Sistema de SMS Seguro
PCS2050 - Projeto de Formatura II
Apresentação Final

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

Departamento de Engenharia de Computação e Sistemas Digitais
Escola Politécnica da Universidade de São Paulo

São Paulo, 09/12/2008

Agenda

1. Introdução
2. Necessidade
3. Solução
4. Conclusão

Motivação e Cenário

- Crescimento do uso do SMS no mundo:

Motivação e Cenário

- Crescimento do uso do SMS no mundo:

  2,3 trilhões de mensagens em 2010 (previsão)

Motivação e Cenário

- Crescimento do uso do SMS no mundo:

  2,3 trilhões de mensagens em 2010 (previsão)

- Plataforma leve e barata, com grande base de usuários:

Motivação e Cenário

- Crescimento do uso do SMS no mundo:

  2,3 trilhões de mensagens em 2010 (previsão)
- Plataforma leve e barata, com grande base de usuários:

  2,4 bilhões de pessoas

Motivação e Cenário

- Crescimento do uso do SMS no mundo:

  2,3 trilhões de mensagens em 2010 (previsão)
- Plataforma leve e barata, com grande base de usuários:

  2,4 bilhões de pessoas
- Diversas oportunidades econômicas:

Motivação e Cenário

- Crescimento do uso do SMS no mundo:

  2,3 trilhões de mensagens em 2010 (previsão)
- Plataforma leve e barata, com grande base de usuários:

  2,4 bilhões de pessoas
- Diversas oportunidades econômicas:

  72,5 bilhões de dólares para operadoras em 2006

Motivação e Cenário

- Crescimento do uso do SMS no mundo:

  2,3 trilhões de mensagens em 2010 (previsão)
- Plataforma leve e barata, com grande base de usuários:

  2,4 bilhões de pessoas
- Diversas oportunidades econômicas:

  72,5 bilhões de dólares para operadoras em 2006
- Possibilidade de produzir pesquisa: inovação

Objetivos

”

Projetar, implementar e implantar um sistema capaz de prover confidencialidade, integridade e autenticidade ao serviço de *SMS* sem extrapolar as limitações de recursos típicas do ambiente.”

Metodologia

- Estudo do cenário, detalhamento do problema e levantamento de requisitos

Metodologia

- Estudo do cenário, detalhamento do problema e levantamento de requisitos
- Estudo de esquemas de segurança em busca de uma solução adequada ao problema

Metodologia

- Estudo do cenário, detalhamento do problema e levantamento de requisitos
- Estudo de esquemas de segurança em busca de uma solução adequada ao problema
- Projeto, implementação e testes

Agenda

1 Introdução

2 Necessidade

3 Solução

4 Conclusão

Aplicações Potenciais

- Comunicação interpessoal

Aplicações Potenciais

- Comunicação interpessoal
- Transações bancárias e pagamentos

Aplicações Potenciais

- Comunicação interpessoal
- Transações bancárias e pagamentos
- Comunicação corporativa e governamental sigilosa

Aplicações Potenciais

- Comunicação interpessoal
- Transações bancárias e pagamentos
- Comunicação corporativa e governamental sigilosa
- Monitoração remota

Serviços de Segurança

- Confidencialidade

Serviços de Segurança

- Confidencialidade
- Integridade

Serviços de Segurança

- Confidencialidade
- Integridade
- Autenticidade

Serviços de Segurança

- Confidencialidade
- Integridade
- Autenticidade
- Irretratabilidade

Definição do Problema

- SMS armazenado em aberto nas integradoras e operadoras

Definição do Problema

- SMS armazenado em aberto nas integradoras e operadoras
- Recursos limitados: processamento, memória, largura de banda

Definição do Problema

- SMS armazenado em aberto nas integradoras e operadoras
- Recursos limitados: processamento, memória, largura de banda
- Algoritmo *A5* da rede *GSM* quebrado

Definição do Problema

- SMS armazenado em aberto nas integradoras e operadoras
- Recursos limitados: processamento, memória, largura de banda
- Algoritmo *A5* da rede *GSM* quebrado
- Poucas soluções de segurança no mercado

Definição do Problema

- SMS armazenado em aberto nas integradoras e operadoras
- Recursos limitados: processamento, memória, largura de banda
- Algoritmo *A5* da rede *GSM* quebrado
- Poucas soluções de segurança no mercado
- *RSA*: cerca de *15 mensagens* para trocar *um* certificado

Definição do Problema

- SMS armazenado em aberto nas integradoras e operadoras
- Recursos limitados: processamento, memória, largura de banda
- Algoritmo *A5* da rede *GSM* quebrado
- Poucas soluções de segurança no mercado
- *RSA*: cerca de *15 mensagens* para trocar *um* certificado
- Algoritmos simétricos: grande quantidade de senhas

Métricas e Requisitos

- Tempo de espera

Métricas e Requisitos

- Tempo de espera
- Espaço útil da mensagem

Métricas e Requisitos

- Tempo de espera
- Espaço útil da mensagem
- Tamanho da chave

Métricas e Requisitos

- Tempo de espera
- Espaço útil da mensagem
- Tamanho da chave
- *Overhead* do protocolo

Agenda

1 Introdução

2 Necessidade

3 Solução

4 Conclusão

Especificação

Especificacao

Arquitetura

Arquitetura

Implementação

- Curvas elípticas

Implementação

- Curvas elípticas
- Chaves menores

Implementação

- Curvas elípticas
- Chaves menores
- Criptografia auto-certificada

Implementação

- Curvas elípticas
- Chaves menores
- Criptografia auto-certificada
- Criptografia baseada em identidades

Implementação

- Curvas elípticas
- Chaves menores
- Criptografia auto-certificada
- Criptografia baseada em identidades
- Gerenciamento de chaves simplificado

Resultados

res

Agenda

1. Introdução
2. Necessidade
3. Solução
4. Conclusão

Conclusão

concl

aplic

pesq

Desenvolvimentos futuros

fut

Referências

fut

Contato

Site do projeto

http://secure-sms.googlecode.com

E-mail

secure-sms@googlegroups.com

Agenda

This is a short introduction to Beamer class.

Motivação

Motivação

- Beamer is a wonderful class

Motivação

- Beamer is a wonderful class
- One can make animations

Motivação

- Beamer is a wonderful class
- One can make animations
- One uses the **pause** command, for example

Motivação

- Beamer is a wonderful class
- One can make animations
- One uses the **pause** command, for example
- in order to bring in important ideas

This is a short introduction to Beamer class.

Introduction

Introduction

- appears from slide 2 on
- appears from slide 2 to slide 4

Introduction

- appears from slide 2 on
- appears from slide 2 to slide 4

- appears from slide 3 on

Introduction

- appears from slide 2 on
- appears from slide 2 to slide 4
- appears on slide 4
- appears from slide 3 on

Introduction

- appears from slide 2 on
- appears from slide 3 on
- 5

Conclusão

- L

Conclusão

- L
- A

Conclusão

- L
- A
- T

Conclusão

- L
- A
- T
- E

Conclusão

- L
- A
- T
- E
- X

- Language used by Beamer: L TEX
- Language used by Beamer: LTEX

- Language used by Beamer: LATEX
- Language used by Beamer: LATEX

appear from slide 2 on

appear from slide 2 on

appears from 3 to slide 4

appears from slide 3 on

appear from slide 2 on
appears from 3 to slide 4
appears on slide 4
appears from slide 3 on

Block title

This is a block in blue

Alert-block title

This is a block in red

Example-block title

This is a block in green