Universidade Federal de Pernambuco

Centro de Informática

Graduação em Ciência da Computação

UM ESTUDO SOBRE SEGURANÇA EM BANCO DE DADOS MÓVEIS

René Araújo Alves (raa2@cin.ufpe.br)

Orientador: *Fernando da Fonseca de Souza*

Recife, Março de 2007

UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE INFORMÁTICA
GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO
TRABALHO DE GRADUAÇÃO

UM ESTUDO SOBRE SEGURANÇA EM BANCO DE DADOS MÓVEIS

René Araújo Alves

(raa2@cin.ufpe.br)

Fernando da Fonseca de Souza

(fdfd@cin.ufpe.br)

Monografia apresentada ao Curso de Bacharelado em Ciência da Computação da Universidade Federal de Pernambuco, como parte dos requisitos para obtenção do grau de Bacharel em Ciência da Computação.

Recife, março de 2007

Resumo

Computação e comunicação móvel são áreas de rápido desenvolvimento. Mas a mobilidade e os *links* sem fio geram inúmeros problemas concernentes a assuntos de segurança como disponibilidade e confidencialidade. As informações processadas nos bancos de dados móveis são postas em perigo por várias ameaças baseadas na mobilidade do usuário e dos recursos restritos dos dispositivos móveis e das redes sem fio. Esse trabalho analisa os novos desafios e investiga os assuntos de segurança envolvidos no gerenciamento, acesso e transferência dos dados móveis. O propósito é alcançar uma proteção adequada e economizar os recursos dos dispositivos.

Abstract

Mobile computing and communication is a rapidly developing area. But mobility and wireless links comprehends a row of problems concerning security issues like availability and confidentiality. The mobile processed information in database systems are endangered by various threats based on user's mobility and restricted mobile resources of portable devices and wireless links. This work surveys the new challenges and the research on security issues in mobile data management, access and transfer. The purpose is to achieve a suitable protection and to spare mobile resources.

“... se o SENHOR não guardar a cidade, em vão vigia a sentinela.”
(Salmos 127:1)

Agradecimentos

Para que a realização desse trabalho pudesse ser concluído, tenho muito que agradecer. Quero agradecer primeiramente a Deus que em todo momento esteve me ajudando e me dando a calma necessária para estar escrevendo tudo aqui, sempre me mostrando que eu seria capaz. As seguintes pessoas quero agradecer, não necessariamente nessa ordem, para não cometer nenhuma injustiça com nenhuma delas: ao professor Fernando Fonseca que primeiramente me aceitou como orientando e esteve me ajudando a estar escrevendo, me mostrando qual o rumo que deveria estar dando a essa monografia e logicamente por sua extrema paciência para comigo, a ele meu muito obrigado. Também a professora Valéria Times pela chance me dada. A minha família (meu pai, minha mãe, meus irmãos, avós, tios e primos) que esteve me suportando durante os bons e maus dias e me dando o amor necessário para que eu pudesse concluir tudo que me dispunha. A minha noiva Diana (e logicamente toda sua família a quem amo: seu pai, mãe, irmãs, irmãos, e cunhados) que também foi muito paciente nos meus momentos ausentes por estar escrevendo esse trabalho, me apoiando e me encorajando a sempre continuar e nunca desistir. Aos meus sócios na mWare Soluções, Thierry e Assis, que também entenderam os momentos apertados que passei em relação ao tempo para o término desse trabalho. Aos meus professores da Universidade Federal de Pernambuco me ensinando os primeiros passos na área da computação para que hoje eu possa andar sozinho e concluir essa monografia. E também a minha igreja a 1ª Igreja Batista na Vila do IPSEP por entenderem o qual importante era o término desse trabalho para a conclusão do meu curso e facilitarem todo o processo envolvido no acabamento dele. E a todos os meus amigos que direta (ajudando em traduções de textos, emprestando livros, entre outras coisas) ou indiretamente (me ajudando a esquecer por uns momentos o que tinha que fazer para relaxar) me ajudaram para que eu terminasse o que eu tinha que terminar. A cada um de vocês meu muito OBRIGADO!!!

Índice

1. Introdução 11

2. Banco de Dados Móveis 13
2.1. Computação Móvel 14
2.1.1. Dificuldades e Desafios 14
2.1.1.1. Dificuldade de hardware 14
2.1.1.2. Dificuldade de Comunicação 15
2.1.1.3. Dificuldades de Mobilidade 15
2.2. Arquitetura 16
2.2.1.1. Arquitetura Cliente/Servidor 17
2.2.1.2. Arquitetura Cliente/Agente-Servidor/Servidor 18
2.2.1.3. Arquitetura Cliente/Agente-Cliente/Servidor 19
2.2.1.4. Arquitetura Cliente/Interceptadores/Servidor 19
2.2.1.5. Arquitetura *Peer-to-Peer* (P2P) 20
2.2.1.6. Arquitetura de Agentes Móveis 21
2.3. Características 22
2.3.1. Difusão de Dados 22
2.3.2. Replicação 23
2.3.3. Sincronização 24
2.4. Transações Móveis 25
2.5. Controle de concorrência 26
2.6. Processamento de consultas 27
2.7. Recuperação de falhas 27

3. Segurança 29
3.1. Princípios Básicos da Segurança da Informação 29
3.1.1.1. Ameaça 30
3.1.1.2. Vulnerabilidade 31
3.1.2. Mecanismos de Segurança 32
3.1.2.1. Controles de Acesso 32
3.1.2.2. Criptografia 32
3.1.2.3. Firewall 34
3.2. Segurança nas Redes Sem Fio 34
3.2.1.1. WEP (*Wired Equivalent Privacy*) 35
3.3. Segurança nos Dispositivos Móveis 35
3.3.1. Autenticação 36
3.3.2. Autenticação biométrica 37
3.3.3. *Logout* automático e reentrada de credenciais 37
3.3.4. Destruição de dados 37
3.3.5. Encriptação do banco de dados 38
3.3.6. Criptografia de nomes de usuário e senha 38
3.4. Segurança em Banco de Dados 38
3.4.1. Controle de acesso 39
3.4.1.1. Controle de acesso arbitrário (discricionário) 40
3.4.1.2. Controle de acesso obrigatório 40
3.4.2. Controle de fluxo 41
3.4.3. Controle de inferência 42

3.4.4. Criptografia 43

4. Segurança em Banco de Dados Móveis 44
4.1. Áreas da segurança em Banco de Dados Móveis 44
4.1.1. Transferência de dados 45
4.1.2. Transferência de metadados 45
4.1.3. Acesso e gerenciamento de dados 46
4.1.4. Acesso e gerenciamento de metadados 47
4.2. Técnicas de segurança 47
4.2.1. Transparência 48
4.2.2. Localização e movimentos seguros 48
4.2.3. Ambientes móveis dinâmicos e com recursos restritos 49
4.3. Segurança dos bancos de dados comerciais 50
4.3.1. Oracle *Lite Mobile Server* 50
4.3.2. DB2 Everyplace 51
4.3.3. SQL *Server Compact Edition* 52
4.3.4. SQL Anywhere Studio 54
4.3.5. Comparação 55

5. Testes realizados 57
5.1. Nokia 6620 58
5.2. Toshiba Satellite A100-SK9 62
5.3. Conclusão 64

6. Considerações finais e trabalhos futuros 66

7. Referências 68

Índice de Figuras

Figura 2-1 - Arquitetura da Computação Móvel - extraída de DUNHAM & HELAL (1995) 17
Figura 2-2 - Arquitetura Cliente/Servidor – extraída de RAINONE (2003) 17
Figura 2-3 - Arquitetura Cliente/Agente-Servidor/Servidor – extraída de RAINONE (2003) 18
Figura 2-4 - Arquitetura Cliente/Agente-Cliente/Servidor – extraída de RAINONE (2003) 19
Figura 2-5 - Arquitetura Cliente/Interceptador/Servidor – extraída de RAINONE (2003) 20
Figura 2-6 - Arquitetura Peer-to-Peer – adaptada de RAINONE (2003) 21
Figura 2-7 - Arquitetura de Agentes Móveis 21
Figura 2-8 - Estratégias de transmissão por difusão pull-based e push-based [ITO (2001)] 23
Figura 5-1 - Criação e Encriptação do BD no Nokia 6620 60
Figura 5-2 - Arquivo do banco de dados antes da criptografia 61
Figura 5-3 - Arquivo do banco de dados depois da criptografia 62
Figura 5-4 - Acesso ao webtogo no cliente móvel 63
Figura 5-5 - Cadastro de Mídias 63
Figura 5-6 - Download da aplicação móvel 64

Índice de Tabelas

Quadro 4-1 - Resumo das características dos sistemas apresentados. Adaptado de AMADO (2002) 55
Quadro 5-1 - Comparação entre o Nokia 6620 e o Toshiba Satelite A100-SK9 57

1. Introdução

Com o avanço da computação ao ponto de existirem os computadores portáteis, surgiu o conceito de computação ubíqua (em qualquer lugar, em qualquer hora, a qualquer jeito). O usuário não precisa ir mais ao computador, este está sendo carregado com o usuário. Com essa nova visão cresceram o número de dispositivos portáteis e com eles os usuários querem sincronizar os dados presentes nos aparelhos portáteis com o seu *Personal Computer* (PC). Eles querem agora perguntar ao seu dispositivo onde é o cinema mais próximo ou onde é o supermercado mais próximo que vende leite mais barato, por exemplo. Com isso surgiu a necessidade de criação de um novo paradigma: os bancos de dados móveis.

Para possibilitar a existência dos SGBD móveis, as características dos bancos de dados centralizados e distribuídos foram integradas e adaptadas ao ambiente móvel. Adaptadas, pois eles possuem características peculiares que precisam ser levadas em consideração, como a grande quantidade de desconexões e a fraca conectividade. Sendo necessária a mudança das técnicas já existentes para ser possível o uso desses bancos de dados.

Mas, com essa nova tendência de acesso à informação em qualquer lugar trouxe novos problemas, como a segurança envolvida na transmissão dos dados na rede sem fio e o gerenciamento e acesso às informações no dispositivo móvel. Pela maior possibilidade de serem roubados ou perdidos, se comparado com os *desktops* torna-se necessário métodos específicos para protegê-los. Outro problema está relacionado a possibilidade da consulta de informações referentes à localidade do usuário, deixando em perigo não só o dispositivo, mas também o próprio usuário, que terá a chance (se não aplicada boas técnicas de segurança) de ter os seus passos rastreados.

Este trabalho tem por objetivo realizar um estudo sobre a área da segurança dos SGBD móveis. Para isso, no capítulo 2 será dada uma introdução aos conceitos da área de banco de dados móveis, destacando características específicas a essa área. No capítulo seguinte, (capítulo 3) estarão em foco os princípios básicos de segurança aplicados nos dispositivos móveis, nas redes sem fio e nos bancos de dados tradicionais.

Para então, no capítulo 4, serem integrados esses conceitos em um único que é chamado de segurança em banco de dados móvel. Serão estudadas as medidas aplicadas para proteger o usuário nos principais SGBD do mercado. E por fim, será feito um teste de um específico SGBD em dois dispositivos móveis, para verificar se os conceitos estudados estão sendo utilizados na prática.

2. Banco de Dados Móveis

Nos dias atuais, nota-se um crescimento na computação móvel e esse crescimento tem se tornado realidade graças à convergência de duas tecnologias: a criação de novos computadores portáteis com uma maior capacidade de processamento e o desenvolvimento de redes de comunicação de dados mais velozes e confiáveis. Podendo também ser notada a constante redução das dimensões, peso e consumo de energia de vários componentes, contribuindo assim para que a computação móvel venha se tornar onipresente, pois não se precisa ir à procura do computador. Ele é carregado pelo usuário através de um poderoso laptop, um *palm top* ou até por meio dos celulares. E essa onipresença vem contribuindo para o aumento da demanda de acesso à informação independente da localidade do usuário ou da informação requerida. Um grande desafio é o gerenciamento dessas informações visando garantir a integridade e segurança dos dados envolvidos nos processamentos, bem como a rapidez na resposta a essas consultas.

Como exemplo do uso de uma aplicação de computação móvel é quando uma pessoa se desloca a um outro país ou cidade que não conheça, e está querendo saber onde pode encontrar o cinema mais próximo ou para onde é que ele pode encontrar o principal *shopping* da cidade. Essa pessoa não quer só saber o local específico, mas também deseja saber como ele pode fazer para chegar lá. Quais os principais caminhos e meios de transporte com os seus respectivos tempos gastos para chegar na determinada localidade e o custo envolvido. Todas essas consultas são dependentes da localidade do usuário da aplicação móvel e por isso podem retornar diferentes resultados a cada instante.

Este capítulo tem por objetivo apresentar uma visão sobre sistemas de banco de dados móvel. Primeiramente, é analisada a área da computação móvel, para que possam assim ser mostradas as dificuldades encontradas nessa área, com a intenção de mostrar as diferenças entre sistemas de bancos de dados móveis e demais sistemas de bancos de dados.

2.1. Computação Móvel

Mobilidade pode ser definida como a capacidade de poder se deslocar ou ser deslocado facilmente. No contexto da computação móvel, mobilidade se refere ao uso, pelas pessoas, de dispositivos móveis portáteis, funcionalmente poderosos, que oferecem a capacidade de realizar facilmente um conjunto de funções de aplicação, sendo também capazes de conectar-se, obterem dados e fornecê-los a outros usuários, aplicações e sistemas [LEE et al (2005)].

2.1.1. Dificuldades e Desafios

Um dispositivo móvel deve possuir determinadas características. Por exemplo, deve ser portátil e o usuário ser capaz de transportá-lo com relativa facilidade. Um dispositivo móvel também tem que ser altamente utilizável, funcional e permitir fácil conectividade e comunicação com outros dispositivos. Para o usuário, quanto maior a combinação dessas características disponíveis, melhor será o dispositivo móvel. Mas para existirem essas características nos dispositivos móveis é necessário superar alguns desafios e dificuldades envolvidos. Nessa seção, serão discutidas algumas dessas dificuldades encontradas no mundo da computação móvel.

2.1.1.1. Dificuldade de hardware

Um dos grandes problemas da portabilidade dos computadores móveis é o consumo de energia. Enquanto os computadores *desktop* os computadores foram feitos para ficarem ligados todo tempo a uma fonte de energia, nos dispositivos móveis é totalmente inverso. São ligados à bateria, a qual no caso de um PDA e de um celular, é o componente mais pesado. E essa se torna um problema pelo seu tamanho e pela sua necessidade de recarga. Então, a bateria se torna um dos maiores entraves para não existirem, por exemplo, celulares menores do que já são. Pois o tamanho do dispositivo depende muito de sua bateria.

Outro problema também é o risco da perda de informações devido a danos físicos, perda do dispositivo ou roubo e também o acesso não permitido às informações contidas no aparelho. Para minimizar algumas conseqüências com essas perdas, é sempre aconselhável ao usuário, fazer

operações de backup das informações e o armazenamento dos dados numa base remota, para que possa ser acessado quando necessário.

O tamanho de tela reduzido e a impossibilidade do uso do mouse, em muitos dispositivos móveis, tornam-se um grande desafio para os designers gráficos e programadores, que em muitos casos reduzem as funcionalidades das aplicações.

2.1.1.2. Dificuldade de Comunicação

Por se tratar de uma rede sem fio, que é caracterizada por uma menor e variável largura de banda, uma maior taxa de erros e desconexões indesejadas. Então, uma falha na rede pode causar sérios problemas a processos que estão sendo executados em locais diferentes, pois eles tendem a parar a execução a espera de informações, por exemplo. E outro problema é que uma aplicação deve assumir que a largura da banda é variável e o usuário pode mudar de uma célula para outra, mudando ou não o protocolo de comunicação. Deve-se então construir aplicações que se adaptem aos recursos disponíveis, tanto na rede como no dispositivo móvel.

Com a grande necessidade da conectividade com servidores ou outros dispositivos pela rede sem fio, as informações se tornam um alvo fácil para pessoas não autorizadas que podem tentar acessá-las. Para tornar a rede mais segura, são usados recursos como *firewalls*, sistemas de detecção de intrusos e/ou uso de ferramentas de criptografia. É também importante a conscientização dos usuários que muitas vezes facilitam a abertura de brechas na segurança. Esses e outros mecanismos de segurança serão descritos no capítulo 3 deste trabalho.

2.1.1.3. Dificuldades de Mobilidade

A cada vez que as pessoas se movimentam, seus computadores móveis usam os pontos de acesso à rede referentes àquela localidade. Para que a pessoa possa ser localizada, o sistema armazena o seu endereço de rede, que é geralmente colocado em *cache* com um longo tempo de expiração. Mas, devido à grande freqüência de mudança de localidade, o seu endereço IP (*Internet Protocol*) é alterado a cada nova célula de rede atingida pelo usuário, tornando mais complicada a identificação de sua localização.

Os dispositivos necessitam de informações dependentes da sua localização, trazendo um grande custo de comunicação. E como é necessário o sistema saber onde o usuário se encontra, para retornar o resultado das consultas dependentes de localidade, é necessário que na migração de localidade haja uma mudança no servidor de informações daquele usuário para um servidor mais próximo à sua posição. Esta mudança diminui o risco da perda de dados na rede, o consumo da capacidade da rede e a latência. Mas o armazenamento dessas informações pode deixar o usuário em risco por permitir que seja determinada a sua localização em um dado momento

2.2. Arquitetura

A plataforma móvel tem uma estrutura genérica que toma como base a arquitetura distribuída [OZSU & VALDURIEZ (1999)], na qual diversos computadores geralmente conhecidos por *hosts* fixos e estações de base são interligados a uma rede com fio e de alta velocidade. Os *hosts* fixos são computadores participantes da rede distribuída, não sendo equipados para gerenciar unidades móveis, mas que podem ser configurados de forma a fazê-lo. Para que as unidades móveis possam ter acesso aos dados, as estações de base são equipadas com uma interface para as redes sem fio podendo fazer a transmissão dos dados às unidades móveis ao seu alcance [ELMASRI & NAVATHE (2002)].

Como as unidades móveis, em sua maioria, se caracterizaram por serem de pouca confiança, por estarem expostas a roubos, danos e falhas de segurança e também serem pobres de recursos, elas muitas vezes são tratadas como simples terminais. Então elas apresentam apenas uma interface com o usuário e deixam todo o processamento para as estações localizadas na rede fixa. Mas devido às variações das larguras de banda (muitas vezes lentas), às altas desconexões e às redes sem fio serem pouco confiáveis, os *hosts* móveis também devem conter algumas funcionalidades para diminuir a dependência dos servidores remotos.

Existem dois canais de conexão, o *downlink,* que é utilizado para enviar dados das estações de base para as unidades móveis, e o *uplink*, que é utilizado para enviar dados no sentido inverso [ELMASRI & NAVATHE

(2002)]. A Figura 2-1 apresenta uma arquitetura genérica para um sistema de computação móvel.

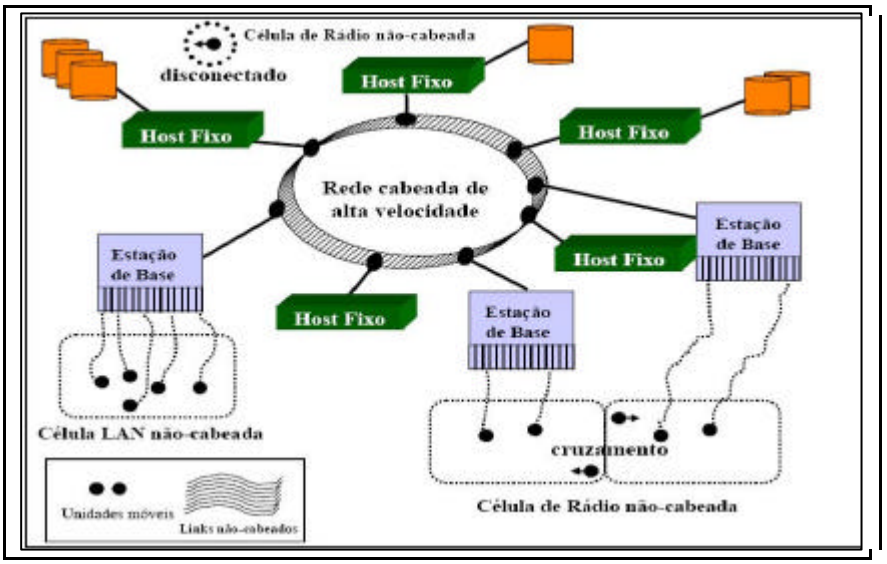

Figura 2-1 - Arquitetura da Computação Móvel - extraída de DUNHAM & HELAL (1995)

Existem variações da arquitetura tradicional que serão discutidas nas subseções a seguir. Algumas dessas variações são apresentadas no estudo de PITOURA & SAMARAS (1998).

2.2.1.1. Arquitetura Cliente/Servidor

Nesta arquitetura, o cliente é o *host* móvel que se comunica com o servidor (estação base), requisitando serviços, como apresentado na Figura 2-2. O servidor realiza o maior trabalho de gerenciamento de dados, enquanto o cliente é responsável pela interface do usuário e pela própria aplicação, além de administrar uma memória local para solicitação de consultas e armazenamento do resultado das consultas realizadas.

Figura 2-2 - Arquitetura Cliente/Servidor – extraída de RAINONE (2003)

Como abordado anteriormente, existem limitações de conexão numa rede sem fio, o que é um problema para esse tipo de arquitetura. A alta ocorrência de desconexões voluntárias ou involuntárias nas redes móveis não é tratada nessa arquitetura, trazendo dificuldades para que o processamento das operações se concretize na unidade móvel. Com isso é necessário extensões dessa arquitetura para suprir esses problemas.

2.2.1.2. Arquitetura Cliente/Agente-Servidor/Servidor

Nesta arquitetura de três partes é introduzido o agente localizado na rede fixa agindo em função do cliente como ilustrado na Figura 2-3. Quando acontece algum tipo de desconexão, tanto o servidor quanto o cliente realizam atualizações. O agente simula a presença do cliente na rede fixa aliviando o impacto das falhas na comunicação, sendo capaz de prover facilidades enfileirando mensagens que seriam trocadas com o cliente móvel, caso não estivesse desconectado. O tempo de resposta entre operações remotas pode diminuir, já que a carga de trabalho do servidor é menor.

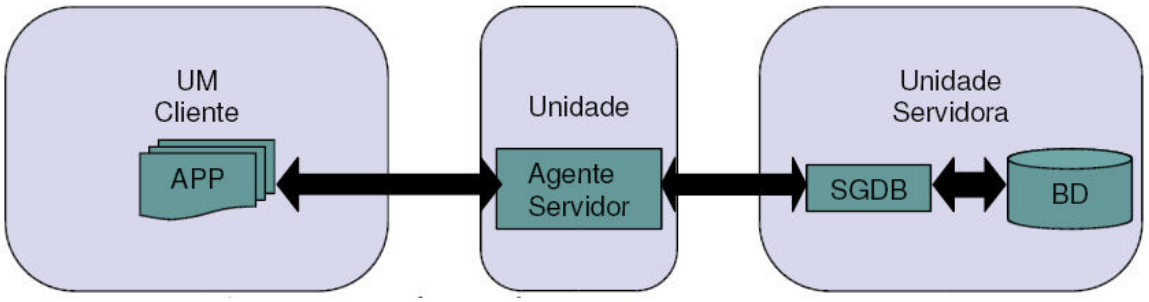

Figura 2-3 - Arquitetura Cliente/Agente-Servidor/Servidor – extraída de RAINONE (2003)

Como o agente está localizado numa rede fixa e com um grande poder computacional, ele pode usar esses recursos em favor dos clientes móveis, transferindo para si muitas das funcionalidades. Para diminuir o tráfego na rede, o agente pode comprimir os dados antes da transmissão para o cliente. Essa arquitetura é mais apropriada para clientes móveis com recursos limitados.

Nessa arquitetura, é necessária a mudança no cliente para a comunicação não mais com o servidor, e sim com o agente, se tornando uma dificuldade. Nessa arquitetura, o cliente não pode operar quando estiver desconectado, pois ele não tem nenhuma funcionalidade. Outro problema é

no sentido da otimização da transmissão já que o agente só aperfeiçoa a transmissão de dados para o cliente móvel e não no sentido contrário.

2.2.1.3. Arquitetura Cliente/Agente-Cliente/Servidor

Assim como a anterior, essa arquitetura é uma extensão da arquitetura Cliente/Servidor, com a inclusão de um agente que atua junto ao *host* móvel, como pode ser observado na Figura 2-4. O agente assume o papel de ampliar as funcionalidades do cliente, que muitas vezes são pobres em recursos computacionais.

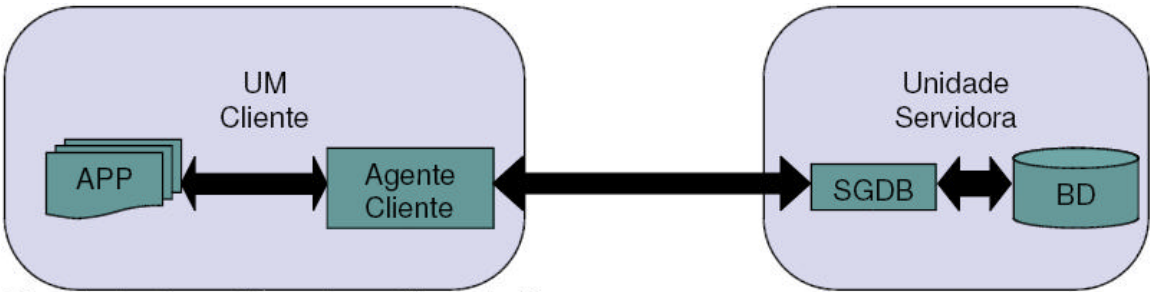

Figura 2-4 - Arquitetura Cliente/Agente-Cliente/Servidor – extraída de RAINONE (2003)

Os agentes localizados no cliente administram a memória *cache* do dispositivo, disponibilizando progressivamente durante o pouco tráfego da rede (*prefetching*). Esses agentes também fazem uma cópia do banco de dados para a memória do cliente móvel (*hoarding*) e também aperfeiçoam a comunicação com a sua estação base.

Contudo, para que o cliente possua um agente integrado é necessário que ele cumpra um requisito mínimo de recursos, o que não é comum a todos os dispositivos móveis.

2.2.1.4. Arquitetura Cliente/Interceptadores/Servidor

Essa arquitetura foi projetada para suprir os problemas das duas anteriores, nas quais os agentes estão apenas em um lado da arquitetura. Nessa arquitetura é incluído o agente situado no cliente móvel, que detecta (intercepta) as solicitações do cliente e o agente situado no servidor, que executa melhorias na transmissão de dados na rede sem fio, com a redução da quantidade de dados transmitidos. O agente situado no servidor também melhora a segurança na transferência dos dados e sustenta a não

interrupção da computação móvel, entre outras possíveis atividades (ver Figura 2-5).

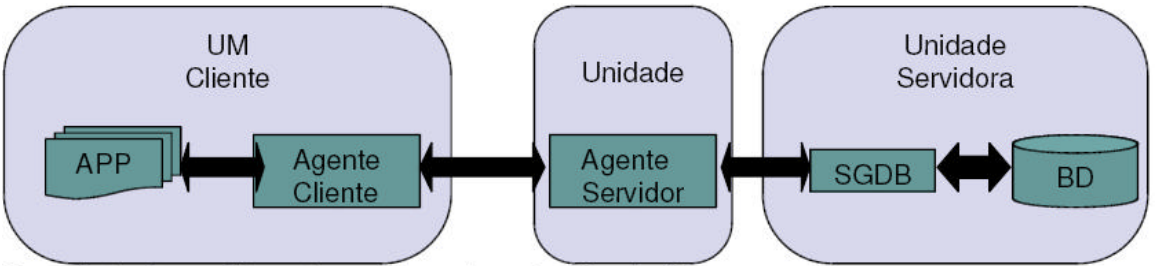

Figura 2-5 - Arquitetura Cliente/Interceptador/Servidor – extraída de RAINONE (2003)

Tanto para o cliente quanto para o servidor, essa arquitetura é transparente. Com os interceptadores, tanto o cliente, como o servidor, podem continuar suas operações mesmo quando houver a perda da comunicação, sendo enfileiradas novas requisições. No momento da reconexão as solicitações são enviadas ou ao servidor ou ao cliente e continuam suas operações normais. A comunicação entre os dois agentes possibilita uma redução (compressão) dos dados e um melhora no protocolo, sem limitar as funcionalidades e a interoperabilidade do cliente.

Essa arquitetura é indicada às aplicações que exigem um grande processamento e armazenamento, além de uma maior autonomia da energia. Entretanto, cada nova aplicação necessita de um trabalho de desenvolvimento tanto no servidor quanto no cliente, mesmo não sendo necessária a criação de um novo agente. Outro problema é que tanto o cliente quanto o servidor realizam processamentos em cada aplicação.

2.2.1.5. Arquitetura *Peer-to-Peer* (P2P)

Nessa arquitetura, não existe a distinção entre servidores e clientes (ver Figura 2-6). Cada estação tem funcionalidade tanto de servidor quanto de cliente. O problema é quando há uma indisponibilidade de uma estação, podendo comprometer uma transação por completo. Para amenizar o problema da desconexão seria necessário introduzir a figura de agentes, agindo como representantes das unidades no caso de desconexões.

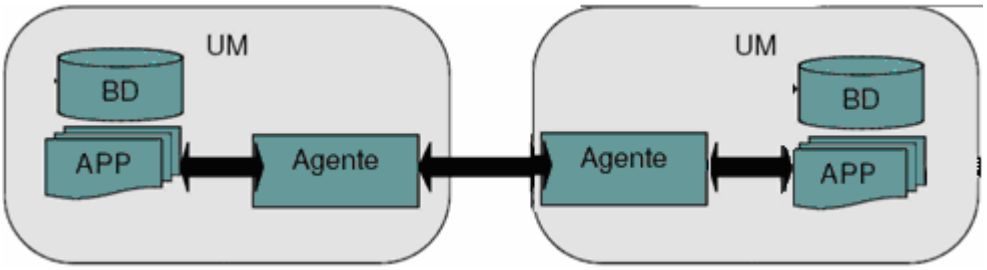

Figura 2-6 - Arquitetura Peer-to-Peer – adaptada de RAINONE (2003)

2.2.1.6. Arquitetura de Agentes Móveis

Agentes Móveis são processos enviados de um computador para executar uma tarefa específica em outro computador. Eles armazenam instruções, dados e um estado de execução e se movem de acordo com um itinerário (direção). Esses agentes possuem um bom desempenho nos sistemas de objetos distribuídos, por possuir características do conceito de multi-agentes. Após a sua submissão, o agente atua de forma autônoma, independente do seu emissor (ver Figura 2-7).

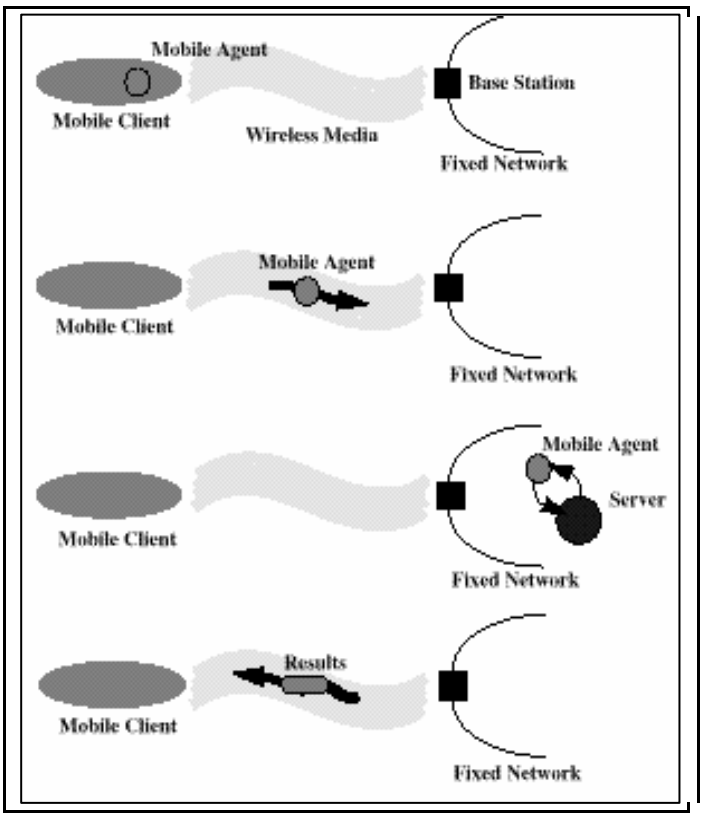

Figura 2-7 - Arquitetura de Agentes Móveis

Essa arquitetura não tem uma grande diferença da arquitetura baseada em agentes interceptadores. O modo como são enviados para coletar informações é semelhante ao modo que as requisições são enviadas

pelos agentes estáticos (interceptadores). Os agentes móveis são dotados de inteligência para poderem resolver problemas, tomar decisões e reagir quando preciso. Um dos principais obstáculos para a utilização e aceitação dos agentes móveis em aplicações comerciais é a sua segurança, como por exemplo, a questão de protegê-los contra vírus.

2.3. Características

Esta seção aborda as principais características existentes nos SGBD móveis como difusão dos dados, replicação e sincronização.

2.3.1. Difusão de Dados

A difusão (disseminação) de dados é o envio de dados para os clientes móveis localizados nas células de rede alcançadas pelo servidor remetente [BARBARÁ (1999)]. Os dados são enviados para vários clientes sem que haja a necessidade dos dados envolvidos em uma requisição (que tem um custo no processamento da solicitação e na comunicação com a estação base) já feita por um outro cliente, em um curto espaço de tempo [SILBERSCHATZ (1997)]. A largura da banda da rede é maior no sentido servidor – cliente que no sentido cliente – servidor.

Existem duas estratégias de envios por difusão, o *pull-based* e o *push-based*. O *pull-based* é caracterizado pelo cliente fazendo o papel ativo, requisitando informações ao servidor através do envio de mensagem. O *push-based* é quando a iniciativa parte do servidor, transmitindo os dados pela rede, nessa estratégia o cliente funciona apenas como receptor (Figura 2-8). Nessa segunda estratégia, o grande problema é decidir quais os dados que serão transmitidos. Uma possível solução é que cada cliente construa um perfil (*profile*) referente aos dados que lhe são de interesse, para que o servidor possa ser capaz de escolher os dados que serão enviados aos clientes. Mais estudos nesse sentido podem ser encontrados em TERRY et al. (1994).

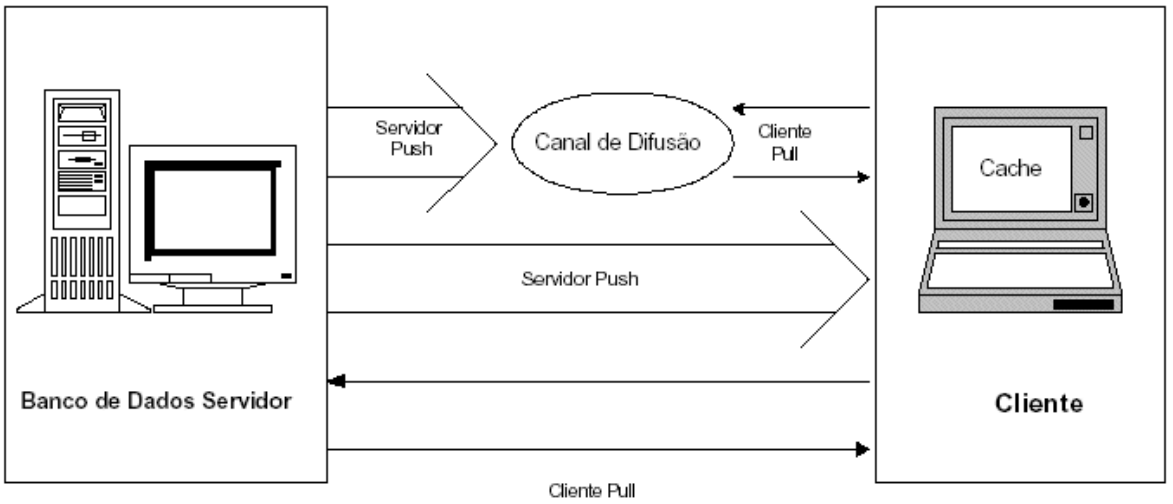

Figura 2-8 - Estratégias de transmissão por difusão pull-based e push-based [ITO (2001)]

2.3.2. Replicação

O processo pelo qual um arquivo ou um grupo de arquivos é copiado de um computador para outro, dentro de um sistema distribuído, é conhecido como replicação. Os clientes móveis armazenam cópias idênticas das informações contidas no servidor, ou parte delas, para aumentar o desempenho das aplicações, pois diminuem o tempo de acesso às informações (quando não é preciso fazer uma requisição ao servidor). Com a replicação, os *hosts* móveis podem continuar as operações quando estiverem impossibilitados de se comunicarem com o servidor ou estejam com conexões fracas [LUBINSKI & HEUER (2000)]. As estações de base também têm um ganho de performance com a replicação, já que em alguns casos não é necessário requisitar seu poder de processamento.

Um dos desafios de um sistema de replicação é garantir a integridade das transações e manter a consistência dos dados replicados em cada banco de dados.

Quanto aos métodos de propagação usados, a replicação de dados é dividida em: baseada em sessão (*session-based*), baseada em mensagens (*message-based*) ou baseada em conexão (*connection-based*) [SYBASE INC. (2002)].

Os dados replicados são armazenados no dispositivo móvel, sendo colocados em uma *cache* local. As operações dos dados armazenados em *cache* podem ser divididos como mostrados em DESPANDE et. Al (1998):

- Dados somente para consultas, nos quais os dados não podem ser alterados localmente, consequentemente não é necessária a sincronização (que é abordada na próxima seção) com o servidor;
- Dados não concorrentes, nos quais os dados podem ser alterados localmente, mas eles estão bloqueados no servidor, evitando atualizações no referido servidor; e
- Dados concorrentes, nos quais os dados alterados tanto no servidor quanto na *cache* serão sincronizados em outra hora.

Nem sempre os dados necessários a uma aplicação estarão disponíveis nessa *cache*. Por isso, as unidades móveis geralmente apresentam a necessidade de receber dados de uma base remota. Uma importante abordagem é a difusão de dados que já foi comentada anteriormente.

2.3.3. Sincronização

Sincronização é o processo pelo qual, os dados distribuídos são mantidos atualizados, de modo que os usuários sempre pensem que estão trabalhando com as informações mais recentes dos dados. Essa atualização pode ser feita a curta ou longa distância através de vários meios, como infravermelho, satélite, radiofreqüência, *spread spectrum* e de vários protocolos de comunicação de dados, incluindo: HTTP [HTTP (2007)], WSP (*Wireless Session Protocol*) [RUI (2000)], OBEX [OBEX (2007)] (*Bluetooth* [BLUETOOTH (2007)], *IrDA* [WEBOPEDIA (2001)]), SMTP [SMTP (2007)], TCP/IP [TCP/IP (2007)] e protocolos proprietários.

Para o controle da sincronização, informações que servem para saber se os dados que serão sincronizado foram atualizados, inseridos ou removidos, são guardados num registro (*log).* As cópias mais recentes dos dados são então replicadas, pelo servidor, para todos os *hosts* móveis que acessam esses dados [NOVEL INC. (2003)].

Portanto, os dados que são compartilhados quando são alterados por uma aplicação, são propagados, seguindo um protocolo, a outros dispositivos que armazenam uma réplica do mesmo dado. Após tal propagação, os dados terão sincronizado suas modificações. Segundo [MANGANELLI (2004)]: “Um protocolo de sincronização define o fluxo de trabalho para a comunicação

durante uma seção de sincronização de dados quando o dispositivo móvel é conectado à rede fixa". Os protocolos devem conter comandos comuns para a sincronização dos dados. Também devem conter a identificação de registros, e também identificar e resolver possíveis conflitos de sincronização [BREITBART et Al (1999)].

Um dos grandes desafios dos sistemas que necessitam de sincronização era a falta de padronização dos protocolos. Foi então que grandes empresas se reuniram e criaram o SyncML [SYNCML (2003)], um padrão aberto para a sincronização universal de dados e informações pessoais entre vários tipos de redes, plataformas e dispositivos. Maiores detalhes do SyncML são encontradas em PABLA (2003).

2.4. Transações Móveis

Segundo [ELMASRI & NAVATHE (2002)]: "Uma transação é uma unidade lógica de processamento de banco de dados que inclui uma ou mais operações de acesso à base. Entre estas operações estão: inserção, exclusão, modificação e consulta de dados".

Uma transação é considerada móvel quando pelo menos um *host* móvel faz parte de sua execução. Quando uma parte da computação é feita na unidade móvel e outra na estação de base, é conhecida como uma transação distribuída. DUNHAM & KUMAR (1998) discutem os efeitos do impacto que a mobilidade traz às transações de bancos de dados.

Devido às freqüentes desconexões, a execução de uma transação pode ser interrompida em qualquer instante. Isso torna necessárias soluções de gerenciamento de transações específicas para o ambiente de bancos de dados móveis. Mas a perda de conexão com a rede não deve ser considerada uma falha, e se o dispositivo móvel contiver dados replicados necessários para a conclusão das tarefas o processamento deve continuar. Como a execução das tarefas continua mesmo se o dispositivo móvel estiver desconectado, é necessário que haja um gerenciamento das transações na própria unidade móvel.

Existem vários modelos de transações móveis como *Clustering, Two-tier replication, Pro-motion, Reporting, Semantics-based, Prewrite, Kangaroo*

Transactions e *MDSTPM (Multidatabase transaction Processing Manager*) [ADIBA et. al (2001)]. Esses modelos levam em conta que as desconexões nas estações móveis podem prolongar-se por um longo período e há limitações na largura de banda. Também levam em consideração quem é o responsável pela transação, se é a unidade móvel (uma vez que está em movimento então se torna responsável pelo gerenciamento das suas transações) ou a estação base. Também tratam como as operações serão feitas quando a unidade móvel estiver desconectada, e quando as alterações serão transmitidas para a base. A maioria destes estudos considera uma transação móvel como parte de uma transação na qual há a flexibilização na consistência e submissão de modificações (*commitments*).

O controle de concorrência e os métodos de recuperação de falhas, que serão abordados nas seções a seguir, devem assegurar as propriedades ACID (atomicidade, consistência, isolamento, durabilidade) das transações móveis.

2.5. Controle de concorrência

Segundo [BRAZ (2002)]: "O controle de concorrência tem a função de garantir que as transações concorrentes enviadas para processamento no banco de dados sejam executadas em isolamento". Esse controle se torna complicado quando há uma participação na transação tanto de um *host* fixo como de um *host* móvel. Por exemplo, no caso do protocolo de controle de concorrência pessimista (com bloqueios), quando uma transação necessitar bloquear um item de dado localizado em um *host* móvel desconectado, a transação então será bloqueada esperando a reconexão daquele *host* móvel.

O controle de concorrência no ambiente de banco de dados distribuído deve ser adaptado ao ambiente móvel [PITOURA & BHARGAVA (1995)], oferecendo suporte às operações quando as unidades móveis estiverem desconectadas, reduzindo ao máximo o consumo da banda da rede, se adaptando à instabilidades das conexões e dando suporte à mobilidade dos usuários.

2.6. Processamento de consultas

Em um ambiente móvel a realização de uma consulta deve considerar o custo envolvido na sua execução, levando em conta quanto de energia ela irá consumir, a quantidade de informação que será transmitida a partir da unidade móvel e também a mobilidade do usuário.

Diversos fatores podem contribuir para o tempo de resposta do sistema [NASSU & FINGER (2000)]. Um desses fatores é a baixa confiabilidade dos meios sem fio, podendo gerar retransmissões para assegurar a integridade dos dados transmitidos, aumentando o tempo de resposta. O tempo em que o usuário permanece desconectado da rede pode ser longo, fazendo com que demore mais para que a sua solicitação seja respondida.

Por se tratar de ambientes móveis com os usuários constantemente migrando para outras localidades, então os resultados das consultas podem variar dependendo do instante de tempo que foram emitidas. No estudo de IMIELINSKI & BADRINATH (1992) foi apresentado o conceito de consultas com restrições de localização. Essas restrições envolvem a localização dos dispositivos móveis como, por exemplo, “encontre a pizzaria mais próxima de onde estou”.

A localização dos dados no processamento das consultas pode incluir dois tipos de dados: os transientes, que trocam de valores de acordo com o processamento das consultas, e os contínuos, que são continuamente atualizados durante o movimento da unidade móvel. A criação de serviços dependentes de localização é possível pelo uso de protocolos que integram o *Global Positioning System* (GPS), que usam endereço IP, facilitando a identificação da localização do *host* móvel. Essas famílias de protocolos podem ser encontradas em IMIELINSKI & NAVAS (1996).

2.7. Recuperação de falhas

Falhas no ambiente móvel são mais comuns que em ambientes estáticos. Assim como, falhas nos *hosts* móveis são mais freqüentes que as falhas nos *hosts* fixos. Isso pela característica da mobilidade, que possibilitando que uma unidade móvel cruze células (chamadas operações

de *handoff),* passando a responsabilidade da comunicação com essa unidade para uma outra estação base.

É possível para o sistema saber, na maioria dos casos, quando a unidade móvel será desconectada (i.e. quando a energia está acabando ou quando está se movimentando para um local que não tenha alcance de nenhuma rede). Tendo acesso a essa informação, ALONSO & KORTH (1993) sugerem que algumas garantias sejam supridas:

- O usuário não precisa solicitar que o processamento da transação seja transferido para a estação de base, sendo feito automaticamente;
- Alguns dados que poderiam ser requisitados pelo usuário devem ser armazenados no dispositivo móvel para continuar operando quando estiver desconectado; e
- A unidade móvel pode desejar não mais participar do conjunto de protocolos de distribuição de informação.

Uma boa estratégia de recuperação de falhas é usar o conceito de *checkpoints,* no qual, na existência de uma falha, o sistema utiliza o último registro de *checkpoint* salvo para dar inicio ao processo de recuperação. O modelo de *checkpoint* em um ambiente móvel, assim como suas características principais e os protocolos são apresentados em CORTÊS & LIFSCHITZ .

3. Segurança

Segundo [*SECURITY* (2007)]: "**Segurança** é a condição de estar sendo protegido contra o perigo ou a perda. Pode consistir em uma proteção física, social, espiritual, financeira, política, emocional, ocupacional, psicológica, educacional ou de outro tipo. Ou ainda, a ocorrência de falhas, danos, erros, acidentes ou algum outro evento que poderia ser considerado indesejado".

Por outro lado, segundo [INFORMAÇÃO (2007)]: "Compreende-se por **informação** qualquer conteúdo que possa ser armazenado ou transferido de algum modo, servindo a determinado propósito e sendo de utilidade ao ser humano. Trata-se de tudo aquilo que permite a aquisição de conhecimento".

Segundo [*INFORMATION SECURITY* (2007)]: "A **segurança da informação** está relacionada com a proteção existente ou necessária sobre dados que possuem valor para alguém ou para uma organização. Tal segurança não está restrita a sistemas computacionais, nem a informações eletrônicas ou qualquer outra forma mecânica de armazenamento".

Na seção 3.1, é abordado os principais conceitos e mecanismos da segurança da informação. Isto permite que seja entendido como é tratada a segurança nas redes sem fio (seção 3.2), a segurança nos dispositivos móveis (seção 3.3) e por último a segurança, de modo geral, nos sistemas de bancos de dados (seção 3.4).

3.1. Princípios Básicos da Segurança da Informação

Podem ser estabelecidas métricas (com o uso ou não de ferramentas) para a definição do nível de segurança existente, e com isto, serem estabelecidas as bases para análise da melhoria ou piora da situação de segurança existente.

A segurança de uma determinada informação pode ser afetada por fatores comportamentais e de uso de quem se utiliza dela, pelo ambiente ou infra-estrutura que a cerca ou por pessoas mal intencionadas que têm o objetivo de furtar, destruir ou modificar a informação.

Segundo ALBUQUERQUE (2002) e KRAUSE (1999) as principais propriedades que, atualmente, orientam a análise, o planejamento e a

implementação da segurança para um determinado grupo de informações que se deseja proteger são:

- Confidencialidade – as informações só podem ser acessadas por pessoas autorizadas pelo seu proprietário;
- Integridade – as características originais da informação, estabelecidas pelo seu proprietário, devem ser mantidas; e
- Disponibilidade – a informação deve estar sempre disponível para os usuários autorizados pelo proprietário da informação.

Outras propriedades são defendidas para que a informação seja considerada segura. O sistema que administra essas informações deve respeitar também os seguintes critérios: autenticidade, não repúdio, privacidade e auditoria, que são discutidas em LAUREANO & MORAES (2005).

Outros conceitos associados à segurança da informação são ameaça, vulnerabilidade (esses conceitos serão descritos nas próximas seções) e ataque que é uma ação executada por um intruso, que encontra uma vulnerabilidade para provocar a ocorrência de uma ameaça.

3.1.1.1. Ameaça

Ameaça em um sistema computacional é definida como qualquer ocorrência potencial que pode levar a um efeito indesejado nos recursos associados ao sistema. A Microsoft classifica essas ameaças em várias categorias importantes que são comumente conhecidas e facilmente lembradas pela sigla STRIDE [HERNAN (2006)], Na qual cada letra representa as iniciais das seguintes ameaças:

- *Spoofing* (invasão disfarçada) – o *spoofing* ocorre quando um invasor (usuário ou sistema) se passa por um usuário legal do sistema;
- *Tampering* (adulteração) – a adulteração ocorre quando um invasor adultera o sistema;
- *Repudiation* (repúdio) – o repúdio ocorre quando não é capaz de provar o responsável por determinadas modificações no sistema;
- *Information disclousure* (revelação de informações) – a revelação de informação ocorre quando as informações de um usuário são visualizadas por um invasor;

- *Denial of Service* (negação de serviço) – um ataque de negação de serviço ocorre quando uma aplicação inunda o processamento ou a memória de um sistema pela grande injeção de mensagens; e
- *Elevation of privilege* (elevação de privilégios) – os ataques de elevação de privilégios são carregados quando um invasor for capaz de elevar ou ganhar privilégios adicionais aos normalmente concedidos.

3.1.1.2. Vulnerabilidade

Vulnerabilidade é uma característica do sistema que torna possível que uma ameaça potencial ocorra. Ou seja, uma vulnerabilidade permite que algo ruim aconteça. Algumas das vulnerabilidades mais comuns são descritas a seguir:

- Atividade de usuário – os próprios usuários podem tornar o sistema vulnerável. Por exemplo, quando um usuário inadvertidamente tenta abrir um anexo de e-mail que possa conter um vírus;
- Nomes de usuário e senhas fracos – nomes de usuário fracos, como “administrador”, “gerente”, e senhas fracas, como uma senha em branco ou “1234” (uma seqüência);
- Permissões excessivas – aos usuários freqüentemente são concedidos mais permissões e privilégios do que são estritamente necessários. Permitindo que os usuários acidentalmente ou intencionalmente gerem brechas na segurança;
- Engano – os usuários podem ser iludidos em revelar informações privadas sobre eles mesmos. Por exemplo, um *site* disfarçado de um *site* de banco para capturar a senha da conta corrente do usuário;
- Serviços e portas excessivos – na qual os serviços e portas que não são utilizados podem fornecer uma abertura para invasores; e
- Ataques de injeção de SQL – esses ataques ocorrem quando uma pessoa mal intencionada usa as entradas de usuário injetando, ao invés do conteúdo requerido, instruções SQL para manipular o retorno das informações.

3.1.2. Mecanismos de Segurança

Nesta seção, serão abordados os mecanismos de segurança mais utilizados. Existem vários outros mecanismos que não serão detalhados por fugir do escopo deste trabalho.

3.1.2.1. Controles de Acesso

Os fundamentos em que os mecanismos de controle de acesso estão construídos começam com a identificação e autenticação, detalhadas a seguir:

- Identificação - é uma afirmação de que alguém é ou do que alguma coisa é. Se a pessoa diz “Oi, meu nome é René Alves.” Ele está fazendo uma reivindicação de quem ele é; e
- Autenticação - é o ato de verificar uma reivindicação de identidade. É uma maneira de comprovar que a pessoa é quem ela está dizendo que é.

Em sistemas de computadores em uso hoje em dia, o *login* é a forma mais comum de identificação e a senha é forma mais comum de autenticação. *Logins* e senhas têm servido para os seus propósitos, mas no mundo moderno eles não são adequados. Eles estão sendo substituídos lentamente por mecanismos de autenticação mais adequados.

Também devem ser determinadas quais as informações e quais as ações que as pessoas são permitidas executar (execução, visão, criação, remoção ou atualização), mesmo depois da pessoa ter se identificado e autenticado. Isso é chamado de autorização.

3.1.2.2. Criptografia

Criptografia é de um conjunto de conceitos e técnicas que visam codificar uma informação de forma que somente o emissor e o receptor possam acessá-la, evitando que um intruso consiga interpretá-la. Para isso é atualmente é usado o conceito de chaves. As chaves fazem com que só as pessoas que tenham posse delas possam decifrar a mensagem. Como uma chave de um baú, que só poderá ser aberto pelos possuidores de cópia da chave dele. Se alguém usar uma chave errada não entenderá a mensagem, assim como não poderia ter aberto o baú.

Com o uso de chaves, um emissor pode usar o mesmo algoritmo criptográfico (o mesmo método) para vários receptores. Basta que cada um receba uma chave diferente. Além disso, caso um receptor perca ou exponha determinada chave, é possível trocá-la, mantendo-se o mesmo algoritmo.

Existe chave de 64 bits, chave de 128 bits e assim por diante. Esses valores expressam o tamanho de uma determinada chave. Quanto mais bits forem utilizados, mais segura será a criptografia. Isto é, caso um algoritmo use chaves de 8 bits, apenas 256 chaves poderão ser usadas na decodificação, pois 2 elevado a 8 é 256. Isso deixa claro que 8 bits é inseguro, pois até uma pessoa é capaz de gerar as 256 combinações (embora demore), imagine-se então em um computador. Porém, ao se usar 128 ou mais bits para as chaves, tem-se gerar uma quantidade extremamente grande de combinações, deixando a informação criptografada bem mais segura.

Existem dois tipos de chaves: simétricas e assimétricas. A chave simétrica é compartilhada pelo emissor e receptor. Essa mesma chave é usada na codificação e na decodificação da informação. Algoritmos como, DES [DES (2007)], IDEA [IDEA (2007)], RC [RC (2006)]. AES [AES (2007)], 3DES [3DES (2007)], Twofish [TWOFISH (2007)] e sua variante Blowfish [BLOWFISH (2007)], entre outros, usam chaves simétricas. Um dos grandes problemas no uso da simetria é que, como o emissor e o receptor devem usar a mesma chave, a transmissão dessa chave de um lado para o outro pode não ser tão segura, permitindo sua captura por uma pessoa não autorizada.

A chave assimétrica, conhecida como "chave pública", trabalha com duas chaves: uma denominada privada e outra denominada pública. Nesse método, uma pessoa deve criar uma chave de codificação e enviá-la a quem for mandar informações a ela. Essa é a chave pública. Uma outra chave deve ser criada para a decodificação. Esta é a chave privada (secreta). Para se entender melhor, pode se pensar no exemplo do baú, apresentado anteriormente. Quando uma pessoa for receber uma mensagem, ela manda o baú e o cadeado abertos, ficando com a chave, dos mesmos, para si. A pessoa que quer enviar sua mensagem põe sua mensagem dentro do baú e tranca com o cadeado. Só quem tem a chave é o receptor, nem mesmo o emissor pode abrir o cadeado após trancado. Entre os algoritmos que usam

chaves assimétricas, têm-se o RSA [RSA (2007)] (o mais conhecido) e o Diffie-Hellman [DIFFIE-HELLMAN (2007)], entre outros.

3.1.2.3. Firewall

Segundo SOARES et al. (1995), *firewalls* são dispositivos, ou grupos de dispositivos e atualmente *software*, colocados entre uma rede segura (rede interna de uma empresa) e uma rede não segura (Internet), com o objetivo de autenticar usuários para utilizarem a rede interna.

O *firewall* por si só, não garante a segurança, mas é uma ferramenta absolutamente necessária. Ele controla o acesso entre uma ou mais redes, como também para uma única máquina, funcionando como uma espécie de barreira contra intrusos. Ao detectar tentativas sucessivas e frustradas de acesso à rede a partir de uma estação de trabalho ou de um *notebook*, o *firewall* faz soar o alarme para o administrador da rede e, dependendo da configuração, pode barrar o intruso por espaços de tempo determinados. É como se alguém, de posse do cartão de banco de outra pessoa, tentasse tirar dinheiro do caixa eletrônico e errasse a senha uma, duas, três vezes. No caso dos caixas, o cartão é recolhido automaticamente. Já o *firewall* pode ser configurado para negar o acesso por determinado tempo.

3.2. Segurança nas Redes Sem Fio

A utilização de uma rede sem fios implica em alguns aspectos especiais em relação à segurança, que não eram encontrados na rede com fios. Com as redes sem fio é impossível controlar o limite físico da abrangência do sinal transmitido. Um invasor, mesmo fora da empresa, por exemplo, pode acessar as informações trafegadas ou até mesmo ocorrer acesso indevido por setores que não deveriam estar participando da rede.

As redes sem fio podem ser classificadas como WLAN (*Wireless Local Area Network*) que interligam redes sem fio com as redes convencionais (com fio), WPAN (*Wireless Personal Area Network*) que são redes de curta distância com uso de, por exemplo, o *Bluetooth*, WMAN (*Wireless Metropolitan Area Networks*) que são utilizadas para prover comunicação entre pontos distantes, WWAN (*Wireless Wide Area Network*) que são as

telefonias de celular. Esses tipos de redes sem fio são mais detalhados em OLIVEIRA (2004).

3.2.1.1. WEP (*Wired Equivalent Privacy*)

WEP é um padrão de encriptação de dados para redes *wireless*, que traz como promessa um nível de segurança equivalente ao das redes cabeadas. Na prática, o WEP tem muitas falhas e é relativamente simples de quebrar, mas não deixa de ser uma camada de proteção básica que sempre se deve manter ativa.

WEP foi originalmente construído para ser de grande confiabilidade, para poder tanto funcionar em *hardwares* como em *softwares*, usar os diferentes tipos de padrões de cada país, que os dados transmitidos só sejam acessados por usuários autenticados (usando dados criptografados) e também que os dados cheguem de forma íntegra para o seu destinatário, sem nenhuma alteração.

Existem dois padrões WEP: de 64 e de 128 bits. O padrão de 64 bits é tem suporte em qualquer ponto de acesso ou interface que siga o padrão WI-FI, o que engloba todos os produtos comercializados atualmente. O padrão de 128 bits por sua vez, não tem suporte em todos os produtos, mas em compensação é bem menos inseguro. Para habilitá-lo, seria necessário que todos os componentes usados na rede dêem suporte ao padrão. Caso contrário, os nós que dêem suporte apenas ao padrão de 64 bits ficarão fora da rede.

Uma das grandes fraquezas do WEP é a falta de gerenciamento de chaves, pois não especifica como deve ser a distribuição das chaves [VERÍSSIMO (2002)]. Por isso foi criado o WPA (*Wi-Fi Protected Access*) para combater as vulnerabilidades do WEP. Em VERÍSSIMO (2002) é estudado o algoritmo do WAP.

3.3. Segurança nos Dispositivos Móveis

A partir do momento em que os usuários interagem com os dispositivos móveis, surgem brechas na segurança. Algumas vulnerabilidades nessa área, como discutidos na seção 3.1.1.2, incluem as atividades do

usuário, nomes de usuários e senhas fracos, permissões excessivas e usuários sendo iludidos de modo a revelar informações demais.

Nessa seção, serão discutidos mecanismos disponíveis para suavizar essas vulnerabilidades causadas pela interação do usuário com o dispositivo, incluindo o uso de autenticação e autenticação biométrica. Outro fator importante é conceder o menor nível de privilégio que um usuário necessite, esse fator também ajudará a suavizar essas vulnerabilidades.

Essas vulnerabilidades são preocupantes porque esses dispositivos podem ser facilmente extraviados, perdidos ou roubados. A perda do dispositivo pode ser algo aborrecedor e caro ao seu proprietário, mas a perda ou invasão das informações contidas no dispositivo pode superar o valor do aparelho. Por exemplo, suponha-se que foram feitos alguns registros no computador móvel e que não puderam ser enviados para o servidor por algum motivo. Depois desse momento, o dono do computador é roubado. Seus registros além de não terem sidos sincronizados com o servidor, causando a perda das informações adicionadas, estão expostos a pessoas não autorizadas, podendo ter várias conseqüências.

Pensando nesses fatores de extravios de dispositivos, vários mecanismos, que serão descritos a seguir, como, *logout* automático e reentrada de credenciais, destruição de dados, encriptação do banco de dados e criptografia de nomes de usuário e senha incorporados no código, foram desenvolvidos para melhor proteger os dispositivos móveis.

Para a segurança da comunicação sem fio com o servidor, poderá ser usada a encriptação dos dados utilizando-se o WEP (descrita na seção 3.2.2.1). Embora o uso da criptografia geralmente seja recomendado, é importante observar que o processo de encriptar e decripitar uma mensagem é custosa para o dispositivo. Pode ser um grande consumidor dos recursos do dispositivo (i.e. processador, bateria). Por isso, geralmente é melhor criptografar os dados seletivamente em vez de criptografar tudo.

3.3.1. Autenticação

A autenticação ajuda a amenizar a ameaça por *spoofing* (seção 3.1.1.1). Para reduzir a vulnerabilidade das aplicações, é necessário sempre o uso de nome de usuários e senhas fortes, e também a configuração de

alguns privilégios mínimos para os usuários. O dispositivo móvel ou a aplicação pode sempre requerer a entrada do nome de usuário e da senha para o uso de algumas funcionalidades. Por exemplo, em alguns celulares é necessária a entrada de uma senha antes de fazer uma ligação. Para o acesso ao servidor, o usuário deverá se autenticar, mas ele deve ter cuidado com os *cookies* de estado persistentes (aqueles que não são automaticamente removidos em determinado período de tempo pelas próprias aplicações), as capacidades de preenchimento de senha automáticas e tantos outros mecanismos que facilitam a vida do usuário por um lado, mas que o põem em risco por outro lado. A partir do momento que o dispositivo armazena essas informações, ele se torna vulnerável, pois a próxima pessoa a utilizar o dispositivo pode não ser um usuário autorizado.

3.3.2. Autenticação biométrica

O uso da biometria como identificação do usuário móvel vem crescendo. Reconhecimento de voz, varredura da retina e leitura da digital vêm se tornando opções viáveis para a autenticação do usuário. Esse tipo de autenticação abranda a ameaça de *spoofing* e reduz as vulnerabilidades das aplicações, visto que a identidade de um usuário é conhecida com muita exatidão, reduzindo a chance de erro de identificação a praticamente zero. Alguns *notebooks*, como o Sony Vaio VGN-SZ350BP, já estão sendo fabricados com um leitor biométrico da digital do usuário, só dando acesso ao computador aos usuários que tenham suas digitais pré-cadastradas.

3.3.3. *Logout* automático e reentrada de credenciais

Muitos dispositivos móveis possuem recursos de *logout* desencadeados pela inatividade do usuário. Caso o usuário perca o seu dispositivo, ou seja, roubado, ele estará mais protegido através desse recurso. Por exemplo, telefones celulares, *Pocket* PC, *Tablet* PC e *Notebooks* podem ser configurados de modo a requerer reentrada de credenciais do usuário depois de algum tempo.

3.3.4. Destruição de dados

Existem vários mecanismos de se implementar algoritmos personalizados de destruição de dados (apagando programas importantes e

dados confidenciais do dispositivo móvel). Um deles é a destruição dos dados caso o dispositivo passe um período longo (com um tempo pré-determinado) sem o contato com o servidor. Outro mecanismo simples seria um programa que removesse os dados desejados após o usuário digitar uma senha incorreta um certo número de vezes. Isto também pode ser possível criando um programa que seja iniciado pelo servidor para excluir os arquivos desejados no dispositivo móvel. O problema nesse último mecanismo é que nem sempre será capaz de encontrar o dispositivo para iniciar essa ação.

3.3.5. Encriptação do banco de dados

É possível criptografar os dados em certos bancos de dados de dispositivos móveis. Portanto, mesmo que o dispositivo seja extraviado, torna-se extremamente difícil para os invasores ler os dados contidos no do banco de dados.

3.3.6. Criptografia de nomes de usuário e senha

Mesmo que os bancos sejam criptografados, caso o invasor tenha acesso ao código da aplicação e tenha também os nomes de usuários e suas respectivas senhas de acesso ao banco de dados incorporados, então nesse código uma ameaça continua existindo. Por isso, torna-se necessário a criptografia dos nomes de usuário e senhas contidas no código, bem como nos arquivos de configuração.

3.4. Segurança em Banco de Dados

Foi visto no início desse capítulo que qualquer sistema de segurança deve prover mecanismos que não permitam a perda ou degradação da integridade, disponibilidade e confidencialidade. No caso do banco de dados, a perda da integridade acontece quando há uma modificação não autorizada nos dados ou por atos intencionais ou acidentais. A perda da disponibilidade dá-se quando os dados tornam-se indisponíveis para um usuário ou programa que tenha um direito legítimo sobre eles. E por fim, a perda da confidencialidade ocorre a quando há uma violação da privacidade dos dados causando uma divulgação não autorizada dos mesmos.

Para proteger o banco de dados contra essas ameaças, quatro tipo de medidas, que serão discutidas nas próximas seções, podem ser implementadas: controle de acesso, controle de inferência, controle de fluxo e criptografia.

É importante que o SGBD armazene informações de todas as operações aplicadas por um usuário a cada vez que ele realizar o *login* até o momento da desconexão. Isso é importante para que o administrador do banco de dados (ABD) possa descobrir qual usuário adulterou as informações contidas no banco. Isso é uma forma de auditoria que consiste na revisão do *log* armazenado, verificando todas as operações aplicadas ao banco de dados durante certo período de tempo. Um aprofundamento sobre auditoria de banco de dados foge do escopo desse trabalho.

3.4.1. Controle de acesso

Em um sistema de banco de dados multiusuário, o SGBD deve ser capaz de prover aos usuários acessos a determinadas partes do banco de dados e ao mesmo tempo impedir que eles acessem dados não permitidos. Também é necessário evitar que usuários não autorizados tenham acesso aos dados, seja para obter informação, seja para realizar alterações mal-intecionadas em uma parte da base de dados. A função controladora desse fato é chamada de controle de acesso que é tratada por meio da criação de contas de usuários.

O ABD é a autoridade principal responsável para conceder privilégios a usuários que precisam utilizar o sistema, e por classificá-los, bem como classificar os dados de acordo com a política da organização. O ABD é o responsável pela segurança geral do sistema de banco de dados.

A concessão e a revogação de privilégios de uma conta de usuário, realizada pelo ABD, é utilizada para controlar a autorização arbitrária. A atribuição de níveis de segurança adequados a cada conta de usuário é utilizada para controlar a autorização obrigatória. Esses dois conceitos serão detalhados nas seções seguintes.

3.4.1.1. Controle de acesso arbitrário (discricionário)

Segundo [ELMASRI & NAVATHE (2005)]: “São utilizados para conceder ou revogar privilégios a usuário, inclusive a capacidade de acessar arquivos de dados, registros ou campos específicos de uma maneira específica (como leitura, inclusão, exclusão ou atualização)”. Em banco de dados existem dois níveis para a atribuição de privilégios para o uso do sistema de banco de dados:

- Nível de conta - o ABD estabelece os privilégios específicos que cada conta tem, independente das relações no banco de dados. Isso se aplica à criação de esquemas ou a criações de tabelas, assim como a adicionar e remover atributos das relações e criar visões e recuperar informações a partir de um banco de dados. Caso uma conta não tenha o privilégio da criação de tabelas, por exemplo, nenhuma tabela poderá ser criada por meio desta conta; e
- Nível de relação (ou tabela) - o ABD pode controlar o privilégio para acessar cada relação ou visão individual no banco de dados. Os privilégios no nível de relação especificam para cada usuário as relações individuais na qual cada tipo de comando pode ser aplicado. Alguns privilégios também se referem às colunas individuais (atributos) das relações.

3.4.1.2. Controle de acesso obrigatório

Segundo [ELMASRI & NAVATHE (2005)]: “São utilizados para impor a segurança em vários níveis por meio da classificação dos dados e dos usuários em várias classes de segurança (ou níveis) e, depois, pela implementação da política de segurança adequada da organização”. Uma extensão disso é a segurança baseada em papéis (*role-based*), que impõe políticas e privilégios baseando-se no conceito de papéis. Essa abordagem de controle de acesso obrigatório deveria ser combinada com os mecanismos de controle de acesso discricionário descritos na seção anterior para uma melhor efetividade.

As classes de segurança típicas são: altamente secreta (*top secret*) (AS), secreta (*secret*) (S), confidencial (*confidential*) (C) e não confidencial (*unclassified*) (NC), em que AS é o nível mais alto e NC é o mais baixo (AS =

S = C = NC). O modelo usualmente utilizado de segurança multinível (onde cada nível é representado por uma classe), conhecido por modelo Bell-LaPadula (BLP), que foca na preservação da confidencialidade dos dados que ele protege. Cada sujeito (usuário, conta, programa) possui um nível de segurança e cada objeto (relação, tupla, coluna, visão, operação) possui uma classificação.

Quando um sujeito requisita um acesso, seu nível de segurança é confrontado com a classificação do objeto solicitado. BLP define as seguintes propriedades de segurança, que devem ser respeitadas:

- A Propriedade Simples de Segurança garante que um sujeito não pode ler uma informação classificada acima do seu nível de segurança (*no read-up*); e
- A Propriedade estrela (*) impede que um sujeito escreva informações em um objeto classificado abaixo de seu nível (*no write-down*).

Um administrador pode, quando necessário, mover informações de uma classificação maior para outra menor (violando a propriedade estrela).

Este tipo de controle de acesso é mais comum em aplicações governamentais, militares e de inteligência, assim como em muitas aplicações industriais e corporativas. No entanto, muitos SGBD comerciais oferecem somente controle de acesso arbitrário.

3.4.2. Controle de fluxo

O controle de fluxo previne que as informações fluam de tal maneira que cheguem aos usuários não autorizados. Neste sentido, devem ser verificados os canais que são o caminho das informações. O controle de fluxo regula a distribuição ou fluxo de informações entre objetos acessíveis. Um fluxo entre o objeto X e o objeto Y ocorre quando um programa lê valores em X e escreve valores em Y. Os controles de fluxo verificam se informações contidas em alguns objetos não fluem explicita ou implicitamente para objetos de menor proteção. Assim, um usuário não pode obter indiretamente em Y aquilo que ele ou ela não puder obter diretamente de X. Segundo [ELMASRI & NAVATHE (2005)]: “A maioria dos controles de fluxo emprega algum conceito de classe de segurança. A transferência de informação de um

remetente para um destinatário somente é permitida se a classe de segurança do receptor for pelo menos tão privilegiada quanto a classe do remetente".

Uma política de fluxo especifica os canais pelos quais a informação tem a permissão de se mover. A política de fluxo mais simples especifica exatamente duas classes de informação: confidencial (C) e não confidencial (NC), e permite todos os fluxos, exceto aqueles que saem de uma classe C e seguem para uma classe NC. Essa política pode resolver o problema do confinamento que surge quando um programa de serviço trata os dados como informações de clientes, algumas das quais podem ser confidenciais.

3.4.3. Controle de inferência

Um dos problemas de segurança em banco de dados é controlar o acesso a um banco de dados estatístico, o qual é utilizado para prover informações estatísticas ou resumos de valores baseados em vários critérios. Suponha-se que um órgão do governo tenha feito uma pesquisa junto à população para gerar algumas estatísticas. E nessa pesquisa foram levantados dados como idade, sexo, renda e outras informações. Esses dados foram armazenados em um banco de dados estatístico. Os estatísticos do governo só devem ter acesso às informações estatísticas da população, não sendo possível o acesso às informações confidenciais detalhadas de um indivíduo em particular. As medidas de controle correspondentes a esse tipo de banco de dados são chamadas controle de inferência.

O controle de inferência é utilizado em banco de dados estatísticos. Nesse tipo de banco de dados o SGBD só deve permitir consultas às informações estatísticas (médias, contagens, valores máximo e mínimo e desvio padrão) de uma população, não sendo permitido o acesso a uma tupla em particular, que contenha informações de um indivíduo em específico.

O controle de inferência também deve prevenir acessos mal-intencionados de usuários que tentam através de uma seqüência de consultas inferir os valores das tuplas. Uma técnica para que isso não venha ocorrer é a proibição de consultas repetitivas para uma mesma população de tuplas. Outro fator é quando se tem armazenado um número pequeno de tuplas e se tenta reduzir a inferência de informações individuais a partir das

consultas estatísticas. Para isso, é necessário que nenhuma consulta estatística seja permitida quando o número de tuplas de uma determinada população especificada pela condição da seleção fique abaixo de algum limite. Também podem ser introduzidas algumas incorreções no resultado das consultas estatísticas, tornando mais complexa à dedução de informações individuais.

3.4.4. Criptografia

A criptografia no banco de dados é utilizada para proteger dados sigilosos (como números de cartões de crédito) que podem ser transmitidos por alguma rede de comunicação. E também é utilizada para prevenir que usuários não autorizados acessem as partes confidenciais do banco de dados, codificando os dados e trazendo assim, dificuldades para serem decifrados.

Os métodos apresentados anteriormente podem não ser capazes de proteger os bancos de dados contra algumas ameaças. Se por exemplo, algum usuário ilegítimo de algum modo teve acesso às informações na hora da transmissão de dados e se a mensagem não estiver sido disfarçada (encriptada) então pode haver perdas irreparáveis. Como já explicado na seção 3.1.2.2 cifrar uma mensagem é um meio de manter os dados seguros em ambientes inseguros. Um sistema de banco de dados confiável mantém seus dados criptografados para não haver acessos indevidos. É muito comum o uso de criptografia simétrica, como o DES e o AES (seção 3.1.2.2), e assimétrica, como a criptografia de chave pública, o RSA (seção 3.3.1) e assinaturas digitais para o armazenamento dos dados.

4. Segurança em Banco de Dados Móveis

A democratização da computação ubíqua (acesso a dados em qualquer lugar, em qualquer hora, de qualquer modo) trouxe à tona a grande necessidade da segurança dos dados, por estarem expostos a pessoas que não se deseja que tenha o acesso àquela informação. Com isso, o uso de banco de dados em dispositivos móveis aumentou, introduzindo novas ameaças à privacidade e à confidencialidade dos dados. A mobilidade dos usuários, o uso da rede sem fio e a pouca quantidade de recursos dos dispositivos portáteis (se comparado com os computadores fixos) são fatores que comprometem a segurança da informação. A existência da mobilidade dos dispositivos se deve aos seus tamanhos cada vez menores e a sua incrível portabilidade, fazendo com que esses computadores portáteis possam ser facilmente perdidos ou roubados.

Para que a ubiqüidade se torne realidade, o uso da comunicação sem fio é indispensável. Porém, esse tipo de comunicação é mais propenso a ataques contra a privacidade e confidencialidade dos dados (e localização do usuário) que podem ser acessados facilmente por uma pessoa mal intencionada. Além disso, os computadores portáteis possuem uma escassez de recursos, restringindo algumas medidas de segurança.

Nesse capítulo, serão abordadas as áreas da segurança em banco de dados móveis na seção 4.1, e em seguida, na seção 4.2, serão discutidas as técnicas de segurança para as áreas abordadas e na última seção, a 4.3, é descrito como é realizada a segurança nos SGBD líderes de mercado.

4.1. Áreas da segurança em Banco de Dados Móveis

Nesta seção, serão apresentadas as áreas envolvidas na segurança do banco de dados móvel. Serão observados os objetos que devem ser protegidos e em que situações, visto que os ambientes móveis apresentam riscos às informações e aos metadados (dados pessoais que devem ser protegidos). Sabendo desses riscos, deve ser apresentada uma proteção que afete no gerenciamento, no acesso e também na transferência dos dados.

4.1.1. Transferência de dados

As freqüentes desconexões envolvidas no ambiente móvel podem por em perigo a consistência dos dados. O SGBD é também o responsável por evitar perdas em casos de desconexões não esperadas, com a ajuda da recuperação das transações. Quanto mais particionada a rede estiver, melhor deverá ser o processo de recuperação de falhas.

Além disso, o uso de *links* sem fio facilita o acesso indevido, porque as informações transmitidas pelo ar são acessadas de maneira simples, sem ser preciso muito esforço. Esse tipo de violação é difícil de detectar. Para isso é necessário o uso de criptografia na autenticação do usuário, para os dados serem mantidos privados A comunicação deve proteger os conteúdos dos dados transferidos contra ataques e acessos indevidos. Autenticação em ambientes móveis é, por exemplo, descrita em FEDERRATH et Al.(1997), NURKIC (1996), VARADHARAJAN & MU (1996) e ZHENG (1996). Muitos autores propõem o uso de encriptação assimétrica para a autenticação e criptografia simétrica (descritas na seção 3.1.1.2) para uma comunicação segura. Também é necessário que a comunicação entre as estações de base seja realizada com segurança.

4.1.2. Transferência de metadados

Os metadados na área de comunicação móvel são conhecidos como o contexto móvel, que pode ser entendido como o perfil do usuário, informação sobre a atual situação dos recursos e informação das características do dispositivo, da localização do usuário e do tempo. Somente o usuário deve saber a sua localização, por questão de privacidade [HARDJONO & SEBERRY (1995); VARADHARAJAN & MU (1996)]. Sua proteção é considerada como o principal objetivo da mobilidade. Todas as informações da identificação do usuário, incluindo a origem e o destino das mensagens, devem ser protegidas com a ajuda da criptografia para esconder a comunicação de uma outra rede de usuários.

Para se ter uma comunicação anônima, apelidos ou pseudônimos são usados. Com a análise do tráfego da rede se torna possível revelar a localização de um usuário. Para prevenir os rastros deixados pelas conexões das redes em ambientes móveis existem duas técnicas: o MIX [CHAUM

(1981); PFITZMANN et. Al (1991)] e o método da não revelação [FASBENDER (1996)]. Ambos os métodos usam criptografia. MIX atrasa e coleta diferentes mensagens e as envia numa seqüência aleatória para os receptores.

O método da não revelação aplica rodeios aos caminhos das informações, passando por vários agentes de segurança (AS), que só sabem seu predecessor e seu sucessor. A segurança aumenta quando os AS estão extremamente dispersos, possivelmente entre diferentes provedores. Contudo esses rodeios só são eficientes em redes cabeadas. Quando envolve banco de dados, MIX e os rodeios aumentam o tempo de resposta numa maneira dinâmica e atrapalham uma otimização eficiente.

Enquanto os usuários cruzam os limites das células, da rede móvel em que se encontram, sua informação, como a localização e o seu perfil, serão transferidos e replicados para estações de base vizinhas. Dessa maneira, aumentam os riscos para com os dados pessoais do usuário devido à "multiplicação dos pontos de ataque" [HARDJONO & SEBERRY (1995)]. Possivelmente, diferentes níveis de confiança são oferecidos por cada nó. As dificuldades se tornam mais fortes devido aos diferentes modelos de segurança.

4.1.3. Acesso e gerenciamento de dados

Os efeitos das desconexões como uma condição especial dos recursos, foram descritos na seção 4.1.1. As unidades móveis estão mais propensas à perda, e esse fato não é levado em consideração em muitos casos. Por decorrência, disso acontece à perda da confidencialidade dos dados pelo acesso indevido a eles. Para que possíveis ameaças venham ser prevenidas, é usada a encriptação dos dados, uma autenticação poderosa bem como mecanismos de controle de acesso. O problema é que os dispositivos móveis possuem poucos recursos, sendo necessário o uso de uma proteção simples. Há casos que se faz necessário que o usuário opte por renunciar alguns métodos de segurança por consumirem muito do dispositivo.

Um outro problema consiste na desproporção entre a quantidade de dados requisitados e os recursos disponíveis, que podem direcionar a uma violação na integridade ou disponibilidade.

4.1.4. Acesso e gerenciamento de metadados

Existe ameaça à segurança pela existência de diferentes níveis de segurança nas estações de base. Nos ambientes de banco de dados deve-se levar em conta a heterogeneidade dos modelos de controle de acesso (multinível, discreto, baseado em regra) e a heterogênea integração dos dados em modelos homogêneos. A mesma informação pode ser classificada diferentemente em diferentes sistemas.

Os movimentos do usuário podem ser tomados a partir das elevadas comunicações ou deduzidos da análise de tráfego. Mas, existe também uma maneira indireta de detectá-los, os usuários móveis estão trabalhando em banco de dados, acessando dados em atividades que têm a ver com o seu ambiente atual. As informações que os usuários têm acessado (criado, lido ou modificado) em tal caso tornam possível uma dedução dos seus movimentos por causa da localização das dependências dos dados. Isso é uma nova ameaça que é apresentada no acesso ao banco de dados móvel.

4.2. Técnicas de segurança

Até esse momento foram abordados os problemas e os desafios envolvidos na área da segurança em banco de dados móveis. Enquanto existe um grande esforço na área de segurança das redes dos ambientes móveis, a segurança dos bancos de dados é menos contemplada. Serão descritas nas próximas subseções proteções para resolverem alguns problemas da segurança no gerenciamento, acesso e transferência dos dados. Primeiramente, na subseção 4.2.1, será investigada a diferença entre sistema de banco de dados e a transparência da segurança. Então, será explicada a segurança da localização e dos movimentos do usuário, na subseção 4.2.2, e depois será descrita, na subseção 4.2.3, uma abordagem para responder a ambientes móveis dinâmicos e com recursos restritos.

4.2.1. Transparência

Para o usuário quando era realizada uma consulta no seu banco de dados, ele só podia visualizar a própria consulta e o resultado informado, que era processado de forma transparente. Como uma janela, na qual o vidro é transparente e invisível, que pode ser visualizado o outro lado. Nos sistemas móveis se deve dar o suporte ao usuário, não só fazer a consulta, mas também interferir no *parsing* e nas otimizações. Isso para reduzir o processamento de consultas remotas e evitar que no resultado haja uma grande quantidade de dados para um dispositivo com poucos recursos, através de um pré-processamento inteligente. Agora o usuário não só vê além da janela, ele quer saber a natureza da janela e verificar se ela não distorce o mundo real atrás dela.

4.2.2. Localização e movimentos seguros

Para que o usuário esteja protegido contra a revelação indevida da sua localização, os dados relacionados à sua localidade não devem ser armazenados. Pois os movimentos do usuário podem ser alcançados pela relação existente na mudança de localidade em um determinado espaço de tempo.

Uma boa prática na computação móvel é trabalhar com a economia de dados, que é um conceito na área de privacidade e endereça a um gerenciamento econômico no uso de dados pessoais. Dados pessoais podem ser entendidos como qualquer informação que possa ajudar a uma pessoa ser identificada. Sem o uso da economia de dados a localização do usuário se torna possível pela análise do tráfego da rede.

Como mencionado anteriormente a informação da localização deve estar protegida com ajuda da criptografia e das técnicas adequadas de controle de acesso. Para que um sistema trabalhe corretamente, somente os sistemas de adaptação podem usar a informação da localização. O contexto móvel deve, portanto, ser acessível somente pelo sistema, ou para o acesso dos próprios usuários para assegurar a transparência pretendida, como abordada na seção anterior.

A investigação indireta da localização pode ser evitada por meio de disfarce do fluxo real da informação. Foram descritas nas seções anteriores

técnicas de disfarce na transferência de dados. Nos sistemas de banco de dados, o fluxo da informação entre o remetente e o receptor é assíncrono por causa do armazenamento dos dados no banco entre a sua leitura e escrita.

Para dificultar o acesso indevido à localização do usuário, existem três técnicas diferentes: separação por agregação, que separa a identidade do usuário da sua localização num determinado tempo, separação vertical, na qual somente pequenas seções da localidade do usuário serão vistas, e separação horizontal, na qual a informação da localização do usuário não deve cruzar os limites do banco de dados (as suas camadas).

4.2.3. Ambientes móveis dinâmicos e com recursos restritos

Métodos de segurança e privacidade são em vários casos muito estáticos, enquanto que o ambiente de comunicação móvel é dinâmico e necessita de ajustes nas consultas e nos resultados. Com a mobilidade do usuário ele passa por várias células de rede, cada uma com seu controle de acesso e também cada dispositivo móvel é provido de diferentes medidas de segurança, por conter poucos recursos computacionais.

De acordo com a adaptação das funcionalidades do banco de dados, devem se tentar usar o conceito de adaptação para responder aos problemas de segurança no ambiente móvel. Um acesso de um SGBD em um *site* móvel para um SGBD fixo pode gerar o problema dos modelos de controle de acesso heterogêneos. A informação pode ser gerenciada, por exemplo, num modelo de matriz, enquanto o modelo de controle de acesso em *site* móvel pode ser realizado em multinível.

Essas incompatibilidades dos modelos não são específicas para a computação móvel. Elas são características de banco de dados distribuídos. Mas as heterogeneidades no hardware e no software aumentam o problema no ambiente móvel. Um processo de adaptação é necessário para selecionar o modelo adequado e para executar um modelo de adaptação. O processo de adaptação pode assegurar que nenhum dado será acessado ou transferido a partir de um domínio inseguro. O outro efeito favorável de um processo de adaptação é que a carga do controle de segurança não é somente do usuário.

Uma outra tarefa para um processo de adaptação é relacionada aos recursos. Isso ajusta o acesso ao banco de dados para os recursos disponíveis. Um outro efeito é que o usuário opta, em alguns casos, em realizar uma operação pretendida, liberando medidas de segurança. O processo de adaptação pode reduzir os métodos de segurança de acordo com a funcionalidade reduzida e ainda manter uma segurança mínima e obrigatória.

Em LUBINSKI (2000) pode se encontrar um maior detalhamento na adaptação da segurança de banco de dados em um ambiente móvel.

4.3. Segurança dos bancos de dados comerciais

Nesta seção serão abordados os quatros maiores sistemas de banco de dados móveis do mercado segundo KOCH (2005). O enfoque principal desta seção é mostrar como vem sendo tratada a segurança nos SGBD atuais. Para isso, foram observados os sistemas: Oracle *Lite*, DB2 *Everyplace*, SQL *Anywhere Studio* e SQL *Server* CE. Para os dados apresentados nessa seção, as informações foram retiradas dos *data sheet, white papers* e dos guias para desenvolvedor de cada um dos sistemas abordados [MICROSOFT (2007), IBM (2007), SYBASE (2007), ORACLE (2007)].

4.3.1. Oracle *Lite Mobile Server*

O produto Oracle *Lite Mobile Server* está construído sob o Sistema Oracle 10g *Application Server*. Suas principais características são:

- Pode ser utilizado nas plataformas Palm, Linux, Windows CE, Symbian EPOC e Windows 95/98/NT/2000/XP;
- O espaço em disco ocupado é cerca de 350 kb;
- Dá suporte às funcionalidades de SQL padrão;
- Possui serviços de mensagens em aparelhos de telefone, *pagers* e computadores portáteis;
- Possui serviços de mensagens *Push-based* e *Pull-based* para difusão;
- Dá suporte a *Binary Large Object* (BLOB); e
- Possui serviços de voz.

O Oracle *Lite* oferece ao usuário a encriptação do banco de dados. Uma vez encriptado, os dados armazenados no banco de dados não podem ser interpretados pelo exame dos arquivos. Uma senha é usada para gerar uma chave de encriptação de 128 bits. O SDBD Oracle *Lite* usa a encriptação AES. Após a encriptação, todo usuário que tentar estabelecer uma conexão com o banco deve prover uma senha de acesso, válida. Se a senha não existir no sistema é retornado um erro. Um banco de dados do Oracle *Lite* não pode ser encriptado ou decriptado caso haja alguma conexão aberta com o banco.

Mesmo com o banco de dados encriptado, isso não impede de o banco ser removido, fazendo necessário o uso de ferramentas extras para proteger que usuários não autorizados, removam o banco.

O Oracle *Lite* faz o uso de *Secure Sockets Layer* (SSL) [SSL (2007)] para prevenir qualquer interceptação e proteger a integridade enquanto os dados transitam entre o dispositivo e o servidor.

4.3.2. DB2 Everyplace

O DB2 *Everyplace* pode ser utilizado como um banco de dados local quando seu *host* está desconectado ou como um cliente acessando o servidor durante a conexão com a rede fixa. Suas principais características são:

- Pode ser utilizado nas plataformas Palm OS, Microsoft Windows CE/Pocket PC, Symbian EPOC, Linux embutido, QNX Neutrino, Linux e Microsoft Win32;
- Possui suporte para sincronização em redes sem fio;
- Pode ser sincronizado como cliente com os produtos da própria DB2, Sybase, Oracle, SQL Server;
- Dá suporte às funcionalidades de SQL padrão;
- Possui interface QBE (*Query-By-Example)* [QBE (2006)] como interface de consulta;
- Dá suporte ao uso de BLOB; e
- O espaço em disco ocupado pelo cliente é cerca de 150 kb, dando suporte a cerca de 10.000 registros.

O DB2 *Everyplace* provê uma solução que permite para uma aplicação implementar uma política de segurança corporativa. O primeiro objetivo é a encriptação secreta da informação sensível armazenada nas tabelas do DB2. Os dados são encriptados usando os métodos de encriptação como DES que usa chaves. O segundo objetivo é prover um *framework* de segurança que seja capaz de gerenciar as chaves usadas para encriptar às tabelas.

É sempre necessário ao usuário prover um ID e uma senha na hora da conexão com o banco de dados. Com isso, na hora que o usuário acessa ou cria tabelas encriptadas, a conexão deve informar ao DB2 *Everyplace* um ID e senha que não estejam em branco. Se a autenticação falhar, a aplicação só poderá acessar tabelas não encriptadas, não podendo criar novas tabelas encriptadas, remover tabelas encriptadas existentes ou acessar e atualizar um dado encriptado.

Antes que seja criada alguma tabela encriptada, a aplicação deve garantir ao usuário o privilégio de encriptação. A tabela encriptada é limitada àquele SGBD, não podendo ser movida, para um outro DB2 *Everyplace* contido em outro dispositivo móvel. Isso porque os diferentes bancos de dados têm diferentes chaves para encriptação e decriptação. Por isso, se uma pessoa é permitida acessar tabelas encriptadas em um banco, essa pessoa não poderá acessar um banco diferente usando o mesmo ID e senha.

O DB2 também oferece mecanismos de verificação da integridade do banco de dados após a sincronização e reparação de problemas ocorridos. Ele também usa SSL para a conexão com o servidor.

4.3.3. SQL *Server Compact Edition*

O Microsoft SQL *Server* 2005 CE é um SGBD relacional para o desenvolvimento de aplicações para equipamentos móveis. Suas principais características são:

- Dá suporte no lado do cliente a plataformas Windows XP, Windows CE, Windows 2003 para Pocket PC e Windows Mobile 5.0;
- Dá suporte à sintaxe de consulta da Linguagem SQL;
- Possui otimização de consultas e processamento de transações;
- Dá suporte a dados como *Image, Money* e *Identity*;
- Projetado para ser integrado com a Plataforma Microsoft .NET;

- Possui seu tamanho em torno de 1 Mb, dá suporte a bancos de até 4 gb e 249 índices por tabela; e
- Mantém interoperabilidade com os produtos da IBM, Oracle e Sybase.

O SQL Server CE confia na combinação dos seguintes modelos de segurança: *Microsoft Internet Information Services* 5.0 (IIS) ou IIS 4.0, SQL *Server* 2000 (*Service Pack* 1 ou mais novos) ou SQL *Server* versão 7.0 (*Service Pack* 4 ou mais novos), e Microsoft Windows 2000, Microsoft Windows XP Professional, ou Microsoft Windows NT® 4.0. Em alguns ambientes, será preciso considerar também o *Microsoft Internet Security* e o *Acceleration Server* 2000 (ISA) [MICROSOFT (2006)]. Como resultados, existem vários *gateways* através dos quais os usuários devem passar para conectar o dispositivo com o SQL Server.

O modelo de segurança IIS dá suporte a três diferentes protocolos de autenticação: Anônima, Básica e Integrada com o *Windows Authentication*. O IIS também dá suporte à encriptação SSL de 128-bit no banco de dados do cliente e no servidor IIS. Todas as plataformas do Windows CE, com suporte no SQL *Server* CE, trabalham com os três diferentes protocolos de autenticação.

O acesso anônimo, como o nome já diz, permite ao cliente um acesso aos recursos do servidor IIS anonimamente. Esse tipo de acesso é mais bem usado em situações nas quais o servidor não precisa manter os passos dos visitantes que estão usando os dados ou nas quais os dados disponíveis não precisam ser protegidos. Geralmente, o acesso anônimo não é recomendado para a distribuição do SQL *Sever* CE, porque ele é inseguro.

A autenticação básica confia em parte do protocolo HTTP 1.0. Os usuários devem prover um *login* e uma senha do Windows válida, e o IIS realiza o *login* no sistema usando a conta do Windows que requisitou o acesso. Se o *login* for rejeitado, a conexão é fechada e um erro é retornado para o cliente. A autenticação básica por si só não é considerada segura pelo fato dos *logins* e das senhas serem transmitidas na codificação 64 bits, que é relativamente fácil de ler. Esse tipo de autenticação deve ser usado com SSL

e tem suporte em todos os dispositivos que usam Windows CE, utilizáveis pelo SQL *Server* CE 2.0.

O Windows *Authentication* permite ao usuário realizar o *login* num site *Web* usando um Windows *Domain Account*. Por causa disso, esse método de autenticação requer uma conta de usuário, podendo somente ser usado em uma *intranet*. Windows *Authentication* usa o algoritmo de *hashing* para proteger as informações do *login* e da senha na transferência.

O SQL *Server* CE dá suporte a senhas de arquivos do banco de dados armazenado no dispositivo e uma encriptação RSA de 128 bits. O SGBD trabalha com uma única senha de segurança.

4.3.4. SQL Anywhere Studio

O produto SQL *Anywhere Studio* 10 da Sybase possui uma solução de banco de dados móvel chamada de Sybase UltraLite. Suas principais características são:

- As plataformas consideradas são Windows (32 ou 64 bit), Mac OS X, Netware, algumas variações do UNIX e Linux (32 ou 64 bit), a popular plataforma handheld com Microsoft Windows CE e o Palm *Computing Platform* e Symbian OS 8 ou superior;
- Acesso aos dados através de JDBC, SQL embutida e API baseada em C++;
- Dá suporte ao uso de BLOB;
- O tamanho máximo do banco de dados é de 2Gb e de cada linha é de 4k, já no cliente o espaço ocupado é cerca de 150 kb;
- O número de linhas de cada tabela depende do tamanho do banco de dados, podendo ter até 1.000 tabelas por banco de dados e até 65.535 tuplas, 65.534 colunas e 65.535 índices por tabela; e
- Possui suporte para sincronização em redes sem fio.

Banco de dados no SGBD UltraLite podem ser criados com uma das seguintes escolhas para a segurança: ofuscação ou encriptação. Uma vez escolhida, não poderá ser mudada, a não ser que seja descarregado todo o banco de dados, removido e carregado novamente. Por padrão, bancos de dados no UltraLite são criados sem nenhuma medida para *ofuscar* os dados no banco. Utilitários que examinam os arquivos que estão contidos no banco

de dados e mostram os caracteres dos dados armazenados podem por em risco a segurança do sistema. O formato do arquivo do SGBD é proprietário, mas seus conteúdos são capazes de serem visualizados.

Para a encriptação do banco de dados é preciso a escolha de uma chave, que pode ser modificada caso necessário. Após encriptação do banco, só poderá ser acessado com o uso da chave especificada. Caso contrário, os dados contidos no banco não poderão ser acessados.

A ofuscação do banco é uma simples máscara dos conteúdos do banco de dados, para prevenir que utilitários revelem os arquivos de dados. A ofuscação é transparente ao usuário e às aplicações.

Para a autenticação no SGBD, o UltraLite pode definir até quatro ID de usuário e suas respectivas senhas. É de responsabilidade do DBA a criação dos ID e das senhas para garantir o acesso de outros usuários ao banco. Esse ID não pode ser modificado.

O SQL *Anywhere* usa os padrões e protocolos de encriptação existentes na indústria, como AES, ECC [ECC (2007)], RSA e SSL para garantir a segurança do sistema.

4.3.5. Comparação

Abaixo, no Quadro 4-1**Erro! Fonte de referência não encontrada.**, é feito uma comparação entre os SGBD do mercado atual.

Quadro 4-1 - Resumo das características dos sistemas apresentados. Adaptado de AMADO (2002)

PRODUTO (versão atual)	Sistemas Operacionais	Espaço em disco	Ferramentas de sincronização	Tecnologias de desenvolvimento e gerenciamento
Sybase SQL Anywhere Studio 10	Windows (32 ou 64 bit), Mac OS X, Netware, Microsoft Windows CE e o Palm; Symbian OS	150Kb	MobiLink; SQL Remote	Sybase Infomaker; Power Designer; Sybase Central; Interactive SQL
IBM DB2 Everyplace	Palm OS, Microsoft Windows,CE/Pocket PC, Symbian EPOC, Linux embutido, QNX, Neutrino, Linux, Microsoft Win32.	150Kb	DB2 Everyplace Sync Server; DB2 Everyplace Sync Client	Mobile Application Builder; Mobile Devices Administration Center; *DataPropagator*

Microsoft SQL Server 2005 Windows CE	Windows XP/CE, Windows 2003 para Pocket PC, Windows Mobile 5.0.	1Mb	Remote Data Access (RDA); Replicação Intercalada (*Merge Replication*)	Microsoft Visual Studio.NET; Microsoft eMbedded Visual Tools; ADOCE, ADOXCE, OLE DB/CE, ADO.NET
Oracle 10g Lite	Palm; Linux; Windows CE; Symbian EPOC; Windows 95/98/NT/2000/XP	350kb	Mobile Server; Message Generator and Processor (MGP)	Mobile Development Kit

5. Testes realizados

Neste capítulo, serão descritos o passo a passo de como foram conduzidos os testes. Foram realizados testes em dois dispositivos móveis, um *SmartPhone* e um *Laptop*. A escolha desses dois dispositivos se deve pelo fato de que eles têm características bastante diferentes. Essas características podem influenciar nos métodos de segurança do SGBD. Na Quadro 5-1 pode-se observar as características de cada um deles:

Quadro 5-1 - Comparação entre o Nokia 6620 e o Toshiba Satelite A100-SK9

Funcionalidades	Nokia 6620	Toshiba Satellite A100-SK9
Sistema Operacional	Symbian OS v7.0s	Windows XP Home Edition
Processador	150 MHz (32-bit)	Intel® Core™ Duo processor T2500, 2 GHz
Armazenamento	12 Mb (Interno) 24 Mb (RAM)	120 Gb SATA 1 Gb (RAM)
Conectividade	GPRS; GSM; EGPRS; USB; Infrared; Bluetooth.	56K V.92 data/fax modem; Ethernet Integrada 10/100 LAN; Intel® PRO/Wireless LAN, 802.11a/b/g.
Velocidade de Conexão	118kbps	56kbps à 100 Mbps
Dimensão de Tela	4.28” 176 X 208 65,536 cores	15.4” TFT WXGA 1280 x 800 16.7 Milhões de cores
Peso	124g	2,8Kg
Bateria	850mAh 8 dias (*standby*)	4000mAh 3.5 horas

O SGBD móvel escolhido foi o Oracle 10g *Lite*, por ser o único que pode ser executado em um dispositivo tão escasso de recursos como o Nokia 6620, se o compararmos a um *Palm* ou a um *Laptop*. O sistema operacional dele é o Symbian versão 7, o DB2 *Everyplace* dá suporte ao uso do seu banco de dados móvel a partir da versão 8 do Symbian. O processador desse *smartphone*, como apresentado, é de apenas 150 mhz, o que influi no tipo de algoritmo a ser utilizado para tratar a segurança do banco de dados. Por isso se faz necessário avaliar como é tratada a segurança nesses dispositivos e qual é a influência do pouco poder de processamento nos dispositivos quanto à segurança dos dados.

Para os testes que serão demonstrados, não foram levadas em consideração, a segurança na hora da transferência dos dados para o servidor ou na hora em que estão sendo acessados os dados através da rede sem fio. Os dados são transmitidos com o uso do SSL para que seja garantida a segurança na sua transmissão. O que será contemplado nos testes desse trabalho é a segurança das informações no gerenciamento e no acesso dos dados contidos no aparelho, que pode ser extraviado, como dito nas seções anteriores. Portanto, se as informações não estiverem sendo seguramente armazenadas, isto colocará o usuário em risco pela perda da privacidade dessas informações.

5.1. Nokia 6620

Para a instalação do Oracle *Lite* nesse dispositivo foi necessário fazer o *download* do *Oracle Database Lite 10g Release 2 (10.2.0.1) for Symbian* encontrado em [LITE (2007)]. A sua instalação no dispositivo se dá através do **olite_core.sis** e o **olite_tools.sis** contidos no arquivo de *download*. Os seguintes componentes são encontrados no dispositivo após a instalação:

- OLAES.DLL - Módulo de encriptação AES;
- OLOBJ40.DLL - Modulo principal do SGBD;
- OLSQL40.DLL - Módulo do *parser* do SQL;
- OLOD2040.DLL - O *driver* ODBC 2.0;
- ZLIB.DLL - Módulo de compressão;
- OCAPI.DLL - Módulo de sincronização;
- POLITE.INI - Arquivo de configurações comuns do sistema;
- ODBC.INI - Arquivo de gerenciamento de nomes dos dados;
- OLITE40.MSB - Arquivo de mensagens em Inglês;
- CREATEDB.EXE - Utilitário para criação de uma nova base de dados;
- REMOVEDB.EXE - Utilitário para a remoção de uma base de dados;
- ENCRYPDB.EXE - Utilitário para criptografar o banco de dados;
- DECRYPDB.EXE - Utilitário para decriptar um banco de dados criptografado; e

- ODBINFO.EXE - Utilitário para mostrar/modificar as configurações do banco de dados.

Após a criação, foi necessário o uso de um aplicativo que simule o *Prompt DOS* do Windows agora no celular, como o **eshell** [XEMACS (2006]. Com esse aplicativo o DBA é capaz de, por exemplo, criar o banco de dados no celular, remover o banco e encriptar a base de dados. Para criação do banco de dados, foi usado o utilitário CREATEDB.EXE que segue a seguinte sintaxe:

CREATEDB *NomeOrigemDados NomeDoBancoDeDados SenhaUsuarioBancoDados [[[IDBanco] TAMANHO_BANCODADOS] TAMANHO_EXTENSÃO] [VALOR_LINGUAGEM]*

Onde os parâmetros e as palavras chave são descritos como:

- *NomeOrigemDados* – Serve para armazenar as informações sobre a conexão com a base de dados requeridas pelo *driver* ODBC;
- *NomeDoBancoDeDados* - É o nome do arquivo do banco de dados que será criado. Como, por exemplo, Cliente.odb;
- *SenhaUsuarioBancoDados* – A senha do usuário do SGBD;
- *IDBanco* - Serve como o identificador do banco de dados;
- *TAMANHO_BANCODADOS* – O tamanho do banco de dados em *byte;*
- *TAMANHO_EXTENSÃO* – Quantidade incremental de páginas em arquivo de banco de dados; e
- *VALOR_LINGUAGEM* – É um valor constante que cria um banco de dados habilitado à classificação do idioma especificado. O padrão é o BYNARY (binário).

Criou-se o banco de dados de nome **clientes** com a senha de acesso "1234", usando o utilitário **CREATEDB** (demonstrado anteriormente). Após a criação do banco de dados, foi realizada a encriptação da base através do comando **ENCRYPBD** que usa AES de 128 bits. Os comandos utilizados são mostrados nas linhas a seguir e na Figura 5-1:

CREATEDB polite clientes.odb 1234

ENCRYPDB polite clientes.odb

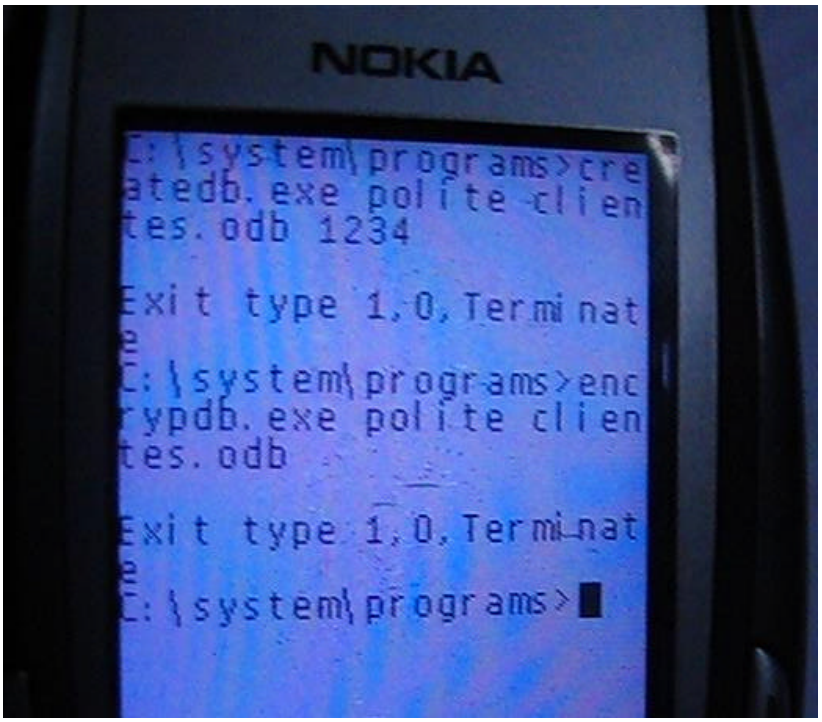

Figura 5-1 - Criação e Encriptação do BD no Nokia 6620

O processo de criação da base de dados durou cerca de 5 segundos. A arquivo do banco de dados gerado é o nome do banco com a extensão ***db*** (i.e. clientes.db) no diretório raiz da memória do celular. Logo após o arquivo ter sido encriptado, como explicado anteriormente, as versões do arquivo, antes e depois da encriptação do banco de dados, foram transferidas para uma máquina *desktop* comum (mas com maior poder de processamento que o dispositivo móvel testado), para ser observado como são armazenadas as informações nesse arquivo.

Na Figura 5-2, pode ser observado o arquivo anterior à encriptação do banco de dados, com 350 linhas, contendo uma mistura de textos indecifráveis (parecidos com arquivos binários) e palavras que podem ser facilmente identificadas. Com isso, uma pessoa mal intencionada pode concentrar seus esforços apenas em partes do arquivo que sejam do seu interesse, por exemplo, na parte na qual é encontrado COLUMN_NAMES, possibilitando descobrir o nome das colunas. O arquivo foi aberto num editor de texto comum.

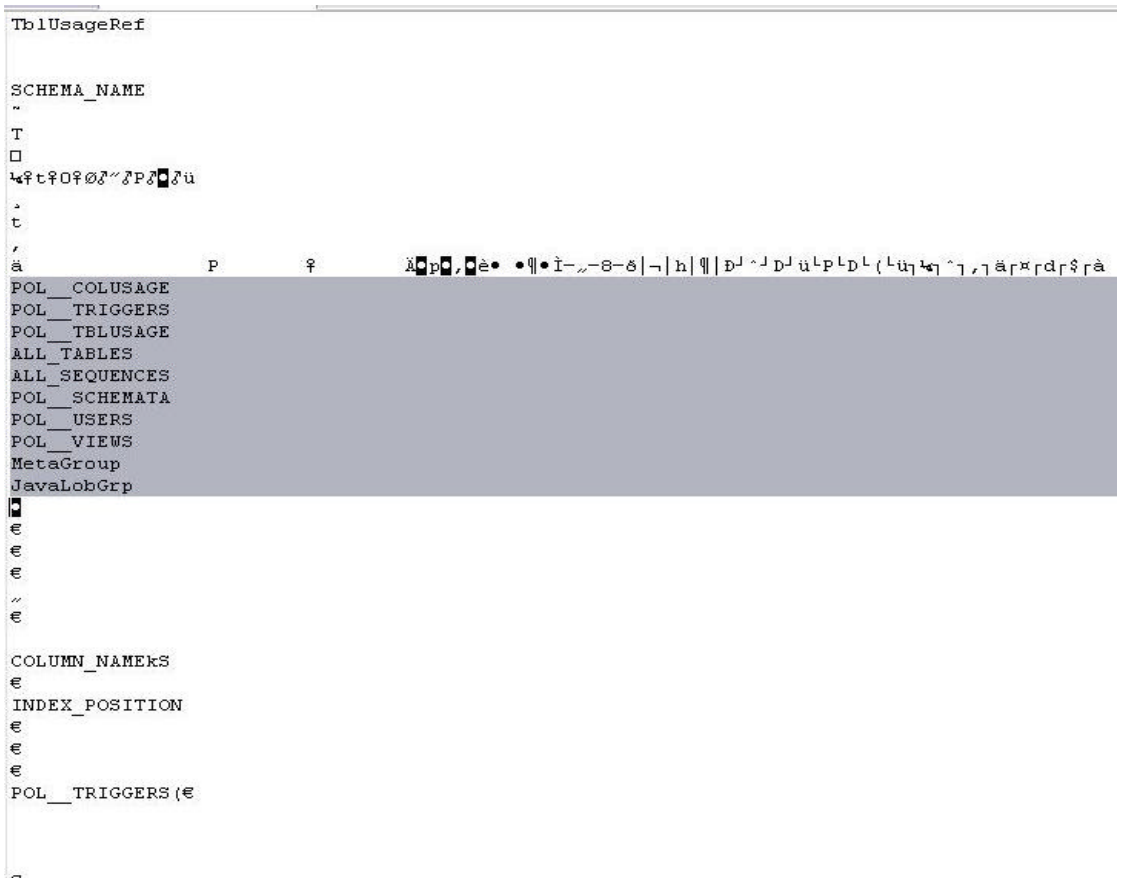

Figura 5-2 - Arquivo do banco de dados antes da criptografia

Logo após, foi aberto no mesmo editor, o arquivo que continha as informações do banco de dados encriptado (ver Figura 5-3). O arquivo agora contém 1551 linhas quase cinco vezes mais do que o arquivo antes da encriptação. Ele agora está indecifrável, sendo impossível identificar qualquer a palavra que esteja no texto. Isso porque o arquivo está encriptado com o algoritmo AES, que é um algoritmo de encriptação avançado que usa uma chave de 128 bits.

Figura 5-3 - Arquivo do banco de dados depois da criptografia

5.2. Toshiba Satellite A100-SK9

Esse dispositivo possui bem mais recursos computacionais que o Nokia 6620 apresentado na seção anterior. Por isso, foi possível a instalação tanto da versão servidora do Oracle 10g *Lite* como da versão cliente. Neste trabalho foram realizados testes na versão cliente do *Lite*. Quando o Servidor do Oracle (*Mobile Server*) é instalado em uma máquina ele disponibiliza algumas aplicações de exemplo, para algumas plataformas.

Para o cliente móvel ser testado foi usado o exemplo de uma aplicação *web*, denominada *WebToGo* disponibilizada pelo servidor do Oracle *Lite*, que também disponibiliza versões clientes para as plataformas Windows 32, Pocket PC e Palm OS.

Para ter acesso a essa aplicação pelo cliente móvel, é necessário fazer o *download* da versão adequada. Para isso deve-se, então, acessar a seguinte página *web*:

http://<<IPMaquina>>:<<Porta>>/webtogo

Onde os parâmetros são descritos como:

- IPMaquina – É o IP da máquina que está instalado o servidor do SGBD Oracle; e

- Porta – É o número da porta configurado para o *listener* HTTP do servidor do SGBD que foi configurada.

Após o cliente ter acessado a página (mostrada na Figura 5-4) no canto superior direito deve-se clicar com o *mouse* em **Configuração**. Será aberta uma página contendo várias aplicações, em várias linguagens, para várias plataformas, como pode ser conferido na Figura 5-5. É necessária a escolha do Oracle *Lite WEB*. Clicando com o *mouse* nele, aparecerá uma forma de salvar o executável na máquina cliente. Após a instalação do executável, o usuário poderá acessar a versão cliente pelo *browser web* com a URL http://localhost/webtogo/index.html. O usuário e senha padrão do cliente é JOHN.

Figura 5-4 - Acesso ao webtogo no cliente móvel

Figura 5-5 - Cadastro de Mídias

Nesse cliente, são disponibilizadas várias aplicações. A aplicação escolhida para este teste foi a *Sample* 3, que é o cadastro/consulta de dados de CD, DVD, entre outras mídias (ver Figura 5-6). Os dados armazenados nessa tabela são armazenados num arquivo com uma extensão odb, que foi instalado na pasta /oldb40/<<Nome do Usuário>> da aplicação. Com isso, já pode ser identificado um problema: é que dentro da pasta oldb40 se encontram os nomes dos usuários do banco de dados, facilitando o trabalho dos usuários mal intencionados.

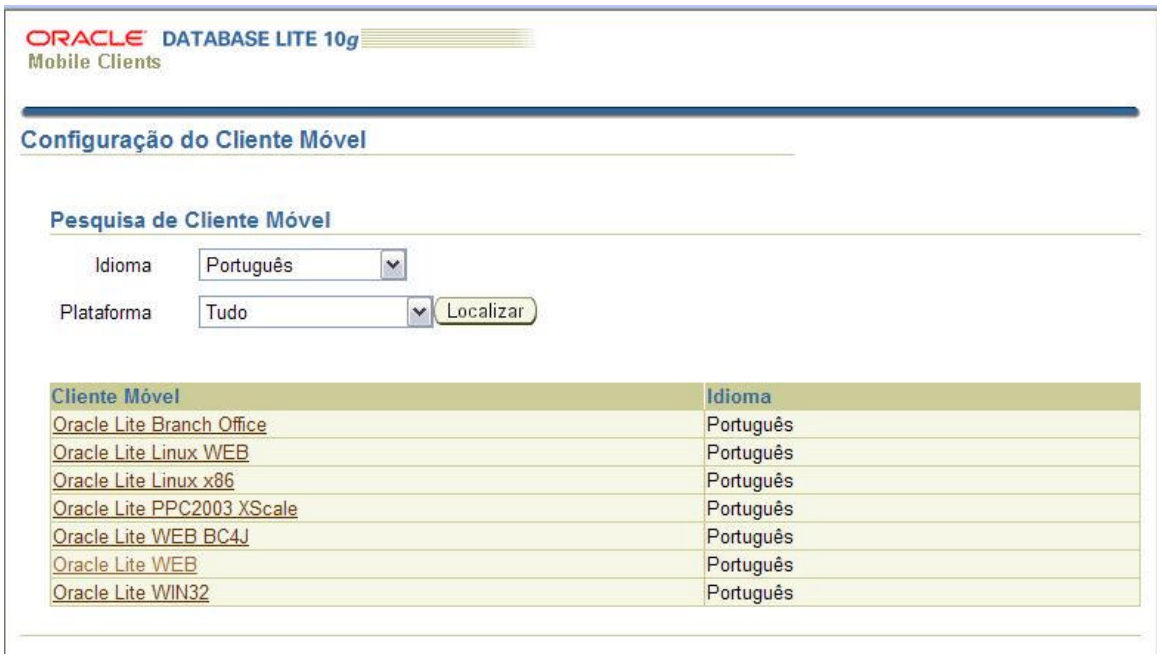

Figura 5-6 - Download da aplicação móvel

Esse arquivo está configurado da mesma maneira que o arquivo criado no aparelho Nokia 6620, encriptado com o algoritmo AES tornando difícil o acesso aos seus dados, como mostrado anteriormente.

5.3. Conclusão

Com a realização desses testes, pôde ser observado que o Oracle 10g *Lite*, mesmo em um dispositivo com pouco poder de processamento e pouco poder de armazenamento, se mostrou bastante seguro com relação ao acesso e gerenciamento das informações armazenadas nele. A Oracle também disponibiliza uma vasta documentação (contida no arquivo de *download*), que ajuda tanto ao desenvolvedor de aplicações nessa plataforma quano ao DBA, na criação e no gerenciamento seguro dos dados.

Com os testes, pôde também ser observada a preocupação da Oracle com a segurança dos bancos de dados móveis desde os dispositivos com poucos recursos até dispositivos mais avançados. Embora existam ataques ao AES [COURTOIS (2007)], usado para a encriptação dos dados, esses ataques só funcionam se a pessoa mal intencionada souber uma parte real do texto que está sendo decifrado. Além do mais, as operações envolvidas para se descobrir a chave de criptografia demoram muito tempo.

6. Considerações finais e trabalhos futuros

No Capítulo 2 desse trabalho, foi apresentada uma visão geral sobre os bancos de dados móveis, iniciando com uma breve descrição da computação móvel tão presente hoje em dia. E logo após, foram abordadas as inúmeras arquiteturas existentes para SGBD móveis, assim como as características principais desses SGBD.

O objetivo desse segundo capítulo foi permitir o entendimento dos conceitos envolvidos nessa área, bem como destacar as dificuldades e os desafios encontrados na computação móvel, que devem ser levados em consideração quando do desenvolvimento em SGBD móvel. Questões como o gerenciamento de transações e suas propriedades como consistência e integridade, não podem ser totalmente aplicadas, uma vez que suas operações por dependerem de dois ambientes, em muitos momentos desconectados, não permitem que as transações de banco de dados possam ser executadas como no seu modelo centralizado e distribuído. Assim, constantes pesquisas se fazem necessárias nessa área, bem como na área de sincronização com os servidores, que mesmo sendo áreas bastante estudadas, precisam sempre estar evoluindo.

No Capítulo 3 desse trabalho, foram abordados os conceitos principais de segurança como confidencialidade, integridade e disponibilidade, sendo os últimos também conceitos envolvidos na área de banco de dados. Foram ainda abordadas as principais ameaças à segurança e as principais vulnerabilidades. Logo após, foi abordada a criptografia, tão discutida quando se trata de segurança da informação, e suas divisões simétrica e assimétrica. Concluindo o terceiro capítulo, foram estudadas a segurança na área dos dispositivos móveis, nas redes sem fio e nos bancos de dados tradicionais.

Os capítulos 2 e 3 foram necessários para permitir o entendimento dos conceitos, abordagens, protocolos já existentes nas áreas de computação móvel, dispositivos móveis, redes sem fio, banco de dados e segurança para que no Capítulo 4 fossem integradas todas essas áreas e estudado como é que elas convivem quando estão interligadas. Foi visto então que nos SGBD móveis não se deve só estar preocupado com a segurança envolvida na hora da transmissão dos dados ou metadados numa rede sem fio, mas também se

preocupar com a segurança no acesso e no gerenciamento dos mesmos, pois devido à mobilidade dos dispositivos portáteis se tornam fáceis de serem perdidos ou extraviados. E como os recursos dos dispositivos móveis são escassos, torna-se complicado construir eficazes métodos de segurança.

Foi relatado também como os principais SGBD do mercado estão garantindo a segurança das informações envolvidas no contexto móvel.

No capítulo de testes, Capítulo 5, foram utilizados dois dispositivos com características bastante diferentes, permitindo perceber que mesmo assim, a Oracle está protegendo os dados do usuário com técnicas eficientes de criptografia.

Em trabalhos futuros é interessante aprofundar mais os estudos área do gerenciamento e acesso às informações contidas nos SGBD móveis, menos contemplados, por priorizar a segurança na hora da transmissão dos dados numa rede sem fio. Isso leva a um grande desafio por se tratarem de dispositivos com pouco poder de processamento e de armazenamento, como o NOKIA 6620 utilizado no capítulo cinco, e mesmo assim serem necessárias eficientes medidas de segurança para não estarem susceptíveis a ataques de usuários mal intencionados. É óbvio que, com o passar do tempo, o poder de processamento e de armazenamento em pequenos dispositivos vai aumentar e então surgirão novos desafios.

7. Referências

3DES. Wikipedia. 2007. Disponível em: http://pt.wikipedia.org/wiki/3DES . [Acessado em 25/03/2007].

ADIBA, M.; SERRANO-ALVARADO, P.; RONCACIO, C. L. ***Mobile Transaction Supports for DBMS: An Overview***. LSR-IMAG Laboratory, 2001.

AES. Wikipedia. 2007. Disponível em: http://en.wikipedia.org/wiki/Advanced_Encryption_Standard . [Acessado em 25/03/2007].

ALBUQUERQUE, Ricardo; RIBEIRO, Bruno. **Segurança no Desenvolvimento de Software – Como desenvolver sistemas seguros e avaliar a segurança de aplicações desenvolvidas com base na ISO 15.408**. Editora Campus. Rio de Janeiro. 2002.

ALONSO, R.;KORTH, H. F. ***Database system issues in nomadic computing***. *Proceedings of the ACM SIGMOD International Conference on Management of Data*. Washington, D.C., páginas 388 - 392. Maio, 1993

AMADO, PAULO. **Bancos de dados móveis: visão geral, desafios e soluções atuais**. Centro de Informática. Universidade Federal de Pernambuco. Outubro, 2002.

ARAUJO, L. V. de; FERREIRA, J. E.. ***Cache* Semântico para Computação Sem Fio Baseado na Abstração de Composição dos Dados**. WorkSIDAM, Workshop de Sistemas de Informação Distribuída de Agentes Móveis. São Paulo, páginas 83-89. Outubro, 2000.

BARBARÁ, D.. ***Mobile Computing and Databases – A Survey***. IEEE *Transactions on Knowledge and Data Engineering*, vol 11, n. 1, Fevereiro, 1999.

BASIC. Wikipedia. 2007. Disponível em: http://pt.wikipedia.org/wiki/BASIC . [Acessado em 25/03/2007].

BLOWFISH. Wikipedia. 2007. Disponível em: http://en.wikipedia.org/wiki/Blowfish_%28cipher%29 . [Acessado em 25/03/2007].

BLUETOOTH. Wikipedia. 2007. Disponível em: http://pt.wikipedia.org/wiki/Bluetooth . [Acessado em 25/03/2007].

BRAZ, FERNANDO J.. **Análise de Mecanismos Para Recuperação de Falhas Em Bancos de Dados Móveis**. Universidade Federal de Santa Catarina. Outubro, 2002.

BREITBART, Y.; KOMONDOOR, R.; RASTOGI, R.. ***Update Propagation Protocols for Replicated Databases***. ACM SIGMOD *International Conference on Management of Data*, página.97-108, 1999.

CHAUM, D.. ***Untraceable electronic mail****. Communications of the ACM*, 1981.

CÔRTES, SÉRGIO DA COSTA; LIFSCHITZ, SÉRGIO. **Banco de Dados para um Ambiente de Computação Móvel**.

COURTOIS, NICOLAS T.. ***Is AES a Secure Cipher ?***. Março, 2007.Disponível em: http://www.cryptosystem.net/aes/ .[Acessado em 28/03/2007].

DES. Wikipedia. 2007. Disponível em: http://en.wikipedia.org/wiki/Data_Encryption_Standard. [Acessado em 25/03/2007].

DESPANDE, P. M.; RAMASAMY, K.; SKUKLA, A. ; NAUGTHON, J. F. ***Caching Multidimensional Queries using Ckuncks***. Procedente de SIGMOD, 1998, p. 259-270.

DIFFIE-HELLMAN. Wikipedia. Disponível em: http://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange. [Acessado em 25/03/2007].

DUNHAM, M. H.; HELAL, S. ***Mobile Computing And Databases: Anything New?****. SIGMOD Record, Vol. 24, No. 4,* páginas 5-9. Dezembro, 1995.

DUNHAM, M.; KUMAR, V. ***Defining Location Data Dependency, Transaction Mobility and Commitment***. Relatório Técnico 98-CSE-1, fevereiro, 1998, p. 1-22.

ECC. Wikipedia. 2007. Disponível em: http://en.wikipedia.org/wiki/Elliptic_curve_cryptography. [Acessado em 25/03/2007].

ELMASRI, RAMEZ; NAVATHE, SHAMKANT B. **Sistemas de Banco de Dados - Fundamentos e Aplicações**. S. B. volume Tradução da terceira edição. Livros Técnicos e Científcos Editora – LTC, 2002.

ELMASRI, RAMEZ; NAVATHE, SHAMKANT B.. **Sistemas de Banco de dados**. Person, Addison Ewsley, 4ª Edição. 2005.

FASBENDER, A.; KESDOGAN, D.; KUBITZ, O.. ***Variable and scalable security: Protection of location information in mobile IP****. In Proc. of the 46th IEEE Vehicular Technology Society Conference*, Atlanta. 1996.

FEDERRATH, H.; JERICHOW, A.; KESDOGAN, D.; PFITZMANN, A.; TROSSEN, D.. ***Minimizing the average cost of paging on the air interface - an approach considering privacy****. Proc. of the IEEE 47th Annual Vehicular International Technology Conference (VTC97).* 1997.

FTP. Wikipedia. 2007. Disponível em: http://pt.wikipedia.org/wiki/File_Transfer_Protocol . [Acessado em 25/03/2007].

HARDJONO, T.; SEBERRY, J. ***Information issues in mobile computing****. Proc. of the IFIP TC 11 Int. Conf. on information security*, Londres. 1995.

HERNAN, SHAWN; LAMBERT, SCOTT; OSTWALD, TOMASZ; SHOSTACK, ADAM. ***Uncover Security Design Flaws Using The STRIDE Approach***. MSDN Magazine. Novembro, 2006. Disponívle em: http://msdn.microsoft.com/msdnmag/issues/06/11/ThreatModeling/default.aspx . [Acessado em 25/03/2007]

HEUER, A.; LUBINSKI, A.. ***Database acess in mobile environments****. Proc. of the Database and Expert Systems Applications*. 1996.

HTTP. Wikipedia. 2007. Disponível em: http://pt.wikipedia.org/wiki/HTTP. [Acessado em 25/03/2007].

IBM. **DB2** ***Everyplace***. 2007. Disponível em: http://www-306.ibm.com/software/data/db2/everyplace/ . [Acessado em 24/03/2007].

IDEA. Wikipedia. 2007. Disponível em: http://en.wikipedia.org/wiki/International_Data_Encryption_Algorithm . [Acessado em 25/03/2007].

IEEE 802.11i. Wikipedia. 2007. Disponível em: http://pt.wikipedia.org/wiki/IEEE_802.11i . [Acessado em 25/03/2007].

IMIELINSKI, T.; BADRINATH, B. R.. ***Mobile wireless computing: Solutions and challenges in data management****. Technical report*, Rutgers University, U.S. 1992.

IMIELINSKI, T.; NAVAS, J. C. ***GPS Based Addressing and Routing***. Relatório Técnico LCSR-TR262, CS Dept, Rutgers University, Março, 1996.

INFORMAÇÃO. Wikipedia. 2007. Disponível em: http://pt.wikipedia.org/wiki/Informa%C3%A7%C3%A3o . [Acessado em 18/03/2007].

INFORMATION SECURITY. Wikipedia 2007. Disponível em: http://en.wikipedia.org/wiki/Information_security . [Acessado em 18/03/2007].

IrDA. WEBOPEDIA, Outubro, 2001. Disponível em: http://www.webopedia.com/TERM/I/IrDA.html . [Acessado em 25/03/2007].

ITO, GIANI C. **Bancos de dados móveis: uma análise de soluções propostas para gerenciamento de dados**. Tese de mestrado em Ciência da Computação. Universidade Federal de Santa Catarina, abril de 2001.

KOCH, GEOFF. ***Always On? Not Quite Yet***. SD Times. Dezembro, 2005. Disponível em: http://www.sdtimes.com/article/special-20051215-01.html . [Acessado em 23/03/2007].

KRAUSE, MICKI E TIPTON, HAROLD F.. ***Handbook of Information Security Management***. Auerbach Publications. 1999.

LAUREANO, MARCOS A. P.; MORAES, PAULO E. S.. **Segurança como estratégia de gestão da informação**. Revista Economia & Tecnologia – ISSN 1415-451X, Vol. 8 – Fascículo 3 – P. 38-44. 2005.

LEE, VALENTINO; SCHNEIDER, HEATHER; SCHELL, ROBBIE. **Aplicações móveis: Arquitetura, Projeto e Desenvolvimento**. Pearson, Makron Books. 2005.

LITE. ***Oracle Database Lite 10g for Symbian OS***. Oracle Database 10g, Oracle Technology Network. 2007. Disponível em: http://www.oracle.com/technology/products/lite/symbian.html . [Acessado em 28/03/2007].

LUBINSKI, A.. ***A model with roles an norms for the conceptual design of security requirements in enterprise information systems***. *Proc. of the VIS (Reliable Information Systems)*. 1993.

LUBINSKI, A.. ***Database Security meets Mobile Requirements***. *University of Rostock, Computer Science Dept*. 2000.

LUBINSKI, A.; HEUER, A. ***Configured Replication for Mobile Applications***. Workshop Grundlagen von Datenbanken, p.1-13, 2000.

MANGANELLI, ELENICE C.; ROMANI, JULIANO. **Protocolos de Sincronização de Dados em Ambientes Wireless: Um Estudo de Caso**. Universidade Federal de Santa Catarina. Fevereiro, 2004.

MICROSOFT. **ISA**. *Microsoft Internet Security and Acceleration Server 2006*. 2006. Disponível em: http://www.microsoft.com/isaserver/default.mspx . [Acessado em 25/03/2007].

MICROSOFT. ***SQL Server 2005 Mobile Resources***. 2007. Disponível em: http://www.microsoft.com/sql/editions/sqlmobile/sqlmobileresources.mspx . [Acessado em 24/03/2007].

NASSU, E. A.; FINGER, M. **O Significado de "Aqui"em Sistemas Transacionais Móveis**. I Workshop SIDAM (Sistemas de Informação Distribuída de Agentes Móveis). Outubro, 2000, p. 55-63.

NOVEL INC. **How does Replication Work?** 2003. Disponível em: http://developer.novell.com/research/appnotes/1997/june/02/03.htm .

NURKIC, I.. ***Difficulties in achieving security in mobile communications***. *Proc. of the IFIP World Conference on Mobile Communications.* 1996.

OBEX. Wikipedia. 2007. Disponível em: http://en.wikipedia.org/wiki/OBEX . [Acessado em 25/03/2007].

OLIVEIRA, RICHARD. **O que é *Wireless*?** Março, 2004. Disponível em: http://www.richard.eti.br/duvidas58.html . [Acessado em 24/03/2007].

ORACLE. ***Oracle Database Lite 10g***. 2007. Disponível em: http://www.oracle.com/technology/products/lite/index.html .[Acessado em 23/03/2007].

OZSU, M.; VALDURIEZ, P. ***Principles of Distributed Database Systems***. New Jersey: Prentice Hall, 2ª ed., 1999.

PABLA, C.. ***A beginner' s look at the SyncML protocol and procedures***. Abril, 2003. Disponível em: http://www.ibm.com/developerworks/library/wi-syncml2/?dwzone=wireless .

PCTECHGUIDE. ***Mobile CPU Technology***. 2006. Disponível em: http://www.pctechguide.com/25mobile.htm .[Acessado 24 de Fevereiro de 2007].

PFITZMANN, A.; PFITZMANN, B.; WAIDNER, M.. ***ISDN-MIXes: Untraceable communication with very small bandwdth overhead***. *Proc. of the IFIP*, 1991.

PITOURA, EVAGGELIA; BHARGAVA, BHARAT. ***A Framework for Providing Consistent and Recoverable Agent-Based Access to Heterogeneous Mobile Databases***. In SIGMOD Record 24(3), Setembro, 1995, p 44-49.

PITOURA, EVAGGELIA; SAMARAS, GEORGE. ***Data Management for Mobile Computing***, Kluwer Academic Publishers, 1998.

PSION. Wikipedia. 2007. Disponível em: http://en.wikipedia.org/wiki/Psion . [Acessado em 25/03/2007].

QBE. Wikipedia. 2007. Disponível em: http://en.wikipedia.org/wiki/Query_by_Example . [Acessado em 25/03/2007].

RAINONE, FLÁVIA. **Banco de Dados Móveis**. USP, SP. Disponível em: http://grenoble.ime.usp.br/movel/bdmoveisflavia.pdf . [Acessado em 18/03/2007].

RC. Wikipedia. 2007. Disponível em: http://en.wikipedia.org/wiki/RC_algorithm . [Acessado em 25/03/2007].

REICHENBACH, M.; DAMBKER, H.; FEDERRATH, H.; RANNENBERG, K.. ***Individual management of personal reachability in mobile communication***. *Proceedings of the IFIP TC11 SEC 97, 13th International Information Security Conference*. 1997.

RSA. Wikipedia. 2007. Disponível em: http://pt.wikipedia.org/wiki/RSA . [Acessado em 25/03/2007].

RUI, HU. **WSP**. University of Helsinki, Departament of Computer Science. 2000. Disponível em: http://www.cs.helsinki.fi/u/kraatika/Courses/wap00s/wap]-wsp.pdf . [Acessado em 25/03/2007].

SECURITY. Wikipedia. 2007. Disponível em: http://en.wikipedia.org/wiki/Security . [Acessado em 18/03/2007].

SEGURANÇA DA INFORMAÇÃO. Wikipedia. Disponível em: http://pt.wikipedia.org/wiki/Seguran%C3%A7a_da_informa%C3%A7%C3%A3o . [Acessado em 18/03/2007].

SMTP. Wikipedia. 2007. Disponível em: http://en.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol . [Acessado em 25/03/2007].

SSL. Wikipedia. 2007. Disponível em: http://en.wikipedia.org/wiki/Transport_Layer_Security . [Acessado em 25/03/2007].

SYBASE. **SQL Anywhere**. 2007. Disponível em: http://www.sybase.com/products/mobilesolutions/sqlanywhere . [Acessado em 24/03/2007].

SYBASE INC. Product Manuals - ***SQL Anywhere Studio Documentation***. 2002. Disponível em: http://sybooks.sybase.com/nav/base.do [Acessado em 18/03/2007].

SYNCML. ***Data Synchronization and device management***. Abril, 2003. Disponível em: http://www.syncml.org/ .

TCP/IP. Wikipedia. 2007. Disponível em: http://pt.wikipedia.org/wiki/TCPIP . [Acessado em 25/03/2007].

TEDESCHI, ENRICO. ***Historic Home Computers***. 2003. Disponível em: http://www.etedeschi.ndirect.co.uk .[Acessado 24 de Fevereiro de 2007].

TERRY, D.; DEMERS, A.; PETERSEN, K.; SPREITZER, M.; THEIMER, M.; WELCH, B. ***Session Guarantees for Weakly Consistent Replicated Data***. *Proceedings of the International Conference on Parallel and Distributed Information Systems*, Setembro, 1994, p.140-149.

VARADHARAJAN, V.; MU, Y.. ***Design of secure end-to-end protocols for mobile systems***. *Proc. of the IFIP World Conference on Mobile Communications,* Canberra, 1996.

VERÍSSIMO, FERNANDO. **Segurança em Redes sem Fio**. Universidade Federal do Rio de Janeiro. Janeiro, 2002.

XEMACS. ***What is Eshell?***. Fevereiro, 2006. Disponível em: http://www.xemacs.org/Documentation/packages/html/eshell_1.html.[Acessado em 28/03/2007].

ZHENG, Y.. ***An authentication an security protocol for mobile computing***. *Proc. of the IFIP World Conference on Mobile Communications*, Canberra. 1996.