



ESCOLA POLITÉCNICA DA UNIVERSIDADE DE SÃO PAULO

Departamento de Engenharia de Computação e Sistemas Digitais

SSMS – Aplicativo de SMS Seguro *Press Release*

Estudantes de Engenharia de Computação da Poli-USP desenvolvem sistema para fornecer serviços de segurança nas transações via mensagens curtas, ou SMS, de maneira mais econômica e eficiente.

São Paulo, 11 de Novembro de 2008

Os estudantes Eduardo de Souza Cruz, Geovandro Carlos C. F. Pereira e Rodrigo Rodrigues da Silva, formandos em Engenharia de Computação (Cooperativo) da Escola Politécnica da Universidade de São Paulo, desenvolveram o sistema como parte de seu Projeto de Formatura, necessário para a conclusão do curso. O grupo foi orientado pelo Prof. Dr. Paulo S. L. M. Barreto, docente do Laboratório de Arquitetura e Redes de Computadores e especialista em segurança.

O SMS Seguro foi projetado para fornecer serviços de segurança nas transações via mensagens curtas de celular, ou SMS. O sistema permite que usuários comuns, empresas, bancos e operadoras de celular trafeguem suas mensagens de modo a garantir a autenticidade, integridade e confidencialidade do serviço.

A adoção da Criptografia Baseada em Curvas Elípticas possibilitou o desenvolvimento de uma solução com chaves de tamanho reduzido e auto-certificadas, garantindo velocidade e economia de banda nas transações em dispositivos móveis, ambiente de recursos tipicamente escassos.

No desenvolvimento do projeto foi gerado um novo protocolo de segurança, denominado BDCPS. Trata-se de uma técnica criptográfica mais eficiente e econômica que mescla o uso de criptografia baseada em identidades com técnicas convencionais, aproveitando pontos positivos de cada abordagem. Até o momento, o trabalho gerou dois artigos científicos publicados nos anais do Simpósio Brasileiro de Segurança da Informação, sendo que um deles recebeu menção honrosa na cerimônia de premiação do evento.

O sistema é implementado na linguagem de programação Java e pode ser utilizado em qualquer telefone celular que possua ambiente JavaME. O aplicativo pode ser obtido em: <http://secure-sms.googlecode.com>.

Contato:

Eduardo de Souza Cruz <eduardo.cruz@poli.usp.br>

Geovandro Carlos C. F. Pereira <geovandro.pereira@poli.usp.br>

Rodrigo Rodrigues da Silva <rodrigo.silva1@poli.usp.br>

Prof. Dr. Paulo S. L. M. Barreto (orientador) <pbarreto@larc.usp.br>