Wiki Credibility Enhancement*

Felix Halim, Wu Yongzheng, Roland Yap
School of Computing
National University of Singapore
13 Computing Drive
Singapore
{halim,wuyongzh,ryap}@comp.nus.edu.sg

ABSTRACT

Wikipedia has been very successful as an open encyclopedia which is editable by anybody. However, the anonymous nature of Wikipedia means that readers may have less trust since there is no way of verifying the credibility of the authors or contributors. We propose to automatically transfer external information about the authors from outside Wikipedia to Wikipedia pages. This additional information is meant to enhance the credibility of the content. For example, it could be the education level, professional expertise or affiliation of the author. We do this while maintaining anonymity. In this paper, we present the design and architecture of such system together with a prototype.

Categories and Subject Descriptors

H.3.5 [**Information Storage and Retrieval**]: Web-based services

General Terms

Security, Standardization, Verification

Keywords

Credibility, login, Wikipedia, OpenID, anonymity

1. INTRODUCTION

Wikipedia is perhaps one of the most successful efforts to create collaborative content. It is an encyclopedia covering a wide range of knowledge to exploit the "wisdom of the crowds" and to which anybody can contribute. Arguably, the success of Wikipedia is due to its open and self-policing nature. Anonymity is also a key feature – anybody can create an online persona with an account, or alternatively, the IP address is used.

One of the criticisms of Wikipedia is that the material is written by "anonymous strangers of unknown qualifications" [1]. Consider an entry on a technical subject, say a medical article, one might prefer an article written by a qualified physician. In this paper, we propose to enhance the credibility of the information contained in Wikipedia.

Consider the following scenario. The ACM maintains a comprehensive library of computer science publications with author information. If a contributor to a computer science Wikipedia article has credentials such as published in x ACM conferences and journals or affiliation being MIT, this information can increase the credibility of an author. We call such information, *credibility information*. In Wikipedia, authors are identified by login id or IP address, but as anybody can make one or more login ids, the login information of an author does not by itself lend credibility. Rather, we want to be able to make use of other information from credible and trusted sources outside Wikipedia to transfer credibility information into Wikipedia. In the ACM example, anonymity could be retained while asserting a statement like published papers in CACM.

Unlike Wikipedia, Google Knol [2] attempts to provide credibility information. In Knol, the credibility of the articles is based on the name of the author which can be certified by credential providers such as credit card companies or manually by phone. The verification mechanism is proprietary to Knol. Furthermore, it means that the author cannot be anonymous. Essentially, name verification tells one that a certain individual with a particular name as certified by Google contributed the article. However, the name by itself may not be very credible with the exception of well known authors. However, ambiguity still exists since several individuals could have the same name. For example, a Wikipedia author with pseudonym Essjay [3] claimed to be a (bogus) tenured professor who taught theology. Such an incident could also take place in Knol since a valid real name does not provide information about expertise or profession (i.e. professor of theology).

In this paper, we propose a simple extension to Wikipedia (and MediaWiki) which enhances the information in Wikipedia to make it more credible by automatically using credibility information from trusted third parties. Our extension maintains the open and anonymous nature of Wikipedia. We transfer information from trusted third parties and associate that securely with the text written by the author. We have implemented a prototype which utilizes the MediaWiki tag extension together with OpenID [4] as either an authentication or credibility provider although other credibility providers could also be used. Some scenarios where we can enhance Wiki:

*This work was supported by SELFMAN (contract: 034084)

WikiSym '09, October 25-27, 2009, Orlando, Florida, U.S.A.

- Verifying the author's name: A credit card provider such as Visa can certify that the author is a human and optionally his/her actual name. This gives a Knol-like flavor to Wikipedia. It can also help to make it more difficult for robots to edit Wikipedia.
- Verifying the anonymous membership with an organization: A provider like ACM can provide university or expertise credentials for an author without his/her personal identity.
- Restricting anonymous voting system: A credibility provider can be used to restrict the voting system in Wikipedia [5] to from certain voters without disclosing the name of the voters.
- Other services: can enhance wiki articles by giving information about the author while preserving the anonymity of the author.

2. DESIGN GOALS

Before discussing the design of the credibility enhancement for Wikipedia, we first give our design objectives:

- **Credibility:** The purpose of the credibility enhancement is to enable Wikipedia to show some external trusted information about the authors. Such information could be the authors' real name, professional affiliations, proof of identity, etc., essentially anything which can give additional credibility to the text in an article. This information has to be verified so that authors cannot easily provide false information. We also want to avoid an author stealing other author's identity to publish/edit pages.
- **Anonymity:** We want to preserve the capability of authors to be anonymous if they want to, i.e. we do not want Knol [2] which requires that the real names of users be verified. Furthermore, we want to ensure that users' private data is not stored in Wikipedia, so that even if Wikipedia is compromised, users' private data will not be exposed.

  There is a trade-off between credibility and anonymity. Authors sometimes want to be anonymous, but that means their statements/edits may be less credible. Less credible edits are more likely to be deleted by Wikipedia administrators. We give the author the freedom of balancing the trade-off and provide different levels of credibility information.
- **Ease of Use:** The enhancement should not make Wikipedia much harder to use, e.g. forcing authors to download and run some software on their local machine is inconvenient and should be avoided.

We remark that the credibility information in our proposal is independent of reputation. We preserve reputation [6] on any edits, and, reputation can be linked to the author's credibility as well.

3. PROTOCOL DESIGN

The credibility extension involves four components including the author which work together as shown in Fig. 1 *C1-4*. *C1* is the Wikipedia web server with our credibility extension installed. *C2* is the credibility proxy. We suggest it

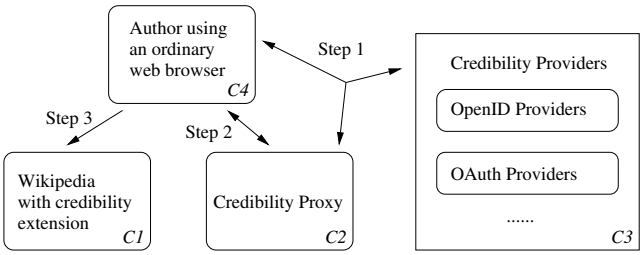

Figure 1: Components and work flow of the credibility extension.

be run in a different host to prevent author's credential being compromised in case *C1* is compromised. The Wikipedia web server stores a certificate of the proxy so that Wikipedia can verify signatures generated by the proxy. Note that it is possible to have more than one proxy, but we use one for the illustration purpose.

C3 is one or more credibility providers. The credibility providers give credible information specified by the author to the credibility proxy. They communicate with the credibility proxy using the respective supported protocol. For example, the OpenID protocol needs three-way communication among the author, OpenID server, and credibility proxy. *C4* is the Wikipedia author using an ordinary web browser.

There are three main steps to get a credible edit in a Wikipedia page:

- **Step 1: acquiring author information**
  In the case of OpenID [4] or OAuth [7] protocol, this step involves three-way authentication. After this step, the credibility proxy should have the author's information. This step can be performed multiple times to get information from multiple providers.
- **Step 2: sign**
  The author selects the appropriate author information (see Fig. 2) to be passed to Wikipedia and enters the text to be published in Wikipedia. The credibility proxy signs the author's information together with the text and generates the signed text, see the screen shot in Fig. 2.
- **Step 3: edit page**
  The author pastes the signed text to Wikipedia (shown in Fig. 3). Note that the author does not have to login to Wikipedia in order to use the credibility extension. The signed text can be published elsewhere on the web and someone else can enter the signed text into Wikipedia. It can also be copied between pages.

When the edited page is viewed, the credibility extension verifies that the edit has been signed correctly using the credibility proxy's certificate. If the edit is verified, the author's information will be displayed — this can be done in various ways, e.g. as in Fig. 4. Our credibility extension is compatible with caching which is important for Wikipedia performance, the signed text does not have to be verified every time it is viewed.

The trust relationships among the four components are:

- Wikipedia trusts the credibility proxy to sign the correct information. Wikipedia also trusts that the proxy's key is not compromised.

- The authors trust the credibility proxy to only release information which they authorize. Note that the information can be filtered by the credibility providers before it is given to the proxy, so the ideal case is that the proxy *only* knows the information to be signed and released. However, some information such as the user ID in the OpenID server and user's IP address are always known to the proxy.

- The credibility proxy does *not* have to trust the credibility providers because the providers' name will be shown together with the signed text. We leave the Wikipedia readers to decide whether to trust the providers or not but Wikipedia could choose to trust predefined providers so as to be able to conveniently display them in the Wikipedia article.

- The authors implicitly trust the credibility providers which are chosen by them.

4. CREDIBLE WIKI PROTOTYPE

We describe a credible wiki prototype to illustrate our ideas. It consists of a credibility proxy and a MediaWiki extension. Our prototype employs the OpenID 2.0 framework [8] to communicate between the credibility proxy and third party credibility providers to share information about the particular user. However, other protocols could also be used. The proxy anonymizes the user information selected by the user and signs it along with the text. Wikipedia only needs a lightweight extension to check the signature of the text sent by the proxy. If the signature matches, it will be published along with the assigned credibility information. Otherwise no special credibility will be given to the text.

4.1 The Credibility Providers

Credibility providers are the source of the additional information for the authors to enhance the credibility of their edits. Recently, `http://www.myid.is` provides a service to certify a digital identity online which is similar to what Knol uses for author name verification. One can imagine a variety of credibility providers to provide a variety of information which could include public and private organizations. The information would be some property associated with the author such as professional association, real name verification, geographic location or country, etc.

The credibility provider must have a protocol to share information to the credibility proxy or any other consumer. We observed that OpenID [4, 8] and OAuth [7] are the two most promising open protocols to be used widely for managing the online identity and sharing information.

OpenID provides a decentralized open standard for user authentication and access control. The user only needs to setup one digital identity on an OpenID provider to gain access to other systems. We take advantage of an OpenID provider not for login but as a way of transferring information about a digital identity, so we use an OpenID provider as a credibility provider.

Our examples with our prototype use a free OpenID provider (`myopenid.com`) as the credibility provider. Since there is no particular trust associated with `myopenid.com`, the information in the examples is only illustrative.

4.2 The Credibility Proxy

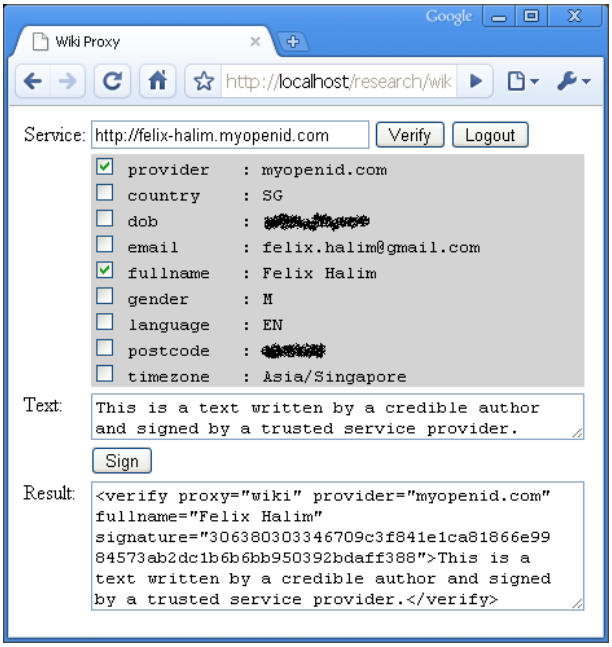

Figure 2: A Proxy for Wikipedia.

Fig. 2 shows our prototype. The service field is filled with the URL of the credibility provider. The gray area is the user information retrieved from the OpenID credibility provider. The *text* area is the text that will be signed by the proxy together with selected user information. The example chooses to include the provider and the full name to be signed with the text. The *result* area is the ready to use wiki text that can be inserted anywhere in a wiki page.

We allow the author to select which information from credibility providers to be attached. This information should be thought of as credibility attributes to be attached to the edit. Wikipedia could have a policy to require certain attributes from trusted credibility providers in order to achieve a certain category of credibility. For example, to get a credibility of a "scientist", the author has to include information such as: institution, position, and perhaps information about publications (as in the ACM example in Sec. 1).

4.3 Wikipedia Extensions

MediaWiki is the software behind Wikipedia. MediaWiki can be extended using extensions such as tag extensions, parser functions, special pages, or template extensions. We implement our credible wiki using a tag extension which we call the *verifier extension*.

4.3.1 Wiki Verifier Extension

The text signed by the credibility proxy can be put inside any page in Wikipedia (as well as outside Wikipedia since verifying the signature can be easily done with the certificate of the credibility provider). We created a verifier extension tag to check that the text and additional attributes inside the tag have been signed by the proxy.

There are three mandatory items and several optional attributes within the verifier tag extension:

- **proxy**: the name or the public key of the proxy. Wikipedia will be able to verify the signed text by having

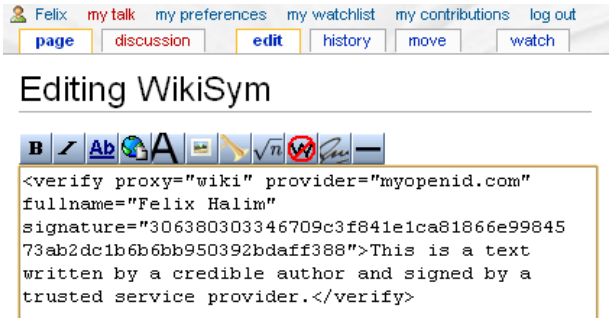

Figure 3: Verifier tag extension for Wiki.

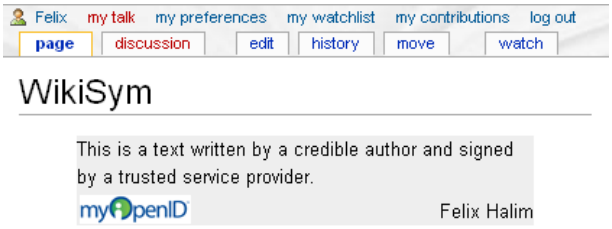

Figure 4: The end result in Wikipedia page.

a list of trusted proxies and their certificates.

- **signature**: the signature of the text inside the tag. The signature should match with the digested text decrypted using the public key of the proxy.
- **text**: the text to add or edit.
- **optional attributes**: such as provider, full name, country, email, etc. can be included as the attribute of the verifier tag. Wikipedia then can use the additional information to display the text.

Fig. 3 shows an example of a verifier extension tag. The content of the signature attribute contains the signed digest of the information in the verify tag. If any of the text or attribute values are changed, the verify tag will treat the text content as regular text rather than as credible text.

Credible text in a Wikipedia page should be presented in a way which can show its credibility information. While there are many ways of doing the presentation, Fig. 4 shows displaying credible text by graying the background. The displayed paragraph with grayed background provides the "context" for the author when editing a paragraph in Wiki. The idea of a context is to make it harder to abuse the credible text (i.e. placing the text in different paragraph or articles that have different context to get different meanings from the same text).

The display of the text can be improved further with more credibility information (other than 8 fields in Fig. 2). For example, a badge-like display can be used to annotate the text with particular properties to be associated with user information matching a Wikipedia credibility category, e.g. "computer scientist".

The presentation of credible text, shown in Fig. 4, changes the flow of text, thus it may not be scalable when there are many small edits, where each sentence in a paragraph is edited by a different author over time. More sophisticated GUIs can be added to present credible text without changing the flow, for example using JavaScript to highlight any credible text upon mouse-over. The credibility provider logo and other credibility information can be listed after the main text which is similar to how citations are handled in Wikipedia.

4.3.2 *Wiki Poll Extension*

The MediaWiki poll extension [5] can also benefit from the credibility extension. Currently, the poll extension stores the IP address and Wikipedia user name pair as the poll account to vote for the poll. If the user does not have a Wikipedia account then only the IP address will be used to vote. The poll doesn't allow duplicate votes for each poll account.

Credibility allows recording additional information about the pool participants. Alternatively, we may want to restrict the participants of the poll by only accepting, for example, users from a particular country. This can be done by requiring a "country" field from a trusted credibility provider (other information could be hidden).

5. DISCUSSION

Wikipedia accumulates information through the efforts of anonymous contributors and volunteers. While this is democratic, it has a weakness that the information may be perceived as being less credible (regardless of whether or not it is actually so). Normally, Wikipedia uses external citations to add credibility to the information entered. However the citation may either not be available or not easily accessible (confidential). The text might also simply be just words of wisdom from an expert author but it is hard to convince the readers that the text they are reading has a certain quality as it may lack sufficient citation.

Well known authors usually have credibility information outside Wikipedia. Our enhancement allows them to transfer the rich information about the author available from the third party credential provider to Wikipedia. Our enhancement can be seen as a complement to the citation mechanism. It is important to note that, in the process of transferring the author information, we can maintain the anonymity of the authors which is consistent with the philosophy of Wikipedia and serves to protect the authors.

Our credibility mechanism can be used to enhance any reputation mechanism. It may be also used by administrators to manage edits.

6. REFERENCES

[1] P. Denning, J, Horning, D. Parnas and L. Weinstein, "Wikipedia Risks", Comm. of the ACM, 48(12), 2005.
[2] "Knol", `http://knol.google.com/k`.
[3] "Essjay Controversy", `http://en.wikipedia.org/wiki/Essjay_controversy`.
[4] `http://openid.net/`.
[5] `http://www.mediawiki.org/wiki/Extension:Poll`.
[6] B.T. Adler, K. Chatterjee, L. de Alfaro, M. Faella, I. Pye and V. Raman, "Assigning Trust to Wikipedia Content", WikiSym, 2008.
[7] `http://oauth.net/`.
[8] D. Recordon and D. Reed, "OpenID 2.0: A Platform for User-Centric Identity Management", Digital Identity Management, 2006.