Construção de um Sistema de SMS Seguro

Eduardo de Souza Cruz, Geovandro C. F. Pereira,
Rodrigo Rodrigues da Silva, Paulo S. L. M. Barreto

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

Agenda

- Objetivos
- Cenário
- Requisitos
- Proposta inicial
- Esquema adotado
- Conclusão

Agenda

- Objetivos
- Cenário
- Requisitos
- Proposta inicial
- Esquema adotado
- Conclusão

Objetivos

- Prover confidencialidade, integridade e autenticidade a mensagens curtas trafegadas pela rede de telefonia celular GSM
- Adequação a limitações de banda e de recursos computacionais típicos desse meio
- Garantir a usabilidade

- Projeto de pesquisa em andamento
- Entrega prevista para dezembro/2008

Agenda

- Objetivos
- Cenário
- Requisitos
- Proposta inicial
- Esquema adotado
- Conclusão

Cenário

- Crescente uso da tecnologia SMS em diversos segmentos de negócios
- SMS Centers: mecanismo *store-and-forward*
- Mensagens armazenadas sem criptografia
- Conteúdo das mensagens está sujeito ao acesso de funcionários das operadoras e eventuais invasores de seus sistemas
- Privacidade do usuário é prejudicada

Cenário

”One of the more high profile victims of such an attack in recent years was England football captain David Beckham, whose SMS exchange with his personal assistant Rebecca Loos was intercepted and published in a tabloid. Two employees from European phone operator mmO2 were dismissed for helping their friend obtain copies of his girlfriend’s SMS messages.”

(Ng, 2006)

Cenário

- Por outro lado, apesar de seus benefícios, o uso da tecnologia SMS fica comprometido em aplicações críticas quanto à segurança da informação:
  - Transações bancárias
  - Comércio eletrônico
  - Comunicação sigilosa (governo, militar, corporativa)
  - Telemetria de consumo (luz, gás, água)
  - *Mobile Business* e *Mobile Marketing*

Soluções atuais

- Criptografia simétrica
- Criptografia assimétrica

RSA

- Solução amplamente utilizada em ambientes convencionais
- Certificados de até 4KB e chaves de 1024 bits

Mas

- SMS: apenas 160 caracteres por mensagem
- Setup inicial: 15 a 30 mensagens por destinatário para troca de certificados
- Overhead do algoritmo, de 256 bytes, sequer cabe na mensagem!

Agenda

- Objetivos
- Cenário
- Requisitos
- Proposta inicial
- Esquema adotado
- Conclusão

Requisitos

- Tempo de espera e usabilidade: sistema deve ser transparente ao usuário
- Portabilidade: equipamentos móveis utilizam diversos processadores e sistemas operacionais
- Eficiência: recursos computacionais escassos
- Uso de banda e espaço na mensagem: limitações da rede celular

Agenda

- Objetivos
- Cenário
- Requisitos
- Proposta inicial
- Esquema adotado
- Conclusão

Proposta inicial

- BLMQ (Barreto et al. 2005)
- Baseado em identidades: dispensa a existência de uma PKI (Public Key Infrastructure)
- Mais eficiente que esquemas de criptografia baseada em identidades anteriores
- Assinatura de 160 bits: nível de segurança equivalente ao RSA de 1024 bits (Kaliski 2003)

Proposta Inicial

- Implementação em linguagem de programação Java (plataforma Java Micro Edition)
- Testes realizados em um celular Nokia 6275

Proposta Inicial

- Desempenho insatisfatório: mais de 5 segundos para cifrassinar ou vericifrar uma mensagem
- Variação do tamanho das chaves e das funções de emparelhamento
- Substituição da implementação da biblioteca BigInteger (BouncyCastle/SUN)
- Inversão da ordem das curvas utilizadas
- Pouco ou nenhum progresso

Agenda

- Objetivos
- Cenário
- Requisitos
- Proposta inicial
- Esquema adotado
- Conclusão

Esquema proposto

- O não atendimento aos requisitos por soluções existentes motivou a criação de um novo esquema: BDCPS (Barreto et al. 2008)
- Isento de certificados
- Validação da chave pública baseada em identidades
- Usuário pode escolher sua chave privada
- Dispensa a PKI
- Evita o comprometimento da chave (key escrow)

Esquema proposto

- Paradigma usual: converter esquemas de assinatura IB em protocolos combinados isentos de certificados
- BDCPS: extensão de um esquema de cifrassinatura de chave pública convencional, validando as chaves públicas através de técnicas baseadas em identidades

Esquema proposto

- Alto custo do emparelhamento é amortizado (validação da chave pública ocorre apenas uma vez para cada par de usuários)
- Custo médio é tão eficiente quanto o esquema de cifrassinatura utilizado
- Nível de segurança diretamente proporcional ao tamanho da chave
- Comparação (tempo em s)
  - BDCPS (160 bits): 0,31 (cifrassinatura)
  - RSA (1024 bits): 0,74 (encriptação)

Aplicação

- Cadastro: usuário envia sua chave privada a uma autoridade de confiança, que gera seu ponto público
- Validação: remetente deve enviar uma mensagem inicial para validação de sua chave pública
- Troca de mensagens: usuários trocam mensagens de maneira transparente, apenas digitando sua chave privada antes do envio

Agenda

- Objetivos
- Cenário
- Requisitos
- Proposta inicial
- Esquema adotado
- Conclusão

Conclusão

- Aplicação prática em um futuro próximo
- Necessidade estimulou a criação de um novo esquema
- Alternativa ao uso de certificados
- Falta especificar o formato da mensagem de modo a acomodar os parâmetros do esquema

Maiores detalhes em relação ao BDCPS:

SBSeg Technical Session 3

Quarta-feira, 14h, auditório Da Vinci

Contato

- eduardo.cruz@poli.usp.br
- geovandro.pereira@poli.usp.br
- rodrigo.silva1@poli.usp.br
- pbarreto@larc.usp.br

- Apresentação disponível em http://stoa.usp.br/rodrigors/files

Obrigado!