Usable User Identification Technique - The Case of European Union Remote Web Access

Temechu Girma
Delegation European Union to the African Union, Addis Ababa, Ethiopia
temechug@gmail.com

Dagmawi Lemma
Department of Computer Science, Addis Ababa University, Ethiopia
dagmawil@yahoo.com

Abstract

Remote Web Access (RWA) has become more common and widely used in different organizations [1]. RWA provides a central web location for remote users to access corporate resources. It also enables to access an email application from a remote location. The European Union (EU) is an organization that uses RWA. However, the user identification technique associated with RWA is one of the key challenges that need to be addressed. To protect the organization from an attack (such as cyber or any other), the EU decided to add more identity checking steps on RWA to identify the user when they try to login remotely. However, survey results show that RWA has a usability issue which is compromised with the security in RWA. Qualitative and quantitative data were collected through a questionnaire, focus group discussion, interviews and document analysis. Usability testing software was used as a tool to assess usability of RWA and user satisfaction.

The study showed that adding more identity checking steps in RWA has an inverse relation with usability and increases the perceived security and trust in RWA. Moreover, the overall usability of the UIT in terms of effectiveness, efficiency, and user satisfaction is very low.

Besides, the more the user identification steps increase, the user frustration of RWA also increased. To minimize this frustration, RWA users start to write a note with a piece of paper to remember their secret such as username and password for ECAS application, domain, and delegations. All these actions make them exposed to intruders (attackers). Moreover, they are not only exposed for stealing their data but also, as a whole, the organization UIT will be vulnerable to attack. Therefore, the new user identification technique of RWA makes them unhappy.

To alleviate the usability problem, an enhanced usable user identification technique (UIT) for RWA is proposed considering the relevant security features regarding UIT and usability of secured system which is looking into consideration of all assessment results.

Keywords: Usability; Security; User Identification Technique; Remote Web Access

1. Introduction

Usability and security are part of design goals that indicate success of the design and the overall quality of software application [1]. According to Nielsen [2], usability is a quality attribute that assesses how easy and satisfactory the User Interface (UI) would be. Also, usability focuses on how users perform their tasks efficiently with minimal or no error. On the other hand, security is a system attribute that reflects the ability of a system to protect itself from internal/external attacks, which can be accidental or deliberate [3]. Security usability is concerned with the study of how security information should be handled in UI. Moreover, it deals on how security mechanisms and authentication systems themselves should be easy to be used [4]. This paper focuses on usability of user identification technique (UIT) on Remote Web Access (RWA).

RWA is a web-based application which is accessed through a web browser. It provides access for remote users to facilities such as email, reading/modifying their data, and enables them to remotely control a machine as if they are sitting in front of it [5].

The European Union is one of the organizations that use RWA. A serious cyber attack on European Union's mailing system has been reported in March

2010 [6]. Because of the attack, there was a "risk" of "unauthorized information disclosure", a way of saying that outsiders may have been able to gain access to even more confidential and sensitive information. It has been indicated that both the Commission and the European Union External Service (EEAS) are "the subject of an on-going widespread cyber attack" [7]. According to the official report "A detailed investigation and assessment of the threat is under way." Meanwhile the RWA of email has been closed for all the EEAS users.

Six months later, RWA of email re-launched UIT with very strict and secured steps that make use of Short Message Service (SMS) authentication. However, these authentication methods have laid down unforeseen influences on usability of the email application when it is accessed by users remotely.

In order to confirm the influence of the new UIT, a preliminary assessment has been conducted. The result showed that the user identification and authentication methods have a significant influence on the usability of RWA.

In order to answer the research question and address the objectives of the research, primary and secondary data collection methodologies were used.

Interview, focus group discussion, questionnaire, and usability testing were used to collect primary data from selected EEAS staff that use RWA.

These were considered to

- find information on the current practice of usability and security (user identification steps) in EEAS,
- know the extent of user satisfaction with RWA, and
- identify the major usability related challenges in user identification steps to access email via RWA.

Usability testing has been conducted to assess how easy is the UI for users of RWA and to measure user satisfaction. Moreover, secondary data from documents such as Information Technology (IT) Security Policies, Procedures, Guidelines and Reports of IT of EEAS were reviewed as a source of information.

2. Usability and Security

2.1 Themes on Usability

It is important to realize that usability is not a single, one-dimensional property of a user interface. There are five usability attributes [8]:

- *Learnability*: The system must be so simple and easy to learn that users can learn it quickly in order to accomplish their work on the system without difficulty.
- *Efficiency*: The system should be efficient to use and save time for users when they work with it. The most common measures of efficiency are time to perform a particular task, number of key presses or interaction to achieve the task, number of screens visited to complete a specific workflow scenario, number of back buttons uses, and time to execute a particular set of instructions.
- *Memorability*: The system should be easy to remember by the users so that when they use the system after some time, they should not need to learn everything again for doing their work.
- *Effectiveness*: The system should have a low error rate, so that users make few errors during the use of the system. The common measures of effectiveness include number (rate) of error, path taken to complete the task, severity of error, and requests for help.
- *Satisfaction*: The system should be pleasant to use, so that users are subjectively satisfied when using it; they like it.

According to ISO standard, usability is "the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction in a specified context of use" [9].

2.2 Themes on Security

Information security is the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities.

Security systems are designed to let authorized people in (the permission problem), and to keep unauthorized people out (the prevention problem) [10]. This involves three distinct steps: Identification, Authentication, and Authorization.

Identification occurs when a user (or any subject) claims or professes an identity. This can be accomplished with a username, a process ID, a smart card, or anything else that can uniquely identify a subject. Security systems use this identity when determining if a subject can access an object.

User identification is required for the following reasons [11]:

- Authorization: deciding whether a user is authorized to use the system.
- Policy enforcement: applying the right policy to the user (e.g., Security, Logging and HTTPS policies).
- Auditing: tracing user activity through logs, i.e., recording (logging) of transactions with details for future viewing and analysis of activities performed by the user.

3. Findings and Discussions

To find out the current practice of usability and security (user identification steps), to know the extent of user satisfaction with RWA, and to identify the major usability related challenges in user identification steps to access email via RWA, interview, focus group discussion, questionnaire and usability testing were used to collect primary data from selected EEAS staff.

Moreover, usability testing was taken as a method to assess how easy the UI for users of RWA is. Additionally, secondary data from documents like IT Security Policies, Procedures, Guidelines, and Reports of IT of EEAS were reviewed as a source of information.

Based on the above fact finding methodologies, the following results were found.

3.1 Questionnaire Survey

The respondents have the main role in performing the usability test and usability survey. They are classified based on their experience.

a. General Usability Perception

For 49% of the respondents RWA is not easy to use but for 31% of them, RWA is easy to use. The remaining 20% of them did not perceive that RWA is easy to use or not.

34% of the respondents agreed that RWA has attractive presentation but 56% of respondents do not agree with the attractive presentation of RWA. The remaining 10% of the respondent neither agree nor disagree.

Around 34% of the respondents agreed that RWA is interesting and engaging, but for 47% of respondents, RWA was not interesting and engaging. For the remaining respondents, RWA is neither interesting nor engaging

The general usability perception is less than average. Figure 1 shows the general usability perception of RWA in terms of its attractiveness, easiness, and satisfaction.

b. The Content of the Page

For more than average of respondents, there is a problem regarding "easy to understand and follow" the content of the page and "clarity and simplicity" of Language while to understand and follow the content of the page of UIT in RWA.

c. Security Perception

Most of the respondents strongly agree (62%) that they receive warning messages when the communication is insecure. Moreover, the remaining 38% also have the same (agree) opinion.

About 93% of the respondents believe that if RWA site addresses contain 'https', they are secured. The remaining 7% of respondents do not decide.

Around 69% of the respondents believe that if they are connecting to RWA with acceptable time limit, they will perceive that they are secure, while the rest of 31% also agree with same condition.

65% of the respondents have a strong trust on RWA and 18% of them also agree that they have a trust on RWA. But around 17% of them do not decide on this matter.

From the above survey result, it can be concluded that as security perception on RWA has marginally positive, the trust for UIT in RWA is also good.

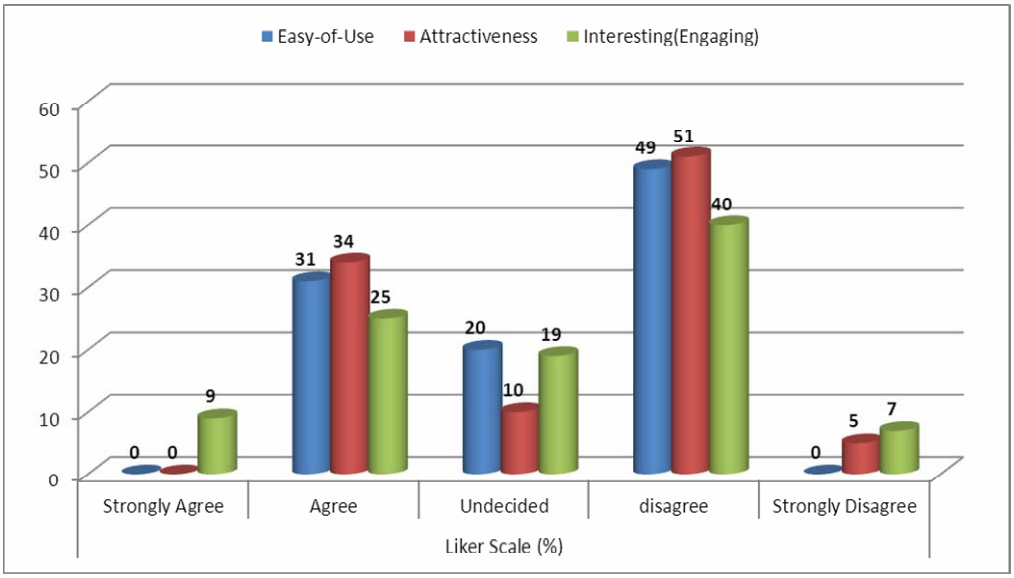

Figure 1: General Usability Perception

3.2 Usability Test Result

During the test, users have been observed while performing their tasks.

a. Task Completion

From the total participants, 66.66% of them successfully complete their tasks while 33.34% of them did not finish their tasks. Figure 2 summarizes the completion of tasks per participant.

One novice user and one expert user did not successfully complete their task. Usability is a generally relative measure of whether a software product enables a particular set of users to achieve specified goals in a specified context of use [12].

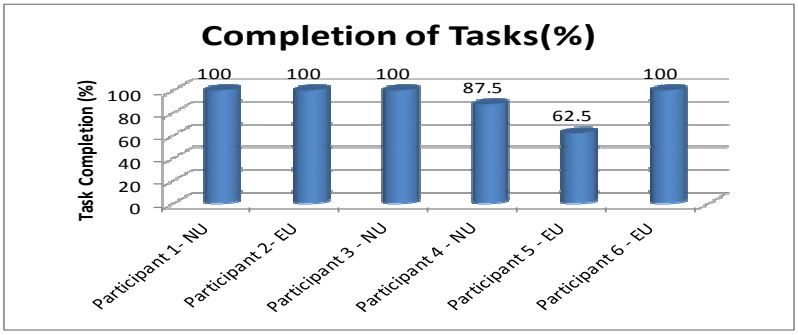

Figure 2: Completion of Tasks per participant

b. User Satisfaction Analysis for Proposed System

According to Aaron *et al.* [12], SUS is an effective tool for assessing satisfaction of a product. Thus, Figure 3 shows the mean score of SUS result per participant.

SUS has 10 questions which measures user satisfaction and the analysis is based on the participants' input. Figure 3 gives an idea about the SUS score ratings corresponding to participants and average SUS mean score for RWA. For novice users 1, 3, and 4, their average rate to perform the tasks (Identification Steps) is 43, 35, and 47.5 out of 100, respectively. Therefore, the satisfaction level for both participants is poor.

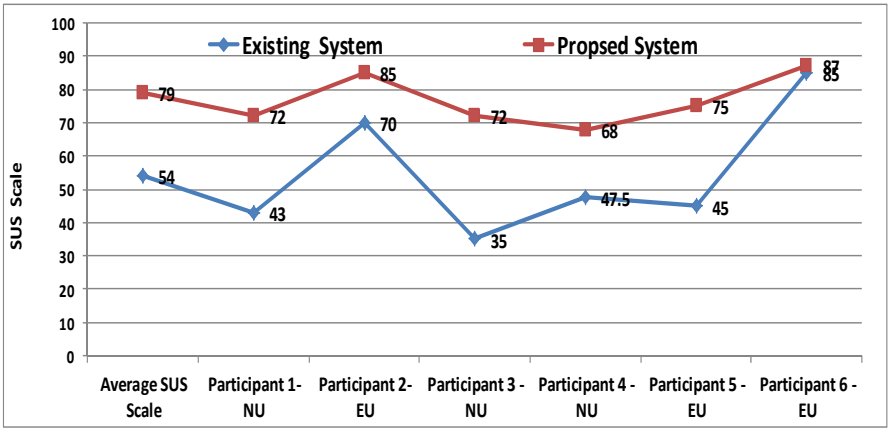

Figure 3: User Satisfaction results

For expert users 2, 5, and 6, their average satisfaction rate to perform the tasks (Identification Steps) is 70, 45, and 85 out of 100, respectively. For participants 2 and 6, satisfaction rate is marginally high (Good) and Excellent which is acceptable, respectively. The overall user satisfaction survey result for the existing RWA is 54, which shows low marginal.

From the above usability testing results, UIT in RWA has efficiency, effectiveness, and satisfaction problems.

4. Enhanced UIT for RWA

Based on the rationale behind the finding and discussion, the enhanced UIT for RWA considers usability features such as effectiveness, efficiency, user satisfaction, learnability, and memorability. Moreover, from security point of view, attention and memorability are also considered.

Figure 4 shows the high level design for the enhanced UIT for RWA.

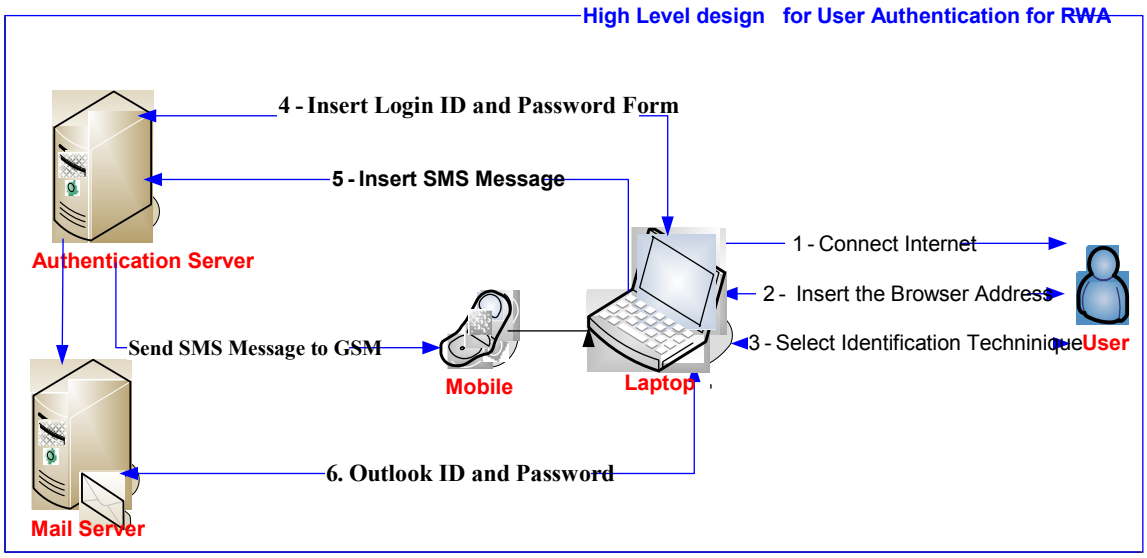

Figure 4: High Level design for UIT for RWA

5. Conclusion

Most of the time users are using RWA when they are offsite. Thus, the overall user satisfaction survey result for the existing UIT is low. Moreover, RWA is not effective with the current user identification steps. The rationale behind this is that users fail to achieve their goals and complete their tasks. The goal must be achieved within the acceptable time and effort but according to this research, the existing UIT is not effective. Therefore, it is possible to say the existing UIT has affected the usability of RWA.

The major finding of this research shows that most RWA users UIT is not easy to use and understand to follow. According to the survey result, for most users, UIT is not interesting and engaging; rather it is complex. Because of this reason, the UIT frustrates users. To minimize this frustration, RWA users start to write a note with a piece of paper to remember their secret such as username and password for ECAS and application, domain, and delegations. Also users discuss about their secret with others to login and access their email easily. All these actions expose the system to intruders. Moreover, they are not only exposed for stealing data but also as a whole the organization's UIT is vulnerable to attacks. Therefore, the new user identification technique of RWA makes them unhappy.

Despite the above conclusion, this study has limitations and future research in terms of accessibility will need to be done. Moreover, if this study is extended to other organizations which are using RWA, the outcome would be more precise.

References

[1] Wikipedia, "Microsoft Remote web Workplace," http://en.wikipedia.org/wiki/Microsoft_Remote_Web_Workplace, last access on March 20, 2012.

[2] J. Nielson, "Introduction to Usability", http://www.useit.com/alertbox/20030825.html, last accessed on February 02, 2012.

[3] L. Sommerville, Software Engineering, 9th ed., Addison-Wesley, 2010, pp. 745.

[4] C. Braz, and J. Robert, "Security and Usability: The Case of the User Authentication Methods", in Proceedings of the 18th International Conference of the Association Francophone D'interaction Homme-Machine, IHM 2006, Montreal, Canada, Vol. 133, 2006, pp. 199-203.

[5] Wikipedia, "European Union," http://en.wikipedia.org/wiki/European_Union, last accessed on March 02, 2012.

[6] CNN World, "European Union under cyber-attack as major summit begins," http://articles.cnn.com/2011-03-24/world/eu.cyberattack_1_cyber-attack-eu-summits-eu-administration?_s=PM:WORLD, last accessed on January 02, 2012

[7] European Commission Information System Security Policy, "C(2006) 3602", Brussels, 2011, pp. 18

[8] J. Nielsen, "Usability Engineering", Academic Press, Boston, 1993, pp. 26.

[9] ISO 9241-11, "Ergonomic Requirements for Office Work with Visual Display Terminals", 1999.

[10] B. Schneider, "Sensible Authentication," ACM Queue 1, 2004.

[11] J. R. Lewis, "Sample Sizes for Usability Studies: Additional Considerations," Human Factors, Vol. 36(2), 1994, pp. 368-378

[12] B. Aaron, K. Philip, and M. James, "Determining What Individual SUS Scores Mean: Adding an Adjective Rating Scale," Journal of Usability Studies, Vol. 4, Issue 3, 2009, pp. 114-123.