PCS2040 – Projeto de Formatura I

Aplicativo Seguro de SMS

Especificação Inicial

Eduardo de Souza Cruz
Geovandro Carlos Pereira
Rodrigo Rodrigues da Silva
Orientador: Prof. Dr. Paulo S. L. M. Barreto

Agenda

- Objetivo
- Motivação
- Especificação Funcional
- Cronograma
- Recursos e Infra-Estrutura
- Referências

Objetivo

- **Implementar uma arquitetura que permita o envio de mensagens SMS de forma segura**
- Solução completa: criptografia nas mensagens, assinatura digital, geração e substituição de chaves
- Modelo de negócio: solução adaptável ao ambiente do cliente, seja ele final ou intermediário

Motivação

- Ausência de soluções no mercado nacional
  - Mensagens podem ser interceptadas por funcionários ou usuários maliciosos
  - Operações bancárias tornam-se inseguras
- Utilização de novas tecnologias de criptografia
- Desenvolvimento em dispositivos embarcados

Especificação Funcional

- Troca de mensagens seguras cliente-cliente e cliente-servidor
- Algoritmos de emparelhamento
- Sistema modular
  - Software embarcado
  - Software servidor central
  - Software interface bancária (exemplo de aplicação)

Especificação Funcional

- Envio de mensagem encriptada de A para B
  - A encripta a mensagem com chave pública de B
  - B decripta a mensagem com sua chave privada
- Envio de mensagem assinada de A para B
  - A assina a mensagem com sua chave privada
  - B verifica a validade da mensagem com a chave pública de A

Especificação Funcional

- Chave pública
  - Número de celular do usuário
  - Dispensa serviço de catálogo
- Chave privada
  - Método que facilita a memorização
  - Gerada por autoridade central
  - Menor que chaves usuais

Cronograma

- 26/02 - Entrega deste documento contendo a especificação inicial do projeto
- 18/03 - Evolução da especificação, e resultados de pesquisas referentes a algoritmos e bibliotecas utilizadas
- 04/04 - Especificação final do projeto, contendo a descrição de todas as funcionalidades, requisitos, casos de uso e protótipos.

Recursos e Infra-estrutura

- Plataforma: Java 2 ME
- Biblioteca: ”Bouncy Castle”
- Ambiente: Eclipse, Plugins, Sun Wireless Toolkit
- Hardware
  - Celulares compatíveis com Java
  - Servidor central/bancário

Referências

- R. Rivest. Selected Topics in Cryptography. Lecture 26. 2004
- Securing your J2ME/MIDP apps. Disponível em http://www.ibm.com/developerworks/library/j-midpds.html. Acesso em 25 fev. 2008.
- Terence Spies on Identity-Based Encryption. Disponível em http://www.onlamp.com/pub/a/onlamp/2003/07/17/ibe.html. Acesso em 25 fev. 2008.

Dúvidas?