Position statement on workshop "Understanding Friend and Family based Security and Privacy issues"
NordCHI 2010, October 17, 2010, Reykjavik, Iceland.

Time and Usability Economics as Upper Boundary in Friend and Family Security and Privacy

Lothar Fritsch
Norwegian Computing Center
Gaustadaléen 23, PO Box 114 Blindern, 0314 Oslo
Lothar.Fritsch@NR.NO

Kristin Skeide Fuglerud
Norwegian Computing Center
Gaustadaléen 23, PO Box 114 Blindern, 0314 Oslo
Lothar.Fritsch@NR.NO

ABSTRACT
In this position paper we describe our position on the change in information privacy as introduced by social networking platforms. We illustrate our argument based on observations in the MARIAGE project and on results from various usability-oriented research activities. We conclude that "Friend and Family based Security and Privacy management" introduce a large magnitude of complexity into information privacy and information security, thereby transforming privacy handling into a constant negotiation process subject to changes in social relationships. Unlike traditional privacy conceptualization with strong regulation targeting single players, the pursuit of security and privacy in "Friend and Family" applications bears a large risk of outperforming the individual's ability to handle complexity both in time and usability dimensions, while the privacy regime is likely subject to personal relationships rather than common rules. This will certainly constitute an upper limit concerning the complexity of possible technical solutions for "Friend and Family" security.

Author Keywords
Information privacy, social networks, usability, accessibility, complexity.

ACM Classification Keywords
H5.m. Information interfaces and presentation (e.g., HCI): Miscellaneous.

INTRODUCTION
The use of on-line photo albums and social networking platforms created platforms for person-to-person sharing of data. Such data often is composed of media objects. These objects are often related to their creators or owners life, and the objects are intended for viewing by - possibly selected - other persons. In consequence, the classic requirements for information privacy and security have to adapt both to a person's social network, and the person's evaluation of risk created by unauthorized access to media objects. As the current paradigm suggests extensive tagging and meta-labeling of such shared objects for the purpose of automated finding, complex situations for security management may arise. However, the users can not be assumed to have either the time or the background knowledge for handling sophisticated access control situations.

NordiCHI 2010, October 16–20, 2010, Reykjavik, Iceland.
 ISBN: 978-1-60558-934-3...$5.00.

Example: Media handling in shared multimedia archives
To illustrate the complexity of managing social network based media objects, we refer to an article published within the MARIAGE project [1]. It identifies three major issues for information privacy in shared, multi-medial collections: Access control, ownership & object tracking, and metadata control (see Figure 1).

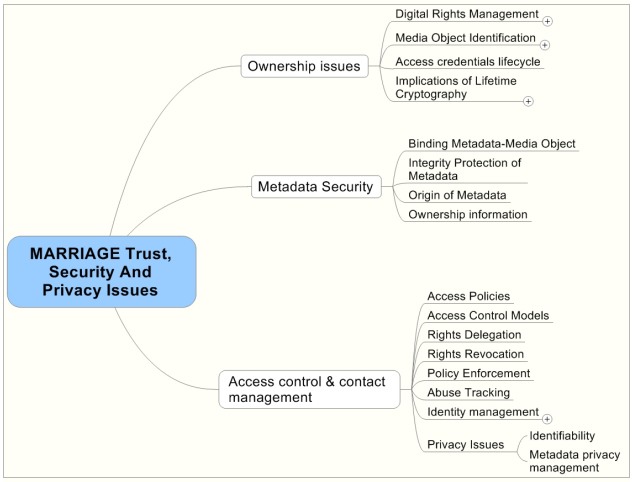

Figure 1: The MARIAGE issues for shared social media [1]

- Access control (AC) focuses on the management and enforcement of access policies to media objects it covers the creation and administration of rules about who is allowed to perform which actions on media objects. From computer science research [10], complex AC models with rights delegation ("Friends of Friends") and classification

are known. However, these models can easily create anomalies in their rules that are hard to remove even for specialists. And, for the time being, AC options in social media are nowhere closer to the state of the art in role-based or policy-based AC. As a further downside, AC often involves explicit identification and authentication of the acting person - which might not be desirable property on digital albums all the time (e.g. in the case an unfavorable but powerful contact should not get knowledge of the existence of a collection of objects).

- Ownership & object tracking issues occur when "receivers" of access privileges copy out objects. These objects can breach privacy and security in many ways, e.g. by being published elsewhere under different AC conditions, or by simply surviving a change in AC privileges of the holder of the copy. Tracking, in addition, might serve detection purposes, and a further use is the proof of ownership against 3rd party sites that publish objects in unauthorized ways.
- Metadata control concerns tagging of images. There are two major concerns. First, on social networks, other people are allowed to add name tags, location tags, face marks and other information to objects they have AC privileges for. These tags might contain information the object owner doesn't want to be visible to all persons with access to the object. The tagging person can easily breach the policy. Today's problem fix forces object owners to confirm all added tags, and to create the proper rules. This is quite an effort if it happens many times a day, involving resulting changes of AC policies. The second problem is the management of own metadata. Not all "Friends and Family" members do need to see the same meta information (e.g. exact time & location of photo taking). However, the establishment of a detailed AC policy involving all metadata categories for all objects and all "friends" is astoundingly complex.

ACCESS CONTROL MODELS VS. SOCIAL NETWORK PLATFORMS

As illustrated above, the introduction of contemporary access control regimes and methods from computer science does come at a price: Dramatically increased privacy management complexity, as well as the potential for rule conflicts and anomalies in rule sets. In addition, the dynamic nature of on-line social networks with their typical transactions (addition & removal of contacts and relationships, re-grouping of groups, change in platform policies) will make the establishment of a persistent access control policy very difficult, and very time-intensive. With each update, all other policies have to be checked for conflicts.

A new aspect in social network security is the implicit delegation of access privileges. The "friends of friends" delegation is a popular example on many platforms. It enables privilege delegation to a group of persons not known to the object owner. The group composition is controlled by a "friend". A simple anomaly example is this:

- User A (object owner) excludes User B from seeing object X.
- User A allows User C to access object X in "friends of friends" mode.
- User B approaches User C, and gets User B to become his "friend"

Result: User C gets to see object x. This is a simple problem, which causes a strong increase in policy complexity if used with discrimination of several groups of friends instead of one. The current solutions to handle complexity in AC research are usually based on the assumption of a single controller of a database or a security system setting the policies. This approach doesn't not seem adaptable to social networks.

PRIVACY ECONOMICS AND USABILITY AS UPPER BOUNDARY

Privacy economics refer to economic considerations and constraints concerning one's information privacy. People often use a pragmatic approach to evaluate privacy risks against benefits when they use IT systems [3, 9]. In sharing media objects with friends, the immediate benefit is the feeling of community with friends or family. The management of access control, risk assessment concerning privacy, and firefighting of access errors however impose cost - either in time used, loss of pleasure and usefulness, or real monetary cost. All explicit privacy handling, policy building and reconfiguring of access rules are cost on users. It must be assumed that users will not invest more resources into managing privacy issues than they experience their perceived benefit of using a social network.

"Friends & family" privacy management is more subject to interpersonal negotiation and re-negotiation than privacy regimes intended to control government or corporate data processing. Rather explicit legal frameworks from these environments can hardly be translated into interpersonal relationships. It must be assumed that those who own power in social relationships will be in a better position to dominate the privacy regimes practically used.

Increased complexity, uncertain policy consequences, and crude user interfaces for security and privacy policy handling are the main sources for usability issues. In addition, social networking faces serious consequences from an ageing population that might, over time, lose cognitive abilities to handle complexity they were handling earlier in their life.

CONCLUSION

Complexity issues, usability issues, and an ageing user population constitute an upper boundary concerning the sophistication of technical solutions for privacy in social media. Unlike in corporate settings, where specialists can develop, plan and update privacy critical systems on

corporate budgets [2], individuals will deploy very limited personal resources for managing their social network security and the dynamics of their relationships mirrored on them. In addition, social network security and privacy properties certainly will center around the "least common denominator" for all participants of a social network - such that the security features will almost completely depend on, e.g., a very young or a very old family member's capability to manage access control policies for his own "friends". We conclude our position statement with these observations and recommendations:

- Security and privacy measures in social networks will be effective as they are used by the "weakest link" of a social network [4].
- Privacy economics are decisive about how much time and other resources users are willing to invest when managing friends and family access control [8].
- Those socially in power (parents, dominant persons, superiors) are likely to dominate access control formulation through their power resulting from both status and the complete negotiability of social networks.
- Usable, secure and inclusive design of privacy features is recommended as a measure to both strengthen the "weakest link" and to reduce resources needed to manage social networks. Methods of Universal Design [5], participatory design, multilateral security analysis [6] and Privacy by Design [7] should be used on the construction of on-line social platforms.

However, some anomalies won't be resolved easily. The individuals participating in sharing online media still will need to assess their individual stakes before sharing personal media objects.

REFERENCES

1. Fritsch L, Holmqvist K, Fretland T (2008) Making Rich Media Accessible for Generations: Trust, Security and Privacy Issues with Personal Media on the Web 2.0, Proceedings of the IFIPTM Web 2.0 Trust workshop, Trondheim, Norway, International Federation of Information Processing (IFIP)
2. Fritsch L, Abie H. A Road Map to the Management of Privacy Risks in Information Systems. In: Gesellschaft f. Informatik (GI), editor. Konferenzband Sicherheit 2008, Lecture Notes in Informatics LNI 128. Bonn: Gesellschaft für Informatik, 2008: pp. 1-15.
3. Acquisti A, Grossklags J. Privacy and Rationality: Preliminary Evidence from Pilot Data. In: Proceedings of the 3rd annual workshop on economics and information security (WEIS) 2004. Minneapolis: 2004.
4. Fritsch L, Fuglerud KS, Solheim I. Towards inclusive Identity Management (under review). Identity in the Information Society (IDIS) 2010
5. Fuglerud, KS. Universal Design in ICT services, in: Vavik, T. (ed), Inclusive buildings, products & services. Challenges in universal design, Tapir academic press, pp. 244-267, ISBN: 978-82-519-2344-6, 2009
6. Fritsch L. Privacy-Respecting Location-Based Service Infrastructures: A Socio-Technical Approach to Requirements Engineering. Journal of Theoretical and Applied E-Commerce research 2007; 2(3): 1-17.
7. Cavoukian, A, Privacy by Design, brochure by the Information & Privacy Commissioner of Ontario, Canada, http://www.ipc.on.ca/images/Resources/privacybydesign.pdf , Version 18.6.2009.
8. Vila T, Greenstadt R, Molnar D. Why we can't be bothered to read privacy policies: models of privacy economics as a lemons market. In: ICEC '03: Proceedings of the 5th international conference on Electronic commerce. Pittsburgh, USA: ACM Press, 2003: pp. 403-407.
9. Samatas M. The Privacy Paradox. In: Second Internal iTrust Workshop On Trust Management In Dynamic Open Systems. Strathclyde, United Kingdom: 2002.
10. Essmayr W, Probst S, Weippl E. Role-Based Access Controls: Status, Dissemination, and Prospects for Generic Security Mechanisms. Electronic Commerce Research 2004; (4): 127 - 156.