specified party. Cookies were also used for access control so that participants save partially-finished surveys and finish them at a later time.

Group one questions gathered general details to provide demographic information such as age, gender, education and place of residence. These were collected to study their effect on some results such as the number of accounts and to describe the sample of people who participated in this survey.
Whilst group two was more about measuring the level of computer usage in general as well as some selected technologies such as Single Sign-On (SSO).

Password related questions were covered in group three to understand how people deal with security measures currently, their awareness of possible methods of breaches to confidential accounts and usage of any alternative authentication mechanisms.

After that, the participants were introduced to possible alternative techniques for initial login with group four. The questions were supported with help tips and images to explain what and how each technique works (e.g. explanation of what recognition-based graphical password solutions are, how they work and then supporting that text with an image or snapshot) followed by a five point Likert scale to let them rate the acceptability of the technique compared to others where 1 is “Very Unacceptable” and 5 is “Very Acceptable”.

Finally, group five introduced the participants to Continuous Monitoring to test the acceptability of the idea initially, the impact of its possible methods on them and finally some other important questions regarding the frequency of false rejection, trust and privacy issues.

The survey was hosted online for four months on a server and the link was distributed to individuals and groups in different countries. To reach many people the survey’s link was sent to members of existing university groups. It was also sent to mailing lists, online forums and social networking groups such as Facebook. This resulted in an overall number of 204 responses where 157 responses were completed and submitted successfully while 47 responses were excluded because they were not completely filled out by the day the survey questionnaire was taken offline.

3.2. Analysis of results

3.2.1. General

Figure 3.1 illustrates the percentage of responses from different age groups. These are used to compare with other result from the survey. For example, Figure 3.14 illustrates the number of accounts for each age group.
3.2.2. Level of computer usage

In terms of computer usage, the vast majority of participants have a fair to very good experience with computers and IT with 99.36% of them having and using a computer either at home or at work, and 96.18% having internet service.
In addition, 91.72% claimed to have used computers for more than 5 years and 79.62% have used the internet for the same period of time.

Due to the increased numbers of systems with access control, a question asked about the number of systems frequently used by participants during their daily life, whether it is a bank account, email or a website as long as it requires text passwords for authentication. The results showed that 47.77% use passwords for more than 10 systems and 8.28% use them for over 30 systems. Figure 3.3 illustrates the results in further detail.

![Figure 3.3: Number of accounts.](image)

One of the proposed solutions to help users who deal with many user accounts is Single Sign-On (SSO). It enables users to log in with a single password to their different email accounts, websites and windows applications without being prompted to enter each system’s password individually. The SSO software does that by saving all user passwords in a secure place (encrypted database). These passwords are then used to open related accounts after the user enters the software master password.

The participants were asked if they use any SSO solution at all and 20.38% replied with a yes.

**3.2.3. Text password related questions**

Public awareness of text passwords security and usability has been examined because it is still adopted by the vast majority of systems for authentication purposes (DTI, 2006).
Our survey showed that only 39.49% of the participants never shared their own passwords, as for those who shared it 16.56% of them shared their work passwords with other people.

74.52% said that friends and colleagues have given them their passwords and an interesting percentage of 22.94% claimed to have or used other people's passwords without their knowledge or permission.

At work, 68.37% of whom have jobs (117 participants) said the system at work enforces a minimum length for passwords and 41.52% claimed it shows them a scale to measure how secure the password they create is.

The results also showed that 56.69% of the users do not change their passwords if the system does not force them to do that, even if the account is considered to be important or critical some way or other, and 21.02% are those who are always careful to use a combination of random letters (a, b, c, ...), numbers (1, 2, 3...) and symbols (?, !, @...) together to create a password. Nevertheless, 20.38% sometimes feel their passwords can be easily guessed.

![Figure 3.4: How often passwords of critical accounts are changed](image-url)

**Figure 3.5:** How often participants avoid simple words available in dictionaries.

**Figure 3.6:** How often a combination of random letters (a,b, c ...), numbers (1, 2, 3...) and symbols (?, !, @...) are used together to create a password.

**Figure 3.7:** How often a password is written down after creating a new account.
Figure 3.8: How often the participants check their new password to be at least 6 characters long when creating a new account.

An expectable result also agreed with other studies such as (DTI, 2006) by showing that 89.81% of the participants use text passwords to access all of their accounts, leaving 10.19% only of those who happened to use finger-prints and security tokens to access one or more of their user accounts.

When another question focused more on the work environment, 95.08% claimed to be using text passwords only.

As for what text passwords consist of, Figure 3.9 illustrates the details and shows that 47% to 52% of the participants use only letters and numbers to access their accounts at work and something similar applies to their internet banking accounts.

The number of participants who claimed to have internet banking accounts is 100 where 92 depends on text passwords and the rest use tokens.
The final text password related question asked the participants how often they use the same password for more than one account, 31.21% of them stated that they frequently do that and a similar percentage of 31.85% selected sometimes. 8.92% thought they always reuse the same password. However, 28.03% responded saying they rarely or never reuse their passwords.

3.2.4. Alternative techniques for initial login

To study public attitudes and perceptions towards different forms of initial user authentication for web applications a Likert scale was provided along with explanations, tips and images to explain how each technique works. Table 3.1 displays the results and the numbers 1 to 5 represent the Likert scale. Under each number is the percentage of people who selected it.

Table 3.1: Results of public acceptability of different initial login techniques, where 1 is very unacceptable and 5 is very acceptable.

<table>
<thead>
<tr>
<th>Text Password</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Question and Answer</td>
<td>4.46%</td>
<td>3.82%</td>
<td>23.57%</td>
<td>27.39%</td>
<td>40.76%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recognition</td>
<td>13.38%</td>
<td>17.20%</td>
<td>33.76%</td>
<td>20.38%</td>
<td>15.29%</td>
</tr>
<tr>
<td>based</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Graphical</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cued Recall</td>
<td>22.93%</td>
<td>26.11%</td>
<td>26.75%</td>
<td>15.92%</td>
<td>8.28%</td>
</tr>
<tr>
<td>based</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Graphical</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pure Recall</td>
<td>28.03%</td>
<td>21.66%</td>
<td>26.75%</td>
<td>16.56%</td>
<td>7.01%</td>
</tr>
<tr>
<td>based</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Graphical</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 3.10 illustrates the data of the previous table in a comparative way. It shows that users are more confident to rely on text passwords whilst many users selected 3 for Question and Answer to say: they are doubtful. Consequently, the rest of the mechanisms gave us almost similar results.
Figure 3.10: Comparison of public acceptability of different initial login techniques, where 1 is very unacceptable and 5 is very acceptable.

3.2.5. Continuous monitoring

Continuous monitoring was finally introduced as the process of tracking user behaviour during a logged-in session to verify identity. This was simplified to the following: if a user leaves his/her email account open and another person tries to use it, the system will log the account out automatically and activate the initial authentication method again.

The survey shows that 44.59% were positive in accepting this feature while 28.03% rejected it and the remaining 27.39% do not have a clear opinion yet.
Mouse and keystroke dynamics and their possible usage have been introduced in brief detail. Figure 3.11 shows that public acceptability to both of them gives similar results, where 1 is very unacceptable and 5 is very acceptable.

**Figure 3.11**: Comparison between the public acceptability to mouse and keystroke dynamics to be used for continuous monitoring.

False rejection is one of the major possible drawbacks of any decision making system. The participants were asked to decide the acceptable frequency of false rejection to them; Figure 3.12 illustrates the results.
Mouse and Keystroke Dynamics are behavioural characteristics of the users, therefore, unlike normal passwords they do not change easily. Participants were asked if they trust their organization or school to collect their behavioural data in order to provide this security feature and 60.51% decided they do not trust it. Furthermore, 63.06% consider it to be an invasion of their privacy.

If continuous monitoring techniques are not used, some web applications automatically log the users out after a certain time of inactivity and force them to log in again for security reasons. The continuous monitoring section was closed by asking about the acceptable frequency of automatically logging a user account out after a period of inactivity. The results are in Figure 3.13.

![Figure 3.12: Acceptable frequency of false rejection.](image1)

![Figure 3.13: Acceptable frequency of automatically logging a user account out after period of inactivity.](image2)
3.3. Discussion

Figure 3.2 shows that most of the participants are residents in Asia, which could be a result of translating our survey questionnaire to Arabic in order to distribute it more easily in the Middle East and North Africa. The reason behind choosing Arabic only as a second language was the author’s ability to use it effectively, thus, making sure the way the questionnaire is presented in Arabic is identical to the English version in a way that does not affect the results.

The number of access controlled systems is increasing rapidly in people’s daily life as more than ever technology plays a key role. If the results from Figure 3.3 are compared with a similar study (Furnell et al., 2000) we notice how the percentage of people using more than 10 systems increased from approximately 13% nine years ago to 47.77% in this survey, though the previous study also argued to have most responses from people with technology fields such as computing, telecommunications and engineering who also happened to have familiarity with IT. This result could explain why 56.69% of the respondents do not change their accounts passwords unless the system forces them. With more passwords to be created, it is more difficult to adopt good security practices. Obviously, people are trying to keep track of their login credentials, so we end up with no more than 21.02% of them who always give extra attention to use good combinations of digits, letters and symbols while creating passwords.

To check whether our previous results apply to people regardless of their demographic information such as their age, place of residence or whether they are students or not, results are further analysed. Figure 3.14 illustrates the number of responses for every age group, this shows how having 5 to 10 accounts at a time is consistence for all ages.
Student seems to indeed need more than 5 accounts, see Figure 3.15. However the graph shows a good percentage of each group using 15 accounts at a time or even over 30 accounts.
Most of the responses came from Asia and Europe, therefore we were able to do the comparison in Figure 3.16 between these two places. There were not enough responses from other continents to involve them as well. Again the diagram lines show that despite the location 5-10 accounts is insistence among users and many people use 10, 15 or even 30 accounts at a time.
The comparison between different initial login techniques showed that people almost had the same response in regards to the different graphical password approaches; this is probably because they did not use them in practice to make a clear decision.

In comparison with text passwords, the results predict how difficult it is for a solution integrated with graphical passwords ideas to be accepted without sufficient proof of its security and usability to users.

The 27.39% who preferred not to give a clear opinion on whether to accept or reject continuous monitoring along with the 28.03% who rejected it should be considered by software developers to keep this feature as an option rather than forcing it in any online service implementation, unless the system belongs to a company where security is favoured over end users opinion. However, there is still a majority of 44.59% who think continuous monitoring is a good idea.

3.4. Conclusion

The analysis has shown the survey’s two assumptions to be valid to a great extent. People are dealing with an increased number of access controlled accounts despite of their age, place of residence or whether they are students or not, and that, text passwords remain the most adopted technique to authenticate end users. In addition, only a limited portion of end users pay attention to adopt all secure practices as seen in
the results of the text password related questions, for instance, only 5.10% change the passwords of their critical accounts on a monthly basis; only 21% always use a combination of letters, numbers and symbols; and sharing passwords is a significant phenomenon with 74.54% of them being given a password of their friends or colleagues.

Many text password related issues have been demonstrated for reference as an evidence for users’ continuous insecure practices especially with the increased number of password protected accounts.

In regards to finding a VP replacement to text passwords, the survey showed this option to be unacceptable to end users. However, these participants did not use a VP before hence their perception could change if a VP system proves itself good enough to be user-friendly and secure at the same time compared to text passwords. This is understandable and expectable, as due to inertia people resist change. For the targeted market such as banks more attention is paid to the security aspects of the systems hence they can provide training for users to learn the procedures of the new security system. This is not a new requirement by our scheme since banks and other companies are already providing security training to their users. Gradually, more people will adapt and it is expected that general public develop better understanding and acceptance of the new system. Nevertheless, no specific VP category was proved to be more favourable by end users in this survey, possibly because of the lack of their field experience with such systems. Hence, usability and then security evaluations of the proposed approaches is the best path to develop an acceptable authentication solution.

The survey also showed that continuous monitoring was not significantly accepted since around half of the users either rejected it or did not post their opinion. This implies that software developers must keep this feature as an optional. Further, end users did not favour mouse or keystroke dynamics among each other. Apparently, what matters is the solution that proves itself to be more accurate and efficient in practice.