Um Modelo de Segurança e Privacidade para Redes Sociais Móveis Aplicadas à Área da Saúde

Jesseildo Gonçalves[1], **Ariel Teles**[1], **Francisco José Silva**[1]

[1]Laboratório de Sistemas Distribuídos - LSD
Universidade Federal do Maranhão - UFMA
São Luís - MA - Brasil

jesseildo@gmail.com, ariel@dee.ufma.br, fssilva@deinf.ufma.br

Abstract. *Mobile Social Networks (MSN) comprise a social structure whose members are related in groups and the interaction is done through portable computing devices with access to wireless technologies. In health care it is possible to apply MSN concepts for conducting collaborative actions related to health care and its education. Recently many middleware for MSN have been proposed. However, the current MSN middleware are in a preliminary stage in relation to security and privacy requirements. This requirements becomes even more essentials when sensitive data are shared, such as in health applications where patient's profiles and their medical records are manipulated. This paper presents a security and privacy model designed for MSN applications with focus in the health care domain.*

Resumo. *Redes Sociais Móveis (RSM) consistem de uma estrutura social cujo os membros se relacionam em grupos e a interação é feita através de dispositivos de computação portáteis com acesso a tecnologias de comunicação sem fio. Na área da saúde é possível aplicar o conceito de RSM para conduzir ações colaborativas relacionadas ao tratamento de pacientes e sua educação. Recentemente muitos middleware para RSM foram propostos. Entretanto, os atuais middleware de RSM estão em um estágio preliminar em relação a atender requisitos de segurança e privacidade. Esses últimos se tornam indispensáveis quando dados sensíveis são compartilhados, tais como em aplicações para saúde, onde os perfis dos pacientes e suas informações médicas são manipuladas. Este artigo apresenta um modelo de segurança e privacidade desenvolvido para aplicações de RSM focadas no domínio da saúde.*

1. Introdução

Uma Rede Social é uma estrutura social cujos membros se relacionam em grupos e a interação é realizada através de tecnologias da informação e comunicação. As Redes Sociais Móveis (RSM) são uma extensão das redes sociais, onde os usuários utilizam dispositivos portáteis com acesso a tecnologias de comunicação sem fio, agregando a capacidade de realizar interações sociais a qualquer hora e em qualquer lugar [Kayastha et al. 2011]. Uma rede social na área da saúde pode ser definida como um grupo de pessoas (e a estrutura social que elas coletivamente constroem) que utilizam tecnologias da informação e comunicação com o propósito de conduzir coletivamente ações relacionadas à assistência médica e sua educação [Demiris 2006]. Redes sociais

na área da saúde podem ter como usuários diversos agentes envolvidos no processo de atenção a saúde, incluindo profissionais e pesquisadores da saúde, pacientes e seus familiares, como também membros da comunidade em geral.

No entanto, o desenvolvimento de RSM é complexo. O desenvolvedores precisam atentar para questões relacionadas ao compartilhamento de dados na rede, a mobilidade dos usuários, escalabilidade, a disponibilização de mecanismos de interação síncrona e assíncrona entre pessoas e questões relacionadas à privacidade e segurança dos dados, entre outras. Em aplicações de RSM para a área da saúde muitas informações compartilhadas são sensíveis e exigem um rigoroso nível de privacidade como, por exemplo, perfis de usuários e informações médicas de pacientes. Portanto, uma RSM segura deve garantir, sobretudo, a privacidade dos dados compartilhados na rede, buscando também manter a integridade e confidencialidade destas informações. Aaron Beach et al. [Beach et al. 2009] chamam atenção para um conjunto de problemas de segurança que uma RSM pode apresentar, enquanto que Hongyu Gao et al. [Gao et al. 2011] apresentam problemas comuns em redes sociais *on-line*, que também se manifestam em RSM. A especificidade do domínio pode acrescentar diversos requisitos de segurança ao software. Por exemplo, no domínio da saúde deve-se seguir um conjunto de requisitos e normas legais definidas por entidades médicas e/ou governamentais que variam de acordo com o país em que o sistema será usado. Assim, a construção de uma RSM segura requer mecanismos de segurança destinados a lidar com problemas e peculiaridades de ambientes de RSM, além do domínio de suas aplicações.

Este trabalho tem como objetivo apresentar um modelo de privacidade e segurança para RSM considerando os requisitos específicos da área da saúde. O desenvolvimento deste modelo está inserido no contexto do projeto MobileHealthNet, desenvolvido em parceria pelo Laboratório de Sistemas Distribuídos da Universidade Federal do Maranhão e o *Laboratory for Advanced Collaboration* da Pontifícia Universidade Católica do Rio de Janeiro. Este projeto tem por objetivo geral avançar o estado da arte em sistemas de *middleware* para redes sociais móveis, e usar o middleware para a criação de serviços de redes sociais móveis para a área da saúde. O projeto MobileHealthNet conta com apoio institucional do Hospital Universitário da UFMA (HU-UFMA). Este artigo está organizado como segue. A Seção 2 descreve o projeto o qual este trabalho está inserido. Na Seção 3 são descritos os componentes que compõem o modelo proposto. Os principais aspectos de implementação são mostrados na Seção 4, enquanto a Seção 5 aborda os principais trabalhos relacionados a esta iniciativa. Por fim, na Seção 6 são descritas as conclusões e os próximos passos do trabalho.

2. O projeto MobileHealthNet

O projeto MobileHealthNet visa permitir serviços para colaboração entre os profissionais da saúde, entre os pacientes e entre profissionais da saúde e pacientes, onde a colaboração ocorrerá em ambientes móveis. Em especial, este projeto foi concebido para ser aplicado a comunidades carentes e remotas. As aplicações previstas no âmbito deste projeto tem por objetivo: (i) encurtar a distância entre profissionais da saúde e pacientes; (ii) facilitar a colaboração entre profissionais da saúde de diversas especialidades; (iii) promover a educação em saúde tanto para pacientes como profissionais da saúde; e (iv) promover um meio de comunicação entre profissionais dos diversos níveis da atenção a saúde de forma a facilitar o intercâmbio e colaboração entre os mesmos.

Após diversas sessões de interação entre profissionais da computação e da saúde, foram definidos os requisitos principais para construção do *middleware* e aplicações. A arquitetura do software foi organizada em cinco camadas, descritas a seguir.

A **Camada de Comunicação** é responsável por gerenciar o envio e recebimento de mensagens entre os dispositivos móveis, definindo os modelos de interação entre os usuários. Ela está sendo construída a partir da especificação *Data Distribution Service* (DDS) da OMG (*Object Management Group*), um padrão para comunicação *publish/subscribe* com qualidade de serviço que visa a distribuição crítica de informações em sistemas distribuídos de tempo real. A **Camada de Serviços Básicos** disponibiliza serviços básicos do *middleware*, como o serviço de gerenciamento de informações de contexto, o serviço de armazenamento de conteúdo e seus meta-dados, e o serviço de gerenciamento de usuários e grupos. A **Camada de Serviços de Aplicação** disponibiliza serviços típicos de redes sociais, como Serviço de Fórum, Serviço de Chat, Serviço de Mural e Serviço de Alertas, sendo este último para notificação de mensagens que exigem atenção prioritára por parte de seus destinatários. **A camada Aplicações**, compreende as aplicações previstas no projeto.

3. Modelo de Segurança para Redes Sociais Móveis

A camada **Serviços de Segurança** é transversal a todas as camadas da arquitetura do *middleware* e disponibiliza os mecanismos que implementam o modelo de privacidade e segurança proposto neste trabalho. Seu desenvolvimento está sendo conduzido através de um processo de desenvolvimento de software seguro, o CLASP[1].

Como primeiro passo para o desenvolvimento deste modelo, foi realizado o processo de elicitação de requisitos funcionais e não funcionais das aplicações do projeto junto aos profissionais da saúde. A seguir, foram identificados os requisitos específicos de segurança e privacidade, onde verificou-se que os mesmos deveriam seguir um conjunto de restrições legais e éticas definidas pelo Conselho Nacional de Saúde[2] e um conjunto de padrões e requisitos presentes no Manual de Certificação para Sistemas de Registro Eletrônico em Saúde [SBIS and CFM 2011], editado pela Sociedade Brasileira de Informática na Saúde (SBIS).

Os requisitos especificados englobam privacidade e confidencialidade das informações compartilhadas na rede social, mecanismos de controle de informações de contexto, notificação de presença, criação e customização de regras de acesso de granularidade fina, uso de processos de encriptação de dados, persistência das interações relevantes entre os usuários e construção de um canal seguro de comunicação para transferência de dados.

Após a fase de elicitação de requisitos, foram iniciadas as fases de identificação dos papéis e recursos do sistema, onde foram identificados os donos (*owners*) e usuários (*users*) de cada recurso do sistema, bem como especificado o controle de acesso a tais recursos. Além disso, foi realizado um levantamento sobre os possíveis ataques que uma RSM pode vir a sofrer, bem como medidas de defesa a estas ameaças.

[1] `https://www.owasp.org/index.php/Category:OWASP_CLASP_Project`
[2] `http://conselho.saude.gov.br/`

Uma visão geral dos componentes que compõem o modelo de segurança proposto pode ser vista na Figura 1 e cada um desse componentes é apresentado a seguir.

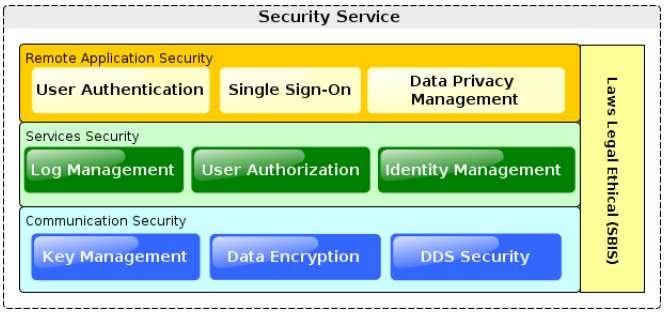

Figura 1. Modelo de Segurança

Em RSM para saúde, todas as operações devem ser realizadas por usuários autenticados, devendo ser garantido também o não repúdio de operações sobre os dados armazenados, uma vez que estas informações estão diretamente relacionadas ao processo de atendimento à saúde das pessoas. Este processo é realizado pelo componente de autenticação (***User Authentication***). Para que o usuário não seja obrigado a autenticar-se a cada serviço que ele necessite utilizar, o modelo dispõe de um mecanismo de autenticação ***Single Sign-On*** (SSO), onde uma única ação de autenticação permite que um usuário acesse todos os serviços aos quais possui permissão de acesso.

O modelo de segurança proposto provê um mecanismo de gerenciamento de privacidade (***Data Privacy Management***), o qual deve disponibilizar aos usuários meios para que sejam definidos as políticas de privacidade a serem aplicadas sobre seus próprios dados e informações de contexto. A implementação das regras definidas na política de privacidade será realizada através de diversos componentes, como o componente de autorização (***User Authorization***), responsável por gerenciar o controle de acesso às informações. Assim, qualquer operação sobre os dados deve passar primeiramente por este componente antes de ser efetivamente realizada.

O modelo também dispõe de um componente que permite registrar o acesso e manipulação de dados e informações de contexto sensíveis, o ***Log Management***. Através deste componente será possível auditar as ações realizadas pelos usuários do sistema. Este componente é também responsável pelo processo de monitoramento da RSM, armazenando as exceções que podem ocorrer no sistema, notificando-as ao administrador do sistema com o objetivo de se identificar tentativas de acesso indevido aos dados ou até mesmo tentativas de intrusão no sistema.

Atualmente o projeto MobileHealthNet possui quatro aplicações sendo desenvolvidas a partir do *middleware*. Para evitar que os mesmos usuários sejam cadastrados em cada uma dessas aplicações, no modelo de segurança é proposto um gerenciamento de identidades (***Identity Management***). Assim, uma vez cadastrado no sistema, o usuário pode acessar qualquer aplicação e serviço dentro do mesmo ambiente utilizando as mesmas credenciais.

Na comunicação DDS, o acesso aos dados é permitido somente aos usuários que estejam participando de um mesmo domínio. O domínio é uma abstração do DDS

usada para isolar e otimizar a comunicação dentro de uma comunidade que compartilha interesses em comum. Porém, todos os usuários participantes de um domínio possuem acesso a qualquer informação nele publicada, através de um processo de subscrição em tópicos. Isto pode representar uma vulnerabilidade que pode levar a uma quebra de privacidade ou a um ataque do tipo *man-in-the-middle*. Portanto, faz-se necessário um mecanismo que torne a comunicação em um domínio DDS mais segura. Este é objetivo do ***DDS Security***, responsável por garantir que somente terão acesso aos dados publicados e a publicar no domínio os usuários que estejam devidamente autenticados e autorizados. Deve-se prover mecanismos para o estabelecimento de canais seguros de comunicação no DDS, garantindo-se ainda as propriedades básicas de autenticidade, integridade e confidencialidade na distribuição dos dados. O componente ***Data Encryption*** é responsável pelos recursos de criptografia, enquanto o componente ***Key Management*** tem por atribuição o gerenciamento das chaves criptográficas necessárias ao processo de encriptação.

4. Aspectos de Implementação

O desenvolvimento dos mecanismos de segurança e privacidade para o *middleware* MobileHealthNet faz uso de algoritmos, protocolos e tecnologias presentes no meio industrial e acadêmico. Os serviços do *middleware* estão sendo desenvolvidos utilizando a tecnologia *Java Enterprise Edition* (J2EE) que, por sua vez, traz um conjunto de recursos destinados a autenticação e autorização, implementados pelo servidor de aplicações. Os mecanismo de autorização será baseado em papéis, por ser facilmente ajustável a mudanças nos requisitos das aplicações. Por outro lado, como as aplicações são destinadas a dispositivos móveis (em particular o Google Android neste primeiro protótipo), os componentes de autenticação e SSO estão sendo desenvolvidos reutilizando os recursos disponíveis na plataforma dos dispositivos.

Para prover o gerenciamento de *logs*, são realizadas interceptações às chamadas dos serviços, utilizando os recursos de interceptações disponibilizados pelo J2EE. Através destes, o desenvolvedor consegue interceptar uma chamada a um método de um objeto instanciado no contexto do servidor de aplicação, possibilitando a execução de instruções antes e/ou depois da execução do método. As informações atualmente armazenadas pelo gerenciador de *logs* correspondem ao nome do serviço, nome do método chamado, nome do usuário responsável pela realização da chamada e parâmetros de entrada passados ao método.

O gerenciamento de identidades está sendo implementado através de um modelo centralizado, onde uma única entidade é responsável por gerenciar as autenticações e atribuições de credenciais, as quais serão utilizadas para acessar os serviços. Este modelo torna o gerenciamento mais eficiente e mais flexível em relação a inclusão de novos serviços.

Para a segurança da comunicação no DDS, estão sendo analisados diversos protocolos: IPSec (*Security Architecture for the Internet Protocol*), TLS (*Transport Layer Security*), SSL (*Secure Sockets Layer*) e SRTP (*Secure Real-time Transport Protocol*). O SRTP provavelmente será o protocolo a ser utilizado, devido ao seu suporte *UDP multicast*, também utilizado pelo DDS.

Para o gerenciamento de chaves, estamos avaliando o uso do protocolo MIKEY (Multimedia Internet KEYing). O MIKEY é um protocolo para gerenciamento de chaves destinado a uso de aplicações de tempo real, com suporte a diversos algoritmos de compartilhamento de chaves. A escolha dos algoritmos a serem adotados, no entanto, ainda não realizada, deve levar em consideração aspectos relacionados à escalabilidade e ao desempenho causado pela execução do algoritmo em dispositivos móveis.

5. Trabalhos Relacionados

Vários *middleware* para RSM foram recentemente propostos [Karam and Mohamed 2012]. No entanto, uma pequena parcela deles fornecem mecanismos de segurança e privacidade, entre os quais destacamos os seguintes.

O Mobilis [Lübke 2011] disponibiliza serviços para o compartilhamento de informações de contexto dos usuários, gerenciamento de grupos, serviços de armazenamento de arquivos e meta-dados a eles associados, como também edição colaborativa de textos e imagens. Ele tem sua comunicação baseada no protocolo *Extensible Messaging and Presence Protocol* (XMPP) e parte dos mecanismos de segurança são obtidos a partir desse protocolo. Isto inclui segurança da comunicação, realizada através do protocolo *Secure Sockets Layer* (SSL), especificado como extensão do XMPP. Além disso, o Mobilis provê um gerenciamento de privacidade e segurança das informações de contexto compartilhadas pelos usuários.

O MobiSoc [Gupta et al. 2009] garante a privacidade dos usuários através de um gerenciamento com granularidade fina, baseado em regras de controle de acesso às entidades no sistema (usuários e aplicações). Cada usuário registra suas preferências de privacidade sobre seus próprios conteúdos. O MobiSoc também provê mecanismo de autenticação e comunicação segura através do RSA em conjunto com o AES.

O MyNet [Kalofonos et al. 2008] disponibiliza um mecanismo de controle de acesso no qual o usuário determina quem terá acesso a suas informações. Para isso ele utiliza uma estrutura chamada de *Passlet*. Os *Passlets* incluem a quem e quais permissões estão sendo concedidas, sobre quais informações elas se aplicam e por quanto tempo as permissões serão válidas. O MyNet também provê mecanismo de autenticação, autorização e comunicação segura dos dados através do protocolo SSL.

Embora os *middleware* analisados reconheçam a importância da segurança, e também provêem alguns mecanismos, eles não atendem as necessidades do domínio da saúde. Por outro lado, o MobileHealthNet está focando neste domínio, portanto deve fornecer mecanismos de segurança e privacidade que atendam suas exigências, resultando em mecanismos de autorização mais rígidos, além dos não encontratos em outros *middleware*, como gerenciamento de identidade e gerenciamento de *logs*, utilizado para auditoria. Além disso, nosso *middleware*, através deste trabalho, inclui como diferencial a concepção de mecanismos de segurança específicos para uma abordagem de desenvolvimento centrado nos dados baseados na especificação OMG-DDS, dado que ainda não foram definidos padrões de segurança para esta especificação.

6. Conclusão e Trabalhos Futuros

Este trabalho propõe um modelo de privacidade e segurança projetado para suprir as necessidades e exigências no contexto do *middleware* MobileHealthNet, destinado a

prover a segurança necessária para RSM voltadas ao domínio da saúde. Este modelo contribui também no desenvolvimento de mecanismos de segurança para o DDS, agregando a ele autenticidade, integridade e confidencialidade das mensagens.

Próximas etapas do desenvolvimento deste trabalho incluem a conclusão da implementação do modelo, começando pela autenticação e autorização, seguido pelo gerenciamento de identidades e *logs* e finalmente a segurança na comunicação. Após a implementação será realizada a avaliação do modelo, esta envolve aspectos quantitativos, como a análise do impacto dos mecanismos de privacidade e segurança no desempenho dos serviços disponibilizados pelo *middleware* e uma avaliação do atendimento aos requisitos especificados e a ameças identificadas para o cenário de RSM. Será ainda avaliado aspectos qualitativos relativas a usabilidade dos mecanismos de privacidade e segurança considerando a perspectiva dos usuários. Para tanto, serão utilizados questionários e técnicas de entrevistas.

Agradecimentos

Os autores gostariam de agradecer a FAPEMA por bolsa de estudo e pelo financiamento deste projeto, processo APP-00932/10, e a CAPES por bolsa de estudo.

Referências

Beach, A., Gartrell, M., and Han, R. (2009). Solutions to security and privacy issues in mobile social networking. In *Proceedings of the 2009 International Conference on Computational Science and Engineering - Volume 04*, pages 1036–1042, Washington, DC, USA. IEEE Computer Society.

Demiris, G. (2006). The diffusion of virtual communities in health care: concepts and challenges. *Patient Education and Counseling*, 62(2):178–188.

Gao, H., Hu, J., Huang, T., Wang, J., and Chen, Y. (2011). Security issues in online social networks. *Internet Computing, IEEE*, 15(4):56 –63.

Gupta, A., Kalra, A., Boston, D., and Borcea, C. (2009). Mobisoc: a middleware for mobile social computing applications. *Mobile Networks and Applications*, 14(1):35–52.

Kalofonos, D. N., Antoniou, Z., Reynolds, F. D., Van-Kleek, M., Strauss, J., and Wisner, P. (2008). Mynet: A platform for secure p2p personal and social networking services. In *Proceedings of the 6th Annual IEEE International Conference on Pervasive Computing and Communications*, PerCom '08, pages 135–146.

Karam, A. and Mohamed, N. (2012). Middleware for mobile social networks: A survey. *Proceedings of the 45th Hawaii International Conference on System Sciences*, pages 1482–1490.

Kayastha, N., Niyato, D., Wang, P., and Hossain, E. (2011). Applications, architectures, and protocol design issues for mobile social networks: A survey. *Proceedings of the IEEE*, 99(12):2130–2158.

Lübke, R. (2011). *Ein Framework zur Entwicklung mobiler Social Software auf Basis von Android*. PhD thesis, Dresden, Germany.

SBIS and CFM (2011). Manual de Certificação para Sistemas de Registro Eletrônico em Saúde (S-RES).

