Um estudo sobre conceitos criptográficos aplicáveis em compartilhamento de informações em rede social com provedor de serviço não confiável

Adriano dos Reis Lopes
Orientador Prof. Dr. Paulo S. L. M. Barreto
Trabalho de formatura supervisionado
Departamento de Ciência da Computação
Instituto de Matemática e Estatística
Universidade de São Paulo

Introdução

Este trabalho tem como objetivo analisar soluções criptográficas para comunicação segura dentro de uma rede social, onde se assume o provedor de serviço como não confiável.

Com a difusão das redes sociais em aplicativos para *smartphones* seu uso se tornou ainda mais cotidiano. Muitas informações pessoais ficam armazenadas nestas redes, o que traz a tona a questão da privacidade de tais dados. Juntando a isso, os casos de espionagem feitos pelo governo estadunidense e divulgados por Snowden [1], temos então um tema de suma importância a ser estudado e aprofundado.

Orientação de estudo

O estudo foi direcionado a fazer uma análise de uso de redes sociais e quais soluções criptográficas poderiam auxiliar na resolução do problema principal, que é garantir a privacidade dos dados em um ambiente com um servidor não confiável.

Estudo de redes sociais

Os estudos foram realizados através de um levantamento de casos de uso. A intenção é manter transparência em relação à utilização hoje feita sem adicionar nenhuma limitação ao sistema.

A rede social tomada por base do estudo foi o *Facebook*, devido sua vasta popularidade. A partir dela foram levantados os seguintes casos de uso:

Informações de contatos

Em toda rede social, algumas informações básicas precisam ser visíveis para que as pessoas possam encontrar seus amigos. Neste ponto a única necessidade é que as informações fiquem visíveis (possam ser decriptografada) por qualquer membro da rede e por ninguém de fora.

Conversas

Existem três tipos de conversas que precisam ser tratadas: as conversas de uma pessoa para uma única outra; conversas onde todos são amigos de todos; e conversas onde nem todos precisam ser amigos uns dos outros. Aqui somente os participantes da conversa poderão visualizar seu conteúdo.

Publicações pessoais

Cada usuário publica em seu mural diversos conteúdos, os quais podem ser compartilhados a todos da rede, a seus amigos, a um grupo determinado de amigos ou mesmo aos seus amigos e aos amigos direto de cada um deles. Aqui também é necessário um controle sobre os comentários da publicação: os comentários dos meus amigos devem ser visíveis aos meus demais amigos.

Publicações em página

Grupos de pessoas, às vezes empresas, organizam propaganda em páginas. Nelas é preciso existir um controle de quem são seus administradores (que terão poder total), moderadores (que podem publicar em nome da página) e os seguidores da página (que poderão visualizar seu conteúdo, avaliá-lo e fazer comentários).

Soluções criptográficas

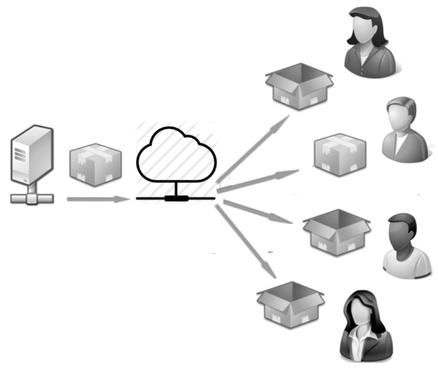
Três conceitos de criptografia foram estudados e são apresentados abaixo

1.Secure broadcast with secure lock

Criptografia de *broadcast* é o conceito criptográfico do envio de um dado de uma entidade central a um subconjunto de indivíduos de um conjunto de participantes do sistema, como mostra a figura 1. Tal conceito é aplicado, por exemplo na distribuição de conteúdo de um servidor de TV a cabo para seus assinantes.

O "secure lock" é uma primeira tentativa de fazer com que em um sistema de *broadcast* não somente a entidade central possa enviar conteúdo, mas que cada participante possa enviar dados a qualquer outro subconjunto de participantes. Para isso ele cria o "lock", que nada mais é do uma "caixa" que contém uma chave de sessão e que poderá ser aberta apenas pelo subgrupo de usuário desejados.

Figura 1: criptografia de broadcast



2. Multi party off the record

O protocolo *OTR messaging* (¨Off The Record Messaging") foi desenvolvido para garantir uma conversa segura entre duas pessoas, simulando um conversa na vida real. Por isso, possui 4 características principais: privacidade, autenticidade, segredo contínuo e negabilidade de autoria. Ele funciona em duas fases: a primeira onde uma troca de chaves garante a autenticidade dos participantes e a segunda onde há uma troca continua de chaves de sessão, que garante o segredo contínuo e a negabilidade de autoria.

O *Multi party OTR* é uma extensão deste protocolo que permite uma conversa com múltiplos usuários, como mostra a figura 2

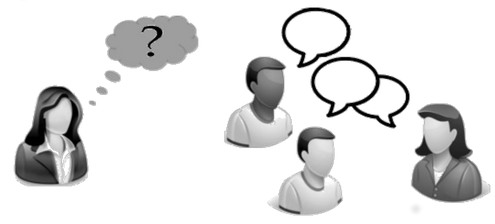


Figura 2: Conversa de múltiplos usuários

3. Criptografia baseada em atributos

Em 1985 Adir Shamir propôs o conceito de criptografia baseado em identidade [2], com a ideia de que cada indivíduo tivesse uma assinatura pública, a época chamada de *smart card*. Assim, qualquer indivíduo poderia criptografar dados e enviar a outro utilizando a assinatura pública do destinatário e assinar qualquer documento utilizando a própria assinatura.

A criptografia baseada em identidade teve em um de seus ramos de desenvolvimento a criptografia baseada em atributos, que apareceu pela primeira vez em 2005 em um trabalho de Adir Shamir e Brent Water [3]. Então a criptografia não mais se baseia em cada indivíduo, mas sim em atributos que serão fornecidos por entidades provedoras de atributos. Existem duas perspectivas possíveis neste caso: a primeira é que cada indivíduo possui uma série de atributos e que os dados criptografados possuem uma política de acesso, deste modo o dado só poderá ser decriptografado por aqueles que possuírem atributos suficientes; e a segunda onde os atributos são colocados nos dados criptografados e os indivíduos possuem as políticas de acesso. A figura 3 exemplifica o caso de um pacote que só pode ser decriptografado por quem possui o atributo "enfermeira".

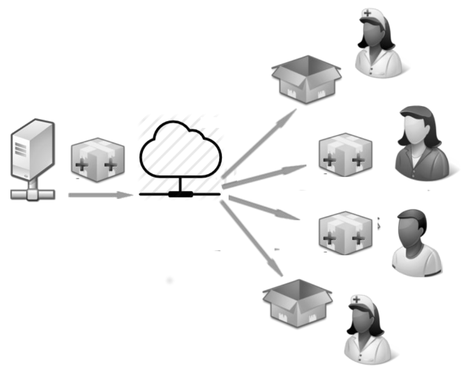


Figura 3: Criptografia baseada em atributos

Conclusão

O Secure lock foi um ponto de partida do estudo por ter sido utilizado no trabalho de Hilder Vitor de Lima, em seu TCC em 2013 [4]. Serviu para o entendimento dos conceitos ligados à criptografia de *broadcast*, o qual permitiu o aprofundamento dos estudos.

O estudo do MPOTR foi muito rico, pois diferente de estudo acadêmicos, seus desenvolvedores buscam os problemas reais levantados no uso cotidiano e sempre levantam os problemas de implementação das tecnologias. Isto é interessante, pois nem sempre o que se consegue no plano teórico se consegue no plano prático. Porém faltam provas matemáticas rigorosas de que seu sistema realmente funciona sem falhas.

Por fim, o estudo da criptografia baseada em atributos foi o que se mostrou mais desenvolvido teoricamente e mais próximo do compartilhamento de informações em redes sociais. Sem dúvida foi o mais enriquecedor para o entendimento dos desafios atuais da criptografia.

Avaliação de soluções para o problema proposto

Com o estudo realizado foi possível concluir que: o "secure lock" não serve ao objetivo do trabalho, que o MPOTR serve parcialmente e que a criptografia baseada em atributos apesar de ainda não servir e estar no campo de desenvolvimento teórico, não de implementação, é o conceito mais promissor do que possa vir a ser usado em um sistema de rede social com provedor de serviço não confiável.

O "secure lock" depende necessariamente de um servidor que distribua as chaves criptográficas. Em outras palavras, seu mecanismo depende da confiança no servidor e por isso não serve ao objetivo almejado por este trabalho.

O MPOTR consegue resolver toda a parte de conversas do nosso estudo de caso de rede social. Isso porque ele foi desenvolvido com tal objetivo e é um protocolo pensado desde o início em sua implementação prática.

A criptografia baseada em atributos poderia resolver todos os demais pontos se contasse com um provedor de serviço confiável ou se na criação já se tivesse todos os participantes interagindo. Muitas limitações deste esquema criptográfico foram, e vêm sendo solucionadas, mas ainda não se atingiu a independência em relação a um (ou mais) servidor central.

Trabalhos futuros

Alguns pontos levantados no estudo merecem destaque e pode servir como trabalhos futuros:

Eficiência dos algoritmos e aplicabilidade

Principalmente pelo estudo feito sobre o MPOTR ficou visível a distância entre os sistemas criptográficos teóricos/acadêmicos e sua aplicabilidade. Verificar a eficiência e usabilidade de cada esquema criptográfico é uma tarefa talvez tão grande quanto desenvolver os algoritmos matemáticos.

Hipóteses dos sistemas criptográficos e seu impacto na implementação computacional.

Juntando a dificuldade de implementar os sistemas e algumas hipóteses por vezes utilizadas em provas matemáticas, temos novo tema de pesquisa. Além disso, muitas vezes não podemos "confiar" no próprio usuário, o que levanta ainda mais a necessidade de levantar com cuidado cada hipótese do sistema.

Estudo do que já foi desenvolvido especificamente para redes sociais

A vasta pesquisa mostrou que muito trabalho já foi feito e muito está sendo desenvolvido. Um trabalho de julho de 2014 (*Secure Data Sharing and Retrieval Using Attribute-Based Encryption in Cloud-Based Online Social Networks* [5]) levanta um pouco do seu estágio de desenvolvimento e coloca a continuidade dos estudo para o tema proposto por este trabalho de conclusão de curso.

Referências bibliográficas: [1] g1.globo.com (2014), <http://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html> Acesso em 20/08/2014. [2] A. Shamir, (1985) Identity-based cryptosystems and signature schemes – Em Proceedings of CRYPTO 84 on Advances in cryptology, pp 47–53. Springer-Verlag New York, Inc., 1985. [3] A. Sahai e B. Waters, (2005) Fuzzy Identity-Based Encryption - Advances in Cryptology – EUROCRYPT 2005, pp 457-473. [4] Perreira, H. V. L.(2013) Um sistema de criptografia de broadcast para navegadores de internet - <https://bcc.ime.usp.br/principal/tccs/2013/vitor> Acesso em 27/03/2014. [5] HUANG, Q., MA, Z., YANG, Y., FU, J., & NIU, X. (2014) Secure Data Sharing and Retrieval Using Attribute-Based Encryption in Cloud-Based OSNs – Chinese Journal of Electronics, 23(3)