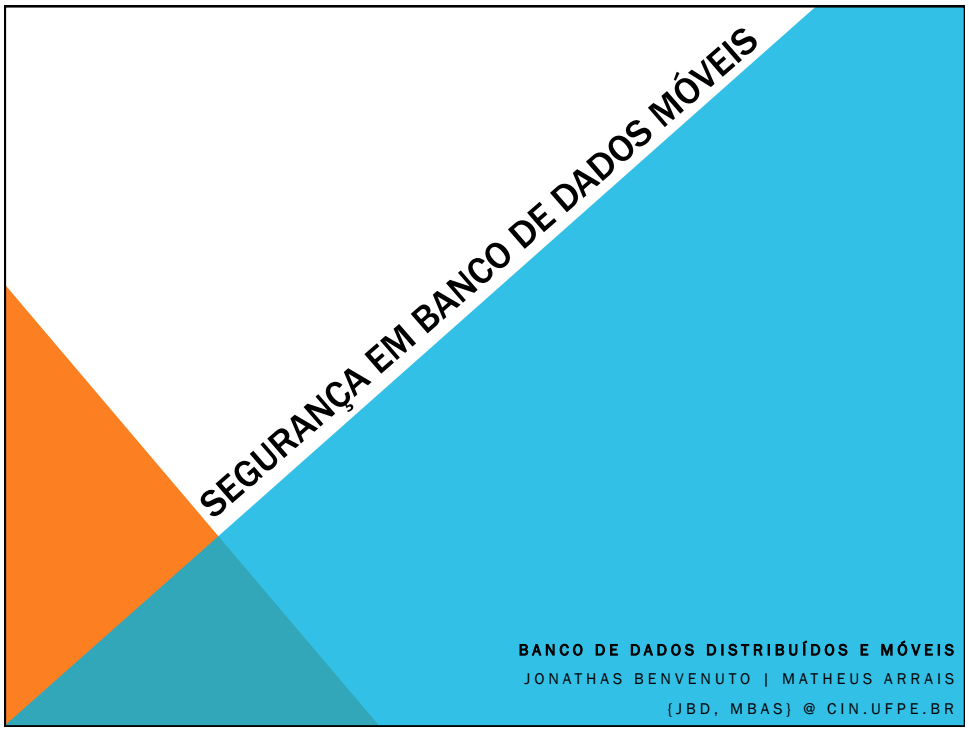


ROTEIRO

- Introdução;
- Computação Móvel;
- Banco de Dados Móveis;
- Segurança;
- Segurança em Banco de Dados Móveis;
  - Dados;
  - Metadados.
- Conclusão.

INTRODUÇÃO

- Negligência das Empresas;
- Segurança da informação não gera receita;
- Impedir que os ganhos não sejam afetados;
- Gasto com medidas corretivas;

"Segurança é a condição de estar sendo protegido contra o perigo ou a perda."

COMPUTAÇÃO MÓVEL

- **Mudança de paradigmas tradicionais**
  - Redes de comunicação
  - Engenharia de software;
- **Canais *Wireless***
  - Celular (EDGE, HSPA (3G));
  - WLAN (*Wireless Local Area Network*);
  - Satélites;
  - ...

COMPUTAÇÃO MÓVEL

- **Elementos**
  - Unidades Móveis;
  - Estações Base;
  - Células (SDMA – *Space Division Multiple Access*).

BANCO DE DADOS MÓVEIS

- **Características próprias**
  - Necessidade de conhecimento da localização;
    - Diferentemente dos sistemas distribuidos.
  - Desligamento voluntário do host móvel não é uma falha do sistema;
  - Técnicas para recuperação de desconexões durante o *handoff.*

A computação móvel pode ser considerada como uma variação da computação distribuída

SEGURANÇA

- **Principais propriedades:**
  - Confidencialidade;
  - Integridade;
  - Disponibilidade.
- **Conceitos:**
  - Ameaça;
  - Vulnerabilidade;
  - Ataque.

SEGURANÇA

- **Conceitos:**
  - Ameaça;
    - Classificação da Microsoft:
      - Invasão disfarçada;
      - Adulteração;
      - Repúdio;
      - Revelação de Informações;
      - Negação de Serviço;
      - Elevação de Privilégios.

SEGURANÇA

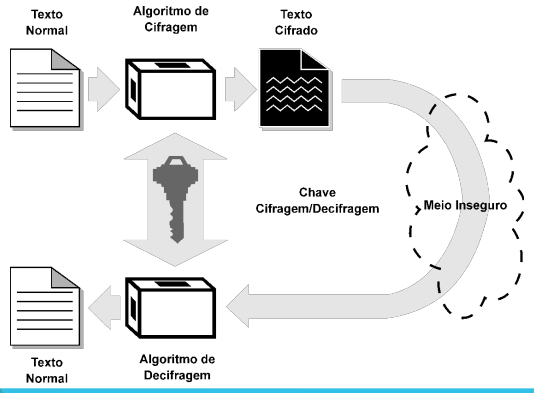
- **Conceitos:**
  - Vulnerabilidade;
    - Atividade do usuário;
    - Login e senhas fracos;
    - Permissões excessivas;
    - Ataques de Injeção SQL.
  - Ataque;
    - Aproveitamento de uma vulnerabilidade.

SEGURANÇA

- **Mecanimos de Segurança**
  - Controle de acesso (login/senha);
  - Criptografia;
    - Transformação da informação;
    - Ocultar;
    - Conceito de chaves;
      - Indispensável para acessar a informação;
      - Qualidade da chave;
      - Simétricas (Emissor/Receptor);
      - Assimétricas (Chave Privada/Pública);

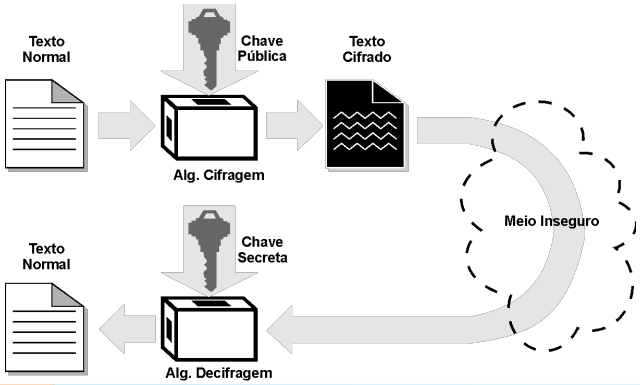
SEGURANÇA

- Criptografia simétrica



SEGURANÇA

- Criptografia assimétrica

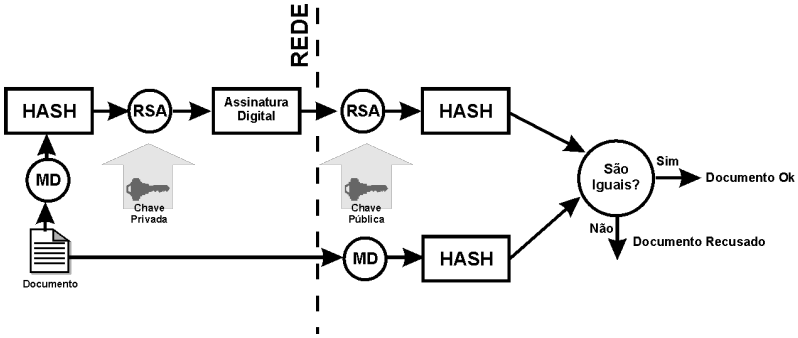


SEGURANÇA

- **Mecanimos de Segurança**
  - Assinatura digital
    - Integridade;
    - Origem.
    - Não-repúdio
      - Autoria inegável.
    - *Message Digest (MD)*
      - *Hash.*

SEGURANÇA

- **Assinatura Digital**



SEGURANÇA EM BANCO DE DADOS MÓVEIS

- **Aumento significativo dos riscos**
  - Mobilidade;
  - Uso de redes *wireless*;
  - Poucos recursos.
- **Ubiquidade exige redes sem fios**
  - Maior exposição;
- **Dinamismo da Mobilidade**
  - Serviços de segurança estáticos.

SEGURANÇA EM BANCO DE DADOS MÓVEIS

- **Mensagens**
  - Dados;
  - Metadados.
- **Transferência;**
- **Gerenciamento e Acesso**

SEGURANÇA EM BANCO DE DADOS MÓVEIS

- **Dados**
  - Conteúdo do banco de dados.
- **Metadados**
  - Informações extras
    - Perfil do usuário;
    - Localização da unidade móvel.
  - Prioridade na segurança;

SEGURANÇA EM BANCO DE DADOS MÓVEIS

- **Transferência**
  - Dados
    - Desconexões
      - Poupar recursos com a comunicação;
      - Falhas.
    - Consistência dos dados comprometida
      - Recuperação de transações.
    - Links sem fio
      - Facilidade em realizar escutas;
      - Dicícil detecção.

SEGURANÇA EM BANCO DE DADOS MÓVEIS

- **Técnicas de segurança para transferência**
  - Dados
    - Criptografia para garantir autenticação e privacidade
      - Servidor de autenticação
        - Confidencialidade emissor/receptor.
    - Proteger contra ataques e escutas.

SEGURANÇA EM BANCO DE DADOS MÓVEIS

- **Transferência**
  - Metadados
    - Localização
      - Idealmente apenas o usuário deve conhecer;
      - Ocultar o máximo possível;
      - Ameaça
        - Escuta do tráfego.

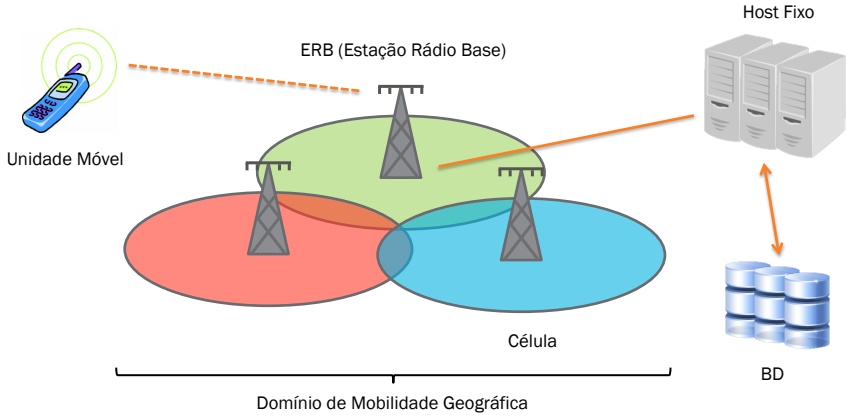
SEGURANÇA EM BANCO DE DADOS MÓVEIS

- **Técnicas de segurança para transferência**
  - Metadados
    - Autenticação
      - Criptografia Assimétrica.
    - Comunicação
      - Criptografia Simétrica.
    - MIXes;
    - Método da Não-divulgação.

SEGURANÇA EM BANCO DE DADOS MÓVEIS

- **Técnicas de segurança para transferência**
  - Metadados
    - MIXes
      - Criptografia;
      - Mensagens embaralhadas;
    - Método da Não-divulgação
      - Criptografia
      - Agentes;
        - Disfarce do caminho por meio de desvios;
        - Sucessor e Predecessor;
        - Maior Segurança quando dispersos.

SEGURANÇA EM BANCO DE DADOS MÓVEIS



SEGURANÇA EM BANCO DE DADOS MÓVEIS

- Gerenciamento e Acesso
  - Perda de unidades móveis
    - Confidencialidade e dados perdidos
      - Identificação;
      - Gerenciamento de falhas.
  - Recursos limitados
    - Tamanho dos dados requisitados.
  - Diferentes níveis de segurança;
  - Modelos de controle de acesso heterogêneo;

SEGURANÇA EM BANCO DE DADOS MÓVEIS

- **Abordagens para a mobilidade:**
  - Transparência;
    - Maior controle ao usuário;
    - Reduzir o processamento de consultas remotas;
    - Preprocessamento inteligente;
  - Localização e Movimentos;
    - Não armazenamento da localização;
    - Economia de Dados.

SEGURANÇA EM BANCO DE DADOS MÓVEIS

- **Técnicas:**
  - Localização e Movimento;
    - Separação por agregação;
    - Separação vertical;
    - Sepraração horizontal;
  - Ambientes móveis dinâmicos;
    - Diversas células de rede;
    - Diferentes medidas de Segurança;
    - Conceito de adaptação;

CONCLUSÃO

- O meio de comunicação *wireless* e a mobilidade geram mais requisitos de segurança aos bancos da dados;
- Criptografia é a base da segurança em sistemas de TI;
- Segurança da informação é uma área desafiadora em franca expansão.

DÚVIDAS

OBRIGADO!!

REFERÊNCIAS

- **CÔRTES, SÉRGIO DA COSTA; LIFSCHITZ, SÉRGIO.** Banco de Dados para um Ambiente de Computação Móvel.
- **ALVES, RENÉ ARAUJO; SOUZA, FERNANDO DA FONSECA.** Um estudo sobre segurança em Banco de Dados;
- **RAINONE, FLÁVIA.** Banco de Dados Móveis. USP, SP. Disponível em: http://grenoble.ime.usp.br/movel/bdmoveisflavia.pdf [Acessado em 07/05/2011].