MAC 5701 - Tópicos em Ciência da Computação
Departamento de Ciência da Computação
Primeiro semestre de 2003

Plano de Estudo

Aluno: Fábio Correa Xavier
fabiocx@ime.usp.br
Orientador: Prof. PhD Routo Terada

1 Objetivo

O assunto a ser abordado na dissertação de mestrado do aluno é a associação de uma Privilege-key Infrastructure (PKI) terceirizada à uma Privilege Management Infrastructure (PMI) controlada pela própria empresa. A dissertação abordará o uso de uma estrutura para autorização (PMI) diferente da estrutura utilizada para autenticação de usuários (PKI).

Os serviços de autenticação de usuários geralmente são fornecidos pelas Public Key Infrastructures (PKI). Estes serviços não satisfazem as necessidades que surgiram com o advento e crescimento das aplicações de comércio eletrônico. Tais aplicações necessitam de informações sobre serviços de autorização, que indicam o que cada usuário pode fazer no sistema.

Neste cenário, certificados de atributos (attribute certificates) propostos pela ITU-T (International Telecommunications Union) através da recomendação X-509 [1] surgiram como uma potencial solução para o problema. Os certificados de atributos foram projetados para serem utilizados em conjunto com os certificados de identidade, que garantem o serviço de autenticação de usuários. Os serviços de autenticação baseados em certificados de identidade só são implementáveis através do uso de uma Public-Key Infrastructure (PKI) [2].

Por sua vez, um serviço de autorização baseado em certificados de atributos também deve possuir uma infra-estrutura capaz de dar confiabilidade e eficiência ao serviço. Esta infra-estrutura é a Privilege Management Infrastructure (PMI).

Como a PKI e a PMI são estruturas independentes que fornecem serviços complementares, os certificados de identidade e os certificados de

atributos são inter-relacionados através de alguma informação comum e unívoca existente nos certificados.

Este relacionamento é justificado pelo fato de que o serviço de autorização confia no certificado de identidade para provar que o usuário é realmente quem ele diz que é, não se preocupando em autenticar o usuário.

A proposta do trabalho de dissertação do aluno é apresentar um *framework* que viabilize o cenário no qual as empresas que terceirizaram a PKI, decidiram manter sob seu controle a PMI. Tal proposta é baseada no fato de que a "identidade" tende a ter um significado global; assim os certificados de identidade podem ser emitidos por Autoridades Certificadoras (CA) externas à organização.

Por outro lado, um "atributo" tende a ter um significado local. Os privilégios são usados em ambientes internos às organizações. Com isso, uma Autoridade Certificadora pode não ter todas as informações necessárias para decidir o que um usuário pode ou não pode fazer. Neste caso, é razoável pensar que alguém do corpo funcional da empresa é quem decide sobre privilégios e, conseqüentemente, emite o certificado de atributos correspondente.

O objetivo deste plano de estudo é aprofundar o conhecimento do aluno sobre funcionamento das Public-Key Infrastructure (PKI) e também das Privilege Management Infrastructure (PMI).

2 Tópicos Selecionados

Como primeiro passo para desenvolver o trabalho proposto, o aluno deverá conhecer os conceitos, padrões e considerações de implementação de uma PKI [2] [3].

Em seguida, o mesmo estudo deverá ser feito em relação aos certificados X.509 [3] [4] e a PMI. [3] [5].

3 Cronograma

01/04 - 17/04 PKI
22/04 - 09/05 X.509
12/05 - 30/05 PMI

02/06 - 16/06 Elaboração do Relatório

4 Referências

[1]. ITU-T Recommendation X.509, “Information Technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks”, Março 2000

[2]. C. Adams, S. Lloyd, “Understanding Public-key Infrastructure: Concepts, Standards and Deployment Considerations”, New Riders, 1999

[3] . Pesquisas na Internet.

[4] . D. Chadwick, “An X.509 Role-based Privilege Management Infrastructure”, Bussiness Briefing: Global Infosecurity, 2002.

[5] . E. Dawson, J. Lopez, J. A. Montenegro, “A New Design of Privilege Management Infrastructure for Organizations Using Outsourced PKI”, 2002