2011 XIX congresso interno de iniciação científica

T1113

PROPOSTA DE MECANISMOS DE ASSINATURA DIGITAL E AUTENTICAÇÃO BASEADOS NO CARTÃO UNIVERSITÁRIO INTELIGENTE E NA INFRAESTRUTURA DE CHAVES PÚBLICAS DE ENSINO E PESQUISA ICPEDU

Mateus José Figueiredo Lara (Bolsista PIBITI/CNPq) e Prof. Dr. Marco Aurelio Amaral Henriques (Orientador), Faculdade de Engenharia Elétrica e de Computação - FEEC, UNICAMP

Neste trabalho aprofundamos os estudos sobre a aplicação de ferramentas de software livre nos chips criptográficos presentes nos cartões inteligentes (smartcards) já em uso na universidade para assinatura digital e autenticação. Para isto, foi feita uma revisão detalhada sobre estes cartões, incluindo a plataforma de software Java Card e princípios de criptografia e segurança de redes, onde foi possível uma familiarização com certificados digitais e suas aplicações. Durante todo o desenvolvimento do trabalho, buscaram-se alternativas abertas, utilizando o projeto M.U.S.C.L.E. e a plataforma OpenSC, que permitem o uso do cartão pelo sistema operacional. Inicialmente procurou-se ampliar para outras combinações de aplicativos/SO os experimentos já realizados em trabalhos anteriores, tais como geração de certificados e envio de e-mails assinados digitalmente utilizando o cartão. Em seguida foram feitos experimentos com diferentes configurações dos programas (aberto e proprietário) instaladas no cartão, nos sistemas operacionais mais comumente usados, Linux e Windows, a fim de viabilizar a criação de assinaturas digitais em documentos da forma mais segura possível e estabelecer uma nova funcionalidade para o cartão, que é o acesso (logon) controlado por certificados digitais (e, portanto, mais seguro) aos sistemas operacionais. Os resultados obtidos comprovam a viabilidade de se empregar o cartão universitário para aumentar a segurança de processos de trabalho.

Smart card - Certificação digital - Assinatura digital