UNIVERSIDADE FEDERAL DE PERNAMBUCO

GRADUAÇÃO EM CIÊNCIAS DA COMPUTAÇÃO
CENTRO DE INFORMÁTICA

2013.2

Um estudo sobre criptografia baseada em atributos

PROPOSTA DE TRABALHO DE GRADUAÇÃO

Aluno – Marcos Vinícios da Silva Machado (mvsm@cin.ufpe.br)
Orientador – Djamel Fawzi Hadj Sadok (djamel@cin.ufpe.br)

29 de Novembro de 2013

Índice

Contexto

Criptografia baseada em atributos é um esquema de criptografia de chave pública proposto em 2005 por Sahai e Waters[1], no qual os atributos tem uma importância fundamental. Esse modelo tem como principal característica a utilização de atributos na geração das chaves ou geração do cifrotexto para controle de políticas de acesso a dados criptografados. Os esquemas criptográficos mais atuais baseados em atributos, além de permitirem um rico controle de políticas, não existe a necessidade de utilização dos certificados de chave pública na infraestrutura tradicional.

[1] A. Sahai and B. Waters, "Fuzzy identity based en-cryption," Advances in Cryptology V EUROCRYPT,vol. 3494 of LNCS, pp. 457-473, 2005.

Objetivo

O objetivo deste trabalho é estudar e analisar o estado da arte desse novo paradigma criptográfico e os seus mais váriados esquemas, nos quais se uni encriptação e atributos, criando assim um leque de novas possibilidades que vão desde políticas de acesso até o uso para classificação de informação.

Cronograma

Atividade	Novembro				Dezembro				Janeiro				Fevereiro			
Pesquisa e levantamento bibliográfico																
Proposição dos cenários																
Elaboração do relatório																
Elaboração da Apresentação																

Referências Bibliográficas

[1] A. Sahai and B. Waters, Fuzzy identity based en-cryption," Advances in Cryptology V EUROCRYPT,vol. 3494 of LNCS, pp. 457-473, 2005.

Datas e Assinaturas

29 de Novembro de 2013

Djamel Fawzi Hadj Sadok
(orientador)

Marcos Vinícios da Silva Machado
(proponente)