

Collaborative Trust Evaluation for Wiki Security

Collaborative authoring systems which support an open and dynamic population of authors, such as the Wiki [1], have become increasingly popular over the past couple of years. Large pieces of documentation, such as the Wikipedia [2], have been compiled using this type of technology and the Wiki technology has become an indispensable part of many computer supported collaborative work (CSCW) tools that support a distributed user base. The Wikipedia project has demonstrated the benefits of this approach by compiling a comprehensive and largely accurate encyclopaedia from the contributions of individual people located around the world. However, the Wikipedia has also exposed one of the weaknesses of collaborative authoring, which is that malicious or incompetent users may compromise the integrity of the document by introducing erroneous entries or corrupting existing entries, e.g., a public figure has found that the entry describing them in the Wikipedia had been modified to defame him [3].

The quality of a collaboratively authored document is determined by a few simple properties, such as whether the document is complete, correct and unbiased. Some of these properties correspond to the properties ensured by existing integrity mechanisms in computer security, so we intend to leverage this work when designing an integrity mechanism for open collaborative authoring systems. Classic integrity mechanisms [4, 5] associate an integrity level with every author (subject) and document (object), so that authors are assigned the integrity level of the documents that they work on and authors with low integrity are prevented from updating documents with higher integrity levels. Data protected by an integrity mechanism, however, normally have well defined syntax and semantics, whereas the syntax and semantics of collaboratively authored documents are difficult to define. This means that existing integrity mechanisms cannot be used directly. The obvious answer to this problem is to rely on feedback from the users, i.e., some reputation system similar to the ones used by Amazon [6], which corresponds to the approach that is already used in a Wiki. Reputation systems have previously been proposed as an effective means to assess the quality of information from uncertain sources [7, 8], but they only help automate detection of undesirable content and are generally unable to prevent undesirable content from being introduced into the document.

A Reputation-based Integrity Mechanism

An integrity mechanism for wiki style authoring systems has been proposed [9], which combines existing assessment techniques with integrity control mechanisms from computer security, in order to provide quality information to the reader and prevent untrustworthy users from corrupting high quality documents.

Documents are internally labeled with an integrity label, which provides the reader with an idea about the provenance of the document and whether the content should be trusted. The system also associates integrity labels with authors, which allows the system to prevent authors who have primarily authored low quality documents from modifying documents with a high integrity (quality) label. The integrity mechanism is designed to ensure that the editing process does not lower the integrity of documents.

The proposed integrity mechanism for open collaborative authoring systems has the following integrity properties:

1. untrusted authors can only modify the documents of other untrusted authors
2. normal authoring procedures will never decrease the integrity label of documents
3. collaborative filtering techniques are used to promote documents that are complete, correct and unbiased to a higher integrity level
4. authors who consistently produce documents of high quality will become trusted by the system and allowed to edit other documents with a high integrity label

Project Assignment

The paper that presents the Wiki security mechanism, only describes one possible mechanism for the promotion of authors. Authors submit their work to a “randomly” selected evaluation board¹ who collectively decide whether the author can be promoted or not. The paper describes one simple policy for deciding on promotions, but many other, and more advanced, policies are possible and may result in more intuitive security systems. The purpose of this project is to propose and evaluate such policies. The report that documents this project must include:

1. a brief introduction to the problem;
2. a description of the Wiki security mechanism and the role of promotion policies;
3. identification of security requirements;
4. a proposal for a promotion policy that address the identified security requirements;
5. a security evaluation of the proposed promotion policy similar to the analysis presented in the paper.

References

1. What is Wiki. <http://www.wiki.org/wiki.cgi?WhatIsWiki>, visited 28 December 2006
2. Wikipedia, the free encyclopedia. <http://en.wikipedia.org/wiki/Wiki>, visited 28 December 2006
3. John Seigenthaler (2005) A false Wikipedia 'biography'. Editorial in USA TODAY, 29 November 2005
4. K. J. Biba (1977) Integrity Considerations for Secure Computer Systems. Technical Report MTR-3153, The MITRE Corporation, Bedford, Massachusetts, U.S.A.
5. Timothy Fraser (2000) LOMAC: LowWater-Mark Integrity Protection for COTS Environments. In Proceedings of the IEEE Symposium on Security and Privacy, Oakland, California, U.S.A.
6. Amazon website. <http://www.amazon.com>, visited 28 December 2006
7. Pierpaolo Dondio, Stephen Barrett, Stefan Weber and Jean-Marc Seigneur (2006) Extracting Trust from Domain Analysis: a Case Study on Wikipedia Project. In Proceedings of the 3rd International Conference on Autonomic and Trusted Computing, IEEE, 2006
8. Ilya Zaihrayeu, Paulo Pinheiro da Silva and Deborah L. McGuinness (2005) IWTrust: Improving User Trust in Answers from the Web. In Proceedings of 3rd International Conference on Trust Management, Rocquencourt, France, 2005
9. C. Jensen (2009) Security in Wiki-Style Authoring Systems. In Proceedings of the Third IFIP International Conference on Trust Management (IFIPTM'09), pp. 81-98. West Lafayette, Indiana, U.S.A., June, 2009.

¹ The selection procedure may be subject to specific criteria.