A Usability Study of an Access Control System for Group Blogs

Indratmo, Julita Vassileva

A Usability Study of an Access Control System for Group Blogs

Indratmo
Department of Computer Science
University of Saskatchewan
Saskatoon, SK S7N 5C9, Canada
j.indratmo@usask.ca

Julita Vassileva
Department of Computer Science
University of Saskatchewan
Saskatoon, SK S7N 5C9, Canada
julita.vassileva@usask.ca

Abstract

Blogs are a medium to express thoughts, feelings, and opinions. Once published, blog articles potentially become persistent and can be read by non-intended audiences, causing hurt feelings and other troubles. In part these problems are due to the lack of access control in blogs. We propose an access control framework for group blogs. Compared to the typical access control in blogging tools, our system differs in a few aspects. First, the system enables bloggers to grant different access privileges to different audiences over a single blog article. That is, it associates access privileges to people rather than to artifacts (e.g., articles, blogs). Second, the system allows a blogger to create a collaborative space with other bloggers, for example by allowing others to edit his or her articles. Third, the management of access control is integrated with the process of writing and editing blog articles, facilitating the main workflow of the user. We conducted a usability study to evaluate our system and get constructive feedback from users. In this article, we present the proposed access control system, the results of the study, and analysis of the results.

Keywords

Blogs, access control, privacy, usability

1. Introduction

Sharing information through blogs brings the risk of privacy violation. Once the information is available online, the author loses control over its distribution [6]. An article written to a particular audience, within a certain context, may be found through search engines, read by other audiences, and interpreted out of its context, which can raise privacy issues and cause troubles. There have been cases where friendships were broken, people were fired or suspended from work because of their blog articles [1, 9, 11]. These examples trigger a question: do bloggers need an access control system to manage who can access their blogs?

On one hand, the examples above show that blog authors can get into trouble because their blogs are found unexpectedly by certain audiences due to the lack of access control in their blogs. On the other hand, don't bloggers want to interact with and disseminate information to as many people as possible? This situation illustrates that there is a tension between sharing and protecting information, which are viewed by some researchers as two facets of the same task [3, 5, 10].

The need for access control is more apparent in a community or group blog—a blog consisting of multiple authors. In such settings, it is often necessary to assign different privileges to different users. For example, to control the quality of posts in a community blog, the administrator may want to give more privileges to reputable members while allowing new members to participate in the community in a limited way. The core members of the community may want to have a protected space where they can discuss certain issues privately among themselves. Such requirements call for flexible, fine-grained access control for blogs, ideally, without adding too much complexity for the authors.

In this article, we outline our approach to designing an access control framework for blogs. Although applicable to personal blogs, our approach is focused on group blogs. In section 2, we review bloggers' practices on protecting privacy. Then we discuss the design of our access control framework (section 3). We conducted an initial study to evaluate our system. We describe the study methods in section 4, present the results in section 5, and analyze the results in section 6. In section 7, we conclude by discussing some design implications.

2. Privacy management in blogs

Most bloggers put their real identity in their blogs [8, 11]. However, when they mention other people in their blogs, they follow some guidelines [11]. First, they use only a first name, a pseudonym, or initials of the person. However, if the person mentioned in the articles is a blogger or has an online persona such as personal web pages, they may provide a link to that information. Second, they disclose a person's real name when they say good things about that person. Third, instead of using any name, they only mention their relationship with the subject in their articles (e.g., my friend).

To deal with privacy issues, some bloggers maintain multiple blogs for different audiences or topics [11]. For example, a blogger may create a blog to talk about general topics, while maintaining another one—using a pseudonym—to write about more sensitive topics such as politics.

Another approach to protecting privacy is by relying on shared knowledge between authors and their audiences to achieve mutual understanding [7]. That is, bloggers write their articles ambiguously—without giving contextual information in detail—so that only their intended audiences (e.g., close friends) can understand the essence of the articles.

Due to the need of limiting the audience of blogs, current blogging tools enable the users to control access to their blogs.

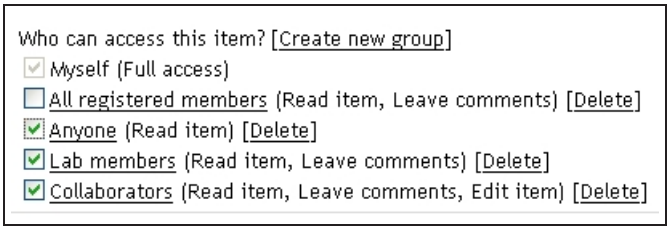

Fig. 1: *A list of user groups and their access privileges*

An access control system can reduce the possibility that non-intended audiences find certain blog articles, thereby helping bloggers protect their privacy. In principle, blogging tools such as Blogger (blogger.com), LiveJournal (livejournal.com), and Xanga (xanga.com) allow the users to specify the accessibility of their articles at three levels: *private* (the articles are accessible only by the author), *limited* (the articles are accessible only by a certain group of people as specified by the author), and *public* (the articles are accessible by anyone).

Along the social dimension above, the users can customize their blog settings further, for example by enabling or disabling comments on their blogs, or restricting comments only to a certain user group. These settings may apply to individual posts (e.g., LiveJournal, Xanga) or to the whole blog (e.g., Blogger).

The typical access control features supported by current blogging tools may meet the requirements of most personal blogs. However, if we want to use blogs in collaborative settings (i.e., group blogs), we need to have finer-grained access control features, which allow the users to create a collaborative space with others. In the next section, we present the design of our access control framework and compare it with the typical access control in current blogging tools.

3. Design of access control framework

We make the following assumptions while designing our access control framework. First, we assume that bloggers write and post their articles to a group of people instead of to individuals. Second, these user groups are stable in terms of their members and access privileges. That is, bloggers rarely need to change the groups' membership and access privileges from post to post. Third, the number of groups that a blogger maintains is small.

Based on these assumptions, we design the semantics of our group-based access control as follows. Bloggers determine who can access their articles and what the audiences can do with the articles by creating user groups and giving the groups access privileges. The list of user groups is accessible while bloggers write or edit articles, so that they can select their audiences from this list (see Figure 1). These groups are visible only to the creator. Displaying such groups publicly may create a social tension, as groups and their privileges, to some extent, reflect the group owner's trust in other users.

There are two types of access privileges: basic rights and meta rights [4]. The basic rights consist of the rights to read articles, leave comments, and edit articles. The meta rights allow a user to grant basic rights to other users. Each basic right has a corresponding meta right. Authors always have full access to their blog articles.

Basic and meta rights are arranged hierarchically. For basic rights, "read items" has the lowest rank, followed by "leave comments" and "edit items." A higher-ranked right includes all lower-ranked rights. For example, a user having the right to leave comments on a blog article implies that the user also has the right to read the item. The order and semantics of meta rights is the same as those of basic rights, except that users receiving meta rights also get the corresponding basic rights. Thus, a user who is able to grant read access to a blog article is also allowed to read the blog article.

Bloggers may put a user into multiple groups and grant different access privileges to different groups. They can post an article to multiple groups having different access privileges. As opposed to most blogging tools which associate access rights to blog articles or to the whole blog (see section 2), our framework associates access privileges to user groups. The reason is that access control is related to trust, and trust is related to people rather than to artifacts (e.g., blog articles). In everyday lives, people may allow their friends to read their diary, but put restriction that only their best friends can leave comments on the diary: the same artifact, different access privileges. As illustrated in Figure 1, a blogger may allow anyone (public audiences) to read only a blog article—to avoid spam, for example—while allowing his or her colleagues (lab members) to leave comments on the article. If they need to do collaborative work, bloggers may allow certain users (collaborators) to edit their blog articles. Thus, using the access control system, bloggers can adapt the accessibility of their writings to different situations, for different users.

Our framework is centered in groups. If bloggers add a user to a group, the user will gain access to both new and old articles previously posted to the group. If a user is removed from a group, the user will lose his or her access privileges as determined formerly by the group's settings. If a group's access privileges are changed, the new settings will apply to both new and old articles previously posted to the group.

4. Study methodology

We conducted a user study to test the usability and perform a formative evaluation of the access control system. Our main research question was, "Can people learn and use the access control system properly without training?" From this study, we aim to get constructive feedback from users to refine the design of the system.

Participants. The participants were eight graduate students in computer science (three females and five males). Five of them were between 18 to 30 years old, and three were between 30 to 45 years old. On a scale of one (beginner) to five (expert), seven participants rated their computer skills as an end-user at level four or five, and one at level three. On average, half of the participants spent one to five hours daily to browse the Web, whereas the other half spent more than six hours daily. Four participants have maintained personal blogs for the last one to two years. Their blogging tools varied from Blogger, MSN Spaces, and Movable Type.

Apparatus. The blog system used in the study was supported by Nucleus (nucleuscms.org). The blog was hosted on a Windows machine running Apache web server and MySQL database server. The access control system extended the core functionality of Nucleus and was implemented as a Nucleus plugin. We conducted the study in the participants' workplaces, using their computers and their choice of web browsers.

Procedure. Participants were introduced to the purpose of the study and asked to fill out a questionnaire about their

Task No.	Description
T1	To post an article to an existing group without needing to modify the group's access privileges
T2	To modify access privileges of an existing group and post an article to the group
T3	To create a new group, configure its access privileges, and post an article to the group
T4	To revoke a user's access privileges
T5	To revoke a group's access privileges
T6	To post an article to a single user
T7	To post an article to multiple groups with different access privileges
T8	To interpret an access control configuration of a blog article

Table 1: *Task description*

background and experience in blogging. After that, they were given an introduction about how to write, edit, and view an article using Nucleus. While introducing Nucleus, however, we excluded describing how to use the access control features.

After the introduction, participants were given a scenario and a set of tasks to complete. We printed each task on an index card and gave one task at a time to them. We did not impose a time limit on each task. While the participants were performing the tasks, we observed them, and took notes to record difficulties faced by them. When they had problems in navigating through Nucleus, we provided some directions, as our purpose was to evaluate the access control features, not Nucleus. The tasks involved posting articles to the blog and setting their accessibility, as well as interpreting the accessibility of a blog article (see Table 1). After performing each task, the participants rated how easy or difficult the task was, and how easy or difficult it was to use the system to perform the task. After the participants finished all tasks, they were interviewed to describe their experience using the system and to give suggestions to improve the system.

5. Results

Our usability study aimed to test if users can configure and use the access control system properly. Therefore, we measured the number of successful and failed tasks completed by the participants. In the study, all participants completed the test session in 45 to 60 minutes, including the post-test interview. Taking ideas from [2], we categorized the completed tasks into three categories: *success* (the participant completed the task correctly without needing to revisit the task), *dangerous success* (the participant completed the task correctly, but either needed to revisit the task or mistakenly changed the accessibility of other articles), and *failure* (the participant completed the task incorrectly).

Table 2 presents the summary of the test results. Overall, the majority of the given tasks (82.8%) were completed successfully. However, some tasks (6.25%) were revisited or completed with side effects; and about 11% of the given tasks were completed incorrectly.

Besides using task correctness to evaluate our system, we also asked the participants to rate how easy or difficult it was to use the system to complete the given tasks. Figure 2 illustrates the average score for each task, on a scale of one (very easy) to six (very difficult). In general, the participants

Task No.	Success	Dangerous Success	Failure
T1	7 (87.5%)	0 (0%)	1 (12.5%)
T2	3 (37.5%)	1 (12.5%)	4 (50%)
T3	8 (100%)	0 (0%)	0 (0%)
T4	8 (100%)	0 (0%)	0 (0%)
T5	8 (100%)	0 (0%)	0 (0%)
T6	8 (100%)	0 (0%)	0 (0%)
T7	5 (62.5%)	3 (37.5%)	0 (0%)
T8	6 (75%)	0 (0%)	2 (25%)
Total	82.8%	6.25%	10.9%

Table 2: *Test results*

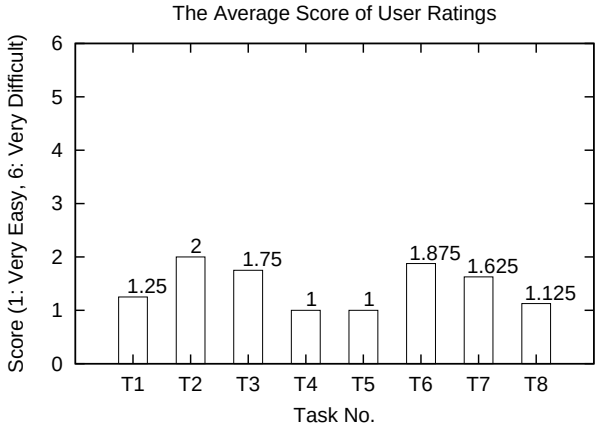

Fig. 2: *The average score of user ratings of how easy or difficult it was to use the system to perform each task (1: very easy, 6: very difficult)*

rated the access control system as easy to use (the maximum average over all users and all tasks was two).

6. Discussion

Table 2 shows that the participants performed tasks T2 and T7 less successfully. T2 required the participants to edit a group's configuration. The main source of confusion was that the user interface did not indicate explicitly how to edit a group's configuration. Instead of using an explicit label, the system provided a hyperlink using the groups' name to provide access to the page that allows the user to edit a group's configuration (see Figure 1). The implicit label was overlooked by the participants who failed to realize that they could edit a group's configuration by clicking on the group's name. Some of the participants who were able to edit a group's configuration suggested that the hyperlink to edit a group should be more explicit, e.g., to put the hyperlink beside "Delete" and use an explicit label such as "Edit group."

Another problem was observed while the participants performed T7. Three participants changed the accessibility of other articles (dangerous success). The user interface did provide a warning about this potential problem. However, the warning failed to attract the participants' attention, as it was unobtrusive. Some participants did not read the warning and completed the task without realizing the side effects. During the post-test interview, a few participants were apparently aware of this potential problem and knew how to prevent the problem, but did not do it. We speculate that

this was in part due to the level of user engagement in performing the task. Using scenarios in controlled experiments helps in establishing the context to some extent. However, the level of engagement is less compared to that in field studies, where the users perform tasks that are directly related to them. Conducting a field study, however, is an expensive process and may not be justified during early design stages.

Design feedback. Managing access to blog articles is part of the workflow of writing, editing, and posting the articles to groups of audiences, consistent with the view that information sharing and access control are essentially the same task [3, 5, 10]. Therefore, we integrate the user interface for writing and editing articles with that for managing articles' accessibility, in this case, through user groups. Using this approach, users do not have to create groups in advance. When they need to create a new group or change the access privileges of a group, they may do so without losing the context of their writings. The interface for managing groups is accessible from the writing page through a popup window. One participant commented that this was a good design decision, as he could maintain the context of his activity (i.e., writing an article) while managing the article's accessibility.

Interestingly, one participant did not take advantage of the feature above. Instead of configuring the user groups from the writing page, he first posted the article to himself, configured his user groups, and then edited the article's accessibility as required by the task descriptions. In the post-test interview, he explained that he got used to this approach; that's what he usually did when managing access control. His answer may indicate that many applications currently separate the management of access control from information sharing. In most cases, however, managing access control is actually a supporting activity rather than a main activity, and hence, it should become an integral part of the main activity [3, 5].

During the study, we also observed that displaying groups' access privileges (see Figure 1) helped the participants prevent mistakes. On a few occasions, prior to posting their articles, the participants realized their mistakes due to these lists of access privileges.

Another suggestion from a participant regarding blogs in general is that blogs should be supported by awareness and communication tools. She used MSN Spaces as an example. MSN Spaces is integrated with MSN Messenger, allowing users to maintain lists of contacts, communicate with them, and get notification when their friends are online or post new articles. Thus, blogs should not be stand-alone applications, but must be able to work with other communication tools.

Limitations of the study. The number of participants in our study was small, which limits the generalizability of the results. Further, our participants were advanced computer users, so their performance in learning and using the access control system might not be representative either.

Our study was limited to testing the usability of the access control interface. It did not examine whether or not our group-based access control framework can meet the requirements of group blogs. Testing the suitability of such framework needs a long-term field study with a real community of bloggers as participants.

7. Conclusion

When designing protection mechanisms such as access control systems, password managers, and encryption systems, the designers must ensure that users can understand and use the systems properly, as the effectiveness of protection mechanisms relies on the users [3, 5]. If users do not understand the systems, they may mistakenly believe that they have protected their data [2, 12]. Conducting a usability study of such systems can help in sorting out any design flaws indicated by the difficulties faced by the users, so that the usability of the systems can be improved.

In everyday lives, managing access control is usually part of other activities [3, 5]. Therefore, it should be integrated into the main activity to facilitate the workflow. Treating access control management as a separate activity distracts and prevents the users from seeing the context of their main activities.

In this article, we have discussed our access control system for group blogs. The main features of our system are the integration of the access control interface with the process of writing and editing articles, and the ability to give different access privileges to different audiences over a single blog article. Overall, results from our study showed that the participants found the system simple and could use it properly.

Acknowledgements

We thank our participants, Joyce Boedianto, and David Pinelle for their valuable feedback about this project.

References

[1] H. Bray. Job blogs hold perils, opportunities. The Boston Globe, http://bostonworks.boston.com/globe/articles/010404_blog.html, 2004.

[2] S. Chiasson, P. C. van Oorschot, and R. Biddle. A usability study and critique of two password managers. In *Proc. USENIX Security Symposium*, pages 1–16, 2006.

[3] R. de Paula, X. Ding, P. Dourish, K. Nies, B. Pillet, D. F. Redmiles, J. Ren, J. A. Rode, and R. S. Filho. In the eye of the beholder: a visualization-based approach to information system security. *IJHCS*, 63(1-2):5–24, 2005.

[4] P. Dewan and H. Shen. Flexible meta access-control for collaborative applications. In *Proc. CSCW*, pages 247–256, 1998.

[5] P. Dourish, R. E. Grinter, J. D. de la Flor, and M. Joseph. Security in the wild: user strategies for managing security as an everyday, practical problem. *Personal and Ubiquitous Comput.*, 8(6):391–401, 2004.

[6] J. Grudin. Desituating action: Digital representation of context. *HCI*, 16(2-4):269–286, 2001.

[7] M. Gumbrecht. Blogs as "protected space". In *WWW workshop on the weblogging ecosystem*, 2004.

[8] S. C. Herring, L. A. Scheidt, S. Bonus, and E. Wright. Bridging the gap: a genre analysis of weblogs. In *Proc. HICSS*, pages 101–111, 2004.

[9] B. Nardi, D. J. Schiano, M. Gumbrecht, and L. Swartz. Why we blog. *CACM*, 47(12):41–46, 2004.

[10] L. Palen and P. Dourish. Unpacking "privacy" for a networked world. In *Proc. CHI*, pages 129–136, 2003.

[11] F. B. Viégas. Bloggers' expectations of privacy and accountability: An initial survey. *JCMC*, 10(3), 2005.

[12] A. Whitten and J. D. Tygar. Why Johnny can't encrypt: a usability evaluation of PGP 5.0. In *Proc. USENIX Security Symposium*, pages 169–184, 1999.