Análise de mecanismos de controle de acesso nas redes sociais

por Vinicius Souza dos Santos, Ed Porto e Bráulio Alturas

RESUMO: As redes sociais na Internet vêm se tornando cada vez mais populares, pois facilitam o contato com amigos, parentes distantes, clientes e consumidores através da troca de mensagens e da visualização de fotos, vídeos e áudios. Contudo, a apresentação de tantos dados pessoais pode expor a vida privada de alguém ou informações internas de uma empresa a pessoas desconhecidas. Desse modo, as redes sociais devem prover mecanismos flexíveis e de fácil utilização para que seus usuários possam manter controlo sobre a visualização de seus dados. Esse artigo apresenta-se como um «survey» onde será analisado como as atuais redes sociais provêem esse tipo de mecanismo, analisando alguns de seus aspectos positivos e negativos e apresentando novas propostas específicas para o âmbito de redes sociais na Internet.

Palavras-chave: Redes Sociais, Segurança, Confidencialidade, Privacidade, Controle de Acesso

TITLE: Analysis of control mechanisms of social networking access

ABSTRACT: Social networking on the Internet are becoming very popular because it facilitates contact with friends, distant relatives, customers and consumers by an exchange of messages, viewing photos, videos and audios. However, the presentation of so many personal data can expose the user's personal life or company private information to people unknown. Thus, social networks should provide flexible and user-friendly mechanisms so that users can maintain control over their private data. This article is presented as a survey describing how the current social networks provide this type of mechanism, analyzing some of their strengths and weaknesses and presenting new proposals for the specific context of social networks on the Internet.

Key words: Social Networks, Security, Confidentiality, Privacy, Access Control

TITULO: Análisis de los mecanismos de control de acceso a las redes sociales

RESUMEN: Las redes sociales en Internet son cada vez más populares porque facilitan el contacto con amigos, parientes lejanos, los clientes y consumidores a través del intercambio de mensajes y de fotos, videos y audios. Sin embargo, la presentación de tantos datos personales puede exponer la vida privada de una persona o la información interna de una empresa a extraños. Así, las redes sociales deberían establecer mecanismos flexibles y de fácil manejo para que sus usuarios mantengan el control sobre la visualización de sus datos. En este artículo se presenta una encuesta donde se analiza como las redes sociales actuales proporcionan este tipo de mecanismo, analizando algunos de sus puntos fuertes y débiles y presentar nuevas propuestas para el contexto específico de las redes sociales en Internet.

Palabras-clave: Redes Sociales, Seguridad, Confidencialidad, Privacidad, Control de Acceso

Cada vez mais *sites* de relacionamento e de compartilhamento de arquivos têm se tornados populares. *Sites* como Orkut[1], MySpace[2] e Facebook[3] permitem aos usuários criarem perfis, fazerem *upload* de fotos e vídeos, encontrarem pessoas e adicioná-las como amigos, etc. Outras ferramentas como Blogues e Microbloggins, tais como o Twitter[4], permitem compartilhar textos e fotos com todos os usuários da Internet.

Não apenas usuários domésticos, mas empresas utilizam cada vez mais as redes sociais. Sua aceitação e utilização estão mudando a maneira como indivíduos e organizações se relacionam com o seu meio. Desta forma, os gestores não podem dar-se ao luxo de ignorar o impacto que as redes sociais podem ter em suas atividades (Barnes e Barnes, 2009).

Muitas empresas já utilizam redes sociais como um meio de comunicação interna entre seus funcionários, mas principalmente como um meio de comunicação direta com seus clientes. Contudo, nem sempre se quer compartilhar determinado conteúdo com todas as pessoas que têm acesso àquela rede. Por exemplo, nem sempre um usuário deseja compartilhar determinadas fotos com todos os seus amigos da rede social, ou quer que apenas determinadas pessoas tenham acesso a algum texto escrito por ele ou até mesmo que todos os seus amigos, com exceção de alguns em particular, tenham acesso a seus vídeos.

Percebe-se então que certo nível de privacidade é desejável pelos usuários das mídias sociais e deve ser fornecido pelas redes sociais para que seus usuários sintam-se mais seguros ao compartilhar seus dados. Muitas vezes o compartilhamento de dados tem o intuito de atingir somente os amigos diretos de um usuário e não todos que possuem acesso à rede. Para que isso ocorra, cada ferramenta de rede social implementa um mecanismo de controle de acesso que deve ser de fácil uso e ao mesmo tempo eficaz.

Mas será que os mecanismos de controle de acesso atuais conseguem ser flexíveis o bastante para proporcionarem aos usuários de redes sociais meios de permitir fácil acesso e controle de determinadas informações? E ao mesmo tempo,

Vinicius Souza dos Santos
vinicius@compose.ufpb.br
Mestrando em Informática, Bacharel em Ciências da Computação. Departamento de Informática da Universidade Federal da Paraíba (UFPB), João Pessoa, PB, Brasil. Atualmente pesquisador do grupo COMPOSE (Component Oriented Software Engineering) do Departamento de Informática da UFPB.
M.Sc. in Computer Science, Bachelor of Computer Science. Department of Informatics, Federal University of Paraíba (UFPB), João Pessoa, Brazil. Currently a researcher with the group COMPOSE (Component Oriented Software Engineering), Department of Informatics UFPB.
Maestría en Informática, Licenciado en Ciencias de la Computación. Actualmente investigador del grupo COMPOSE (Component Oriented Software Engineering) del Departamento de Informática de la UFPB (Universidade Federal da Paraíba), Joao Pessoa, PB, Brasil.

Ed Porto Bezerra
edporto@di.ufpb.br
Doutor em Engenharia Elétrica, Mestre em Informática, Tecnólogo em Processamento de Dados. Professor Associado II do Departamento de Informática da Universidade Federal da Paraíba (UFPB), João Pessoa, PB, Brasil. Programa de Pós-Graduação em Informática e Programa de Pós-Graduação em Comunicação.
Ph.D. in Electrical Engineering, Master of Information Technology, Technologist in Data Processing. Associate Professor II, Department of Informatics, Federal University of Paraíba (UFPB), João Pessoa, Brazil. Graduate Program in Computer Science and Graduate Program in Communication.
Doctorado en Ingeniería Eléctrica, Maestría en Tecnologías de la Información, Tecnólogo en Procesamiento de Datos. Profesor Asociado II de la Universidad Federal de Paraíba, João Pessoa, PB, Brasil. Departamento de Informática, Programa de Posgrado en Ciencias de la Computación y el Programa de Posgrado en Comunicación.

Bráulio Alturas
braulio.alturas@iscte.pt
Doutor em Gestão, Mestre em Ciências Empresariais, Licenciatura em Organização e Gestão de Empresas. Professor Auxiliar no ISCTE – Instituto Universitário de Lisboa, Departamento de Ciências e Tecnologias da Informação. Investigador e Associado da ADETTI – Associação para o Desenvolvimento das Telecomunicações e Técnicas de Informática, Lisboa, Portugal.
Ph.D. in Management, Master in Business Administration, Bachelor in Organization and Management. Assistant Professor at ISCTE – Lisbon University Institute, Department of Science and Information Technology. Researcher and Associate ADETTI – Association for the Development of Telecommunications and Computer Science, Lisbon, Portugal.
Doctorado en Management, Master en Administración de Empresas, Licenciatura en Organización y Gestión. Profesor Asistente en ISCTE – Instituto Universitario de Lisboa, Departamento de Ciencia y Tecnología de la Información. Investigador Asociado ADETTI – Asociación para el Desarrollo de las Telecomunicaciones y la informática, Lisboa, Portugal.

Recebido em Fevereiro de 2010 e aceite em Setembro de 2010.
Received in February 2010 and accepted in September 2010.

rígidos o suficiente para garantir a confidencialidade e privacidade dos dados àqueles que não têm autorização de acessá-los?

Segundo Lenhart e Fox (2006), a popularidade de *sites* de relacionamentos, blogues, galerias de fotos *on-line*, *sites* de compartilhamento de vídeos e outros *sites* de compartilhamento de conteúdo tem explodido, resultando em mais informações pessoais e opiniões sendo disponíveis com menos controle de acesso. Levando em consideração que redes sociais são redes de compartilhamento, portanto com o intuito de difundir tudo o que nela se apresenta, compreende-se a falta de ênfase na preocupação com o controle de acesso evidenciado por Lenhart e Fox (2006).

Entretanto, pode-se perceber que a má implementação ou a falta de controle de acesso pode gerar alguns resultados frustrantes, como alguns evidenciados por Hart, Johnson e Stent (2006):

- Blogueiros perderam o emprego quando seus patrões descobriram seus blogues (Simonetti, 2004);
- Blogueiros têm sido vítimas por postarem suas informações pessoais (Rowse, 2006);
- Predadores sexuais usam redes sociais para buscar vítimas (Poulsen, 2006).

Dessa maneira, será abordado nesse artigo como algumas das redes sociais mais populares proporcionam mecanismos de controle de acesso aos seus usuários, verificando os pontos fortes e fracos de cada uma. Como o artigo é apresentado em forma de *survey*, os gestores de empresas podem perceber como os mecanismos de controle funcionam nas redes sociais mais utilizadas, podendo assim escolher o meio mais coerente de comunicação de mídia social de acordo com seu contexto. Também serão abordados trabalhos que apontam para novas formas de controle de acesso específicas para redes sociais e quais as vantagens e desvantagens que estas podem trazer.

O artigo está estruturado do seguinte modo: de seguida são vistas algumas características de cada rede social pesquisada; depois se aborda o que é e o que se pretende garantir com a aplicação de mecanismos de controle de acesso nas redes sociais; em seguida serão apresentadas algumas propostas de mecanismos de controle de acesso definidos especificamente para redes sociais; e finalmente apresentam-se as considerações finais.

Os gestores de empresas podem perceber como os mecanismos de controle funcionam nas redes sociais mais utilizadas, podendo assim escolher o meio mais coerente de comunicação de mídia social de acordo com seu contexto.

Redes sociais

Uma rede social, como explica Castells (2003), nada é mais do que «uma rede eletrônica de comunicação, interativa, auto-definida, organizada em torno de um interesse ou finalidade, embora, em alguns casos, a própria comunicação se transforme no objetivo central». Para o propósito deste estudo sobre mecanismos de controle de acesso nas redes sociais foram analisadas as seguintes redes, escolhidas em função de sua popularidade e natureza: Orkut, Facebook, MySpace, Blogger[5], WordPress[6], Twitter, Youtube[7], Flickr[8], Wikipédia[9] e DokuWiki[10].

As redes sociais analisadas foram divididas com base na natureza de cada uma delas em cinco classes: *sites* de relacionamento, blogues, microbloggins, *sites* de relacionamento de mídias e wikis. Todas elas possuem uma grande característica em comum que, segundo Recuero (2005), é a interação social proporcionada, aliada à noção de percepção de usuários através de um perfil que o faz se diferenciar dos demais. Outra característica em comum, não obrigatoriamente encontrada nas wikis, é o fato dos usuários exporem suas características pessoais, fotos e vídeos de seu cotidiano, bem como pontos de vistas pessoais sobre determinados assuntos. Esses mesmos mecanismos são utilizados pelas empresas para exporem seus produtos e serviços, aproximando seus clientes e mantendo um meio de comunicação aberto entre eles.

Nos *sites* de relacionamento, um usuário cria um perfil ou *profile* com várias informações pessoais, coisas de que gosta de fazer, hobbies, etc. Além disso, usuários podem colocar fotos e vídeos, adicionar outro usuário como amigo, mandar recados, etc., a fim de manter um relacionamento de amizade. No âmbito comercial, empresas criam perfis descrevendo-as e podem criar comunidades para que seus

clientes possam entrar em contato, criar discussões, etc. Nessa classe estão Orkut, Facebook e MySpace.

Blogues são diários *on-line* onde um usuário cria uma conta e tem um espaço na *web* para escrever sobre o que quiser. Geralmente as pessoas escrevem coisas do cotidiano, como num diário pessoal, mas, como evidenciado por Orduña (2007), os blogues estão se tornando meios de comunicação jornalística. Também são utilizados internamente nas empresas como forma de publicação de comunicados, afazeres do dia, etc. Outros usuários podem visualizar e comentar cada assunto proposto nos blogues. O Blogger e o Wordpress estão nessa classe.

Microbloggins são semelhantes aos blogues, mas geralmente têm restrição no tamanho das mensagens postadas, pois estes prezam pela agilidade na disseminação da informação. Possuem uma característica semelhante aos *sites* de relacionamentos no tocante a atribuir outros usuários como amigos. Esse meio de comunicação vem ganhando grande adesão das empresas, pois é um meio ágil onde a informação é disseminada para todos os usuários da rede muito rapidamente, atingindo grande quantidade de usuários. O Twitter encontra-se nessa classe.

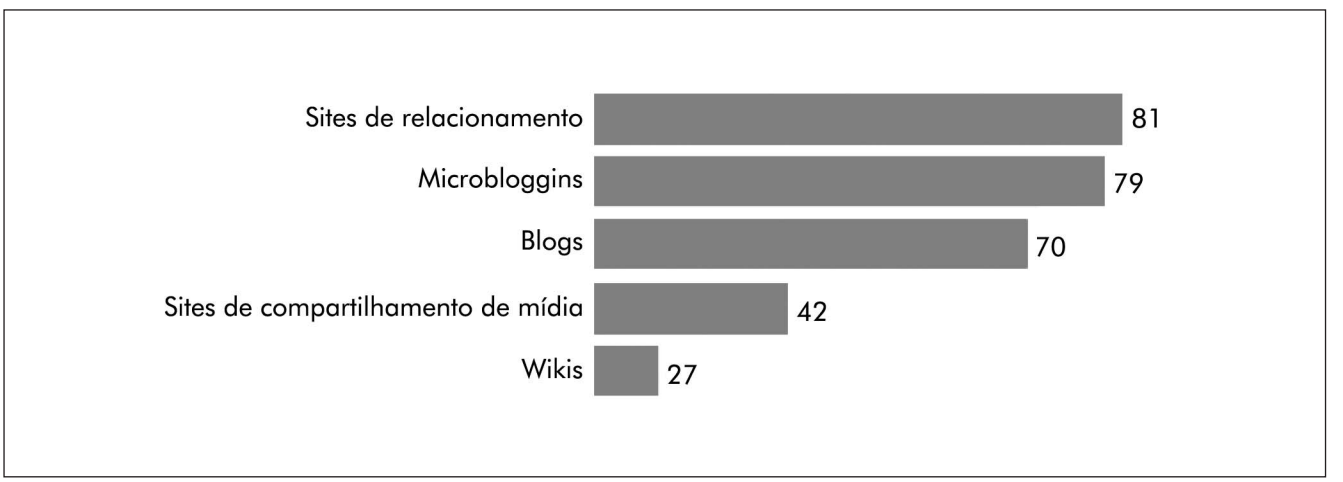
Os *sites* de compartilhamento de mídia têm como principal característica o fato de proverem espaço para divulgar uma mídia específica. No caso do Youtube são divulgados vídeos. Já no Flickr também são divulgadas fotos. Outros usuários podem comentar sobre as fotos ou vídeos postados.

Nas wikis a característica principal é a produção de conteúdo colaborativo. Diferentemente do blogue, onde o conteúdo geralmente é escrito por uma pessoa apenas, nas wikis todos trabalham em cooperação para a produção de um mesmo conteúdo. Wikipédia e DokuWiki fazem parte desta classe.

Atualmente, segundo uma pesquisa realizada pela Deloitte (2010), as redes do tipo *sites* de relacionamento ainda são as mais utilizadas pelas empresas, seguidas dos microbloggins, blogues, *sites* de compartilhamento de mídia e por fim wikis, como pode ser visto na Figura 1.

Ainda assim, como ressaltado por Sousa e Azevedo (2010), deve-se entender que, no âmbito empresarial, o modo de compartilhamento das informações deve ser adequado para a cultura, identidade e público das empresas, já que no meio social *on-line*, este se torna o mecanismo de comunicação entre a empresa e seu público. Já do ponto de vista interno de uma empresa, alguns diretores acreditam que o acesso às redes sociais pelos seus empregados pode lhes desviar a atenção de suas tarefas, diminuindo o rendimento, além disso, ainda temem que alguns funcionários

Figura 1
Tipo de mídias sociais mais utilizadas pelas empresas (%)



Fonte: Deloitte (2010)

possam difamar a empresa ou divulgar informações que deviam circular apenas internamente.

Desse modo, o tipo de mecanismo utilizado para controlar a divulgação das informações, que varia de rede social para rede social, pode influenciar na escolha de quais redes sociais são mais adequadas para o contexto da empresa. É necessário ressaltar que nem sempre se quer divulgar informações para todos os participantes de uma rede social. Por vezes determinadas informações têm a intenção de atingir apenas alguns usuários de uma rede. Para se conseguir ter controle de quem deve acessar quais informações, se faz necessário um mecanismo para o controle de acesso de fácil manipulação mas que garanta a privacidade e integridade da informação.

Mecanismos de controle de acesso

Segundo Ferraiolo, Kuhn e Chandramouli (2003), o controle de acesso é «crítico na preservação da confidencialidade e integridade da informação», evidenciando assim que qualquer aplicação que demande certo nível de confidencialidade necessita de algum mecanismo de controle de acesso.

O controle de acesso pode ser dividido em três tipos distintos, como explicado por Bishop (2002):

- Controle de acesso discricionário (CAD) – é aquele em que um usuário pode definir o controle de acesso para negar ou permitir acesso a um objeto;
- Controle de acesso compulsório (CAC) – é aquele onde o sistema define o controle de acesso e não pode ser modificado pelo usuário;
- Controle de acesso controlado pelo originador (CACO) – é aquele onde o controle de acesso ao objeto é definido pelo criador do mesmo.

Na literatura podem ser verificados vários mecanismos distintos que implementam controle de acesso. Alguns deles podem ser vistos em Bishop (2002), tais como: matriz de controle de acesso, listas de controle de acesso (ACL), *capabilities*, chave-cadeado, etc. Nasirifard (2007) comenta a existência de alguns estudos sobre controle de acesso especificamente para redes sociais, onde em sua maioria são adaptações dos mecanismos de controle clássicos citados anteriormente. No contexto das redes sociais, o controle de acesso é parte crítica, tanto na prevenção da integridade, quanto na prevenção da confidencialidade da informação.

- **Integridade**

Para Ferraiolo, Kuhn e Chandramouli (2003), a integridade refere-se a proteger um dado de ser alterado inapropriadamente ou modificado por usuários não autorizados. Para Bishop (2002), a integridade se refere à credibilidade do dado ou recurso, usualmente em termos de prevenir alterações inapropriadas ou não autorizadas. Para ele, a integridade pode ser vista de duas formas: integridade do dado e integridade de origem.

Essa distinção é interessante, pois no que diz respeito à integridade do dado, a grande parte das redes sociais permite que apenas o dono da conta utilizada para autenticação no sistema possa alterar ou excluir dados. Essas permissões não podem ser passadas adiante para demais usuários da rede, tornando difícil a alteração não autorizada dos dados. Desse modo, quanto à integridade do dado, não há uma preocupação tão grande por parte da maioria dos mecanismos de controle de acesso das redes sociais quanto à modificação ou exclusão de dados de um usuário feita por um usuário indevido, pois para isso se necessitaria saber o *login* e senha do usuário de uma conta, para assim se autenticar no sistema e fazer alterações não autorizadas. Uma exceção a esse tipo de mecanismo são as wikis, as quais permitem uma edição colaborativa do conteúdo sem a necessidade de autenticação no sistema.

Quando se fala em integridade de origem, refere-se à autenticidade do conteúdo ou dos usuários que o apresentam. Para tentar melhor exemplificar estas duas formas de integridade (dado e origem), serão explicadas a importância da integridade do dado no contexto das wikis e a integridade de origem no contexto dos *sites* de relacionamento, como o Orkut.

O propósito das wikis é criar textos de uma forma colaborativa. Como afirma Wales (2005) sobre a Wikipédia, ela é «um esforço para criar e distribuir uma enciclopédia livre e em diversos idiomas, da mais elevada qualidade possível, a cada pessoa do Planeta, em sua própria língua». Isso evidencia o fato da liberdade que os usuários têm na construção do conteúdo das wikis. Desse modo, quanto mais

pessoas tiverem acesso à wiki, mais robusta é a produção de conteúdo da mesma. No entanto, por permitirem acesso a todos, wikis como a Wikipédia podem ser vítimas de vandalismo, onde seu conteúdo pode ser denegrido sem maiores dificuldades. Assim, surge a seguinte questão: como garantir a integridade do dado de uma wiki?

A DokuWiki implementa um mecanismo de ACL que permite restringir as operações que os usuários podem exercer na wiki. Este mecanismo permite restringir acesso às páginas e *namespaces*[11], definindo para cada usuário ou grupo de usuários uma restrição para o elemento (página ou *namespace*) em questão. Desse modo, cada elemento possui uma lista com a restrição de acesso que cada usuário possui. As restrições são divididas em sete categorias, niveladas conforme sua importância: *none, read, edit, create, upload, delete* e *admin*. Cada categoria de nível mais alto contém as de nível mais baixo, sendo *delete* a de mais alto nível e *read* a de mais baixo nível.

Esse mecanismo de ACL pode ser bem trabalhado quando considerado um universo de poucos usuários, de modo que quanto maior o número de usuários, mais difícil se torna fazer o controle individualizado de permissões. Este controle pode se tornar complexo, pois geralmente as permissões são modificadas com o tempo para cada usuário ou grupo de usuários. Além disso, se a wiki possuir várias páginas, torna-se inviável, por exemplo, revogar todas as permissões de um determinado usuário, pois para isso seria preciso consultar as ACL de cada página, a fim de verificar as permissões do mesmo.

Então, ao considerar uma wiki de grande porte como a Wikipédia, que potencialmente pode possuir milhões de usuários colaboradores e páginas criadas, percebe-se que o modelo de ACL se torna impraticável. Contudo, esse mecanismo se torna eficaz, por exemplo, para a utilização de uma wiki internamente numa empresa, pois se pode garantir que as informações sejam acessadas apenas dentro da empresa e apenas àqueles credenciados que tenham acesso à informação.

Quanto a Wikipédia, a atual política de controle de acesso implementada é não ter mecanismos de controle de acesso à edição de páginas, ou seja, qualquer pessoa, mesmo que não esteja autenticada no sistema, pode editar uma página. Por mais contraditório que isso possa parecer, esta solução é viável e eficaz para essa rede. Isso se dá justamente pelo tamanho da rede e o número de usuários colaboradores, pois teoricamente, quanto mais colaboradores uma wiki possuir, maior o número de pessoas que ajudam a manter sua organização.

O maior problema na integridade dos dados em wikis se refere a erros não propositais na exposição de conteúdos, como datas, nomes e locais errados escritos erroneamente. Entretanto, quanto mais colaboradores existirem, mais organizada e confiável pode se tornar uma rede.

O que se apresenta na Wikipédia é, na verdade, uma política (e não um mecanismo de controle de acesso) que rege algumas normas e boas condutas feitas pela própria comunidade a fim de manter a organização. Apesar de não ser um mecanismo de controle de acesso, um mecanismo que pode ser utilizado na Wikipédia é o de detecção e correção de erros e *backups*, de modo que permita que um vândalo altere livremente uma página, e logo após seu ato, a página original seja recuperada com a verificação da mudança inapropriada e restauração através do *backup*. Contudo, esse método pode se tornar complexo devido ao grande número de páginas existentes. O maior problema na integridade dos dados em wikis se refere a erros não propositais na exposição de conteúdos, como datas, nomes e locais errados escritos erroneamente. Entretanto, quanto mais colaboradores existirem, mais organizada e confiável pode se tornar uma rede.

Sobre integridade de origem, em redes de relacionamento populares como o Orkut, é comum a criação de falsos *profiles*, principalmente de usuários que se fazem passar por empresas ou pessoas famosas, com o intuito de disseminar *spam* ou vírus. Na maioria das vezes, a mensagem insinua que o remetente conhece de algum modo o destinatário, que viu seus dados pessoais em algum outro *site* ou menciona fotos de algum suposto evento em que ambos estavam. Alguns usuários, por não reconhecerem que se trata de uma mensagem falsa, acabam por acessar os *links* contidos na mensagem e com isso adquirem algum vírus ou até perdem

acesso à sua conta que será usada para propagar ainda mais *spam* ou vírus. Para contornar essas situações, as redes sociais utilizam o esquema de *captcha*[12] sempre que algum link estiver contido na mensagem postada. Desse modo, os programas que enviam mensagem em massa às redes sociais ficam impossibilitados de disseminar mensagens falsas em grande quantidade.

Falsos *profiles* também são criados com o intuito de obter informações através de engenharia social. Fazendo-se passar por quem não são usuários maliciosos podem obter informação sigilosa das pessoas ou empresas através de espionagem industrial. Contudo, quanto à engenharia social, os mecanismos de controle dessas redes não testam se os usuários dizem ser quem realmente são e devido a isso os próprios usuários devem tomar este cuidado de reconhecer um falso *profile*.

• **Confidencialidade**

Segundo Bishop (2002), confidencialidade é «a ocultação de informações ou recursos». Para Ferraiolo, Kuhn e Chandramouli (2003), confidencialidade «refere-se à necessidade de manter a informação segura e privada». Outra definição, feita pela *International Organization for Standardization* (ISO 2000), é que confidencialidade é a «segurança de que a informação é acessível apenas por aqueles que possuem autorização». Esta última aborda a autorização de usuários, que é um dos pontos principais quando se trata de controle de acesso em redes sociais.

Quanto à confidencialidade das informações pessoais contidas nos perfis de usuários, a maioria das redes usa um mecanismo baseado no nível de relacionamento que um usuário possui com a pessoa que acessa o dado. Geralmente, o nível de relacionamento é dividido em *Todos, Amigo de Amigo* e *Amigo*. O dado também pode ser marcado como *privado*, dando acesso apenas ao dono da conta. Esse mecanismo é bastante popular, pois proporciona um bom balanceamento entre flexibilidade e facilidade de uso e consegue capturar certo nível de confiança que um usuário possui para com aqueles que fazem parte da rede.

Todavia, como discutido por Hart, Johnson e Stent (2006), esse sistema não consegue fazer uma distinção entre amigos e «amigos», ou seja, amigos que são tanto da rede como fora dela, de «amigos» apenas da rede social. Em algumas ocasiões, essa distinção pode fazer diferença já que um usuário pode querer compartilhar alguns dados pessoais apenas com pessoas que de fato conhece. Além disso, mesmo que um usuário conheça os amigos pessoalmente, podem existir certas informações que se queira compartilhar com alguns e com outros não. Esse modelo ainda pode gerar ambigüidade: num exemplo, descrito por Gates (2007), tem-se uma mãe que é considerada amiga de um usuário (sua filha), mas sua filha pode não querer lhe revelar algumas informações pessoais, mesmo conhecendo-a fora da rede e sendo amiga dentro da mesma. O mesmo pode acontecer com usuários que desejam compartilhar informações pessoais com seus amigos de rede, mas não com seu chefe de trabalho.

O Orkut e o Facebook apresentam um mecanismo diferente em relação a quem tem acesso aos álbuns de fotos dos usuários. No Orkut, um usuário pode criar um álbum contendo várias fotos e escolher quais usuários ou grupos de usuário que podem visualizar as fotos. Já no Facebook, o mecanismo além de proporcionar a seleção daqueles que podem ver, pode-se criar restrições pessoais restringindo o acesso a alguns usuários específicos. Embora estas redes sociais possuam mecanismos que permitam visualização de álbuns, esse nível de granularidade poderia ser ainda maior, caso as restrições fossem aplicáveis para cada foto individualmente.

No Twitter só existe uma opção de controle de acesso das mensagens enviadas através da opção *Protect my updates* (proteger minhas actualizações), que faz com que apenas as pessoas indicadas pelo usuário possam acompanhar seus *posts* (ou, como conhecido na rede, seus tweets), diferentemente da opção padrão que deixa os *tweets* visíveis a todos da rede. Essa simplicidade provavelmente se dá ao fato de que o Twitter é, entre as redes analisadas, a rede social com menos opções de preenchimento de informações pessoais. Portanto, há menos dados pessoais para proteger. Contudo, por ter mais simplicidade no controle de acesso, ele possui menos flexibilidade.

Por exemplo, mesmo permitindo separar os amigos em grupos (listas), não se pode permitir que apenas o grupo A ou B possa ler a mensagem X ou Y. O controle de acesso às

O Twitter vem ganhando espaço entre as empresas que a utilizam para notificar seus clientes e consumidores sobre novidades e até promover promoções de seus produtos.

mensagens é feito para todas as mensagens em conjunto e não para cada mensagem individual, com exceção do chamado *direct message* que é uma mensagem privada visível apenas para o usuário que mandou e o que recebeu. Essa simplicidade do Twitter é o que o torna tão popular, pois cada mensagem postada por um usuário é recebida por todos aqueles que o seguem na rede, que, por sua vez, podem repassar essa mensagem (através do chamado RT ou *retweet*) para seus seguidores e assim por diante. Olhando desta forma, a confidencialidade das informações é na verdade desprezada, pois o intuito é que as informações se espalhem o mais rápido possível para a maior quantidade de pessoas. Devido a esse fato, este tipo de mídia social vem ganhando espaço entre as empresas que a utilizam para notificar seus clientes e consumidores sobre novidades e até promover promoções de seus produtos.

O Youtube e Flickr também apresentam um mecanismo bastante simples em relação à exibição da mídia enviada pelos usuários. No Youtube, a mídia pode ser privada (só o usuário pode ver), não listada (só aqueles com acesso ao link do vídeo podem visualizá-lo) ou pública (todos podem ver, mesmo os que não participam da rede), enquanto no Flicker existem apenas as opções público e privado.

Contudo, existe uma diferença no controle de mídia privada nas duas redes. No Youtube, caso a opção seja privada, a mídia ainda pode ser compartilhada com até 25 outros usuários escolhidos pelo dono da conta. Já no Flickr, a mídia ainda pode ser compartilhada com sua família ou seus amigos que fazem parte da rede, assim negando acesso a pessoas que estão fora dela.

No Flickr existe a opção de criação de grupos com três formatos. O primeiro formato é público e qualquer pessoa tem acesso tanto para visualizar, quanto para ingressar no grupo. O segundo formato de grupo permite que qualquer pessoa visualize as fotos, mas que só pessoas com convite possam fazer parte do grupo. A terceira opção, mais restritiva, define que só as pessoas convidadas a participarem do grupo podem visualizar as fotos. Neste formato de grupo, um usuário ganha um maior controle sobre quem pode ver suas fotos. Uma ambigüidade no Flickr é que uma foto marcada como particular deveria ser visualizada apenas pela pessoa que a postou, contudo, caso essa foto seja incluída na galeria de um grupo, todas as pessoas daquele grupo podem visualizá-la. Isso pode confundir os usuários, pois uma foto que é privada se torna pública para membros do grupo.

Algumas redes como Orkut, Blogger e Wordpress possuem um mecanismo que permite ao usuário não exibir nos resultados de ferramenta de buscas, como o Google, o seu profile. Isto é interessante no ponto de vista da ocultação da informação, pois não só algumas informações pessoais são ocultadas, mas a existência do perfil como um todo. No Wordpress ainda existe a opção de ocultar o perfil para mecanismos de busca, mas habilitar para usuários a procura manual dentro da própria rede.

Agregar controle a nível de «post» e não do blogue como um todo é interessante, pois permite que um usuário use o mesmo blogue para postar coisas para pessoas diferentes, sem que elas tenham conhecimento do que se passa em outro «post».

Nos blogues do Blogger e do Wordpress, o mecanismo de permissões para acesso a leitura dos *posts* é semelhante. Em ambos existe a opção de deixar a leitura pública ou apenas para usuários selecionados. No Blogger ainda existe a opção de permitir que apenas os autores possam ler os *posts*. Uma opção presente no Wordpress permite que usuários possam definir para posts individuais o controle de privado, público ou protegido por senha. Agregar controle a nível de *post* e não do blogue como um todo é interessante, pois permite que um usuário use o mesmo blogue para postar coisas para pessoas diferentes, sem que elas tenham conhecimento do que se passa em outro *post*. Desse modo, uma empresa pode utilizar um blogue interno e postar informações referentes a apenas os funcionários alvos que necessitam ter o conhecimento da informação, garantindo assim certo nível de confidencialidade.

Propostas de mecanismos de controle de acesso

Apesar dos mecanismos de controle de acesso das redes atuais serem simples, eles não são flexíveis o bastante, e aqueles que garantem uma maior confidencialidade e privacidade são por vezes mais complicados de serem utilizados por usuários comuns.

Devido a este fato, novos estudos sobre mecanismos de controle de acesso vêm sendo feitos especificamente para o âmbito das redes sociais.

• **RelBAC**

Giunchiglia, Zhang e Crispo (2008) propõem um modelo chamado *Relation Based Access Control* (RelBAC) que modela as permissões como um relacionamento entre os usuários e os dados, enquanto as regras de controle de acesso são instanciações em conjuntos específicos de usuários e dados. A novidade que esse modelo traz é a forma de apresentar a política e as permissões do modelo do sistema. Essa apresentação é feita através de um diagrama entidade-relacionamento que permite uma fácil compreensão das regras existentes, proporcionando um meio simples de analisá-las a fim de validar ou melhorar a política de segurança adotada.

Diferentemente de *Role Based Access Control* (RBAC), esse modelo não rotula usuários, assimilando permissões aos usuários e não a papéis, o que faz sentido nas redes sociais, já que pessoas geralmente não têm funções, apenas estão em algum tipo de grupo. O fato de o modelo ser representado por um diagrama é interessante, pois proporciona aos usuários comuns um meio fácil de gerenciar seus dados pessoais. Porém, esse modelo pode se tornar complicado com o aumento do número de usuários e informações passíveis de compartilhamento.

• ***Trust network***

Em Hong e Shen (2008), é descrito um mecanismo de controle de acesso que não é visto de forma isolada mas como uma plataforma denominada *trust network* ou rede de confiança. Esse esquema se baseia na transitividade das relações dos membros da rede. Essa transitividade pode ser vista como no seguinte exemplo: João confia em Maria e Maria confia em Pedro; logo, João tem certo nível de confiança em Pedro, representada em apenas uma direção, já que não necessariamente Pedro confia em João. Nesse mecanismo, cada usuário (*private data owner* ou PDO) atribui um valor aos dados que ele quer compartilhar. Quando outro usuário (*private data request* ou PDR) tenta acessar o dado, é feita uma análise da confiança que este tem com o PDO, baseando-se em três pontos.

Primeiro, no valor de permissão atribuído ao dado. Depois, no grau de proximidade que o PDR tem com o PDO, como o exemplo citado de João e Pedro; e por último, o nível de confiança dado pelo PDO ao primeiro PDR da transição. Desse modo, os usuários definem o nível de confiança que eles possuem em seus amigos da rede social e a permissão para os demais usuários é atribuída automaticamente pelo sistema. Esse mecanismo, diferentemente dos vistos até agora, consegue definir permissões automaticamente, provendo portanto uma grande facilidade para o usuário. Contudo, existe uma perda de autonomia nesse sentido, já que o usuário deixa de definir as permissões.

• **CBAC**

O *Content Based Access Control* (CBAC) proposto por Hart, Johnson e Stent (2006) se baseia na definição de uma política de permissão de um dado a partir das características do mesmo. Por exemplo, permitir que apenas os usuários contidos numa foto possam visualizar a foto. A partir dessa política, o sistema pode gerar automaticamente permissões para novos objetos configurados como semelhantes, portanto possuindo características em comum. Para isso, o CBAC se vale de processamento de linguagem natural, reconhecimento de imagens e aprendizagem de máquina.

Assim como no *trust network*, o CBAC procurar simplificar o mecanismo para o usuário através da redução de operações que o mesmo precisa definir, deixando que o sistema faça definições automáticas. Este sistema pode até informar ao usuário que o mesmo pode estar revelando informações que não deveria, como por exemplo colocar no *post* de um blogue o endereço de sua residência. Outra aplicação interessante desse modelo seria em wikis que, por terem acesso público, podem ser alvo de vândalos. Nesse contexto, o CBAC poderia verificar se as partes editadas do texto con-

dizem com o assunto do mesmo, ou se contém palavras pejorativas, por exemplo, através de expressões regulares.

Outro fato interessante é que, pelo fato de permissões serem atribuídas automaticamente a novos objetos, essas atribuições podem não condizer com a expectativa do usuário. Por isso, o CBAC possui um sistema de aprendizado de máquina que pode com o tempo aprender e diminuir o número de erros gerados.

Apesar de parecer proeminente, o CBAC tem fundamento em tecnologias que ainda não são totalmente confiáveis ou que não produzem ainda resultados precisos, como é caso de aprendizagem de máquina. Com o amadurecimento dessas tecnologias, o CBAC pode se tornar melhor e mais confiável.

- **Toomim**

Toomim (2008) propõe um mecanismo onde perguntas são geradas pelos usuários e apenas aqueles que sabem as respostas têm acesso ao conteúdo. Esse mecanismo prima pela facilidade de uso, já que os usuários não precisam, por exemplo, controlar ACL ou mecanismos do gênero. Para esse esquema são definidas três classes de *guessers*[13].

A primeira possui estranhos que não têm ligações com o usuário dono da conta e possuem pouca informação sobre o mesmo. Para esses, o número de respostas que podem ser atribuídas às perguntas é limitado.

A segunda classe contém usuários da rede que podem possuir um grau de relacionamento com o dono da conta, mas que teoricamente não deveriam saber a resposta da pergunta. Para esse caso, se o usuário errar certo número de perguntas, as tentativas são postas num log e informadas para o dono da conta, para que esse tenha ciência de que outro usuário tentou acessar seus dados.

Finalmente, a terceira classe possui usuários que devem ter acesso aos dados, mas que porventura esqueceram a resposta; então, o mesmo procedimento de gravar as tentativas de acesso e mostrar ao usuário é tomado, só que agora o usuário pode tomar as devidas ações para que o acesso seja garantido.

Esse sistema, à primeira vista, parece ser um dos que provêem a maior facilidade ao usuário, porém, quanto maior a quantidade de dados compartilhados, maior o número de perguntas que devem ser elaboradas. Além disso, nem sempre é garantido que o usuário faça perguntas que realmente quem saiba as respostas seja só quem ele imaginava: usuários podem fazer perguntas inocentes e óbvias achando que estão fazendo perguntas seguras.

Outro fator negativo nesse esquema é a facilidade do vazamento da informação. Considere que João sabe a resposta de uma pergunta para acessar uma foto de Maria e que ela e João têm um desentendimento. Nada impede João de divulgar a resposta à pergunta da foto de Maria para os demais usuários da rede, desse modo provendo um vazamento da informação que deveria ser confidencial.

Considerações finais

Redes sociais têm facilmente provido aos seus usuários meios de garantir a confidencialidade de seus dados. Porém, esse mesmo mecanismo que protege os usuários comuns também protege pessoas que as utilizam para outros propósitos, tais como pessoas que fazem apologia às drogas, racismo, discriminação de religião, de orientação sexual e até pedófilos (Oliveto, 2006), alem de vândalos e usuários que criam falsos perfis fingindo serem outras pessoas. Portanto, os mecanismos de controle de acesso devem pesar até quanto à privacidade é necessária para as pessoas manterem um relacionamento num ambiente virtual de interação social, garantindo certo nível de privacidade, mas não privado o bastante para que possa ser utilizado para outros fins que não os definidos para as redes sociais da Internet.

As redes sociais estão se popularizando cada vez mais e demandando de mecanismos de controle de acesso mais flexíveis e de fácil utilização. Neste artigo foram analisados os mecanismos utilizados atualmente por várias redes sociais, verificando alguns pontos fortes e fracos. Depois, foram abordados trabalhos que visam garantir novas formas de controle de acesso para redes sociais, buscando sempre um equilíbrio entre a flexibilidade e a facilidade de uso.

Quanto a esses novos estudos, percebe-se que há uma tendência de se tentar gerar automaticamente as permissões ou de tirar o máximo possível a função dos usuários fazerem controles complexos e extensos, mas mais precisos, atribuindo essa funcionalidade ao próprio sistema. Assim, o usuário pode prover apenas as configurações necessárias e observar

se o controle condiz com o que ele espera, alterando-o caso o resultado não seja o desejado.

Por não se tratar na maioria das vezes de dados que necessitem de extrema confidencialidade, esses mecanismos tendem a ter um uso desejável no âmbito das redes sociais. Porém ainda têm falhas, que, como foram vistas, devem ser melhoradas antes de colocá-los em prática. A contribuição deste trabalho está no sentido de prover uma visão geral do estado da arte, no que se diz respeito aos mecanismos de controle de acesso no âmbito das redes sociais. Também serve como base para estudos para pessoas e empresas que desejam utilizar o meio on-line das redes sociais para se manterem em contato com seus amigos e clientes. ■

Notas

1. http://www.orkut.com
2. http://www.myspace.com
3. http://www.facebook.com
4. http://twitter.com
5. http://www.blogger.com
6. http://wordpress.org
7. http://www.youtube.com
8. http://www.flickr.com
9. http://www.wikipedia.org
10. http://www.dokuwiki.org
11. *Namespaces* são *containers* que provêem um contexto único a itens, a fim de resolver problemas de ambigüidade.
12. *Captcha* é uma ferramenta que apresenta uma figura geralmente com um nome que deve ser digitado. Com este mecanismo pode-se diferenciar se o acesso está sendo feito por um humano ou por um computador, a fim de evitar *spam*.
13. *Guessers* são os usuários que podem tentar responder as perguntas.

Referências bibliográficas

BARNES, N. D. e BARNES, F. R. (2009), «Equipping your organization for the social networking game». *Information Management Journal*, vol. 43(6), pp. 28-33.

BISHOP, M. (2002), **Computer Security: Art and Science**. 1.ª ed., Addison Wesley, Estados Unidos.

CASTELLS, M. (2003), **A Galáxia da Internet**, 1.ª ed., Jorge Zahar, Brasil.

DELOITTE (2010), «Mídias sociais nas empresas: o relacionamento on-line com o mercado». Pesquisa disponibilizada em www.deloitte.com.br, Agosto.

FERRAIOLO, D. F.; KUHN, D. R. e CHANDRAMOULI, R. (2003), **Role-Based Access Control**, 1.ª ed., Artech House, Londres, e Boston.

GATES, C. (2007), «Access control requirements for Web 2.0 security and privacy». *W2SP 2007: Web 2.0 Security & Privacy*, Oakland, Califórnia.

GIUNCHIGLIA, F.; ZHANG, R. e CRISPO, B. (2008), «RelBAC: Relation based access control». *The International Conference on Semantics, Knowledge and Grid (SKG)*, Pequim.

HART, M.; JOHNSON, R. e STENT, A. (2006), «Content-based access control». *IEEE Symposium on Security and Privacy*, Oakland, Califórnia.

HONG, D. e SHEN, V. Y. (2008), «Setting access permission through transitive relationship in web-based social networks». *Social Web and Knowledge Management*, Pequim.

SOUSA, L. M. e AZEVEDO, L. E. (2010), «O uso de mídias sociais nas empresas: adequação para cultura, identidade e públicos». *IX Congresso de Ciências da Comunicação na Região Norte*, Rio Branco, AC, Brasil.

ISO (2000), «International organization for standardization, Iso security solutions». http://www.isosecuritysolutions.com/standard-main.html, Novembro 2009.

WALES, J. (2005), «Wikipedia is an encyclopedia, Wikipedia-l@wikimedia.org». http://lists.wikimedia.org/pipermail/wikipedia-l/2005-March/020469.html, Novembro 2009.

LENHART, A. e FOX, S. (2006), «Bloggers: a portrait of the Internet's new storytellers». http://www.pewInternet.org//pdfs/PIP Bloggers Report July 19 2006.pdf, Novembro 2009.

NASIRIFARD, P. (2007), «Context-aware access control for collaborative working environments based on semantic social networks». *Sixth International and Interdisciplinary Conference on Modeling and Using Context (CONTEXT'07)*, Roskilde, Dinamarca.

ORDUÑA, O. I. R. (2007), **Blogs: Revolucionando os Meios de Comunicação**. 1.ª ed., Thomson Learning, Reino Unido.

OLIVETO, P. (2006), «Pedofilia no Orkut». http://www.safernet.-org.br/twiki/bin/view/ SaferNet/Noticia20060823013403, Novembro 2009.

POULSEN, K. (2006), «MySpace predator caught by code». http://www.wired.com/news/ technology/0,71948-0.html, Novembro 2009.

RECUERO, R. (2005), «Redes Sociais na Internet: considerações iniciais». *E-Compós*, Brasília, Brasil.

ROWSE, D. (2006), «Blog stalkers: personal safety for bloggers». http://www.problogger.net/archives/2006/02/07/blog-stalkers-personal-safety-for-bloggers/, Novembro 2009.

SIMONETTI, E. (2004), «I was fired for blogging». http://news.com.com/ I+was+fired+for+blogging/2010-1030_3-5490836.html, Novembro 2009.

TOOMIM, M. et al. (2008), «Access control by testing for shared knowledge». *Proceeding of the twenty-sixth annual SIGCHI conference on Human factors in computing systems*, Florença.