Avaliação de técnicas para melhoria da privacidade de usuários de nuvens ownCloud usando certificados digitais.

Marcela H. R. Sgavioli*, Marco A. A. Henriques

Resumo

O presente trabalho objetiva implementar, validar e avaliar os protocolos criptográficos em desenvolvimento no Departamento de Engenharia de Computação e Automação Industrial (DCA) da FEEC/Unicamp de maneira a permitir, de forma simples e intuitiva, a criptografia de dados e dar ao usuário um controle eficaz sobre a segurança e o sigilo de seus arquivos armazenados na nuvem.

Palavras-chave:

Computação em nuvens, segurança de dados, certificação digital.

Introdução

Visando proporcionar uma maior segurança para os dados e mais privacidade e confiança aos usuários de serviços de armazenamento em nuvens, é necessário oferecer recursos de segurança baseados nas mais avançadas técnicas de proteção disponíveis, destacando-se entre elas a criptografia¹.

Alguns softwares de armazenamento em nuvem disponibilizam serviços de criptografia que são simples de usar, mas, ao mesmo tempo, são questionados por realizar a criptografia no lado do servidor e gerenciar as chaves criptográficas de seus usuários. Esta prática pode ser mais simples de implementar e pode apresentar menor sobrecarga aos usuários (estes não terão que gerenciar suas chaves), mas coloca o provedor de serviço de nuvem em uma posição privilegiada em relação aos dados de seus usuários, o que pode gerar desconfortos e suspeitas de violação de sigilo.

Tendo em vista esse cenário, torna-se necessário o investimento em protocolos criptográficos para fornecer ao usuário um maior controle sobre a segurança de seus dados e arquivos armazenados na nuvem.

Resultados e Discussão

O estudo sobre a segurança de dados foi baseado, inicialmente, na leitura de artigos científicos e livros sobre o tema, dando ênfase à criptografia. Posteriormente, as atividades prosseguiram com a participação da aluna no grupo de estudos sobre segurança chamado ReGrAS², formado pelos pesquisadores e desenvolvedores da equipe de pesquisa do Professor orientador.

A aluna iniciou as atividades recebendo instruções e informações de como organizar o trabalho, montando um modelo de utilização de um software criptográfico, estudando possíveis casos de teste e estruturando um protótipo de acesso do programa (Figura 1).

A aluna, então, iniciou sua familiarização com os conceitos necessários a partir da aplicação prática dos mesmos em diferentes linguagens de programação com as quais estava mais familiarizada antes de iniciar o projeto em Java. Os principais temas estudados foram: funções hash, criptografia simétrica e criptografia assimétrica.

Figura 1. Menu de acesso principal do programa.

Conclusões

O projeto proporcionou a aluna grande conhecimento sobre a área da segurança de informação, criptografia e armazenamento em núvens, além de instigar a curiosidade e apresentar grandes fontes de informação para o desenvolvimento de atividades nesse ramo da computação.

A aluna interropeu o projeto no mês de abril. Todas as atividades desenvolvidas até então podem ser encontradas na webpage do grupo ReGrAS².

¹ Sashank Dara, "Cryptography Challenges for Computational Privacy in Public Clouds", ePrint Archives, <https://eprint.iacr.org/2013/272.pdf>, último acesso 03/07/2016

² ReGrAS: Research Group on Applied Security, file sharing, meeting schedule, <http://calhau.dca.fee.unicamp.br/wiki/index.php/ReGrAS:Espace>, último acesso 03/07/2016