



E198

INTEGRAÇÃO DE UMA INFRA-ESTRUTURA DE CHAVES PÚBLICAS AO SLM.

Eduardo Fernandes Piva (Bolsista PIBIC/CNPq) e Prof. Dr. Paulo Lício de Geus (Orientador), Instituto de Computação - IC, UNICAMP

O IPSec é um protocolo que tem como objetivo prover segurança através de dois cabeçalhos, o AH e o ESP. Esta segurança é realizada através do estabelecimento de associações de segurança através do protocolo IKE, utilizando políticas pré-estabelecidas na configuração do IPSec. Estes parâmetros de segurança são complexos de serem mantidos e por isso surgiu o projeto SLM, que visa simplificar a manutenção e configuração de uma rede utilizando uma base LDAP para o armazenamento das políticas de segurança e alguns módulos de traduções de políticas de alto nível para políticas de baixo nível. Para que o sistema se torne mais seguro, é necessário que haja uma autenticação das máquinas. Tal autenticação pode ser obtida de forma segura e confiável através de uma infra-estrutura de chaves pública, que pode ser integrada na mesma base LDAP que o SLM, centralizando ainda mais a configuração do sistema. Através desta integração, foi possível garantir uma maneira mais eficiente e mais escalável de autenticação, visto que a confiança entre as máquinas deixou de ser através de um segredo pré-compartilhado.

PKI - LDAP - IPSEC