Document and Author Promotion Strategies in the Secure Wiki Model

Kasper Lindberg and Christian Damsgaard Jensen

Department of Informatics and Mathematical Modelling
Technical University of Denmark
Christian.Jensen@imm.dtu.dk

Abstract. Wiki systems form a subclass of the more general Open Collaborative Authoring Systems, where content is created by a user community. The ability of anyone to edit the content is, at the same time, their strength and their weakness. Anyone can write documents that improve the value of the wiki-system, but this also means that anyone can introduce errors into documents, either by accident or on purpose.

A security model for wiki-style authoring systems, called the *Secure Wiki Model*, has previously been proposed to address this problem. This model is designed to prevent corruption of good quality documents, by limiting updates, to such documents, to users who have demonstrated their ability to produce documents of similar or better quality. While this security model prevents all user from editing all documents, it does respect the wiki philosophy by allowing any author who has produced documents of a certain quality to edit all other documents of similar or poorer quality. Moreover, authors who consistently produce top quality documents will eventually be allowed to edit all documents in the wiki.

Collaborative filtering is used to evaluate the quality of documents that an author has contributed to the system, thus determining what other documents that the author can edit. This collaborative filtering mechanism, determines the promotion and demotion of documents and authors in the Secure Wiki Model. The original Secure Wiki Model only considers explicit promotion and demotion of documents, authors are implicitly promoted/demoted depending on the promotion/demotion of the documents that they contribute. In this paper, we revisit the question of promotion of documents and authors and propose a new security policy with explicit promotion of authors. This policy also incorporates a new collaborative filtering mechanism with a higher degree of parametrisation, so that the new policy can be adapted to the specific needs of a particular wiki.

1 Introduction

A *wiki* is a system that relies on user contribution to generate the content it provides. Wikis can be used by any group of people such as friends doing small projects, colleagues needing knowledge sharing in companies, companies engaging with their user base through crowd-sourcing and worldwide knowledge sharing between strangers. The open nature of wiki systems makes them ideal as a knowledge sharing platform to which everyone can contribute a small piece of the bigger picture. However, the strength of such an Open Collaborative Authoring System (OCAS) is also its weakness since it

T. Dimitrakos et al. (Eds.): IFIPTM 2012, IFIP AICT 374, pp. 247–252, 2012.

is equally easy to delete good content or for malicious or incompetent people to add erroneous information to the OCAS.

This problem has been addressed by the *Secure Wiki Model*, which has been proposed to ensure the correctness and accuracy of documents in wiki-style systems [3]. The secure wiki model introduces a classification of both documents and authors into a set of *integrity levels*, which indicate the quality of the documents or the quality of the authors based on their previous contributions to the wiki (the Secure Wiki Model is introduced more formally in Section 2). The model combines ideas from two classic multi-level access control mechanisms: a *static integrity model* that governs authors' ability to update documents based on the well known Biba integrity model [1], and a *dynamic integrity model* that governs the promotion and demotion of documents and authors among the different integrity levels inspired by a watermark based access control mechanism [5].

In the original model, the dynamic integrity model only considers explicit promotion of documents – authors are implicitly promoted, according to the watermark model, along with the promotion of documents that they have authored. Promotion is explicit and is normally initiated by one of the authors in the wiki. The promotion is based on a vote between a set of randomly selected authors with integrity levels higher than the integrity level of the considered document; this protects the voting mechanism against the Sybil attack [2]. One problem with this approach is that voters are being explicitly asked to evaluate the quality of a document, but this evaluation is implicitly used to determine the integrity level of the author who is the main contributor to the document, i.e. voters are asked a single question, but their answer is used for two separate purposes. In order to make promotion more transparent, we need to make promotion of both documents and authors explicit.

In this paper, we revisit the question of promotion of documents and authors and propose a new policy for the dynamic integrity model that explicitly promotes authors. This new policy then leaves it to the discretion of the authors to explicitly promote documents that they have improved to an appropriate integrity level, up to and including their own integrity level.

The rest of this paper is organised in the following way: Section 2 gives a brief description of the original Secure Wiki Model which forms the basis for the new policy proposed in this paper. In Section 3, we revisit the question of document and author promotion and analyse the requirements for a successful policy in relation to wiki-systems. Based on this analysis, we propose our new policy in Section 4 and discuss this policy in Section 5.

2 The Secure Wiki Model

The Secure Wiki Model[3] combines existing assessment techniques, based on collaborative filtering, with computer security integrity control mechanisms. The integrity control mechanism is based on the Biba integrity model, which defines a Simple Security Property (*No Read Down*) and * (star) property (*No Write Up*).

The proposed system recognises that the simple security property cannot be enforced due to the fact that the security mechanism does not have complete mediation over authors' access to information. The primary contribution of the Biba integrity model to

this system is therefore the star property. The system requires every author to have an identifier that allows the system to recognise authors and assign quality confidence values (QCV) to them. The QCV indicates the general level of correctness, completeness and lack of bias in documents by that author. Similarly, the system assigns integrity levels (IL) to each document. The IL of a document is an indication of the correctness, completeness and lack of bias for that particular document as perceived by the community.

2.1 Access Control

The static integrity model is the component of the Secure Wiki Model that controls the access to the edit-feature of documents and thereby ensures that authors do not corrupt high-quality documents. The static integrity model is based on the sets $\mathbb{A}$,$\mathbb{D}$ and $\mathbb{I}$, where $\mathbb{A}$ is the set of identifiers of authors who have registered to use the system, $\mathbb{D}$ is the set of documents that are managed by the system and $\mathbb{I}$ is a totally ordered set of integrity levels. Using these sets, two functions are defined, that allow the system to compare the QCV of authors to the IL of documents, using the total order of $\mathbb{I}$. These functions are $qcv(a : \mathbb{A})$ which returns the quality confidence value of the author $a \in \mathbb{A}$ and $il(d : \mathbb{D})$ which returns the integrity level of the document $d \in \mathbb{D}$. These functions are used to define the predicate:

$$can\_edit(a : \mathbb{A}, d : \mathbb{D}) = '1' \text{ iff } il(d) \leq qcv(a)$$

which returns '1' if the author a is allowed to edit the document d ('0' otherwise) and thus prevents authors with a low(er) QCV from editing documents with a high(er) IL.

2.2 Dynamic Integrity Model

The dynamic integrity model is responsible for dynamically changing the IL of documents such that authors with a low QCV cannot corrupt a document that have been improved by an author with a higher QCV. The dynamic integrity model uses a variant of the watermark model [5], which says that when a subject reads an object with a label with a lower classification, the label of the object increases to the level of the subject, i.e., when an author with a QCV higher than the IL of a document edits the document, the resulting document will have its IL set to that of the authors QCV. The system does this on the assumption that authors that, in the past, have written accurate, complete and unbiased documents are likely to do so in the future.

Review Process. The description above shows how the integrity level of documents are raised. To raise the QCV of authors, the system uses a document review model that allows a contributor to submit a document for a review that will determine if the IL of the document should be raised. If the IL of the document is raised, so is the QCV of the *principal author*. To prevent denial of service through spurious document review requests, the proposed system limits the number of people that can request a promotion-review to the authors that contributed to the document, while allowing all authors, for which the can_edit predicate is '1', to request a demotion-review.

In order to analyse the security of the original model, it is assumed that each level L_i in the hierarchy contains $|\Lambda_i|$ registered users, of which z_i are assumed to be malicious and in collusion with each other. When reviewing a document, a number of users (r_i) of the $|\Lambda_i|$ registered users, from each of the levels that are participating in the review, are randomly selected to perform the review. The set of reviewers at level L_i defines a subset $\Lambda_{R_i} \subseteq \Lambda_i$. When reviewing a document d, each reviewer j makes his decision $\delta_j(d)$ on whether to promote a document or not. A yes-vote is represented as the value '1' and a no-vote is represented as the value '0'.

In the original policy, referred to as Π_1, the authors at each integrity level independently reach a decision. A simple majority of these decisions then decides the overall outcome of the vote.

3 Policy Analysis

In the following, we examine two problems that arise in the policy Π_1, namely the lack of transparency surrounding the promotion of authors and the problem of quorum.

3.1 Author and Document Promotion

The dynamic integrity model governs the promotion and demotion of both documents and authors. It is assumed that high level authors will work to improve the quality of the documents in the wiki, so the original model automatically promoted documents when they had been edited by a high level author. Work with the first prototype implementation of the secure wiki model [4], made us realise that authors will often make minor contributions, e.g. correct a spelling error, which in itself does not justify promotion, so it was left to the discretion of authors to promote documents that they edited. After editing a document, the author is allowed to increase the integrity level of the document up to and including her own integrity level; the default is to leave the document at its current integrity level. The resulting mechanism now has two explicit ways to promote documents, but only an implicit mechanism to promote authors. We therefore propose a new policy for the dynamic integrity model, which uses the voting mechanism to promote authors instead of documents – promotion of documents will be done explicitly by higher level authors who contribute to the document using the mechanism from the first prototype.

3.2 Voter Participation

The original policy Π_1 suggests that promotion of a document at level $i \in [0, 1, 2]$, would require two out of the three levels L_i,L_{i+1},L_{i+2} to have a simple majority for the promotion, but it does not specify any conditions on voter-participation which raises some interesting issues, e.g. does one positive vote out of 100 authors, who were asked to vote but did not respond, represent a sufficient majority?

This suggests that there is the need for a critical mass of reviewers that must be met or the vote should be rejected due to the result being unreliable. One way to mitigate the risk of having too few participating reviewers will be to select only active contributors

to perform a review. This will have the added benefit that dormant malicious users would not participate in reviews. If a user is malicious, with the intent of compromising reviews, the user would have to be active and potentially expose himself as malicious.

Despite mitigating actions, some reviewers will fail to participate in a review. It is assumed that the number of reviewers, at each level, that fails to vote on a review is equal, such that it does not skew the vote inappropriately. This can however be checked and guarded against.

4 New Promotion Policy

The original policy proposed for the secure wiki model is called Π_1, so we decided to call the new policy proposed here Π_2.

To promote an author from level L_i to L_{i+1}, a set of randomly selected members of the levels L_i,L_{i+1},L_{i+2} perform a review to decide if the author should be promoted. Each vote is weighed according to the weight of the integrity level of the member who cast the vote and the weighted sum of the votes must reach a level-specific threshold. In order to increase the security of the higher integrity levels, this threshold increases as the levels gets higher.

For each reviewer j at level L_i, the review decision ($\delta_j(a)$) is multiplied by the weight of the level ($\mathcal{W}_i$). The resulting score, for each level L_i, will be termed $\mathcal{S}_i(a)$ and calculated as shown in (1).

$$\mathcal{S}_i(a) = \sum_{j \in \Lambda_{R_i}} \delta_j(a) \cdot \mathcal{W}_i \tag{1}$$

For the purpose of determining the percentage of approval, the term $\mathcal{S}_i^{\max}(a)$, defined in (2), will be used to denote the maximum score possible for a given level L_i.

$$\mathcal{S}_i^{\max}(a) = |\Lambda_{R_i}| \cdot \mathcal{W}_i \tag{2}$$

In Π_2, τ_i is used to denote the threshold of weighted yes-votes to reach for a promotion vote to be successful. To promote author a from level L_i to L_{i+1}, Π_2 uses the condition that the score of yes-votes is greater than the score of no-votes and that the score of yes-votes exceeds the threshold τ_i. This condition is denoted as $\mathcal{D}(a)$ and shown in (3).

$$\begin{aligned} \mathcal{D}(a) = \mathcal{S}_i(a) + \mathcal{S}_{i+1}(a) + \mathcal{S}_{i+2}(a) \geq \\ \left(\mathcal{S}_i^{\max}(a) + \mathcal{S}_{i+1}^{\max}(a) + \mathcal{S}_{i+2}^{\max}(a)\right) \cdot \tau_i \\ \text{for } i \in \{0, 1, \ldots, |\mathbb{I}| - 2\} \end{aligned} \tag{3}$$

A third condition for the success of a review, is that the participation percentage must be sufficiently high to ensure the reliability of the review. If the participation percentage is not met, the result of the review must be considered as failed due to the unreliability of the result.

One extra author level is needed to be able to control documents at the highest integrity level using the common case condition. This extra level is there to control voting only and does not gain any extra privileges. In order for an author a to be promoted

above the normal document integrity levels, the condition in (4) will be used with an especially high value of τ_i to preserve the integrity and security of the vote.

$$\mathcal{D}(a) = \mathcal{S}_i(a) + \mathcal{S}_{i+1}(a) \geq \left(\mathcal{S}_i^{\max}(a) + \mathcal{S}_{i+1}^{\max}(a)\right) \cdot \tau_i \quad \text{for } i = |\mathbb{I}| - 1 \tag{4}$$

If an author no longer deserves the QCV currently associated with her, a demotion of the author is necessary. In general, demotion of authors works in the same way as promotion, but τ_i is replaced with τ_i^{dem}.

If all users at a given level has been promoted, so the level becomes empty, the members needed at that level will be selected from the next level above. With a system administrator at the top-most level, who can be trusted not to act maliciously, this also allows the system to securely populate the levels with users from the lowest levels, during the bootstrapping phase of the system.

5 Discussion

Controlling access without restricting it is difficult. The secure wiki model suggests how controlling the authors in Open Collaborative Authoring Systems, such as a wiki, can be done without restricting authors' ability to improve documents. The contribution of this paper is the presentation of an alternative security policy for explicit promotion of authors and documents in the secure wiki model.

The policy Π_2 has been designed for systems that are sufficiently populated. Small systems with only a few authors at each level will be able to use Π_2, but they may not get the full benefit of the policy since the small number of authors will all be asked to vote every time their level is involved in a promotion. However, the high degree of adaptability of Π_2 should provide even small systems with a useful policy.

In addition to the promotion policy, we have made references to a demotion policy, without specifying the demotion conditions explicitly. Specifying and analysing the formal policy for demotion is left for future work as well as an actual implementation of the proposed policy in a system using the secure wiki model.

References

1. Biba, K.J.: Integrity considerations for secure computer systems. Technical Report MTR-3153, The MITRE Corporation, Bedford, Massachusetts, U.S.A. (1977)
2. Douceur, J.R.: The Sybil Attack. In: Druschel, P., Kaashoek, M.F., Rowstron, A. (eds.) IPTPS 2002. LNCS, vol. 2429, pp. 251–260. Springer, Heidelberg (2002), http://portal.acm.org/citation.cfm?id=646334.687813
3. Jensen, C.D.: Security in Wiki-Style Authoring Systems. In: Ferrari, E., Li, N., Bertino, E., Karabulut, Y. (eds.) IFIPTM 2009. IFIP AICT, vol. 300, pp. 81–98. Springer, Heidelberg (2009)
4. Sander, P.: Sikkerhed i wiki-lignende systemer. Master's thesis, Technical University of Denmark, Department of Informatics & Mapthematical Modelling (2009) (in Danish)
5. Weissman, C.: Security controls in the adept-50 time-sharing system. In: Proceedings of the Fall Joint Computer Conference, Las Vegas, Nevada, U.S.A., November 18-20, pp. 119–133 (1969)