Análise de criptografia fim-a-fim em serviços de mensagens instantâneas para aplicações corporativas

RESUMO EXPANDIDO - Disciplina de TCC290009

Kristhine Schaeffer Fertig
Estudante do Curso de Engenharia de Telecomunicações

Emerson Ribeiro de Mello
Professor orientador

Semestre 2018-1

Resumo- *Nos últimos 10 anos, a Internet e a comunicação móvel têm reformulado intensamente a forma como vivemos e nos comunicamos no dia a dia. Surgem então uma infinidade de sistemas e aplicações voltadas à comunicação multimídia em tempo real e instantânea. Para uma aplicação de mensagens instantâneas (IM) de única finalidade, independente de sua utilização em âmbito popular ou organizacional, novos métodos e protocolos já são desenvolvidos para cenários Web e Móvel. Tais serviços possuem ainda a característica de interoperabilidade e multiplataforma, sendo na maioria das vezes apresentados de forma distribuída. Assim, com este aumento da interconectividade, do número de usuários e da variedade de dados transmitidos, cresce cada vez mais a preocupação com a segurança dos dados e privacidade dos usuários de tais serviços. Este trabalho tem como objetivo analisar as principais ferramentas e os atuais cenários adotados no mercado de serviços de mensagens instantâneas. Será realizado um comparativo de tais tecnologias atentando-se à aplicação de criptografia fim-a-fim com a finalidade de garantir a privacidade dos usuários e segurança de seus respectivos dados. Propõe-se ainda apresentar uma solução de estrutura básica para um serviço IM com segurança de ponta-a-ponta (E2E). Por fim, a proposta é implementada a fim de fornecer prova de conceito e avaliar a dificuldade técnica de satisfazer os requisitos de segurança e privacidade estipulados na transmissão de informações classificadas em um ambiente de uso corporativo.*

Palavras-chave: Mensagens Instantâneas. Criptografia. Fim-a-Fim.

1 Introdução

Nesta era atual, caminhando-se para a aplicação real da Internet das Coisas e com os demais estudos de novas gerações de comunicações móveis, o requisito básico exigido por milhares de usuários é a conectividade de múltiplos dispositivos conectados sob uma única estrutura de comunicação. Essa comunicação unificada está evoluindo a cada dia, fazendo com que sua presença seja sentida em vários cenários como na exibição de informações de presença, de texto e vídeo através de mensagens instantâneas etc. Dessa forma, o principal serviço que possibilita essa agilidade e interoperabilidade na comunicação é o serviço de sistemas IM (*Instant Messaging*). Ele permite que os clientes obtenham dados por meio de vários canais de informações, proporcionando assim uma entrega de mensagens mais rápida. Estudos recentes apontam ainda que tal tecnologia está sendo amplamente acessada através de dispositivos móveis e utilizada ainda mais na esfera Web, onde a mobilidade e a conectividade apresentam-se como fortes requisitos.

Essas características fazem com que tal serviço seja usado tanto no âmbito popular quanto no âmbito organizacional, onde empresas possuem um ritmo acelerado visando a entrega de soluções e suporte para clientes a um nível internacional. No entanto, tratando-se de um ambiente corporativo, onde informações classificadas de suas soluções transitam a todo instante, surgem preocupações relacionadas à segurança e privacidade das informações e usuários. Uma grande questão, por exemplo, é a preocupação com a corrupção de dados durante o fluxo de informações através da rede.

Por isso, a aplicação de sistemas de mensagens instantâneas criptografadas é primordial em tais cenários. Porém, a simples utilização de criptografia aplicada no envio de mensagens entre servidores e clientes web/móveis não é suficiente (MUJAJ, 2017). A tecnologia TLS (DIERKS, 2008), tomando como exemplo, garante a segurança destes dados contra a invasão de terceiros que queiram interceptar o fluxo de informação. No entanto, o administrador de tais sistemas IM, estes armazenados em servidores locais, pode estar autorizado a interceptar e visualizar a troca de informações confidenciais. Portanto, nestes casos, é de suma importância a aplicação da criptografia E2E (Fim-a-Fim), onde as mensagens são transitadas e armazenadas em todo momento de forma cifrada. Por fim, os dados são somente decifrados e corretamente visualizados nas pontas do sistema IM, onde estarão presentes os usuários participantes das conversas em questão (STALLINGS, 2014).

Dessa forma, este trabalho visa a análise dos demais esquemas de criptografia e seus protocolos disponíveis atualmente no mercado de serviços de mensagens instantâneas. Tem-se como objetivo realizar um comparativo de tais tecnologias atentando-se à aplicação de criptografia fim-a-fim com a finalidade de garantir a privacidade dos usuários e a segurança de seus respectivos dados. Propõe-se ainda apresentar uma solução de estrutura básica para um serviço IM com segurança ponta-a-ponta (E2E). Por fim, a proposta é implementada a fim de fornecer prova de conceito e avaliar a dificuldade técnica de satisfazer os requisitos de segurança e privacidade estipula-

dos na transmissão de informações classificadas em um ambiente de uso corporativo. Para atingir o objetivo principal deste estudo, os seguintes objetivos e métodos foram definidos:

- Estudar e compreender o funcionamento de padrões de criptografia aplicados a sistemas de mensagens instantâneas;
- Revisar a aplicação de gerenciadores de notificações e fila de mensagens no contexto de sistemas IM;
- Analisar os protocolos de aplicações e serviços IM mais consolidados no mercado atual;
- Realizar comparativo das ferramentas estudadas;
- Conceber uma proposta como prova de conceito de um sistema IM com criptografia ponta-a-ponta;

2 Metodologia

Quanto à metodologia científica (VIANELLO, 2013) aplicada neste trabalho, tem-se o uso da pesquisa aplicada e descritiva, porém de caráter exploratório, partindo da revisão bibliográfica e análise de exemplos práticos com a finalidade de estabelecer uma nova configuração quanto à criptografia aplicada em sistemas de mensagens instantâneas.

A abordagem adotada utiliza-se do método dedutivo, na forma quali-quantitativa, através da análise dos dados coletados, ou seja, das características principais das tecnologias de protocolos e criptografia em uso nos serviços IM. Busca-se ainda os conceitos e relações entre essas ferramentas, resultando em um comparativo para então identificar a melhor proposta de um sistema IM criptografado de ponta-a-ponta. Os resultados numéricos e valorativos são então obtidos levando-se em conta os requisitos de usabilidade e segurança de um cenário de aplicação corporativo.

Em relação aos procedimentos técnicos, esses estão classificados em: pesquisa bibliográfica em sua maioria, assim como documental, analisando-se documentos informativos e referenciais dos devidos protocolos e plataformas estudados; e pequenos estudos de casos das principais ferramentas atualmente em uso nos serviços de mensagens instantâneas criptografadas.

Em um primeiro momento, será realizada um revisão bibliográfica integrativa, buscando-se a contextualização no assunto de comunicações instantâneas e padrões de criptografia, como por exemplo, criptografia simétrica e de chave pública (STALLINGS, 2014). A partir de então será estudado o conceito de fila de mensagens e suas principais ferramentas utilizadas em serviços de mensagens instantâneas, como por exemplo, RabbitMQ. As plataformas de gerenciamento de notificações/mensagens na nuvem também serão abordadas neste trabalho, apresentando as suas características para diferentes sistemas operacionais Android e iOS. Tais ferramentas e tecnologias

são essenciais na concepção de um sistema IM, que necessite realizar a comunicação entre dispositivos móveis e ambientes web de forma distribuída. Após a descrição destes conceitos, será tratada a pesquisa de trabalhos relacionados, já presentes e aplicados no mercado de comunicação instantânea, como as aplicações Signal, Telegram, WhatsApp, assim como outras de menor visibilidade, mas de igual importância técnica, como Rocket.Chat, e demais plataformas *open source*, como OpenFire e MongooseIM. Por fim, um resumo comparativo será descrito para permitir então identificar a melhor proposta de solução de um sistema de mensagens instantâneas com criptografia fim-a-fim, para ambientes web e mobile.

3 Resultados e Discussão

4 Considerações Parciais/Finais

Referências

DIERKS, T. *The Transport Layer Security (TLS) Protocol Version 1.2*. [S.l.]: RFC 5246, 2008.

MUJAJ, A. *A Comparison of Secure Messaging Protocols and Implementations*. [S.l.]: Master Thesis, University of Oslo, 2017.

STALLINGS, W. *Criptografia e segurança de redes: princípios e práticas*. [S.l.]: São Paulo: Pearson Prentice Hall, 2014.

VIANELLO, L. P. *Métodos e Técnicas de Pesquisa*. [S.l.]: EAD - Educação a Distância, 2013.