2013 Fourth International Conference on e-Learning "Best Practices in Management, Design and Development of e-Courses: Standards of Excellence and Creativity"

Security and Collaborative Groupware Tools in Education

A Case Study at the University of Bahrain

Resala AlAdraj
PhD candidate
Department of Computer Science, University of Warwick
Coventry, UK
r.aladraj@warwick.ac.uk

Mike Joy
Associate Professor
Department of Computer Science, University of Warwick
Coventry, UK
m.s.joy@warwick.ac.uk

Abstract — This paper presents an evaluation of the security, safety, and privacy of selected Online Collaborative Groupware (OCG) tools such as Skype, Facebook, Wikis and Gmail (SWFG) used to support learning activities from the perception of the students, and with a particular focus on the impact of their usage on student trust. A case study was conducted with two groups of undergraduate students at the University of Bahrain to identify and develop an efficient model for using SWFG tools securely within learning. In doing so, questionnaires were distributed post case study among two different students groups A and B. The overall finding of this study is that there are differences between two groups in their usage with respect to security, privacy, and trust for SWFG tools.

I. Introduction

During the last decade, the web has changed from a simple hypertextual repository of documents to a powerful communication medium. This change has caused educational activities to be highly supported by web applications which often include collaborative sessions. A wide range of technologies has been prepared by educational institutions in order to support collaboration between learners and between learners and teachers. In recent years, web-based technologies have allowed people who are located in different places to interact with each other in synchronous and asynchronous ways, which can then support good collaborative learning activities. Collaborative groupware can broadly be defined as a process of learning in which two or more people learn something together.

Discovery of the right tools to support groupware, and intensive use of technology which supports social activities such as chatting and messaging, should support student learning and hence ensure a successful educational outcome.

The ubiquity of the Internet and online technologies provides a framework within which Online Collaborative Groupware (OCG) tools become widely available and provide benefits for student learning. However, there are challenges facing OCG tools, and student concerns about their usage, for example security. Hence, the researcher has chosen Skype, Facebook, Wikis and Gmail (SWFG) as a an example of the OCG tools to evaluate the security, safety, trust and privacy from the perceptions of the students .In doing so, a case study was conducted at the University of Bahrain (UOB) with two groups of undergraduate students A and B. Group A used SWFG without applying security mechanisms and group B used SWFG with security mechanisms.

Hence, the aim of this paper is to answer the following research questions.

1) Do SWFG tools used by group B have higher levels of security when compared to the use of these tools by group A?
2) Do SWFG tools used by group B have higher levels of trust when compared to the use of these tools by group A?
3) Do SWFG tools used by group B have higher levels of privacy when compared to the use of these tools by group A?
4) Do SWFG tools used by group B have higher levels of safety when compared to the use of these tools by group A?

In order to answer the research questions four hypotheses were formulated related to the groups A and B in the cases of security, safety, privacy, and trust. The hypotheses are as follows.

A. Hypothesis 1

Ho: SWFG tools used by group B post- experiment do not give a higher level of security when compared to the use of these tools by group A post- experiment.

Ha: SWFG tools used by group B post- experiment give a higher level of security when compared to the use of these tools by group A post- experiment.

B. Hypothesis 2

978-0-7695-5036-7/13 $26.00 © 2013 IEEE
DOI 10.1109/ECONF.2013.56

Ho: SWFG tools used by group B post- experiment do not give a higher level of safety when compared to the use of these tools by group A post-experiment.

Ha: SWFG tools used by group B post- experiment give a higher level of safety when compared to the use of these tools by group A post- experiment,

C. Hypothesis 3

Ho: SWFG tools used by group B post- experiment do not give a higher level of privacy when compared to the use of these tools by group A post- experiment.

Ha: SWFG tools used by group B post- experiment give a higher level of privacy when compared to the use of these tools by group A post- experiment.

D. Hypothesis 4

Ho: SWFG tools used by group B post- experiment do not give a higher level of trust when compared to the use of these tools by group B post- experiment.

Ha: SWFG tools used by group B post- experiment give a higher level of trust when compared to the use of these tools by group A post- experiment.

The rest of the paper is organized as follows. Section 2 provides a literature review for this study, section 3 discusses the experimental design, data collection, and analysis, and section 4 concludes and discusses future work.

II LITERATURE REVIEW

This section reviews the relevant related literature for this case study, focusing on authentication and security issues, related to trust and privacy of OCG tools.

Social media and collaborative groupware. Every day, social networking sites have been gaining popularity and influence, particularly in education, and Treepuech (2011) comments that "the application of using social network sites with available online tools will benefit in teaching and learning management as it helps teachers to access students and able to communicate conveniently in a timely manner" and considers that communication and collaboration can easily help the students gain experience with the technology.

Solomon *et al.* (2011) note that Social Media Collaborative Work systems are an evolution of Computer Supported Cooperative Work (CSCW) systems. They further state that "email systems can be integrated with wikis and social networking, and be used by product development teams working with engineers to build silent wind-turbine technology for houses around the world and so solve some of the world's renewable energy needs".

Trust. Technological solutions are not only designed to keep the users safe from any threats, but also to increase "trust". According to May and George (2011), trust is defined as a confidence in someone's competence and his or her obligation to a goal. Trust is also a vital for enabling meaningful and commonly beneficial interactions that construct and maintain learner collaboration and community. At the moment, privacy and trust are fundamentally connected as privacy is a natural concern, increasing the importance of trust in any learning environment. For example, in a closed learning environment where all learning services are provided internally, students can have higher confidence that their personal data will be treated properly. Thus, working collaboratively with other learners could be effectively conducted if there is sufficient trust between the learners.

Usage of social networks in learning. The new structure of web 2.0 provides the ability to share information, opinions and experiences. This new technology enhances the relationship between the user and the information sharing in an environment of mutual collaboration (Rodrigues *et al*., 2011). The ability of learners to edit, post new content and participate in discussions with other students forces them to be more active in the learning process rather than merely passive. For example, Wikis are a web technology for massive collaborative writing which can allow free and easy access for learners. However, security and privacy of the wiki contents is definitely an issue. Rodrigues *et al*. (2011) have conducted a case study on the security and privacy of Wikis which has shown the positive effect of them on the learning process. However, the authors have commented that security and privacy "have up to now been neglected in this context , though they are an important factor".

III. EXPERIMENT DETAILS

This section discusses the experimental details of the study. The researcher adopted a case study design in order to compare two groups of students in their usage of secure SWFG tools. The following sections discuss the participants, research instruments, and the data collection.

A. Participants

Two classes of 51 undergraduate students in the IS department of the IT college at UOB were chosen as participants, and each class was divided into two approximately equal groups, A and B.

B. Research instruments

Using more than one research method for data collection to achieve the research aims and objectives is known as a

Mixed Methods approach. The mixed method of data collection used in this study employs both qualitative and quantitative methods, since these are regarded as highly complementary, rather than mutually exclusive (Creswell, 2003). Moreover, the mixed method of data collection permits the researcher to undertake triangulation. In this study, data were collected using a combination of questionnaires, interviews and observations.

1) Triangulation

Leedy (1997) defines triangulation as the way in which different methods of data collection, varying data sources; different analyses or theories may be used to check the accuracy and validity of the findings. Creswell (2003) puts forward the argument that the use of varying methods of data collection and analysis should lead to greater validity and reliability than a single method of data collection and analysis. Therefore, both qualitative and quantitative methods were used for the purposes of triangulation. The researcher considers that by deploying the qualitative and quantitative method of data collection and analysis, the credibility and interpretation of the findings may be enhanced, since evidence and themes emerge from different sources. In this study, triangulation was performed by comparing data collected from the interviews against the questionnaire and observation data.

2) Qualitative data (interviews, observations and logs)

The qualitative data of this study includes non-numerical data obtained from interviews conducted with some of the participants and their teachers, and their interpretation. Interview data were collected pre- and post-experiment with seven randomly selected students and two teachers. In addition, the researcher gathered qualitative data from observations of the students and from log files generated by the SWFG tools. Log files here refer to the chat and communication history of the participants during the experiment.

3) Quantitative data (questionnaires)

Quantitative data communicate meaning and interpret information by means of numerical analysis. This is accomplished by statistical methods that help to generalize findings. Quantitative researchers adopt an objective stance regarding participants and their settings, and use sample research to apply their findings to a larger population (Neuman, 2000; Dillman, 2000).

The researcher distributed a questionnaire to the students in the classroom after the experiment. The questionnaire was preceded by a pilot study. The main body of this survey addressed questions relating to secure SWFG tools. The questionnaire consisted of three main sections, including seven questions relating to personal information, experience of usage of SWFG, trust and security. Section one gathered demographic information about the participants, including age, year of study and education background. Section two sought to collect information on the students' experiences of SWFG and their usage of SWFG tools when working on collaborative group work during their learning activities. Section three served to gather information about how the students felt when they used SWFG regarding trust, security, safety and privacy.

C) Data collection

In the present study, different types of data collection methods were used pre and post-experiment for both groups, A and B. The details of the data collection methods and the reason for choosing these methods are summarized in the following sections.

The security, safety, privacy and trust of the four SWFG tools were critically evaluated by the researcher and studied on the basis of the factors depicted in Table 1.

TABLE 1: Security Mechanisms of SWFG Tools

Learning activities	OCG tools	Security mechanisms
Real-time data conferencing, electronic display, video conferencing and audio conferencing	Skype	Authentication and authorization
Assignment submission	Gmail	Verification
Chatting / discussion / idea generation	Wikis	Authentication and authorization
Chatting / discussion / idea generation	Facebook	Authentication and authorization

Two assignments were chosen as a means of evaluating the usage of SWFG tools within a period of three weeks. The first assignment asks the students to work in group in order to search about "What is the difference between pipelining and parallel processing?"

Assignment 2 was to search about "the term SOLID STATE and give three examples of SOLID STATE storage devices".

The case study contained the following activities.

Both groups from both classes started their assignments using the SWFG tools above to solve the assignments, and the experiment started as follows.

Group (A) from each class used the SWFG tools and their learning tools without setting the security and privacy mechanisms depicted in table 1.

Group (B) used the SWFG in security mode, as depicted in Table 1.

After group B had set security settings for the SWFG tools, both groups undertook the following learning activities.

1. Both groups edited the wikis to answer the questions of Assignment 1.

2. They shared information with other students in the same group and their teachers, and shared pictures, ideas and information related to the assignment, using Facebook, as depicted in figure 2.
3. Skype and Gmail were used to exchange files, and to support discussion and chatting with each other and with their teacher during the day.

The second assignment was submitted using one of the tested SWFG tools. Following this, a second questionnaire was distributed among the participants. The following section will discuss the data analysis and discussion of the result

IV. DATA ANALYSIS AND DISCUSSION OF RESULTS

A. Data analysis:

The perceived security, safety, privacy and trust of SWFG tools were measured using a t-test for both groups A and B at the post-experiment stage.

The t-test (independent sample t-test) was used to evaluate whether the means of two groups are statistically different from each other. The researcher used SPSS software to calculate the result of the t-test. The results of the questionnaires analysis and hypotheses result for security, safety, privacy and trust are discussed in the following section:

B. Discussion of results

1) Security

Both groups A and B answered question 5 of the questionnaire (2). The question was related to security. Secure SWFG means that the information shared by such tools will only be accessible to those for whom it is intended during the experiment.

There was an improvement in the feedback of the students of experimental group B who obtained a significant result (t=2.115, df=20.04), (t=2.020, df=23.52), (t=3.261, df=22.5) for Facebook, Wikis, and Skype respectively, and all are significant at P<0.005. This provided further evidence for accepting the first hypothesis for the three SWFG except Gmail, which had (t=0.069, df=42, P>.05). These results seem to indicate that Skype, Facebook, and Wikis are perceived by students in group B to provide a higher level of security when compared to students in group A.

In addition, qualitative evidence from students' comments confirmed these conclusions, from group B, namely that the SWFG (Skype, Wikis, and Facebook) have security. Seven students commented that these tools were secure. For example, as student Z stated: "We really found such tools are more secure, we could use them without any problems".

2) Safety

Both group A and B were asked to answer question 6 of the questionnaires. The questions were related to safety. Saved SWFG means that these tools are protected from harm such as viruses, spyware, etc.

Data analysis using a t-test, which measured students' perceptions of safety of SWFG tools during their learning activities, revealed the following:

Gmail (t= 2.036, df=42, significant at P<0.05),
Wikis (t= 1.561, df=41, P>0.05),
Facebook (t= 1.107, df=39, P>0.05),
Skype (t= 1.321, df=41, P>0.05)

Hence, the second hypothesis, which states that SWFG tools used by group B post- experiment gives a significantly higher level of safety when compared to group A, is accepted for Gmail only.

Qualitative evidence from students' comments further supports this result for Wikis, namely that the majority of the students reported a lack of safety while using Wikis. For example, Student W reported "Using wikis by sign up is difficult to use and we did not feel any safety during using it in the experiment".

3) Privacy

The privacy of SWFG was measured by question 7 of questionnaires. The ability of the participants to isolate the information about themselves and thereby reveal themselves selectively when using SWFG is called OCG privacy.

Data analysis using a t-test revealed the following:

Gmail (t= 0.464, df=41, P> 0.05),
Wikis (t= 0.211, df=38, P>0.05),
Facebook (t= 1.644, df=8, P>0.05),
Skype(t=2.232, df=39, P>0.05)

Therefore the third hypothesis, which stated that SWFG tools used by group B post- experiment give a significantly higher level of privacy when compared to group A, is rejected for Gmail, Wikis, Facebook and Skype.

4) Trust

Data analysis using a t-test for question 4, which measured the trust for SWFG during learning, revealed the following:

Gmail (t= 2.228, df=40, significant at P<0.05),
Wikis (t= 0.953, df=39.8, P>0.05),
Facebook (t= 2.671, df=39, significant at P<0.05),

Skype (t= 2.532,df=41, significant at P<0.05)

Therefore the fourth hypothesis, which states that SWFG tools used by group B post- experiment are perceived to give a significantly higher level of trust when compared to group A, is accepted for Gmail, Facebook and Skype.

Qualitative evidence from students' comments further supports these results. The researcher noticed from her records and log files that the majority of students in group B enjoyed using Gmail, Facebook and Skype after they applied security, safety and privacy settings.

Two course teachers noticed that the majority of group B students used Facebook and Skype. For example teacher X commented: "…. I cannot believe what I observed, most of group B students join Facebook and send me comments and share the assignment information".

The researcher noticed the participants of group B chased her up for using Skype and tried to Skype her all the day. Student Y commented, "We cannot imagine how these SWFG tools can facilitate our learning process, Skype shortens the way between ourselves as students as well as the teachers and ourselves."

V .CONCLUSIONS AND FUTURE WORK

1) Discussion and conclusions

The aim of this case study was to identify the level of security, privacy, safety, and trust in the usage of SWFG tools within learning, especially among students at UOB. The findings of this investigation, together with hypotheses testing, have assisted the researcher in achieving this goal.

The overall finding of this study is that there are differences between groups A and B. Regarding security, Wikis, Facebook, and Skype are perceived to have a higher level of security. In addition to this, there were enhancements in the students' trust towards SWFG in the learning process. These results are very encouraging for the use of secure SWFG tools in the difficult and complex technical aspects of e-learning at university of Bahrain. On the other hand, secure Gmail was *not* perceived to have a higher level of security when it was used in learning. However, group B participants used Gmail for more than two hours daily. This differences in result serve to indicate potential certain limitations in the survey.

Furthermore, log files and observations during the experiment support what the researcher has concluded. This history may be taken as support for the t test result and emphasize comments collected during the interviews.

Figure 1 shows some of students' chat history in Skype. The researcher had interviews with some of them and took their points into consideration.

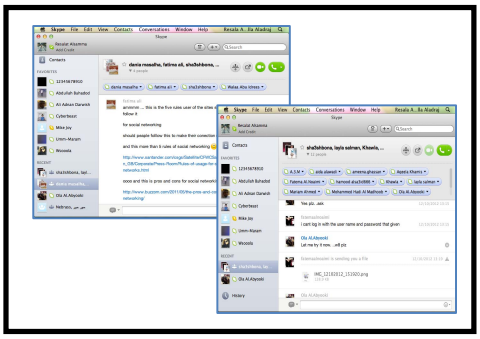

Fig 1. Screenshots of the Skype conversations between participants

Thus, the researcher in her future work will focus on the security and trust of Gmail only because Gmail since June 5, 2012, has a new security feature which was introduced to protect users from state-sponsored attacks. In addition to that Gmail has a large user base compared to Facebook and Wikis.

The researcher will focus on the reasons behind the results reported above, and will investigate the culture of the students, authentication settings, and the reputation of Gmail.

2) Limitations

Several limitations may be commented on regarding the experiment. First of all, the research was only conducted at UOB, whereas including other universities in Bahrain might provide a better representation of Bahraini students. This would have enabled the researcher to work towards more comprehensive findings, representative of students all over Bahrain. Furthermore, only first-year students at UOB participated in this study. A wider study would comprise students at different stages of their studies.

A further limitation of the study may be the validity and reliability of the investigations conducted. However, the researcher has attempted to minimize the impact of this investigation by using multiple methods of data collection to complete this study. For example, a mixture of interviews, log files and observations were widely used throughout to ensure that data was collected from different sources, and triangulation was performed wherever possible.

3)Future work

The main results have been translated into actionable suggestions to be implemented. The study has demonstrated that implementing secure SWFG tools provides a more suitable corrective to the lack of collaborative group work in the classroom environment, and can help to motivate the students to trust OCG tools, increase trust in such tools, whilst assisting in the teaching of difficult technical

knowledge in a more efficient and practical manner.

It is clearly shown that all SWFG tools tested in the experiment can have high level of safety, privacy, security and trust, with the exception of Gmail, which was perceived not to have a level of security. The researcher will conduct a second case study in order to test the security and trust of Email. This will involve a further consideration of those factors that affect the failure of Email to be secure, leading to greater trust in Email usage. These factors will include culture, authentication settings, availability of multiple free email tools, and the emergence of social networks as communication providers.

REFERENCES

1. Beca, L. and Podgorny, M., "Security issues in web-based collaborative systems", CollabWorx Research Publications and Document Library, 2000.

2. Terpstra, L., "A security model for the work space groupware architecture", [online] Available at http://symbiosis.rmc.ca/pub/terpstra-meng-thesis-2002.pdf [accessed 02 September 2011], 2002.

3. May, M. and George, S., "Using students' Tracking Data in E-learning: Are we always aware of security and privacy concerns?" *Proc. IEEE 3rd International Conference on Communication Software and Networks (ICCSN),* pp. 10-14, 2011.

4. Rodrigues, J.J.P.C., Sabino, F.M.R. and Zhou, L., "Enhancing e-learning experience with online social networks". *Communications of the IET*, v. 5, pp. 1147-1154, 2011.

5. Treepuech, W., "The application of using social networking Sites with available online tools for teaching and learning management". *Proc. 2011 International Symposium on IT in Medicine and Education (ITME)*, pp. 326-330, 2011.

6. Solomon, B.S., Duce, D. and Harrison, R., "Methodologies for using Social Media Collaborative Work systems". Proc. First International Workshop on Requirements Engineering for Social Computing (RESC), pp. 6-9, 2011.

7. Dillman, D. A., "Mail and Internet surveys: The tailored design method", 2nd ed., New York, NY: John Wiley & Sons, 2000.

8. Neuman, W. L., "Social research methods: Qualitative and quantitative approaches", (4th ed.). Boston: Allyn & Bacon, 2000.

9. Leedy, P. D., "Practical research: planning and design", (6th ed.), Upper Saddle River, NJ: Prentice-Hall, Inc,, 1997.

10. Creswell, J. W., "Research Design: Qualitative, Quantitative, and Mixed Approaches". Thousand Oaks, Ca: Sage, 2003.