Risk Analysis of Privacy Protection in Social Networking Sites

Heidi E. I. Dahl	Mass Soldal Lund	Ketil Stølen
SINTEF ICT	SINTEF ICT	SINTEF ICT
Heidi.Dahl@sintef.no	Mass.S.Lund@sintef.no	Ketil.Stolen@sintef.no
Norway	Norway	Norway

Extended Abstract

The interest in social networking sites such as Facebook and MySpace have exploded in recent years, and it is a common conception that such networking sites will be central to public participation in the future. Though the main use at the moment is social interaction between individuals, it is clear that communication through social networking could be beneficial in other context. The presence of government agencies and politicians on Facebook is an example of this.

Another emerging use of elements from online social networks is collecting information for research. When doing large scale surveys, enabling social networking features such as user generated content and discussion among the participants allows researchers to collect other kinds of inputs than those accessible through more traditional information collection techniques. These kinds of interaction data are traditionally only available through face to face interaction between researchers and groups of participants.

However, allowing for interaction between participants in a survey entails new challenges in terms of how researchers handle sensitive information, and how the participants are asked to provide details. How to obtain privacy protection in social networking sites is still an open question, but it is evident that security risk analysis must be a key component when the privacy of participants is considered [1][2][3].

We present risks in relation to privacy issues, based on an analysis of the Design Feedback Tool (DFT), an application (in development) for conducting large scale surveys. The DFT combines features from traditional questionnaires with elements from social networking sites. The analysis was performed according to the CORAS method for security risk analysis [4][5][6]. We show how the CORAS method was applied for analysing privacy in the DFT; how this analysis influenced the solution, and how privacy issues of the system are addressed.

Security Risk Analysis of the Design Feedback Tool

The scope of the analysis was the handling of privacy issues in the DFT focusing on privacy and data protection issues connected to the use of DFT, both by researchers and survey participants.

The direct assets focusing the analysis were therefore sensitive personal information and identifying information [7], as two types if information regulated by Norwegian law in terms of privacy. In the following we will use the term sensitive information to mean information of either type. We chose to distinguish between two sources of information, the researcher's data set and user created content.

The risks associated with the researcher's data set are essentially the same as for any sensitive data stored in electronic form, no matter how it was collected. Improper storage and handling of the data before it has been anonymized may lead to sensitive information going astray. Examples of this kind of risk are

- Unencrypted memory stick with data is forgotten in taxi, and accessed by a later passenger.
- Researcher accidentally emails data set to wrong person.
- Researcher not involved in the project associated with the data set gains access because the data set is stored on a common server.

When the survey is conducted online, the researcher needs to keep track of where data is stored and make sure it is secure and not kept when it should be deleted. The DFT is run by the researchers on an external server, so the contract regulating maintenance and backup of the server should take into account possible privacy issues. An example risk related to this is

- Sensitive information from the survey is backed up on the server, and not deleted when the survey has ended.

Using an online community tool such as the DFT to conduct surveys introduces new risk elements compared to more traditional methods where only the researcher sees each participant's responses. There are of course parts of DFT surveys that will remain private (e.g. demographic questions such as gender and age), but even when the information asked for is not necessarily sensitive, participants may include sensitive information by accident. Unless each contribution is moderated, with the time lag this involves, the interaction between the participants may involve disclosure of sensitive data. An example of this kind of risk is

- A woman mentions how she uses an application in relation with her daughter's illness.

Another factor is the use of user generated rich media such as pictures and movies. A rich media file may by itself identify the participant and the surroundings and things that happen in the background may disclose either type of sensitive information about the participant and people close by. An example risk related to this is

- A participant contributes a movie taken at what is clearly a union meeting, showing the people participating in the background.

The above examples were the main risks uncovered in the security risk analysis.

Acknowledgements

The security risk analysis and this extended abstract were completed with funding from the SINTEF-internal project *Rik og Sikker*.

References

[1] Dwyer, C., Hiltz, S. R., & Passerini, K. (2007). Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace. Proceedings of AMCIS 2007. Retrieved 12 March, 2009, from http://csis.pace.edu/~dwyer/research/DwyerAMCIS2007.pdf

[2] Olsen, T., Mahler, T., Seddon, C., Cooper, V., Williams, S., Valdes, M., et al. (2005). Privacy in Relation to Networked Organisations and Identity Management: Legal-IST

[3] Woo, J. (2006). The right not to be identified: privacy and anonymity in the interactive media environment. New Media and Society, 8(6), 649-967.

[4] Folker den Braber, Ida Hogganvik, Mass Soldal Lund, Ketil Stølen, and Fredrik Vraalsen. Model-based security analysis in seven steps – a guided tour to the CORAS method. BT Technology Journal, 25(1):101-117, 2007.

[5] Heidi E. I. Dahl, Ida Hogganvik, and Ketil Stølen. Structured semantics for the CORAS security risk modelling language. Technical Report A970, SINTEF ICT, 2007.

[6] The CORAS tool. Retrieved 12 March, 2009, from http://coras.sourceforge.net/

[7] Personvernombudet for forskning, Ord og Begreper. Retrieved 12 March, 2009, from http://www.nsd.uib.no/personvern/forsk_stud/begreper.html