Security and privacy engineering for corporate use of social community platforms

Lothar Fritsch
Department of Applied research in ICT
Norwegian Computing Center / Norsk Regnesentral
0314 Oslo, Norway
Lothar.Fritsch@NR.NO

Abstract: Social media (SM) platforms are being used for many purposes. As they were successful in accumulating a large number of well-networked user communities over the recent years, those platforms and their communities became interesting for corporate and commercial use, visible in a wave of books on businesses and SM. However, the "corporate user" normally is composed of many individual users that implement a subset of corporate functions, and has other security needs as those of private consumers. This article reviews corporate use cases for SM, and presents an overview of information security and information privacy requirements following from these uses. The article concludes with a comment on today's SM platforms capabilities to support these requirements.

1 Corporate use of social communities

Social communities are computer platforms that allow their users to represent themselves in profiles to establish social relationships to other users, and to supply and share media objects with subsets of their network [1, 2]. Such sharing produces many problems related to user's roles and user's access and object use permissions that should be aligned with the collaboration workflows intended by the users. Roles and permissions for individual users are defined in a single place, where the object access permissions and personal relationships (from here on called "policy") are defined. SM have grown to become popular private interaction platforms for multimedia [3]. However, policy management is different for corporate users. A corporate user is here defined as:

A corporate user of SM is an organization based on workflows using communication and collaboration in SM as part of their organizational strategy.

Complementing this definition, these assumptions on corporate users are made: Other, more seasoned communication channels, such as telephony, e-mail, paper messages, video conferencing, web portals and personal meetings are used as well to implement corporate strategy. Next, there are information objects and interactions that are restricted to the public, e.g. business secrets, patent applications, customer data records, price lists and contract conditions to particular customers. For many of the restricted objects above, the corporate user has developed rules and processes. These involve both the definition of access restrictions on objects, and the definition of workflows and processes for the handling of typical business actions.

erschienen im Tagungsband der INFORMATIK 2011
Lecture Notes in Informatics, Band P192
ISBN 978-3-88579-286-4

Business actions and the objects they handle are subject to legal regulation, e.g. archival requirements. The publication of objects on social network platforms may have legal consequences for the corporate user, e.g. concerning publication duties for stock-exchange listed companies, inside trading issues, or data protection issues. Participation in SM is targeted, and involves, external persons. It is assumed that internal interactions are carried out on own interaction systems (e.g. platforms for Computer-supported collaborative work, CSCW).

It must be presumed that a corporate user's involvement in SM platforms will be aligned and organized in the same way and with similar restrictions as the other business processes. There will be defined roles, privileges and workflows that will be adapted to the corporate user's actions on SM. The article will first examine typical strategic actions of corporate users on SM. Next, these actions will be analysed for their information security and privacy implications based on the background in [4]. Finally, a discussion over the availability of functionality on SM platforms will conclude the article.

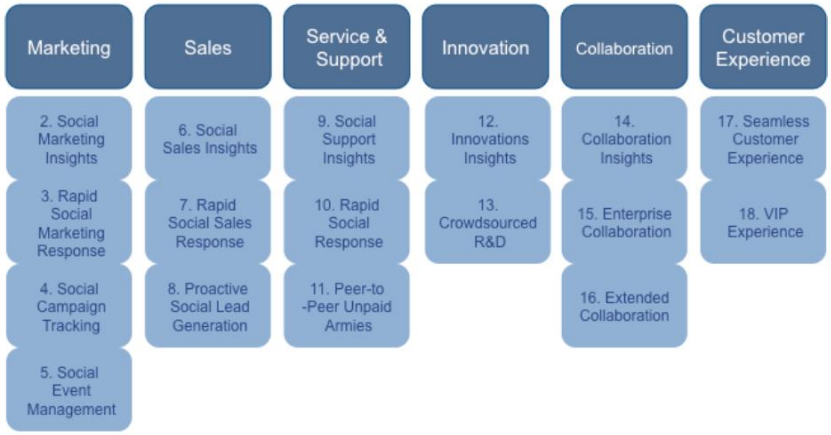

Figure 1: Basic corporate user actions on social media [5].

2 Analysis of corporate actions and roles in social networks

A corporate user's actions on public social networks can, according to [5], get divided into six different groups of actions: Marketing, Sales, Service & Support, Innovation, Collaboration, and Customer Experience. In each of these six areas, several business actions can be carried out. These are shown in Figure 1, and will be explained below.

2.1 Corporate users' actions in social media

A corporate user carries out these actions targeting external parties on SM platforms:

Marketing: Actions that generate market intelligence, actions that quickly reach the marked participants, campaign intelligence, and event handling.

Sales: Actions that support the sales function by generating sales insights, quick responses, and by generating new sales leads.

Service & Support: Support insights, Rapid response, Crowdsourcing.

Innovation: Actions that generate new innovation insights, or harvest research and development innovations through crowdsourcing.

Collaboration: Collaborative actions internally or with external partners.

Customer experience: Actions which service customers, e.g. the extension of normal services to SM, and the extension of the VIP experience.

These actions are different in nature of interactivity, and in their crossing of the corporate border. Marketing activities can be unidirectional, either disseminating information or harvesting feedback. Sales activities are interactive processes involving internal and external collaboration partners. Support activities presume an established relationship between the corporate user and the serviced partner, and so are customer experience activities. More difficult in analysis are innovation and collaboration actions, as their particular processes very much depend on the publicity of the activities, and the underlying intellectual property assumptions and contracts.

2.2 Roles and obligations in corporate actions in social media

The roles under which a corporate user acts in SM are many. Depending on any of the actions from section 2.1, various roles participate in business processes. Typically, a business action is carried out as a result or a part of a business process, based on a goal, constrained by a budget and other limited resources, and regulated by a set of rules composed of internal and external regulation. Common to most processes is the fact that participants need to be identified according to their roles and privileges in the process. Identification is carried out using Identity management systems (IDMS) along with policy management systems such as for example Role-based access control (RBAC) [6]. Therefore, any integrated corporate use of SM as part of business processes needs adequate forms of process definitions, policies, and digital identities. The handling of obligations that result from policies is particular complicated. Depending on obligations such as archival needs, financial record keeping, data protection versus data subject consent, or confidentiality requirements, the participation and interaction of corporate users can face serious challenges.

3 Challenges in designing security and privacy into social networks and business processes

From the above assumptions and considerations, we group the areas of concern for security design on corporate SM use into three areas. These areas will be described below.

ISBN 978-3-88579-286-4

3.1 Control over social media software, configurations and content

The physical control over the software platform, its configuration, and the content data bases are an important issue. Either the platform is owned and operated by the corporate user, or, more likely, the platform is an external party providing a platform for the corporate user. SM platforms operate contrast to classical IT outsourcing where system operations are run exclusively for the corporate customer, and in contrast to cloud computing, where the physical platform and management services of dedicated software are outsourced. SM platforms "own" the user relationship, and its users normally have vast possibilities to modify both content and content access policies. Many established SM firms claim ownership or unrestricted use licences for all content uploaded by users. Strategic IT projects, however, are often packed into tight service level contracts, liability agreements, and contracts on intellectual property concerning the data content. Both specific processes and specific business secrecy needs lead to custom-tailored service-level contracts. In addition, regulatory requirements such as privacy impact assessment, operational risk management and others need to be adapted to the corporate user's needs. For information security and privacy, these topics require a solid chain of service level contracts providing availability, along with convincing security management and security technology efforts that ensure content ownership, confidentiality, and integrity.

Challenge 1: Regulatory obligations

Regulatory obligations impose age control, "membership control", and real identification of a person, along with reporting and archiving duties. SM platforms are owned by independent companies basing their business models on advertising and associate marketing. They are designed as an arena for private individuals that share private data objects with their personal social networks, or anyone else. Examples for regulatory challenges are: Secrecy and confidentiality, e.g. as a result from health regulation, data protection, handling of business secrets, or protection of future intellectual property in innovation processes. Another challenge are liability for actions on SM, for example concerning service contracts, intellectual property, or inside trading issues when the corporate users speaks out in public or in large audiences.

Challenge 2: Integrity and ownership

Integrity of the shared information objects, their archiving, and ownership over them is an important challenge. As the corporate user is subject to the various regulations and liabilities mentioned above, proper unmanipulated presentation and archival and well-defined ownership over information objects is an essential requirement. Conflicts over possible falsification vs. authenticity of content may arise, and quickly revolve around integrity and ownership. Copyright and intellectual property can be long from clearly settled in crowdsourced information on SM. Neither its origin nor its owner may be easily constituted. Parts of the crowdsourced information might contain other party's intellectual property (plagiarism, careless quoting, or intentional sabotage).

ISBN 978-3-88579-286-4

Access to the objects might turn information public, potentially destroying patent or business opportunities. With today's policies on publicly available SM, it might in addition be hard to remove an error, as some of the platforms reserve themselves the right to keep objects. In addition, users beyond the corporate domain that were part of the object sharing social network might have made their copies of the object already. Integrity and ownership issues extend into the physical space. Who exercises physical and virtual control over the media objects while they reside on disks (access, backup, deletion)? In case of doubt or conflict with subcontractors, cloud computing operators, or other providers -who owns disk, database and content?

3.2 Control over electronic identities

In SM, content is connected to users. However, the community providers' efforts in user identification are low. Registration against an operative e-mail address, or an arbitrary, free-of-charge OpenID provider [7] is often the available assurance level. Authentication is performed based on username/password or e-mail-address/password. Such simple IDM schemes have a number of consequences for the quality and trustworthiness of electronic identities on SM platforms. In particular, the identity assurance about the other users a corporate user shares objects with is not easily established. Plus, a corporate user's business processes may involve several roles and persons that are involved in planning, approving and execution interactions on SM. Enterprise identity management is considered a vital part of corporate security management. In the case of SM, the identity management is both weak, and controlled by the SM platform. Mechanisms to grant control over a subset of the SM platform's identity domain, or to temporarily join in and federate identities from the corporate identity domain are imaginable using identity federation technologies. However, these technologies were developed with single-sign-on in mind, not as a tool to manage employee access, authorization and authentication tokens in complex identity federations. Hence, their security assumptions and threat models must be redone before these protocols can securely be deployed.

Challenge 3: Identity Management

The authenticity of persons and their respective electronic identities (e-ID) is a crucial challenge in corporate use of SM. The identity management issue has many facets:

- Who is talking on behalf of the organization, and in which role? Who is creating, federating or translating these roles from the corporate IDM into the SM identity domain?
- Who is talked to? SM platforms supply a profile to any person in any name, no assumptions can be made about who the person behind some profile and related e-ID is.
- Who does a person in a social network have access to within the corporate user's groups/staff/information objects? In SM, all objects are "owned" or "posted" by someone. In some cases, it is counterproductive to reveal the identity of the company's expert to the whole social network.

ISBN 978-3-88579-286-4

- Who owns and manages these e-IDs? With manipulation, theft or simple denial-of-service, the corporate user loses secrets, business or customer support opportunities. When SM e-IDs get detached and out of control, recovery is difficult.
- Some SM platforms reserve the right to censor content, and to exclude users. However, filtering for undesired content is often based on other user's ratings or complaints. Without proper identity management, such a mechanism might easily be used for sabotage.
- ID theft can expose internal affairs to other parties, as those get access to internal groups and objects, and might gather intelligence on the social networks.

The identity management challenge is an issue that touches information security, business process definition, risk assessment, and trust management. It is central to the corporate user's strategy for SM.

3.3 Enforcement of the chain-of-command: Who talks to whom on social media?

Another problem is related to identity management. How are legitimate collaboration partners identified in SM? As discussed above, the identity assurance in SM is mostly insufficient for assured identities. Even if we assume that the corporate user joins in an identity federation enabling the control over own identities into the SM platform's identity domain, a chain of command is still to be defined and enforced. Such workflows follow patterns aligned with the job at hand. Several persons may be involved, while the flow possibly needs documentation in the corporate archive, and the documents and/or personal data that is being handled might be subject to confidentiality constraints. In consequence, the corporate user must organize workflows involving several persons in different roles. Authorization and documentation steps are normal operations in such processes, and often occur before a work process or a public statement is made. Today's SM, however, are badly adapted for processing corporate-internal workflow steps including authorization and archival. Even with corporate-managed SM user profiles, the possibilities are restricted to groups of users and views defined with access policies.

Challenge 4: Authorization and responsibility

Many processes need authorization from a person with a certain role, or certain privileges. Press officers or the legal department often clear public statements on behalf of a company. There is a significant difference between a company's official statements and its employees' personal statements. Stock exchange listed corporations, for example, might have report duties that get undermined by employees public tale. An important question is whether the workflow steps are carried out on the SM platform, or kept on a corporate-internal system. The definition of this border is relevant, as the functionality of a CSCW system and a SM platform are different. As of today, an object shared on a SM platform must more or less be considered as finalized, and published. In addition to personal responsibility and corporate roles, a code of conduct on what is communicated on SM platforms is an essential challenge.

ISBN 978-3-88579-286-4

Just as the corporate user might not wish that any corporate roles gets visible on SM, there might be topics an issues with restrictions concerning sharing on SM platforms. At last, most hierarchies in corporations define clear responsibilities for processes. SM communications and information sharing need to get aligned with these responsibilities, both in terms of liability as well as in terms of responsibility.

4 Tackling the challenges

For handling of various challenges in information security and information privacy, a distinction on every role's and participants particular responsibilities in the workflows that involve SM is necessary. A differentiation of identification, authentication and authorization based on electronic identities is necessary. Figure 2 shows a conceptualization of the use of electronic identities used in two research projects, PETweb II [8] and e-Me[9]. The middle layer shows the planned purpose of the use of e-ID tokens. The three possible uses are identification, authentication and authorization. These three uses are basic building blocks for the security infrastructure from the corporate processes into the SM activities. They will be used below to analyse requirements for corporate user interaction.

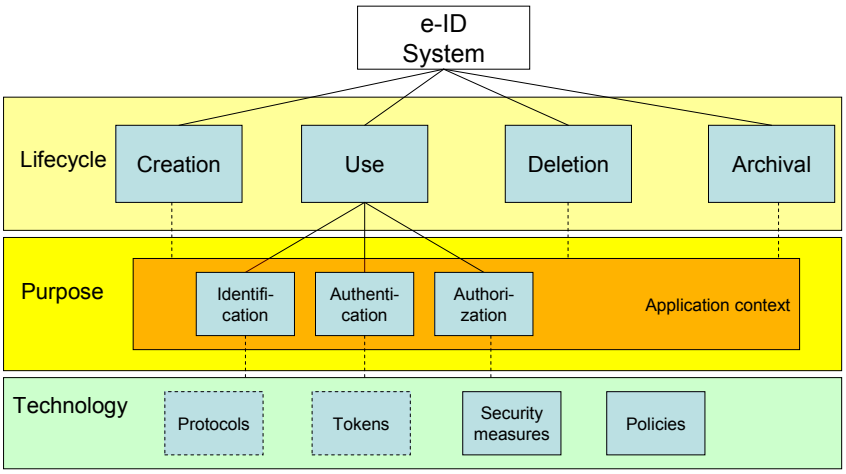

Figure 2: Taxonomy of electronic identity application (from [4]).

The following sections will analyze the security needs, especially with focus on privacy and identity management, for the above challenges. The security requirements are presented in tables in non-formal prose, divided into sub-challenges and topical areas.

4.1 Meeting challenge 1: Regulatory obligations

The meeting of regulatory challenges is a complex subject. It, of course, depends on the regulation that the corporate user is subject to. To represent one type of regulation, data protection regulation has been chosen, out of many other possible options. Data protection regulation requires both the securing of stored personal data, and transparency and documented consent of the persons whose data is being processed. Interaction in SM happen based on personal profiles, linking to individuals. As an implication, documenting consent of identified users, links between the documentation and the data, processing of the data along some communicated processing purpose, and local protection of the data against non-conformant use all are in focus of data protection legislation.

Challenge	Identification	Authentication	Authorization	Data flow control	Security measures	Other
Privacy compliance and data protection	Of data controller, and submitter of consent	Of access to personal data	Of changes to personal data or use policy	Purpose binding Restrictive content management, explicit policy	Integrity, Access control	Use of privacy enhancing technology and policy control. Privacy impact assessment (PIA). Data scarcity principle

One interesting question is that of the how far data protection legislation has to apply (art. 7 of the Data Protection Directive), and in addition, on who the data controller on SM is. Recent literature points out, however, that users in SM can legally be treated as data controllers, according to European legislation [10, 11].

4.2 Meeting challenge 2: Integrity and ownership

Technical measures for integrity and ownership control should be complemented by a policy agreement all participants should comply to. Access control and usage policies matching process needs should be in place. Integrity controls ranging from hashing and time stamping up to advanced methods from the domain of digital rights management (DRM) can be deployed. The tracking of change histories and contributors might require mechanisms for information flow control, e.g. as mentioned in [12] and [13].

Challenge	Identification	Authentication	Authorization	Data flow control	Security measures	Other

ISBN 978-3-88579-286-4

Integrity of data	Identify accessing user	Authenticate access	Collect authorization on especially important actions.	Control movement of data objects into archives.	Non-repudiation Integrity control	Time stamping Access history Role-based access control
Ownership and origin	Identify origin of contribution.	Authenticate user before action on object	Proper authorization for data manipulation	Tracking of actions on objects.	Integrity control	Non-repudiation Change history Licenses Ownership (e.g. DRM)

4.3 Meeting challenge 3: Identity Management

Authentic e-identities and roles, robust identities, and reliable lifecycle management from registration to deletion of the e-IDs are required. This requirement holds specifically for the SM platform. Particular challenges are roles pseudonyms usable by several people, a practice not supported by many social networks. The concept of multiple faces supported by the CLIQUE community [14, 15] is an exception to this.

Challenge	Identification	Authentication	Authorization	Data flow control	Security measures	Other
Identity registration	Hard identification sufficient for the business domain (e.g. passport verification)	Authentication of receiver of credentials			Secure creation and delivery of identity credentials Protection of registration data (confidentiality, integrity)	Possible expiry periods, role constraints, requirements on the registration authority or identity provider
Identity control &	Identification of the corporate	Authentication of use of a	Authorization to modi-		Secrecy of ID token; robustness	Access to the ID management

ID lifecycle	employees handling a role pseudonym	role pseudonym	fy attributes (profiles)		against copy or unauthorized use.	system. Separation of professional and private roles
Non-person roles	Translation of person ID to a role pseudonym	Who is authenticated based on a role?	Is an authorization based on a role, but not a person valid legally?	Appropriate use of roles in intended function within workflow.	Application of context specification, workflow specification, security policies, certificate policies.	Keeping a record of role-person mappings with traceable history.
Handling ID theft	Verify owner of ID credential	Multi-factor authentication	Revocation of past authorizations possible?	Roll-back of actions with stolen ID	Cryptographic protocols and identity management	

4.4 Meeting challenge 4: Chain-of-command, authorization and integration

Both a policy for use of SM and well-defined roles for various functions are useful. Processes with explicit authorization, especially concerning confidential documents or regulated issues, are needed. However, roles in workflows might change often, and a single person might assume many roles, while at the same time a role can be assumed by many persons. Keeping track of such role assumptions, while fulfilling documentation needs, might be challenging on SM platforms that do not offer any role concept. In addition, the support and enforcement of workflow steps collides with the arbitrariness of object handling on today's platforms.

Challenge	Identification	Authentication	Authorization	Data flow control	Security measures	Other
Authorization models	Identification of legitimate user/role	Authenticate use of ID/role	Types of authorizations (documented, revision safe, electronic signatures,	Distribution of authorization data to all		Definition of policies for e.g. RBAC

			receipts)	stake-holders		
Non-repudiation	identification of originator	authentication of originator	Subject really submitted to action (policy)?	Archival of non-repudiation evidence	cryptographic protocols for non-repudiation	Archival / Log file
Workflow control	Identify role that an action is carried out in		Check action authorization. Document authorization evidence.	Proceed workflow to the next step.		RBAC, information flow control, separation of networks managed by the same ID/role

5 Conclusion

The integration of corporate user workflows with SM is challenging. Security requirements in corporate work flows pose demanding requirements on information processing, information protection, and identity management. Today's SM platforms evolved in a consumer-centric, simplistic manner with simple, private interactions in mind. Some of the SM business models are targeted to maximized number of interactions and shared objects for the sake of increased advertising click rates. These goals do not align well with corporate information management and information security needs. SM platforms, not even advanced research prototypes, meet the complexity of document and access control provided by CSCW platforms. Unsurprisingly, many of the business applications of SM involve one-way communication, branding, and marketing activities that are not integrated with the corporation's internal IT systems. As SM platforms are far from fulfilling security and information control requirements, it is not surprising to see a persisting border between them and corporate workflow systems, turning SM into one-way marketing communication channels. Identity proxies, workflow control, and advanced privacy and identity management systems with interfaces to workflow systems will need to be specified into SN platforms to turn them into competitive tools for businesses.

Acknowledgements

The work leading to this article was carried out within the Norwegian **e-Me** research project [9] sponsored by the Research Council of Norway within the VERDIKT program. E-Me aims at increased accessibility and usability of secure identity management on SM platforms.

References

[1] d. m. boyd, and N. B. Ellison, "Social Network Sites: Definition, History, and Scholarship " *Journal of Computer-Mediated Communication,* vol. 13, no. 1, pp. art. 11, October 1, 2007, 2007.

[2] J. Schrammel, C. Köffel, S. Weiss *et al.*, *PICOS deliverable D2.2 Categorisation of Communities*, PICOS FP7 EU project, 2008.

[3] L. Fritsch, K. Holmqvist, and T. Fretland, "Making Rich Media Accessible for Generations: Trust, Security and Privacy Issues with Personal Media on the Web 2.0," in IFIP Trust Management (IFIPTM) 2008 Web 2.0 Trust Workshop, Trondheim, 2008.

[4] L. Fritsch, *Social Media, e-ID and Privacy - Background for the e-Me project*, DART/02/2011, Norsk Regnesentral, Oslo, 2011.

[5] R. Wang, and J. Owyang, *Social CRM: The New Rules of Relationship Management*, Altimeter Group, 2010.

[6] A. Tsolkas, and K. Schmidt, *Rollen und Berechtigungskonzepte : Ansätze für das Identity- und Access-Management im Unternehmen*, 1. Aufl.. ed., Wiesbaden: Vieweg + Teubner, 2010.

[7] D. Recordon, and D. Reed, "OpenID 2.0: a platform for user-centric identity management." pp. 11 - 16

[8] "PETweb II project - VERDIKT programme of the Norwegian research council.," 3/2011, 2011; http://petweb2.projects.nislab.no.

[9] "e-Me — Inclusive Identity Management in New Social Media," 5.5.2011, 2011; http://www.nr.no/pages/dart/project_flyer_e-me.

[10] R. Wong, "Social networking: a conceptual analysis of a data controller," *Communications Law*, vol. 14, no. 5, pp. 142-149, 2009, 2009.

[11] A. D. P. W. Party, *Opinion 5/2009 on online social networking*, 2009.

[12] M. Casassa Mont, S. Pearson, and P. Bramhall, "Towards Accountable Management of Identity and Privacy: Sticky Policies and Enforceable Tracing Services," p. 377: IEEE Computer Society, 2003.

[13] M. Deng, L. Fritsch, and K. Kursawe, "Personal Rights Management," *Taming camera-phones for individual privacy management*, Berlin: Springer, 2006.

[14] B. v. Berg, and R. E. Leenes, "Audience Segregation in Social Network Sites."

[15] B. van den Berg, and R. Leenes, "Masking in Social Network Sites — Translating a Real-World Social Practice to the Online Domain," *it - Information Technology*, vol. 53, no. 1, pp. 26-33, 2011/01/01, 2011.

ISBN 978-3-88579-286-4