UNIVERSIDADE DO EXTREMO SUL CATARINENSE – UNESC
CURSO DE CIÊNCIA DA COMPUTAÇÃO

DAVID FRASSON JUNIOR

ANÁLISE DE VULNERABILIDADES ENVOLVENDO APLICAÇÕES MÓVEIS: ESTUDO DE CASO NA APLICAÇÃO MÓVEL DE ACESSO À BASE DE DADOS DE UM SISTEMA DE REGISTRO ELETRÔNICO EM SAÚDE PARA UTI

CRICIUMA, NOVEMBRO DE 2008

DAVID FRASSON JUNIOR

ANÁLISE DE VULNERABILIDADES ENVOLVENDO APLICAÇÕES MÓVEIS: ESTUDO DE CASO NA APLICAÇÃO MÓVEL DE ACESSO À BASE DE DADOS DE UM SISTEMA DE REGISTRO ELETRÔNICO EM SAÚDE PARA UTI

Trabalho de Conclusão de Curso apresentado para obtenção do Grau de Bacharel em Ciência da Computação da Universidade do Extremo Sul Catarinense.

Orientador: Prof. M.Eng. Evânio Ramos Nicoleit
Co-Orientador: Prof. M.Sc. Paulo João Martins

CRICIUMA, NOVEMBRO DE 2008

DAVID FRASSON JÚNIOR

ANÁLISE DE VULNERABILIDADES ENVOLVENDO APLICAÇÕES MÓVEIS: ESTUDO DE CASO NA APLICAÇÃO MÓVEL DE ACESSO À BASE DE DADOS DE UM SISTEMA DE REGISTRO ELETRÔNICO EM SAÚDE PARA UTI

Submetido ao corpo docente do Curso de Ciência da Computação da Universidade do Extremo Sul Catarinense como um dos requisitos para obtenção do grau de Bacharel em Ciência da Computação.

Profa. MSc. Ana Claudia Garcia Barbosa
Coordenadora do Curso de Ciência da Computação

Banca Examinadora:

Prof. M.Eng. Evânio Ramos Nicoleit (UNESC)
Orientador

Prof. MSc. Paulo João Martins (UNESC)
Co-Orientador

Prof. MSc. Rogério Antônio Casagrande (UNESC)

Profa. MSc. Priscyla Waleska Targino de Azevedo Simões (UNESC)

Dedico este trabalho aos meus pais e a minha noiva Patrícia, que não mediram esforços para fazer desse sonho uma realidade.

AGRADECIMENTOS

Agradeço primeiramente a DEUS, que me deu o dom da vida e a força necessária para superar todos os obstáculos em meu caminho;

Aos meus pais, David e Janete, pelo amor, educação e terem se dedicado na minha formação para me tornar uma pessoa digna e de caráter;

À Patrícia, minha noiva, pelo amor, carinho, paciência e compreensão nas minhas ausências;

Ao meu orientador Evânio, pelos ensinamentos, sugestões, críticas e conselhos;

Ao meu Co-Orientador Prof. M.Sc. Paulo João Martins, por toda dedicação e ajuda para concretização deste trabalho;

Agradeço aos professores do curso de Ciência da Computação que foram responsáveis pela minha formação, e estavam sempre dispostos a auxiliar;

Enfim, agradeço a todos que, de alguma forma, contribuíram para que este trab fosse realizado.

“A sabedoria consiste em compreender que o tempo dedicado ao trabalho nunca é perdido.”

Ralph

RESUMO

Observa-se uma grande evolução nos dispositivos móveis e altos investimentos em sistemas de informações específicos para a área da saúde. Um sistema de Registro Eletrônico em Saúde (S-RES) faz uso de informações sigilosas que só dizem respeito ao paciente. Mas é de responsabilidade dos profissionais da saúde a guarda destas informações. Cada vez mais os dados estão percorrendo caminhos alternativos que fogem ao controle dos administradores. Isto amplia consideravelmente as possibilidades de afetar a integridade de dados e prejudicar dessa forma a qualidade dos sistemas. Por outro lado, as aplicações atualmente envolvem tecnologias diferentes, o que aumenta a dificuldade em se prover segurança. Para cada segmento há um conjunto diferenciado de vulnerabilidades e a identificação de métodos corretivos é uma tarefa complicada. Este trabalho aborda a identificação de vulnerabilidades nos itens que compõem o ambiente associado com uma aplicação móvel visando propor recomendações para orientar a escolha das tecnologias adequadas. Para validação das recomendações propostas, será realizado um estudo de caso na aplicação móvel de acesso ao S-RES UTInfo 2.0. Serão identificados os pontos que possuem vulnerabilidades e quais métodos podem ser aplicados para minimizá-las.

Palavras – Chave: Registro Eletrônico em Saúde, Wireless, Vulnerabilidades, Aplicações Móveis, Dispositivos Móveis.

ABSTRACT

There is a great evolution in mobile devices and high investments in specific information systems to the area of health. An Electronic Health Record (EHR - S-RES) System makes use of classified information that only concern the patient. But it is of the responsibility of health professionals to guard such information. Increasingly, the data are traveling alternative ways that are beyond the control of network administrators. This considerably expands the possibilities to affect the integrity of data and thus impair the quality of systems. Moreover, applications currently involve different technologies, which increase the difficulty in providing security. For each segment there is a differentiated set of vulnerabilities and identifying the corrective method is a complicated task. This work approaches the identification of vulnerabilities in the items that compose the environment associated with a mobile application seeking propose recommendations to guide the choice of appropriate technologies. For validation of the proposed recommendations, a case study will be accomplished in a case study in the mobile application of access to the S-RES UTInfo 2.0. They will be identified the points that have vulnerabilities and which methods can be applied to minimize them.

Keywords: Electronic Health Record, Wireless, Vulnerabilities, Mobile Applications, Mobile Devices.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
AES	Advanced Encryption Standard
ANSI-HISB	American National Standards Institute – Healthcare Informatics Standards Board
API	Application Programming Interface
CDC	Connected Device Configuration
CDMA	Code Division Multiple Access
CEN	Comitê Europeu de Normatização
CFM	Conselho Federal de Medicina
CLDC	Connected Limited Device Configuration
CRC	Cyclic Redundancy Check
DES	Data Encryption Standart
DM	Dispositivo(s) Móvel(eis)
DoS	Denial of Service
EAP	Extensible Authentication Protocol
EDGE	Enhanced Data Rates For Global Evolution
ER	Entidade Relacionamento
ESS	Extended Service Set
ESSID	Extended Service Set Identifier Disable
GPRS	General Packet Radio Service
GSM	Groupe Special Mobile
HL7	Health Level Seven
http	Hypertext Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
IDEA	International Data Encryption Algorithm
IEEE	Institute of Electrical and Electronics Engineers
IOM	Institute of Medicine
IrDA	Infrared Data Association
ISSO	International Organization for Standardization
J2EE	Java 2 Enterprise Edition
J2ME	Java 2 Micro Edition

J2SE	Java 2 Standard Edition
JVM	Java Virtual Machine
KVM	Kilo Virtual Machine
MAC	Media Access Control
MIDP	Mobile Information Device Profile
NGS1	Nível de Garantia de Segurança 1
NGS2	Nível de Garantia de Segurança 2
OFDM	Orthogonal Frequency Division Multiplexing/Modulation
PAN	Personal Area Network
PDA	Personal Digital Assistant
PIN	Personal Identification Number
PUK	Personal Unblocking Key
RADIUS	Remote Authentication Dial In User Service
RC	Rivest Cipher
RES	Registro Eletrônico em Saúde
RIPSA	Rede Interagencial de Informações para a Saúde
RSN	Robust Security Network
SGBDR	Sistema Gerenciador de Banco de Dados Relacional
SIM	Subscriber Identity Module
SQL	Structured Query Language
S-RES	Sistema de Registro Eletrônico em Saúde
SSID	Service Set Identifier
SSL	Secure Sockets Layer
TIC	Tecnologias da Informação e da Comunicação
TKIP	Temporal Key Integrity Protocol
UML	Unified Modeling Language
UTI	Unidade de Terapia Intensiva
VPN	Virtual Private Network
W3C	World Wide Web Consortium
WAP	Wired Protected Access
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
XML	Wired Equivalent Privacy

SUMÁRIO

1 INTRODUÇÃO

As organizações estão se adaptando ao uso de Dispositivos Móveis (DM) para proporcionarem mais flexibilidade aos profissionais envolvidos. Na área da saúde também é possível notar tais transformações, já que os serviços de saúde estão sendo oferecidos em locais distintos e por vários profissionais. Para acompanhar está evolução, as soluções de tecnologia da informação devem estar em constante evolução, garantindo assim, que as necessidades da informática médica sejam atendidas (MASSAD, 2003).

A mobilidade proporcionada pelos (DM) introduz algumas restrições, como por exemplo: questões de privacidade e segurança no tráfego de informações; alta variação na largura de banda disponível e na latência da comunicação (desconexões freqüentes); ambientes heterogêneos; variação no tipo, na quantidade e na qualidade de serviços e recursos disponíveis à medida que o usuário se desloca e; problemas de localização (MAIA; RODRIGUES; ENDLER, 2005).

Um Sistema de Registro Eletrônico em Saúde (S-RES) requer serviços que atendam a tais exigências, disponibilizando sistemas capazes de auxiliar a prática médica, como o gerenciamento de tratamentos clínicos prestados ao paciente (MACERATINI; SABBATINI, 1994).

Estas soluções de tecnologia da informação para a área médica devem disponibilizar recursos para o apoio de tratamentos clínicos no âmbito da instituição, bem como, em ambientes externos, garantindo o acesso às informações, independente da localização dos profissionais (MASSAD, 2003).

A flexibilidade de acesso às informações pode ser alcançada com a utilização de DM tais como: Celulares, *Smartphone, Handhleds,* PDA e *Pocket* PC, com

suporte às tecnologias/protocolos *WAP, GPRS/EDGE, IrDA, Bluetooth,* IEEE 802.11, entre outros. Sua utilização vem abrindo novos domínios de aplicação para o acesso à informação em um vasto conjunto de atividades, dentre elas, a área da saúde.

Uma das linhas de pesquisa do Grupo de Pesquisa Informática Médica e Telemedicina - Kiron - da Unesc envolve o Sistema de Registro Eletrônico em Saúde (S-RES). O Grupo já desenvolveu um S-RES para utilização em UTI, bem como uma aplicação móvel específica para ser utilizado nos DM, possibilitando acompanhamento de pacientes da Unidade de Terapia Intensiva (UTI).

O desafio atual do S-RES é disponibilizar acesso às informações para os profissionais de saúde, via DM, com segurança adequada. A heterogeneidade dos dispositivos e a integração com as tecnologias de comunicação *Wireless,* têm imposto desafios para o desenvolvimento de aplicações. Entre os desafios, neste trabalho, busca-se estudar e descrever um modelo de recomendações para o desenvolvimento de aplicações móveis seguras, de maneira a garantir uma maior confidencialidade das informações transmitidas.

1.1 OBJETIVO GERAL

Analisar aspectos de segurança nos dispositivos móveis, nas aplicações e nas redes *Wireless* visando o desenvolvimento e utilização de aplicações móveis, tais como uma aplicação móvel para acesso a informações de um S-RES de forma segura.

1.2 OBJETIVOS ESPECIFICOS

Os objetivos específicos desta pesquisa consistem em:

a) analisar os itens do ambiente móvel integrados ao S-RES;
b) analisar os aspectos de segurança nas redes *Wireless* no padrão IEEE 802.11g em dispositivos móveis;
c) identificar métricas para a definição do nível de segurança existente;
d) utilizar um DM para acessar e processar informações de modo seguro a partir da aplicação móvel desenvolvida para acesso à base de dados de um S-RES;
e) estabelecer bases para melhoria da segurança existente na aplicação móvel.

1.3 JUSTIFICATIVA

A computação móvel vem conquistando cada vez mais espaço nos dias atuais graças à convergência de duas tecnologias: a dos DM e a das redes de comunicação de dados *Wireless.* Existem diferentes protocolos e tecnologias para garantir segurança e confidencialidade das informações que trafegam por essas redes, e cada uma delas possui maneiras diferentes de proteger as informações, como o uso de chaves públicas, algoritmos de criptografia e autenticação do cliente, entre outros (MARTINS; ROCHA; HENRIQUES, 2006).

Nota-se uma constante redução de dimensões, peso e consumo de energia dos DM, o que vem contribuindo para o aumento da demanda de acesso à rede, independente da localidade do usuário ou da informação requerida. Neste aspecto, eles

podem ser utilizados juntamente com o S-RES, como uma ferramenta para os profissionais da saúde que necessitam estar em constante movimento.

Este trabalho analisa os aspectos de segurança que envolvem os DM e propor um conjunto de recomendações para auxiliar o desenvolvimento de aplicações móveis provendo segurança. A segurança é um fator primordial que deve ser levado em conta no desenvolvimento das aplicações.

O S-RES é um sistema constituído de um conjunto de informações, sinais e imagens registradas, geradas a partir de fatos, acontecimentos e situações sobre o paciente onde as mesmas são sigilosas (PIRES *ET AL,* 2004).

Para que as recomendações propostas possam ser validadas, um estudo de caso será abordado, na aplicação móvel desenvolvida para acesso à base de dados de um S-RES.

1.4 ESTRUTURA DO TRABALHO

Essa pesquisa é constituída de 6 capítulos, sendo o primeiro formado pela introdução à pesquisa desenvolvida, onde também são descritos os objetivos e a justificativa para a realização do trabalho.

O Capítulo 2 contém uma abordagem sobre aspectos de segurança das informações médicas.

No Capítulo 3 são discutidos os conceitos de segurança da informação envolvendo o S-RES, bem como, os requisitos de segurança requeridos pelo SBIS-CFM para certificação de *software* na área da saúde.

Os conceitos fundamentais das tecnologias utilizadas no desenvolvimento da aplicação móvel, bem como, todas as tecnologias que compõe este ambiente são abordadas no Capítulo 4.

No Capítulo 5 são apresentados os trabalhos correlatos inerentes a está pesquisa, relacionando trabalhos desta instituição, bem como, trabalhos de outras instituições.

O trabalho desenvolvido, a descrição dos cenários analisados e o estudo de caso são apresentados no Capítulo 6.

Por fim, tem-se a conclusão desse trabalho onde também são sugeridos alguns temas para trabalhos futuros.

2 REGISTRO ELETRÔNICO EM SAÚDE (RES) E ASPECTOS DE SEGURANÇA DAS INFORMAÇÕES MÉDICAS

Atualmente o Registro Eletrônico em Saúde (RES) é um dos documentos mais importantes no âmbito hospitalar, sendo constituído de informações relacionada à saúde dos pacientes, bem como evoluções e os resultados dos tratamentos aplicados. Sua utilização se faz necessária para garantir o acompanhamento correto do atendimento aos indivíduos. Todo o conjunto de informações que o compõe, possuem caráter sigiloso. Portanto medidas de segurança devem ser tomadas para garantir a integridade e confiabilidade destas informações (FURUIE ET AL, 2003).

2.1 SISTEMA DE REGISTRO ELETRÔNICO EM SAÚDE (S-RES)

Com o intuito de garantir que as informações necessárias para o correto atendimento do paciente fossem mantidas mesmo com a permuta de enfermeiros e médicos, viu-se a necessidade de criar um documento para armazenamento de tais informações que é denominado prontuário do paciente e vem se tornando o meio de comunicação mais utilizado entre os envolvidos no tratamento destes (MASSAD, 2003).

As informações contidas no prontuário médico oferecem suporte ao tratamento clínico e as evoluções envolvendo os pacientes, mantendo um histórico de quais métodos surtiram efeitos sobre o problema que originou o atendimento, bem como métodos que fracassaram. A decorrência destes processos pode levar a identificação de novos problemas envolvendo a saúde do paciente ou os métodos aplicados (COSTA, 2001).

De modo geral o prontuário médico se tornou o documento mais importante no sistema de saúde de um país, pois é constituído de informações que dizem respeito à saúde das pessoas que o integram (FARINAZZO, 2004).

Hoje em dia o prontuário médico atende a funções como (MASSAD, 2003):

a) apóia o andamento dos tratamentos aplicados nos pacientes;
b) fonte para tomada de decisão;
c) documento legal do tratamento clínico;
d) apoio a pesquisas clínica;
e) possibilita o enriquecimento dos processos médicos;

Para suportar as mais variadas funções, o modelo clássico vem sofrendo transformações que envolvem as prestações de serviço de saúde. Os aspectos gerais deste novo modelo são (MASSAD, 2003):

a) o atendimento é fundamental nos hospitais, e estes devem se atualizar constantemente para suportar tratamentos complexos;
b) devem ser aplicados procedimentos que vertem resultados mais satisfatórios;
c) a integração das informações permitindo análise completa do quadro clínico de um paciente identificando possíveis fracassos ou sucessos;
d) a equipe envolvida nos tratamentos geralmente é formada por profissionais de áreas distintas, colaborando entre si visando à recuperação dos pacientes;

Os processos clínicos que englobam o tratamento de um paciente implicam no envolvimento de vários profissionais da saúde e ocorrem em ambientes distintos, tais como: recepção, enfermaria, UTI, ambulância dentre outros, e geram informações dos mais variados tipos, tais como: eletrocardiograma, ultra-som, raios-X e informações

descritivas geradas a partir de processos executados pelos profissionais. Todo este conjunto de informações diz respeito a um único paciente e devem ser organizadas de tal forma a produzir um documento integrado que dará suporte para a tomada de decisão no que diz respeito ao tratamento que deve ser utilizado, bem como a orientação de todo o processo de atendimento ao paciente (COSTA, 2001).

O prontuário armazenado em papel ainda é muito utilizado, mas considerando o volume de informações pertinentes a ele, bem como a falta de padronização destas, nota-se que este não é mais suficiente para suprir as necessidades (MASSAD, 2003). Dentre estas insuficiências podem-se citar:

a) fica disponível apenas para uma consulta por vez;
b) não pode estar em mais de um setor ao mesmo tempo;
c) editado por diferentes profissionais o que em muitos casos pode o tornar ilegível;
d) impossível configurar para disparar avisos aos profissionais.

Estas insuficiências impulsionaram a implementação dos S-RES junto com a possibilidade de compartilhar informações, rapidez no acesso destas além de estarem disponíveis para mais de um usuário simultaneamente, tornando assim o atendimento muito mais eficiente e coibindo consideravelmente a margem de erros médicos (PINTO, 2006).

Este novo modelo que surge, tendo como base os sistemas de informação, é nomeado como S-RES e tem como foco principal a integração e organização das informações, disponibilizando-as aos envolvidos de forma clara e simples.

O S-RES é um sistema que armazena as informações adquiridas por intermédio de atendimentos prestados no decorrer da vida dos pacientes em um meio físico, agregando vários benefícios a está prática (MASSAD, 2003).

2.1.1 Vantagens e Desvantagens do S-RES

Inúmeras são as vantagens obtidas com a utilização do S-RES, assim como (SITTIG, 1999):

a) maior legibilidade das informações;
b) menor incidência de dados repetidos;
c) melhor organização das informações;
d) possibilidade de acessos remotos e simultâneos;
e) informações atualizadas para todos os usuários;
f) rapidez na consulta de informações bem como o relacionamento destas;
g) segurança dos dados, pois possibilita a implementação de processos como o backup, tornando possível reverter alterações indesejadas ou percas;
h) monitoramento dos acessos feitos a base de dados;
i) restrição de acesso, possibilitando disponibilizá-los em níveis diferentes;
j) diferentes maneiras de visualização das informações;
k) automatização de rotinas como: capturar os dados de monitores, resultados de exames dentre outros;
l) informações padronizadas possibilitando a integração com vários sistemas de informação;
m) verificação constante nos dados inseridos, possibilitando a identificação de falhas e emissão de alertas, como e-mails automáticos para o profissional responsável pelo paciente;
n) relatórios, possibilitando um acompanhamento mais detalhado dos pacientes.

Diante de muitas vantagens, é importante ressaltar que existem algumas desvantagens na sua utilização, como (PINTO, 2006):

a) dificuldade de educar os profissionais para o uso de novas tecnologias;
b) investimentos em hardware e software incluindo manutenções e suporte;
c) resultados em longo prazo;
d) indisponibilidade do sistema em caso de falhas;
e) dificuldade para aquisição de todas as informações;
f) insegurança;

Uma desvantagem que tem gerado polêmica é a segurança das informações que trafegam pelos sistemas, pois o acesso indevido pode colocar a confiabilidade e integridade destas em risco (COSTA, 2001).

2.1.2 Aspectos de Desenvolvimento

Ao desenvolver um S-RES, é necessário compreender todo o processo que o envolve, desenvolvendo assim um software com a capacidade de gerenciar os procedimentos clínicos prestados aos pacientes.

Alguns modelos foram propostos para o desenvolvimento, implantação e utilização do S-RES, entre eles podem ser citados os modelos apresentados por Peter Waegemann (1996), diretor do Medical Records Institute nos Estados Unidos, pelo Institute of Medicine dos Estados Unidos (IOM, 1997) e os modelos apresentados por McDonald e Barnett (1990).

2.1.3 Padrões de Registro e Transmissão de Dados em Saúde

A aplicação de padrões no desenvolvimento e utilização de um software implica que as técnicas que estão sendo utilizada já foram testadas e comprovadas que beneficiarão quem as utiliza, além de facilitar possíveis integrações com sistemas diferentes, mas construídos empregando o mesmo padrão.

Massad (2003), afirma que padrões e normas servem como um ponto de referência para desenvolvedores e usuários, disponibilizando um apanhado geral de regras que devem ser seguidas para a correta organização e otimização das informações em sistemas de saúde.

A elaboração e manutenção destes padrões são de responsabilidades de organizações espalhadas em todo o mundo, assim como a *International Standards Organization* (ISO), que é uma das mais respeitadas, disponibilizando padrões e normas em áreas diversas. O *American National Standards Institute – Healthcare Informatics Standards Board* (ANSI-HISB) é responsável pela coordenação de várias organizações que pesquisam e desenvolvem regras localizadas nos Estados Unidos, já na Europa existe o Comitê Europeu de Normatização (CEN), que criou um subcomitê denominado CEN/TC251 que é responsável pela informática em saúde (MASSAD, 2003).

No Brasil o órgão responsável pela definição de normas e padrões é a Associação Brasileira de Normas Técnicas (ABNT) que disponibiliza e mantém padrões em diversas áreas, já na área da saúde foi criado em 1996 pelo Ministério da Saúde a Rede Integrada de Informações para Saúde (RIPSA) onde se pretende estabelecer regras para possibilitar a união de diversos sistemas (MASSAD, 2003).

2.1.4 Padrão Health Level Seven (HL7)

É controlada pelo ANSI-HISB e tem como responsabilidade os padrões a serem empregados em nível de aplicação, disponibilizando aspectos referentes à composição dos dados utilizados em transferências, bem como as maneiras de efetuar tais trocas e o reconhecimento de erros comuns entre as aplicações (MASSAD, 2003).

Em resumo, este padrão tem como objetivo unificar os termos técnicos inerentes a prática médica.

2.1.5 Utilização de XML para Comunicação

O padrão XML foi desenvolvido para possibilitar que tecnologias diferentes pudessem se comunicar, ou seja, muitos sistemas foram concebidos e somente em um segundo momento houve a necessidade de comunicação com um terceiro sistema, o qual pode acontecer por meio deste padrão.

A necessidade da criação de um documento que fosse independente de sistema operacional, formatos entre outros, deu origem ao SGML em meados de 1960 que fez utilização de um sistema denominado Marcação Generalizada para dar mais flexibilidade ao usuário, dessa forma pode fazer as marcações necessárias ao seu contexto, seguindo deste conceito nasceu o XML, que se tornou o padrão mais difundido no meio digital para comunicação de dados (FARIA, 2005).

Entre as vantagens de utilização deste padrão está seu reconhecimento pelo grupo *World Wide Web Consortiun* (W3C) que define alguns padrões para Internet e a possibilidade de armazenar qualquer tipo de dados, organizando-os da melhor forma possível (W3C, 2008)

Dessa forma, como qualquer tipo de arquivo poderá ser cifrado e assinado o XML também o faz, disponibilizando *tags* especificas que identificam que estes foram assinados. A utilização de XML assinado é de suma importância no ambiente computacional, pois permite identificar a origem das informações que estão prestes a serem recebidas, bem como o autor destas.

2.1.6 Aspectos Legais

Como o S-RES é um sistema utilizado por vários profissionais na área da saúde para o preenchimento de dados relevantes ao tratamento de pacientes, sendo que grande parte destes são individuais ou confidenciais, que só dizem respeito ao indivíduo e aos envolvidos no seu tratamento. Para garantir a segurança dos pacientes foi desenvolvida uma legislação especifica para tais sistemas (PINTO, 2006).

O Conselho Federal de Medicina (CFM) é o órgão que cuida dos aspectos éticos e de segurança do S-RES, e aprovou a resolução CFM no 1.331/89, que diz respeito à temporalidade do S-RES, e portarias como a de nº 1.638/2002 e nº 1.639/2002 reconhecem o uso de sistemas computacionais para o manuseio do S-RES (PINTO, 2006).

A completa exclusão de papéis no ambiente médico no que diz respeito a prontuários médicos e a substituição por prontuário eletrônico é necessário que o sistema contemple integralmente o conjunto de requisitos tidos como obrigatórios nos níveis de garantia e segurança NGS1[1] e NGS2[2] estabelecidos pelo SBIS-CFM (MACHADO, 2007)

[1] NGS1: Nível 1 de Garantia de Segurança definidos pelo SBIS-CFM (2008).
[2] NGS2: Nível 2 de Garantia de Segurança que contempla o uso de certificados digitais e é definido pelo SBIS-CFM (2008).

2.2 OBSTÁCULOS NA IMPLANTAÇÃO DO S-RES

Obstáculos são encontrados na implementação e implantação do S-RES, tanto por capacitação inadequada para o uso das tecnologias de informação e comunicação (TIC) quanto por parte dos desenvolvedores, que em muitos casos, implementam sistemas que não suportam as reais necessidades dos usuários, devido à dificuldade encontrada na análise de requisitos (MASSAD, 2003). Estes problemas podem dificultar, por exemplo, na definição de interfaces com o usuário, já que no prontuário em papel a aquisição dos dados se dá de forma livre, e a disponibilização de campos livres no S-RES pode inviabilizar sua captura (MEZAROBA; MENEGON; NICOLEIT, 2008).

Quanto às dificuldades relacionadas com a segurança, pode-se afirmar que é um dos pontos mais importantes na implementação e implantação de tais sistemas e é onde deve se levar mais tempo e recursos, pois a constituição de um sistema seguro inicia com sua análise, onde devem ser levantados todos os riscos e vulnerabilidades envolvendo a aplicação, bem como todo o ambiente que o cerca, incluindo padrões de desenvolvimento, intercambio de informações, normas e inclusive os usuários envolvidos, pois estes podem engajar sabotagens ao sistema, devido à dificuldade de adaptação (MASSAD, 2003).

Uma análise no fluxo de informação ao qual a aplicação móvel se encaixa em relação ao S-RES UTInfo 2.0, possibilitou o levantamento dos pontos que necessitam de segurança, a Figura 1 representa estes pontos bem como os itens que o compõe.

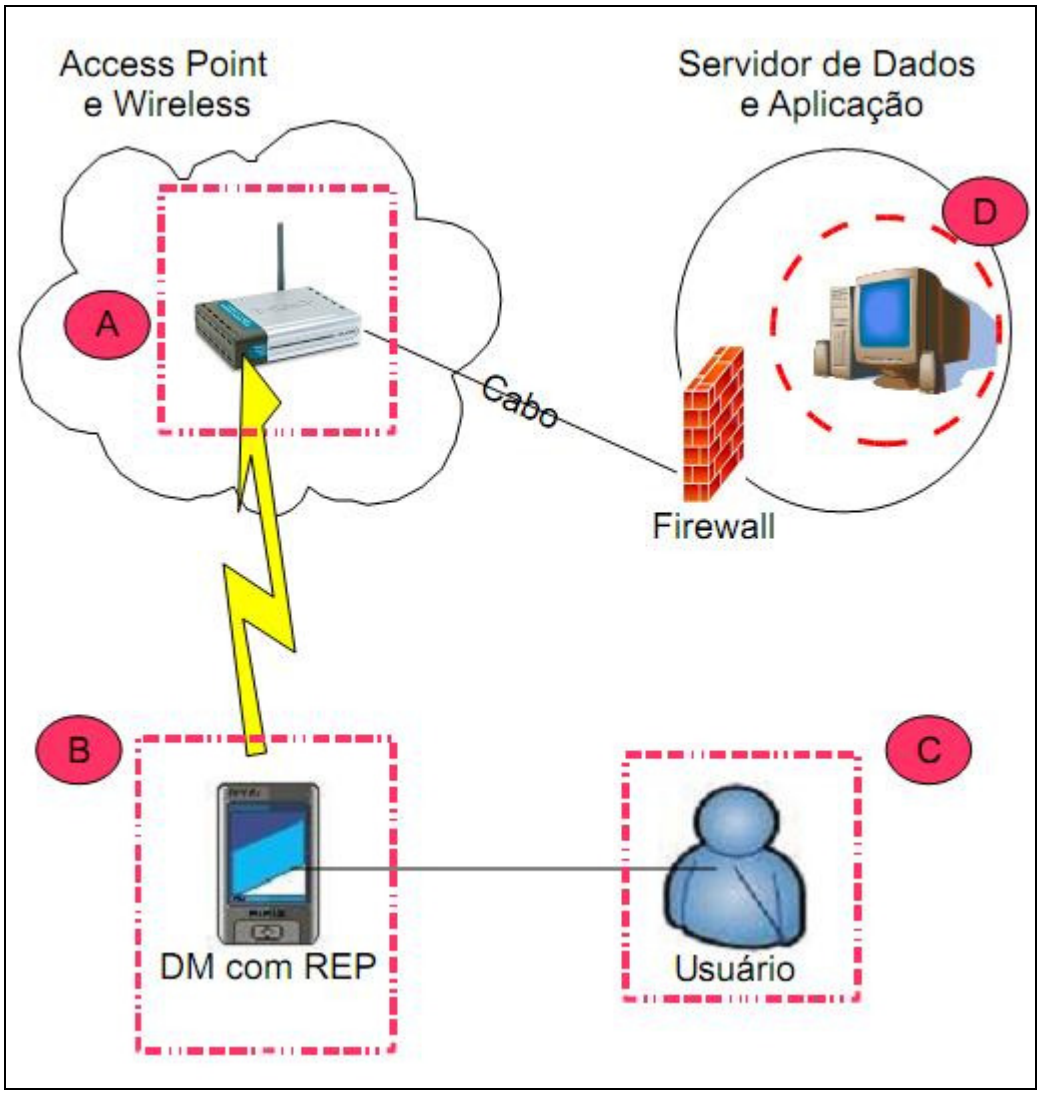

Figura 1: Pontos que necessitam de segurança

Os pontos D e C não serão tratados com tanta ênfase nesta pesquisa já que a mesma tem foco na comunicação móvel, mas não significa que não precisem de tratamentos especiais. O servidor de informações para a aplicação móvel, por exemplo, deve ser cercado de vários mecanismos de segurança, pois se trata do coração do sistema e os usuários devem ser tratados como um risco constante, pois os ataques podem ser desencadeados de dentro da própria organização originado por usuários mal intencionado.

Os demais pontos que necessitam de segurança serão abordados com mais detalhes nos capítulos seguintes.

3 SEGURANÇA DA INFORMAÇÃO NO S-RES

A grande evolução dos sistemas de informações, mas especificamente na área da saúde onde dados sigilosos de pacientes são manipulados, os aspectos de segurança passam a ser tratados como requisitos importantes, pois visam zelar pela privacidade e integridade das informações (MACHADO, 2007)

No sentido geral de segurança da informação, segundo definições do dicionário Aurélio trata-se de algo em que se pode confiar, algo seguro, sendo que é definido como algo livre de riscos, protegido, segurado.

A informação é considerada como um ativo de grande importância para as organizações e para as pessoas em geral, pois possui diversos valores agregados. Nas organizações, está ligada diretamente com os produtos finais e o mais importante que está totalmente relacionada com os processos que a regem, representando grande valor a quem possuí-la (LAUREANO, 2008).

A norma ABNT NBR ISO/IEC 17799:2005 descreve que a informação pode aparecer de diversas formas, tanto físicas como, impressões e lógicas como banco de dados, mas independente do meio em que ela se encontra, deve-se protegê-la adequadamente.

A dificuldade em prover segurança aumentou com o advento da utilização dos computadores e vem crescendo muito, pois logo após o surgimento dos computadores, surgiram às redes de computadores que a cada dia ganham mais usuários pelo mundo todo, outro fator que a impulsiona é a geração móvel, que elimina várias limitações físicas antes impostas pelas redes cabeadas (DIAS, 2000).

Antes da disseminação da informática, garantir a segurança de determinadas informações era tarefa fácil, pois estas eram gravadas na sua grande maioria em papéis e

bastava armazená-lo em um local seguro impedindo que pessoas sem autorização tivessem acesso a estas (CARUSO; STEFFEN, 1999).

A segurança da informação não se resume apenas em restringir o acesso lógico a elas, mas também garantir que todo o ambiente seja seguro, possuindo uma política de acesso, um plano de proteção contra eventos naturais (inundação, terremoto, entre outros), bem como a prevenção de falhas físicas como a interrupção do fornecimento de energia, Internet e até mesmo invasões (DIAS, 2000).

É de grande importância para uma organização, que uma política de segurança, seja elaborada e aplicada, visando diminuir as vulnerabilidades e tendo como conseqüência um sistema mais confiável, alguns aspectos relacionados a políticas de segurança serão abordados a seguir:

a) **confidencialidade/privacidade:** garante que as informações manipuladas pelo sistema em questão só serão acessadas por pessoas autorizadas, esse objetivo pode ser alcançado com o uso de técnicas como a criptografia, que permite cifrar todo o fluxo de informação (DIAS, 2000);
b) **integridade:** podendo ser subdividida em integridade de dados garantindo que estes não sofrerão alterações indesejadas, preservando a veracidade das informações e integridade de software que garante o correto funcionamento dos processos internos ao sistema, mantendo sua integridade desde o desenvolvimento a execução (BATISTA, 2007);
c) **disponibilidade:** garante acesso a usuários e processos autorizados ao sistema, bem como ao conjunto de informações associadas, sempre que necessário. Seu maior objetivo é prevenir que falhas ou ataques não impeçam o usuário autorizado de ter acesso ao sistema, para tal pode ser

usado backup da dados bem como equipamentos tolerante a falhas (DIAS, 2000);

d) **consistência:** garante que a aplicação vai funcionar da maneira correta, obedecendo à lógica de negócio. Por exemplo, o usuário altera o cadastro de apenas um paciente informando que este possui uma doença grave e o sistema registra está informação para mais de um paciente. Falhas como essa podem ser irreversíveis, prejudicando o correto funcionamento da aplicação (DIAS, 2000);

e) **auditoria:** é a rastreabilidade das alterações feitas no sistema, identificando quais informações foram alteradas, qual usuário ou processo efetuou estas alterações e em que data e horário aconteceram. Se a auditoria for implementada de forma correta, possibilita desfazer alterações indesejadas e verificar exatamente como as informações foram corrompidas (BATISTA, 2007)

f) **confiabilidade:** garantir que a aplicação funcionara corretamente mesmo diante de falhas (DIAS, 2000).

Mesmo diante de vários aspectos de segurança da informação, está pode ser alcançada se apenas a confidencialidade, integridade, disponibilidade e auditoria forem implementadas corretamente. A Figura 2 demonstra está relação entre os aspectos de segurança.

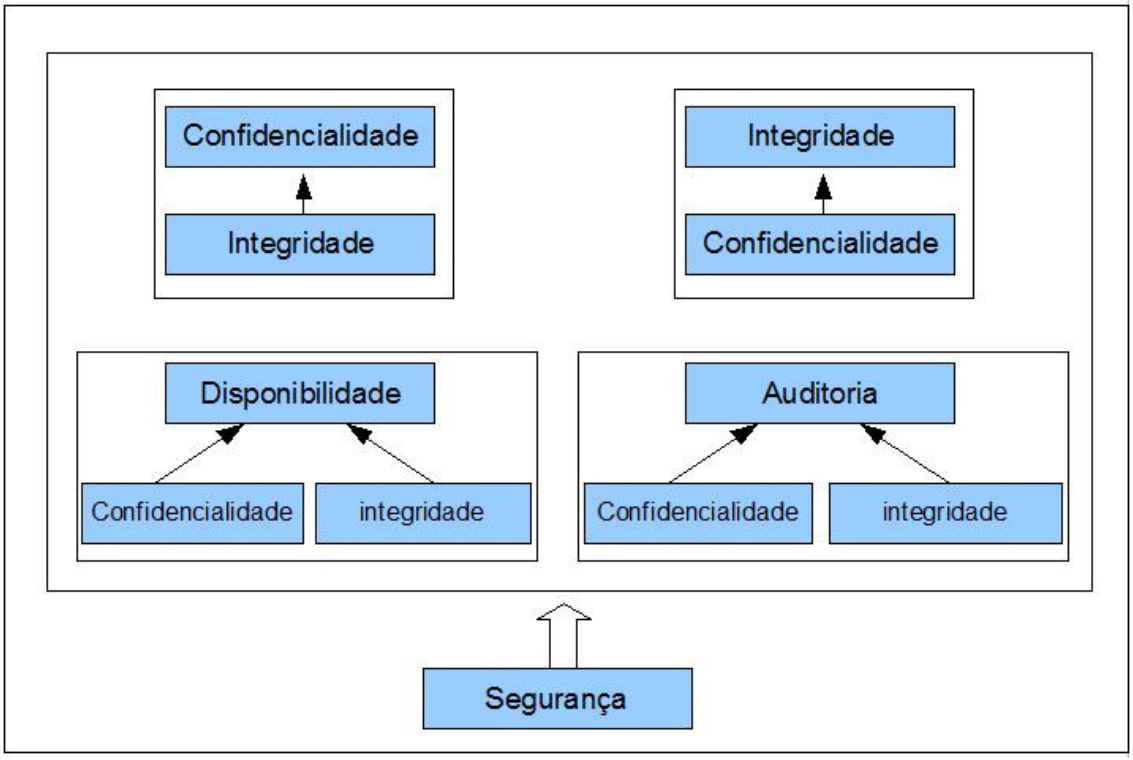

Figura 2: Relação entre aspectos de segurança
Fonte: (BATISTA, 2007)

3.1 SIGILO E PRIVACIDADE

A importância do sigilo e da privacidade aplica-se a diversas profissões. Na medicina, devido ao seu caráter legal de confidencialidade no tratamento de informações de pacientes, estes aspectos, bem como o exercício da profissão, os profissionais são submetidos a regras rigorosas de conduta. Existem normas jurídicas e éticas que asseguram e requerem sigilo médico no tratamento de informações de pacientes. Tais normas se estendem à utilização da informática médica, para garantir a confidencialidade e privacidade das informações pertinentes ao paciente, pois estas só podem ser divulgadas por meio de autorização dos pacientes ou familiares (FRANÇA, 2008).

França (2008) afirma que a utilização de informações relacionadas com a privacidade dos pacientes na informática médica, implica na atenção redobrada em

aspectos relacionados à segurança, pois nestes ambientes existem diversas vulnerabilidades que se não tratadas corretamente podem beneficiar possíveis ataques, colocando assim a integridade moral dos envolvidos em risco. Mesmo que as informações sigilosas são de posse do paciente, a obrigação de manter a privacidade é de responsabilidade dos profissionais da saúde e das instituições envolvidas.

No entanto, nota-se uma grande mobilização por parte de programadores e pesquisadores na área da saúde, engajando-se com pesquisas relacionadas à segurança envolvendo a área medica, mas mesmo com todo este esforço é impossível desenvolver métodos capazes de garantir a privacidade dos pacientes. Sem a segurança necessária, os envolvidos podem se tornar alvos de crimes digitais, podendo ate serem chantageados e manipulados por terceiros (FRANÇA, 2008).

Em todos os países existem leis que garantem o direito de privacidade dos indivíduos; no Brasil este direito é regulamentado pelo Código Penal, já no âmbito hospitalar de acordo com a resolução do CFM nº 1.246/88 Art. 108 do Código de Ética Médica as informações contidas no prontuário necessitam ser conservadas em sigilo profissional (BRASIL, 2003)

Problemas podem ser evitados se os sistemas na área de saúde forem projetados, a fim de não revelar informações que põe em risco a privacidade dos pacientes (FRANÇA, 2008).

Para o desenvolvimento de sistemas mais seguros deve-se seguir padrões reconhecidos de desenvolvimento e na área da saúde existem organizações que certificam tais sistema se estes cumprirem com os requisitos de segurança impostos por eles.

3.2 REQUISITOS DE SEGURANÇA

Com o crescente desenvolvimento da informática médica, a segurança da informação se torna um fator primordial que deve ser levado em conta no desenvolvimento das aplicações.

A SBIS-CFM é responsável pela certificação de softwares na área da saúde, e para tal disponibiliza um conjunto de requisitos de segurança que foram baseados nas normas ISO/NBR 17799 e na ISO/NBR 15408 (SBIS; CFM, 2004).

Dentre estes requisitos, pode-se citar o Nível de Garantia de Segurança 1 (NGS1) o qual não dispensa o uso de papéis. As informações devem ser impressas e assinadas à mão pelos responsáveis e o Nível de Garantia de Segurança 2 (NGS2) que, através do emprego de certificados digitais ICP Brasil, eliminam o uso de papéis. Importante salientar que para abranger o NGS2, estes sistemas devem estar em total conformidade com o NGS1 (SBIS; CFM, 2004).

3.2.1 Nível de Garantia de Segurança 1

Este nível é direcionado a sistemas que não contemplam a utilização de assinaturas digitais, ou seja, as informações ainda devem ser assinadas a mão pelos profissionais.

A Figura 3 apresenta todos os requisitos de segurança exigidos que devam ser atendidos para que os sistemas de RES sejam certificados com o NGS1.

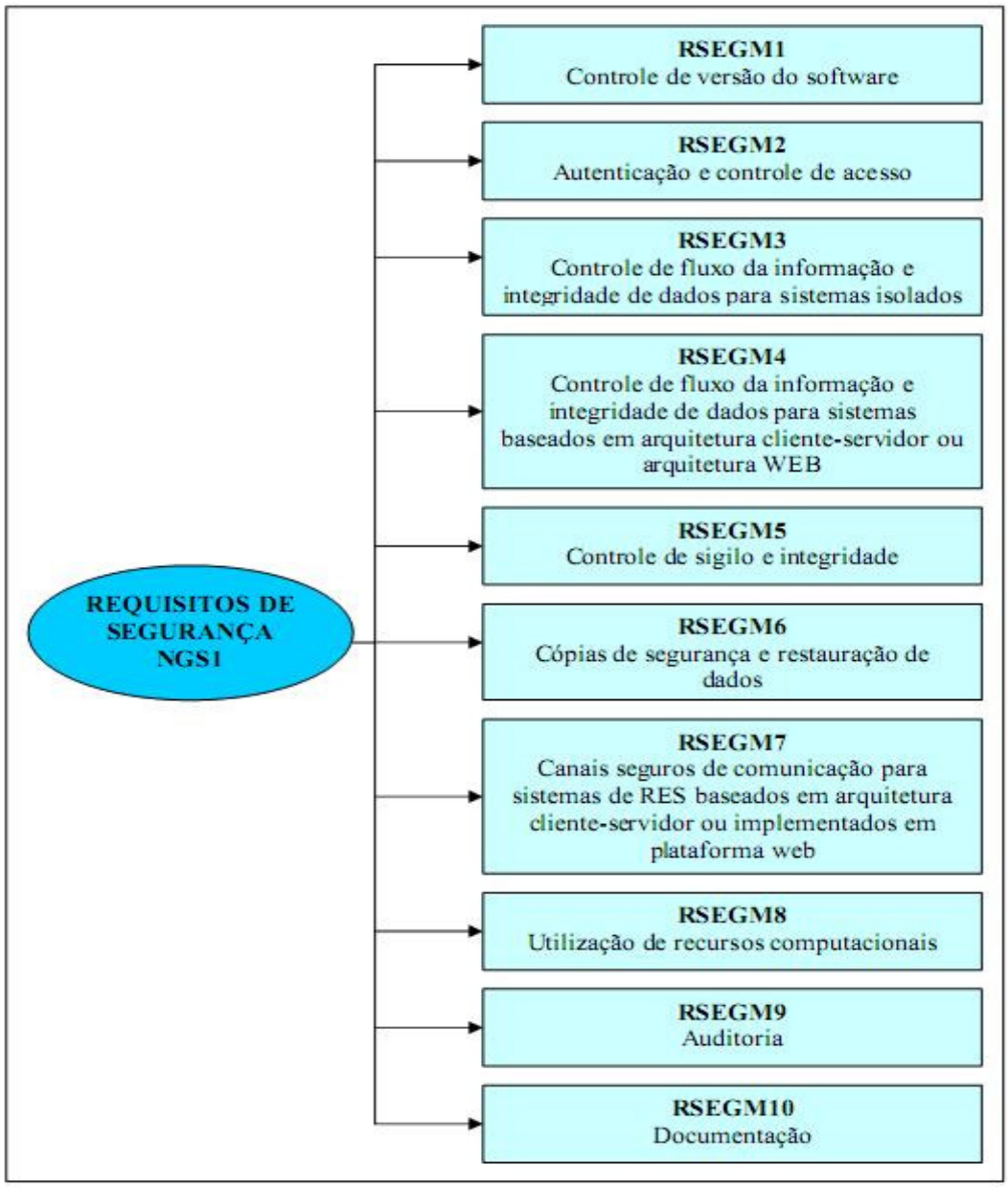

Figura 3: Requisitos de Segurança aplicados ao nível de garantia de segurança 1
Fonte: (MACHADO, 2008)

3.2.2 Nível de Garantia de Segurança 2

Este nível é direcionado aos sistemas que contemplam a utilização de certificados digitais para a assinatura das informações médicas.

A Figura 4 apresenta todos os requisitos de segurança que devem ser atendidos para que os sistemas de RES sejam certificado com o NGS2, salientando que

para estes serem certificados com o NGS2 devem contemplar todos os requisitos obrigatórios do NGS1.

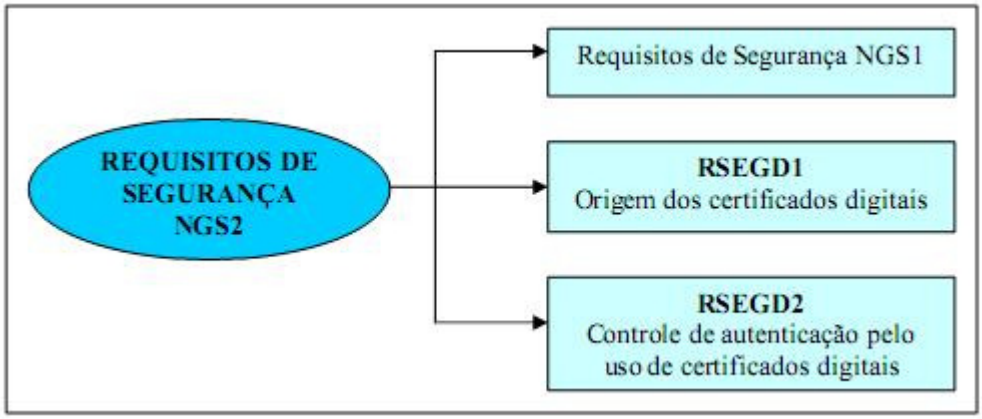

Figura 4: Requisitos de segurança aplicados ao nível de garantia de segurança 2
Fonte: (MACHADO, 2008)

3.3 CRIPTOGRAFIA

A criptografia consiste em modificar dados legíveis de modo a torná-los ilegíveis, mas não eliminando a possibilidade de reversão destas informações ilegíveis em legíveis novamente (BURNETT; STEPHEN, 2002).

Segundo Bianchin (2006) a criptografia vem desde o início da espécie humana, pois sempre houve a necessidade de sigilo das informações, ou seja, as pessoas em gerais zelam pela sua privacidade e sempre estão em posse de algo que não querem que seja revelado, sendo que o vazamento destas informações poderiam cair em mãos erradas, gerando maiores transtornos.

De acordo com Tiziano (2006) o sistema de escrita hieroglífica dos egípcios já possuía vestígios de criptografia. Está vem sendo utilizada e aprimorada para suprir as necessidades impostas pela realidade atual e no mundo da computação é muito utilizada para garantir o sigilo dos dados armazenados e na transferência destes por redes de comunicação.

A utilização de criptografia no meio computacional dá suporte aos seguintes serviços (TIZIANO, 2006):

a) confidencialidade;

b) integridade;

c) autenticação;

d) autoria;

e) não repúdio;

f) controle de acesso.

Seu funcionamento se da pela utilização de dois elementos que são: algoritmo e a chave[3]. O algoritmo refere-se a um conjunto de métodos matemáticos que podem ser utilizados juntamente com a chave para que se possa criptografar algo. A utilização de chaves criptográficas permite que o algoritmo seja utilizado por diversas pessoas sendo que empregando chaves distintas terão resultados diferentes. Está união também possibilita que, caso a chave utilizada para cifras das mensagens seja descoberta, esta seja substituída por outra (MACHADO, 2006).

A criptografia pode ser dividida em dois tipos, que se diferenciam no número de chaves utilizadas:

a) **simétrica:** a chave e o algoritmo utilizado para cifrar as mensagens são os mesmos utilizados para decifrar as mensagens, conforme Figura 5 (BURNETT; STEPHEN, 2002);

[3] Cadeia de bits utilizada em algum algoritmo (MACHADO, 2006)

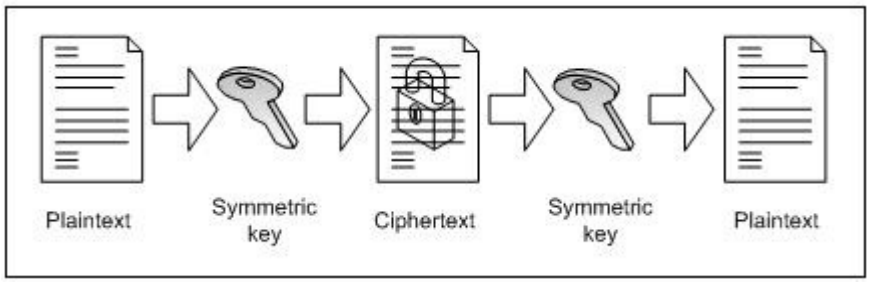

Figura 5: Criptografia simétrica
Fonte: (MICROSOFT, 2008)

b) **assimétrica ou de Chave Pública:** são utilizados um par de chaves, sendo uma para cifrar as mensagens e outra para decifrar as mensagens, conforme Figura 6 (TIZIANO, 2006).

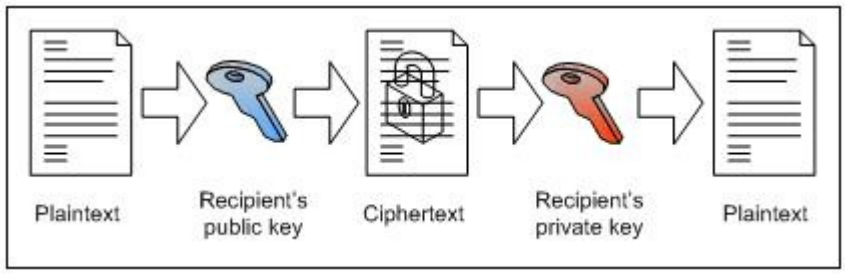

Figura 6: Criptografia assimétrica
Fonte: (MICROSOFT, 2008)

3.3.1 Algoritmos de Criptografia

A criptografia vem sendo utilizada há muito tempo, e neste período foram desenvolvidos e aperfeiçoados vários algoritmos, tanto do tipo simétrico como do tipo assimétrico.

Dentre os algoritmos do tipo simétrico mais utilizados estão (BURNETT; STEPHEN, 2002):

a) **DES:** fazendo uso de chaves de 56 bits possibilita até 72 quatrilhões (72.057.594.037.927.936) de combinações distintas, mas já houve relatos que este foi desvendado com a utilização de força bruta;

b) **IDEA:** tendo estrutura semelhante ao DES, se diferencia pela utilização de chaves que chegam até 128 bits;

c) **RC:** possibilita chaves de 8 a 1024 bits e deu origem a algumas variações, tais como, RC2, RC4, RC5 e RC6 se diferenciando pelo emprego de chaves mais intricadas.

Os algoritmos assimétricos que fazem uso de um par de chaves apresentam maior segurança em comparação com os algoritmos simétricos, os mais comuns são (BURNETT; STEPHEN, 2002):

a) **RSA:** cifra as mensagens utilizando a chave pública que é formada por dois números: um módulo e um expoente público. As mensagens são decifradas com a utilização da chave privada que é composta pelo mesmo módulo da chave pública mais um expoente privado;

b) **El-Gamal:** mesmo utilizando o padrão de chave pública para geração de suas chaves, ele é capaz de aprovar a autenticidade de mensagens ainda que enviadas em canais inseguros. Faz uso de algoritmo discreto.

Os algoritmos assimétricos tendem a ser mais lentos que os simétricos devido a sua natureza, mas apresenta vantagens no gerenciamento e distribuição de chaves, o que permitiu a disponibilização de assinatura digital.

3.3.2 Assinatura Digital

A assinatura digital originou-se pela necessidade de se comprovar autoria no meio eletrônico, ou seja, em documentos físicos basta à assinatura manuscrita para garantir a autenticidade deste, já no meio eletrônico está autenticidade deve ser comprovada com a utilização de métodos matemáticos.

A utilização da assinatura digital resolve dois problemas encontrados na criptografia, que é autenticidade e não-repúdio. A autenticidade é garantida se a chave pública decifrar a mensagem desejada corretamente, já o não-repúdio é alcançado, pois a assinatura digital é um processo unidirecional, ou seja, uma vez cifrado é impossível retornar ao estado original, com isso a modificação de apenas um bit faz com que o documento não seja autêntico (BURNETT; STEPHEN, 2002).

Tal tecnologia pode ser empregada em diversos casos no meio eletrônico, não se resumindo apenas em autenticar documentos (VOLPI, 2001):

a) comércio eletrônico;
b) processos judiciais e administrativos em meio eletrônico;
c) transações seguras entre instituições financeiras;
d) comprovar autenticidade de sites;
e) certificação digital;
f) autenticação de usuários em sistema da informação;
g) até o desenvolvimento do presente trabalho não houve relatos de ataques envolvendo a tecnologia de assinatura digital, nem mesmo chegaram próximo de tal proeza.

3.4 RISCOS E AMEAÇAS ENVOLVENDO INFORMAÇÕES

Risco pode ser considerado a combinação de vulnerabilidades, ameaças e impactos, estando quase sempre ligado a prejuízos. É importante destacar que, para uma política de segurança funcionar corretamente é necessário que se tenha uma análise de riscos bem detalhada, pois só assim pode-se adquirir conhecimento sobre as vulnerabilidades, ameaças e respectivamente qual o impacto sobre o sistema ou

organização se determinadas ameaças ocorrerem. Está análise não consiste apenas em definir mecanismos para proteger o sistema contra possíveis ataques, mas define quais medidas devem ser tomadas se algum destes virem a se concretizar (LAUREANO, 2008).

A análise de riscos permite conhecer as ameaças com antecedência, fazendo com que medidas de segurança sejam reformuladas de acordo com elas, agindo de forma preventiva possibilitando amenizar possíveis impactos e simplificar as medidas corretivas (DIAS, 2000).

Dias (2000) ressalta que não existe um sistema totalmente seguro e livre de falhas, ameaças e vulnerabilidades, o que existe são sistemas que implementam medidas rígidas de segurança diminuindo consideravelmente os riscos, mas é importante advertir que por mais que um sistema seja seguro sempre haverá vulnerabilidades que poderão ser exploradas, tudo é uma questão de tempo.

3.4.1 Gerência de Riscos

Os riscos sempre estarão presentes, independente do ambiente analisado, eles estão apenas passando por processos de modificações, pois antes os maiores riscos eram físicos, como terremotos, inundações e hoje estão ganhando caráter lógico, sendo que grande parte das organizações são movidas através do conjunto de informações que as cercam, o acesso indevido a estas, pode ser considerado como um dos maiores problemas nos tempos atuais, com isso a gerência de riscos visa identificar quais caminhos devem ser tomados, bem como quais informações devem ser protegidas (LAUREANO, 2008).

Este processo identifica os riscos com o intuito de analisar e controlar os problemas ao qual o sistema em questão está exposto, para tal é identificado quais partes do sistema são importantes, quais informações e ou processos devem ser seguros e qual a conseqüência se tais riscos vierem a acontecer, com essas informações é possível definir quais medidas devem ser tomadas para diminuir a probabilidade de ocorrência destes (LAUREANO, 2008).

Um ponto importante na gerência de risco que fará com que este tenha sucesso é a identificação clara de itens como: utilidade da informação, validade da informação e o mais importante, estimar o valor da informação que se quer proteger para então definir quais passos devem ser tomados. Este processo se faz necessário para que seja possível definir com clareza se é cabível proteger as informações.

A Figura 7 demonstra os passos para identificar a existência de riscos em uma aplicação, bem como se estes são aceitáveis.

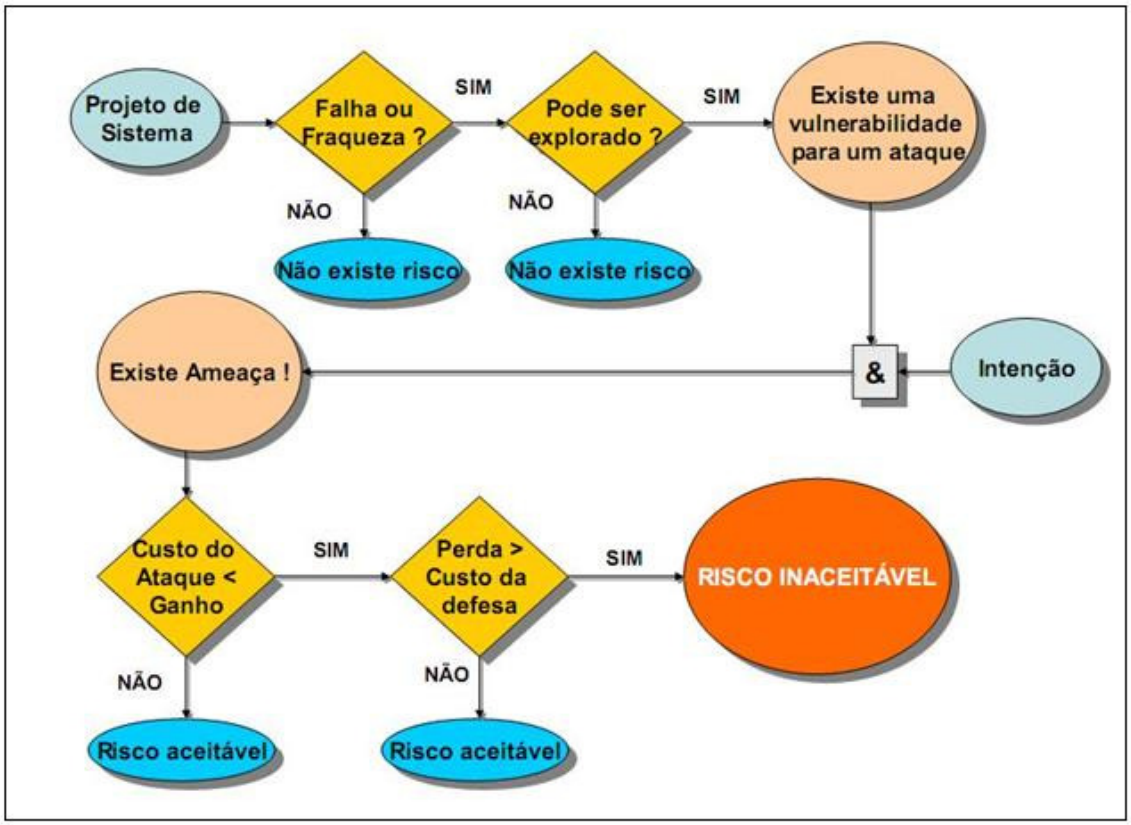

Figura 7: Definição de riscos e ameaças
Fonte: (LAUREANO, 2008)

A análise de risco, por ser um processo crítico, deve ser executada no menor tempo possível e deverá ser atualizada periodicamente, pois a cada dia são identificadas novas vulnerabilidades e desenvolvidas novas tecnologias. Assim, o que em um primeiro momento estava seguro, posteriormente pode não apresentar a segurança necessária.

Está análise deve abranger todos os itens do ambiente móvel, para garantir a segurança em todos os níveis.

4 TECNOLOGIAS ENVOLVIDAS

A utilização de qualquer sistema computacional implica na união de várias tecnologias envolvendo *hardware* e *software.* Neste capítulo serão abordadas as tecnologias aplicadas nos ambientes móveis bem como as falhas e os mecanismos de segurança inerentes a cada uma delas.

4.1 REDES DE COMPUTADORES

A sociedade humana, desde o princípio, possui como uma das suas principais necessidades a comunicação. A partir deste ponto, diferentes maneiras são utilizadas a fim de possibilitar a propagação das informações, tendo-se uma evolução não somente no tratamento destas, como também nos meios de comunicação. Portanto, a integração entre a comunicação e o processamento das informações permitiu novas formas de se comunicar, bem como aumentou a eficácia dos sistemas computacionais (SOARES; LEMOS; COLCHER, 1995).

Neste contexto, têm-se as redes de computadores que são constituídas por um conjunto de módulos processadores[4] que compartilham informações e recursos por meio de um sistema de comunicação (SOARES; LEMOS; COLCHER, 1995).

As redes de computadores para realizarem a comunicação, utilizam-se de alguns meios de transmissão que se diferenciam em função da banda passante, do tipo de conexão, da limitação geográfica, custo, confiabilidade, entre outros. Os meios físicos são divididos em meios guiados que englobam as transmissões por cabos de

[4] Qualquer dispositivo capaz de se comunicar por intermédio do sistema de comunicação por troca de mensagens (INTEGRAL SISTEMAS, 2008).

cobre e fibras ópticas, e em meios não-guiados que englobam as transmissões por ondas eletromagnéticas (SOARES; LEMOS; COLCHER, 1995).

Dentre estes, estão as redes sem fio cuja transmissão acontece por meio de sinais de radiofreqüência, dispensando totalmente a utilização de cabos. Em lugares em que é inviável a instalação de redes, pois é impossível empregar cabos tanto metálicos como de fibra ótica, nota-se um grande cenário para utilização de redes sem fio baseadas em radiodifusão bem como, aplicações que necessitam de confiabilidade no meio de transmissão.

Como está tecnologia não necessita de um meio físico de transmissão, a mesma faixa de freqüência pode ser compartilhada. Entretanto existe a possibilidade de interferências. Redes baseadas em cabos utilizam de mecanismos físicos para garantir a segurança. Já redes baseadas em radiodifusão devem utilizar mecanismos de criptografia para que a privacidade seja garantida e impedir que o sinal seja interpretado por receptores não autorizados (SOARES; LEMOS; COLCHER, 1995).

4.1.1 Wireless

Muitas tecnologias estão incluídas na categoria de redes sem fio, mas as que são abordadas nessa pesquisa estão relacionadas com o padrão 802.11.

As redes sem fio vêm se tornando cada vez mais utilizadas nos mais variados ambientes, haja vista que, o ganho na flexibilidade, na mobilidade e a tendência moderna de eliminação de fios juntamente com os baixos custos, tornam está estrutura vantajosa (DUARTE, 2003).

Dentre estas vantagens oferecidas está o poder de mobilidade, permitindo que dispositivos possam ser transportados de um lugar para outro sem que a conexão

com o sistema de dados da rede seja perdida. Várias extensões foram implementadas para as redes sem fio desde a sua criação, com isso novas características técnicas e operacionais foram acrescentadas (RUFINO, 2005).

4.1.1.1 Características Wireless

As redes sem fio foram desenvolvidas tendo como base as redes cabeadas, algumas das suas características foram herdades de lá. Outras características são da própria rede sem fio. A seguir serão conceituadas algumas destas características (RUFINO, 2005):

a) ***Extended Service Set Identifier* (ESSID):** deve ser conhecido tanto pelos clientes para que seja possível fazer uma requisição de conexão e pelos concentradores, estes responsáveis por enviar sinais com o ESSID que são definidos como sendo o nome da rede. A emissão desse sinal não é obrigatória já que os dispositivos permitem sua configuração, sendo que para redes em que concentradores não os enviam é necessário que o cliente tenha conhecimento dos ESSID deles para que uma conexão possa ser estabelecida;

b) **BEACON:** *beacon frames* são sinais enviados pelos concentradores para que os clientes saibam de sua existência, a ausência desses sinais pode dificultar a utilização destes ambientes;

c) **Meio compartilhado**: todo o tráfego nas redes sem fio fica visível para as interfaces conectadas a um mesmo concentrador, assim o tráfego destinado a uma interface pode ser capturado facilmente por uma terceira. Este já é um grande problema nas redes cabeadas e nas redes

sem fio ganham proporções ainda maiores, pois não se tem controle dos dispositivos que serão conectados ao meio. *Switches* ou concentradores mais novos podem resolver este problema sendo que conseguem isolar o tráfego para uma ou mais interfaces do meio. O padrão *Spread Spectrum* o mesmo utilizado no *Code Division Multiple Access* (CDMA) é a tecnologia mais utilizada hoje, pois tem a segurança como uma de suas principais características;

d) ***Ad-hoc*:** mesmo com problemas de segurança, pois não utiliza concentradores, as redes *ad-hoc* são muito utilizadas por permitirem conexões diretas entre equipamentos e se um destes falhar, seu funcionamento é mantido e apenas o equipamento com falha perde a conexão com a rede;

e) **Infra-estrutura**: está configuração permite maior segurança sendo que todos os clientes se conectam a um concentrador e este dentre outras características dita todas as regras de segurança.

4.1.1.2 Padrões Wireless

O *Institute of Electrical and Electronics Engineers* (IEEE) é a principal organização que define padrões para serem utilizados nas redes *Wireless,* por meio destes, empresas podem desenvolver dispositivos que funcionem corretamente garantindo também que grande parte das tecnologias mais antigas ainda possua suporte, alguns desses padrões serão conceituados a seguir (RUFINO, 2005):

a) **padrão 802.11b:** operando na freqüência de 2,4 GHz e tendo como transmissão máxima 11Mbps de velocidade, este foi o primeiro

sub-padrão definido. Mesmo sendo o padrão mais popular e tendo o maior numero de equipamentos e sistemas de administração e segurança que se adéquam a ele, podemos encontrar algumas restrições de uso, bem como, a quantidade de usuários conectados que se limitam apenas a 32;

b) **padrão 802.11a:** foi definido com o intuito de resolver muitos dos problemas encontrados nos padrões 802.11 e 802.11b, como o aumento significativo na quantidade máxima de usuários conectados que passou para 64, bem como, a velocidade máxima que aumentou para 54 Mbps. A segurança foi reforçada permitindo chaves de ate 256 bits para serem usadas com o WEP. Mesmo com estas vantagens surgiram alguns problemas, pois operando na faixa de 5 GHz gera incompatibilidade com os outros padrões que operam em faixas diferentes;

c) **padrão 802.11g:** operando na faixa de freqüência de 2,4 GHz, permitiu que equipamentos dos padrões 802.11, 802.11b possam ser utilizados no mesmo ambiente. Algumas das características positivas do padrão 802.11a foram mantidas, como a velocidade de 54 Mbps e a modulação OFDM. Utiliza WEP para autenticação bem como WPA com criptografia dinâmica. A utilização de dispositivos que fazem uso de tecnologias anteriores como 802.11a podem comprometer a segurança da rede;

d) **padrão 802.11i:** a busca por mecanismo mais eficientes de segurança e autenticação deu origem a este padrão que utiliza do *Robust Security Network* (RSN) para permitir meios mais seguros, assim como o

protocolo WPA que é mais seguro que o WEP e o WPA2 que utiliza o *Advanced Encryption Standard* (AES) como algoritmo de criptografia;

e) **padrão 802.11n:** não possui melhoras significativas em termo de segurança, sua maior vantagem é o aumento de velocidade que pode chegar a 500 Mbps, e também a possibilidade de ampliação da área de cobertura;

f) **padrão 802.1x:** não se trata de um padrão de redes sem fio. Refere-se a um modelo de autenticação que pode utilizar servidores RADIUS para permitir o acesso a rede. Busca disponibilizar uma única forma de autenticação, independente da tecnologia que está sendo utilizada para conexão que podem ser: redes sem fio, redes cabeadas, acessos discados, entre outros.

4.1.1.3 Mecanismos de Segurança Wireless

No início da utilização das redes de computadores a segurança não fora devidamente considerada, pois estas eram aplicadas apenas para fins educacionais e para compartilhamento de equipamentos. Essa visão mudou completamente, sendo que hoje muitas operações estão sendo executadas por intermédio destas, como transações bancárias e compras *on-line* onde a segurança e privacidade são importantes.

Além dos problemas de segurança encontrados nas redes cabeadas, com a utilização de redes sem fio são encontrados novos problemas (TANENBAUM, 1997).

A seguir serão conceituados alguns mecanismos de segurança que visam tornar as redes sem fio mais seguras.

4.1.1.3.1 Endereçamento MAC

Dispositivos mais novos possuem um número único de identificação que é controlado pelo *Institute of Electrical and Electronics Engineers* (IEEE) e definido pelo fabricante, com isso, pode-se restringir o acesso a uma rede sem fio permitindo que apenas dispositivos conhecidos ou previamente cadastrados possam acessá-la, mas existem *softwares* que emulam facilmente esses números fazendo com que qualquer dispositivo possa ter acesso ao meio utilizando a identificação de um equipamento já cadastrado.

Deve-se levar em consideração que apenas o *hardware* pode ser identificado e não o usuário. Essa técnica pode ser usada também de forma inversa, ou seja, o usuário pode especificar o concentrador no qual quer estabelecer conexão através do endereço MAC (RUFINO, 2005).

A grande desvantagem deste método é que não implementa um bom nível de segurança, e gera retrabalho quando qualquer equipamento da rede for trocado, bem como a incorporação de novos equipamentos.

4.1.1.3.2 Wired Equivalent Privacy (WEP)

As redes cabeadas utilizam os cabos para transmitir as informações, com isso identifica-se facilmente os clientes que as receberão, mas nas redes sem fio basta ter um receptor para receber o sinal. Para que as redes sem fio tenham privacidade, o padrão 802.11 permite que os dados sejam cifrados. O WEP está presente em todos os dispositivos do padrão Wi-Fi e foi o protocolo sugerido para resolver estes problemas. As mensagens trafegadas são cifradas pelo algoritmo simétrico RC4 que usa

criptografia de 64 e 128 *bits* fazendo uso das chaves secretas compartilhadas entre o cliente e servidor, essa autenticação é feita na camada de enlace. Utiliza-se também o padrão CRC-32 para checagem de redundância cíclica nos pacotes de dados verificando a integridade destes.

Utilizando pouco poder de processamento o WEP cifra o tráfego utilizando uma chave formada por um componente dinâmico e por uma chave estática disponível em todos os equipamentos da rede. Quatro novas chaves são geradas a partir da chave estática, a operação matemática utilizada para gerá-las é feita após a conexão ser estabelecida e apenas uma delas será utilizada para cifrar as informações em andamento (RUFINO, 2005).

4.1.1.3.3 Wi-fi Protected Access (WPA)

O protocolo WPA foi liberado devido aos vários problemas de segurança e autenticação encontrados no WEP, com isso, suas principais mudanças foram na cifração dos dados para garantir um tráfego seguro e na autenticação de usuários que faz utilização do padrão 802.1x e *Extensible Authentication Protocol* (EAP). A seguir serão conceituadas as áreas utilizadas pelo WPA (RUFINO, 2005):

a) **criptografia:** para resolver os problemas dos mecanismo de criptografia utilizados no WEP, o WPA propõe tanto combinações de algoritmos como temporalidade de chaves. Buscando atender as diversas necessidades e ambientes distintos, diferentes modelos de segurança e protocolos de cifração foram desenvolvidos, sendo que um atende as redes de pequeno porte, como redes domésticas e o outro atende redes

mais elaboradas, pois necessita de um servidor de autenticação (RADIUS);

b) **chave compartilhada**: destaca-se pela sua simplicidade e como a troca de chaves geralmente é feita manualmente dispensa o uso de dispositivos auxiliares. Importante lembrar que até então não existem problemas para os protocolos utilizados com o WPA-PSK.TKIP que em uma comunicação é responsável pela troca dinâmica de chaves;

c) **troca dinâmica de chaves:** corrigindo a falha no protocolo WEP que utiliza chaves estáticas, o protocolo WPA utiliza chaves dinâmicas por meio do protocolo Temporal Key Integrity Protocol (TKIP) preservando seu segredo. Para garantir a segurança o vetor de inicialização aumentou de 24 para 48 bits, aumentando consideravelmente as combinações e permitindo a sua substituição a cada pacote, diminuindo os riscos de ataques;

d) **Extensible Authentication Protocol (EAP):** este modelo se destaca, pois permiti a autenticação de várias tecnologias desde conexões discadas às redes sem fio integrando soluções existentes e já testadas, assim como certificação digital. Vantagens são encontradas também na parte de gerência que dispensa o uso de várias bases de acesso.

Mesmo com todos esses métodos de autenticação de usuário e equipamentos como, endereçamento MAC dos equipamentos, senhas fixas e dinâmicas, certificados digitais entre outros, cada um possui um nível de segurança. Falhas nesses níveis de segurança podem resultar em informações capturadas por equipamentos não pertencentes ao meio, pelo simples fato de utilizar o ar como meio de transporte (RUFINO, 2005).

A Tabela 1 apresenta as diferenças e semelhanças entre os protocolos WEP e WPA.

Tabela 1: WEP x WPA

MECANISMO DE SEGURANÇA	WEP	WPA
CRIPTOGRAFIA	RC4	RC4
TAMANHO DA CHAVE	40 BITS	128 BITS ENCRIPTAÇÃO 64 BITS AUTENTICAÇÃO
PACOTE DA CHAVE	CONCATENADA	MISTURANDO FUNÇÕES
INTEGRIDADE DO DADOS	CRC-32	MIC
INTEGRIDADE DO ENCABEÇAMENTO	NÃO POSSUI	MIC
GERENCIAMENTO DE CHAVE	NÃO POSSUI	EAP - BASEADO

Fonte: (CARVALHO FILHO, 2005)

4.1.2 Vulnerabilidades e Mecanismos de Invasão

Dispositivos utilizados na implementação de uma rede sem fio já possuem mecanismos de segurança implementados de fabrica, mas por motivos de incompatibilidade ou até mesmo para facilitar a instalação estes vêm desabilitados (RUFINO, 2005).

Com está facilidade, em muitos casos os mecanismos de segurança oferecidos pelo próprio dispositivo não são configurados corretamente pelos administradores da rede, tornando este ambiente vulnerável (PEREIRA JUNIOR; BRABO; AMORAS, 2004).

Estas vulnerabilidades podem facilitar a invasão por indivíduos que não possuem acesso a rede e a obtenção de informações provenientes dos dados que nela trafegam.

Essas invasões podem ser concebidas de quatro maneiras diferentes (PEREIRA JUNIOR; BRABO; AMORAS, 2004):

a) **interrupção:** as informações são interceptadas antes que cheguem ao seu destino;
b) **interseção**: utilizada para se ter noção das informações pertencentes ao meio;
c) **modificação:** as informações são interceptadas, alteradas e retransmitidas;
d) **fabricação:** as informações são geradas pelo próprio invasor e inseridas ao meio.

Mesmo nas redes criptografadas, a possibilidade dos dados em tráfego serem interceptados e decifrados não deve ser desconsiderada, pois os invasores podem ser identificados como membros da rede e obterem quaisquer informações inerentes a está (PEREIRA JUNIOR; BRABO; AMORAS, 2004).

Os invasores já contam com várias técnicas e ferramentas que auxiliam na invasão e exploração das redes sem fio, algumas delas serão abordas com mais detalhes nas seções seguintes.

4.1.2.1 Denial of Service (DoS)

Ataques de negação de serviço consistem em explorar a freqüência utilizada pelos dispositivos que gerenciam as redes sem fio, sendo que uma quantidade elevada

de sinais emitidos na mesma freqüência pode causar interferências e prejudicar o funcionamento das redes sem fio ou até mesmo derrubar o ponto de acesso (RUFINO, 2005).

Tais ataques podem ocorrer de maneira involuntária, pois em redes vizinhas que utilizam os mesmos dispositivos gerenciadores de redes sem fio e fazem uso da mesma faixa de freqüência para transmissão de sinais, sendo que a falta de isolamento pode permitir que estes sinais causem interferências (PEREIRA JUNIOR; BRABO; AMORAS, 2004).

Essa vulnerabilidade pode ser explorada por ferramentas simples, como, o Void11 que permite a execução de ataques por associação, dissociação e autenticação.

4.1.2.2 Scanners

As redes sem fio trabalham em *broadcast* para facilitar a conexão dos usuários, possibilitando assim sua identificação por possíveis invasores.

Mesmo com a possibilidade de configurar os dispositivos para inibirem estes sinais, ferramentas como o *NetSumber* foram desenvolvidas com o intuito de auxiliar os gerentes de redes na identificação dos dispositivos pertencentes a redes bem como a qualidade do sinal, mas ela pode ser usada de forma maliciosa.

Seu funcionamento consiste na emissão de pacotes em *broadcast* para identificar o ponto de acesso, sendo que após este ser identificado o invasor fará uso de outras ferramentas para alcançar seus objetivos.

Além da inibição de pacotes em *broadcast*, o SSID default que é emitido em *broadcast* pode ser alterado e configurado para não ser mais emitido, tornando a rede menos vulnerável (PEREIRA JUNIOR; BRABO; AMORAS, 2004).

4.1.2.3 Vulnerabilidades do WEP

Muitos métodos e ferramentas foram desenvolvidos para explorar as falhas de segurança do protocolo WEP, a grande maioria utiliza ataques baseados em dicionário e força bruta para quebrar suas chaves, a seguir serão apresentadas algumas dessas ferramentas (RUFINO, 2005):

a) **Airsnort**: considerada uma ferramenta fraca para ataques dessa natureza e por não obterem muitas informações da rede, ela pode ser utilizada com sucesso na quebra de chaves de redes com grande tráfego;
b) **Wepattack**: podendo utilizar qualquer dicionário disponível e combinações de palavras, está ferramenta pode ser muito eficiente na tentativa de quebra de chaves;
c) **Weplab**: utiliza métodos de força bruta e quebra eficiente de chaves do protocolo WEP a partir de falhas analisadas;
d) **Aircrack**: sendo uma suíte completa contendo ferramentas para coleta de pacotes, quebra de chaves e outra para decifrar o tráfego capturado, atualmente é considerada a mais eficiente na quebra de chaves WEP.

4.1.3 Identificação de Níveis de Segurança

No decorrer da pesquisa, foram levantadas outras questões de segurança que não se enquadram no trabalho desenvolvido, como o IPSec que é uma extensão do protocolo IP e visa dar privacidade ao usuário, bem como as redes privadas virtuais mais conhecidas como VPN, que transferem as informações por uma conexão segura

conhecida como túnel, onde é criada uma rede virtual simulando uma conexão ponto a ponto (CARVALHO FILHO, 2005).

A Tabela 2 relaciona os protocolos e tecnologias de proteção utilizados em redes sem fim, definido os níveis de segurança alcançado.

Tabela 2: Níveis de segurança

Nível	Tipo de proteção	Protocolos comuns
0	ESSID	Sem segurança
1	WEP	Apenas criptografia básica
2	WPA	Criptografia e autenticação
3	VPN	Protocolos avançados de criptografia e autenticação
4	Criptografia e Autenticação para 802.11i	Criptografia AES e autenticação 802.1x

Fonte: (CARVALHO FILHO, 2005)

4.2 DISPOSITIVOS MÓVEIS

A utilização de dispositivos móveis vem crescendo a cada dia e isso está tornando essa tecnologia parte da rotina de muitas pessoas, essa grande demanda por estes dispositivos tem ocorrido pelo fato de estarem diminuindo consideravelmente as diferenças entre estes para os *desktops* ou *laptops*, bem como a diminuição considerável nos custos (CAMINHA, 2006).

Outro fator que impulsiona esse crescimento é o fato da junção de várias tecnologias de comunicação como o acesso a *internet* sem fio e estarem englobados com muitas opções desde simples agendas a editores avançados de texto. Junções estas que deram origem ao *smartphone*, um dispositivo móvel que engloba as funções de PDA bem como as funções de um telefone celular (PITOMBEIRA, 2006).

Contendo todas estas qualidades vêm se tornando ferramentas indispensáveis para profissionais que estão em constante movimentação e necessitam de informações atualizadas bem como a edição destas, independente da sua localização.

Vários aspectos devem ser lavados em consideração na utilização de dispositivos móveis, bem como no desenvolvimento de soluções para este. A seguir serão apresentados alguns dos aspectos mais importantes.

4.2.1 Mobilidade

Pelo fato de dispositivos móveis estarem em um ambiente diferente dos dispositivos fixos, surgem questões antes não existentes e que devem ser analisadas para manter a integridade das informações e garantir segurança no acesso as funcionalidades proporcionadas por eles (PITOMBEIRA, 2006).

Não dependendo de meios físicos para transmissão de dados, pois sua comunicação é sem fio, problemas como localização do dispositivo móvel, taxa de transferência das redes sem fio, autenticação de dispositivos e por falhas externas, como falta de bateria (PITOMBEIRA, 2006).

4.2.2 ESS (Extended Service Set)

Garantir a conectividade a uma rede fixa e manter as transações em execução mesmo com a movimentação dos dispositivos móveis entre os pontos de acesso que oferecem um serviço de comunicação sem fio é gerado um processo

transparente ao usuário mais conhecido como ESS, este ocorre tanto na movimentação dentro da mesma área bem como em áreas vizinhas (PITOMBEIRA, 2006).

A compreensão deste aspecto, só será alcançada com a utilização do modo infra-estruturado, onde redes diferentes se comunicam por meio de *Access point* para que seja possível criar uma única rede (LUIZ OTÁVIO DUARTE, 2003).

4.2.3 Desconexão

É impossível prever as desconexões causadas pelos mais variados motivos nos ambientes que provêem mobilidade. Identificam-se diferentes tipos de desconexões, como voluntária que o próprio usuário executa, bem como as involuntárias que podem ser ocasionadas pelo deslocamento do usuário a uma região que não possui cobertura do serviço de comunicação sem fio, descarregamento da bateria ou até mesmo cancelamento do serviço de comunicação.

Mesmo não considerada uma desconexão a variação na qualidade do sinal pode prejudicar a transação em andamento, sendo assim, tanto os protocolos de comunicação como os software devem estar preparados para tal (PITOMBEIRA, 2006).

4.2.4 Gerenciamento de Energia

Para que a mobilidade possa ser garantida existe a necessidade da alimentação dos dispositivos móveis ser feita por baterias, mas a vida destas varia muito de aparelho para aparelho, bem como a sua utilização e tecnologia. Tanto engenheiros

de hardware como de software devem analisar o problema de energia e projetar soluções que otimizem o seu consumo (MATEUS; LOUREIRO, 2008).

Processos como armazenamento e transferência de dados, estabelecimento de conexões, localização de pontos de acesso e processamento são fatores importantes e devem ser considerados para a otimização de consumo energia. É importante frisar que os dados são mantidos na memória temporária somente enquanto o mesmo estiver ligado, então com o desligamento provocado pelo próprio usuário ou pela falta de bateria, implica na perda total desses dados (PITOMBEIRA, 2006).

Na Tabela 3 pode-se observar o tempo médio de duração da bateria de alguns dispositivos móveis.

Tabela 3: Duração média da bateria

Tipo de dispositivos móveis	**Duração típica de bateria**
Dispositivos de pager/RIM	Semanas
Telefone cellular	Dias
PDA/Smartphone	Horas/dias
Tablet PC	Horas
PC laptop	Horas

Fonte: (LEE; SCHNEIDER; SCHELL, 2005).

4.2.5 Tecnologia de Comunicação Sem Fio

Para que a mobilidade seja garantida e os dispositivos não necessitem de conexões físicas, é essencial a utilização da comunicação sem fio, que englobam Bluetooth, telefonia celular e wireless, estes serão conceituadas a seguir (LEE; SCHNEIDER; SCHELL, 2005):

a) **Bluetooth:** mesmo sendo de curto alcance, está tecnologia vem sendo muito utilizada, pois necessita de pouco poder de processamento e tem um baixo consumo de energia. Pequenas redes podem ser formadas utilizando está tecnologia que são denominadas *Personal Area Network* (PAN);

b) **Telefonia celular**: sem duvida a telefonia móvel celular é a tecnologia sem fio mais utilizada, provendo serviços como, *General Packet Radio Service* (GPRS) e *Enhanced Data Rates For Global Evolution* (EDGE) para permitir a transmissão de dados, além de serviços de comunicação por voz. O protocolo *Wireless Application Protocol* (WAP) é utilizado para garantir que as transmissões de dados funcionem corretamente independentes de dispositivos e sistema celular empregados.

4.2.6 Recursos Computacionais Limitados

A grande evolução dos dispositivos móveis bem como a agregação de novas tecnologias e recursos, ainda pode ser encontrada algumas limitações que não devem passar despercebidas. Limitações como, energia, processamento, gerenciamento de dados e taxas reduzidas de transmissão de dados são um exemplo destas (PITOMBEIRA, 2006).

O impacto destas limitações podem ser minimizados com a otimização dos esquemas de gerenciamento de dados permitindo alto desempenho na realização das tarefas nos dispositivos móveis (PITOMBEIRA, 2006).

4.2.7 Gerenciamento de Dados

Como visto anteriormente, existem vários tipos de desconexões nos ambientes móveis, sendo que estas podem implicar na integridade dos dados que estavam sendo processados no momento, bem como a perda de informações nas transações em andamento.

No tempo que o dispositivo ficou desconectado do servidor, informações podem ter sido alteradas. Para garantir que as alterações efetuadas não sejam perdidas, estas devem ser enviadas para o servidor no momento que o usuário se reconectar.

Estes processos podem alocar muitos recursos dos dispositivos móveis, desde processamento a transmissão de dados. Para minimizar o trabalho dos dispositivos móveis, a análise de aspectos como, quais dados devem ser recuperados e quais dados devem ser atualizados no servidor é indispensável (MATEUS; LAUREIRO, 2008).

4.2.8 Usabilidade

O conjunto de soluções tanto de *hardware* como de *software* desenvolvidas sobre um dispositivo móvel devem garantir que todos os aspectos vistos anteriormente sejam executados de forma transparente ao usuário (MATEUS; LAUREIRO, 2008). Disponibilizando alto grau de segurança nas transações e diversas funcionalidades numa interface simples. Questões estas, garantem o crescimento na utilização de dispositivos móveis, bem como o estudo de novas tecnologias.

4.2.9 Segurança no Dispositivo Móvel

Uma das maiores barreiras para o aumento no uso de aplicações, tais como acesso aos dados de um RES por meio de DM, é a questão relacionada com a segurança da informação. Sua natureza móvel e portátil permite abranger grandes áreas contribuindo para a volatilidade da segurança (DUARTENN, 2008). Está carência de segurança pode ser relacionada aos métodos simples de controle de acesso disponíveis para dispositivos móveis.

Com isso, as aplicações desenvolvidas para está plataforma devem oferecer segurança da informação como: criptografia, assinatura digital, autenticação de usuários, destruição de dados sigilosos, entre outros. A seguir serão listados aspectos importantes referente à segurança da informação nos DM (LEE; SCHNEIDER; SCHELL, 2005).

4.2.9.1 Confidencialidade do Sistema

O RES contém informações sigilosas a serem acessadas somente por médicos e enfermeiros de uma unidade hospitalar específica. O acesso ao RES por meio dos DM não deve interferir na confidencialidade requerida, assim como nas aplicações em computadores *desktops* para acesso ao RES local, ou em rede local. Os DM são dispositivos portáteis, que podem eventualmente ser extraviados e terem suas informações acessadas por terceiros. É importante garantir, por meio da imposição de restrição de acesso, que as informações do sistema não sejam visualizadas (LEE; SCHNEIDER; SCHELL, 2005).

É de grande importância que a arquitetura da aplicação do S-RES que esteja rodando no servidor de aplicação, possua mecanismos capazes de bloquear o acesso a dispositivos dados como extraviados, perdidos ou ate mesmo roubados. Isso se faz necessário para que a integridade do sistema seja mantida, pois mesmo se o sistema apenas disponibilizar dados sobre um paciente, estes podem ser alterados e manipulados de muitas formas.

4.2.9.2 Destruição de Dados

Muitos dos dados utilizados para que a conexão entre o dispositivo móvel e o servidor seja estabelecida, assim como dados retornados deste, continuam disponíveis no dispositivo móvel mesmo depois que a conexão é encerrada e a aplicação é finalizada. Políticas de destruição de dados podem ser implementadas na própria aplicação de acesso ao RES instalada no dispositivo, fazendo com que em determinadas situações todos os dados sigilosos sejam destruídos garantindo a integridade do sistema (LEE; SCHNEIDER; SCHELL, 2005).

Estas políticas podem ser baseadas na identificação de que um dispositivo móvel, foi extraviado o que implicaria na próxima conexão ao servidor, este dispararia comandos que iniciariam rotinas na aplicação móvel responsáveis por apagar todos os vestígios de conexões ou de informações sigilosas ou baseadas em informações erradas passadas a aplicação móvel, disparando as mesmas rotinas quando o binômio *login* e senha forem negadas por mais de três vezes por exemplo.

4.2.9.3 Acessibilidade e Controle de Acesso

Os dispositivos móveis impõem mais uma barreira no que diz respeito a controle físico de acesso, pois se torna difícil identificar o usuário que está utilizando-o e para que fim terá a utilização, diferente de sistemas locais que se tem o controle devido as políticas de acesso físico ao próprio ambiente em que está localizadas as máquinas (LEE; SCHNEIDER; SCHELL, 2005).

O controle de acesso nas máquinas *desktops* na rede local pode ser implementado de várias formas, indo desde simples criptografias de senha até criptografias avançadas acompanhadas de autenticação biométrica, reconhecimento de retina, entre outras, mas nos dispositivos portáteis fica quase que impossível adicionar um *hardware* específico para autenticação de usuários, ficando disponível apenas os mecanismos implementados no próprio dispositivos na sua fabricação.

4.2.9.4 Mecanismos Necessários de Segurança

Sem contar com mecanismos de segurança desenvolvidos na aplicação móvel e nem nos pontos de acesso, o próprio *smartphone Nokia* E61 que será o dispositivo móvel utilizado nesta pesquisa para efetuar o estudo de caso, assim como outros modelos compatíveis, possuem uma série de configurações que se seguidas corretamente possibilitam segurança para quem o utiliza, algumas destas configurações julgadas como requisitos indispensáveis de segurança serão listadas a seguir (NOKIA, 2008):

a) **Solicitação do código PIN:** se ativado o código Personal Identification Number (PIN), este deverá ser informado toda vez que o dispositivo for

ligado, a digitação errada por mais de três vezes implica no bloqueio do cartão Subscriber Identity Module (SIM) sendo necessário o código Personal Identification Number (PUK) para desbloquear;

b) **Código de travamento**: o dispositivo solicita um código predefinido de 4 a 255 caracteres incluindo números e letras fazendo diferença entre maiúsculas e minúsculas. É possível definir o tempo limite para que o dispositivo seja bloqueado, após o bloqueio será obrigatório a digitação do código para que seja liberado o uso;

c) **Bloquear SIM diferente**: é possível definir uma lista de cartões SIM que poderão ser usados no dispositivo, ao ser inserido um cartão SIM que não esteja na lista será solicitado o código de bloqueio;

d) **Travamento remoto**: com está opção habilitada é possível bloquear o aparelho enviando uma mensagem predefinida de outro dispositivo;

e) **Certificados:** mantém uma lista de certificados no aparelho, utilizados para autenticação de conexões com o servidor, autenticação de aplicativos *Java*, aplicativos do sistema operacional *Symbian*[5], entre outras funcionalidades.

4.2.10 Access Point

O *Access Point* ou ponto de acesso é o dispositivo responsável por interligar todos os equipamentos capazes de se conectar em uma rede sem fio, esses pontos de acesso disponibilizam os mesmos serviços encontrados numa rede cabeada normal, mas com a vantagem de não ser preciso a conexão física com tais dispositivo, a distância

[5] Sistema operacional para dispositivos móveis

alcançada, a velocidade de transferência de dados e a quantidade de conexões oferecida por estes dispositivos vária muito de fabricante para fabricante, bem como a tecnologia e protocolos utilizados (BEAVER; DAVIS, 2005).

A utilização de vários *Access Point* dentro de uma empresa ou organização localizados em pontos estratégicos pode criar uma área de cobertura capaz de possibilitar a movimentação por toda a organização sem que a conexão com o servidor seja perdida.

Toda essa facilidade de acesso e instalação de tais equipamentos são prejudiciais as redes, pois se não forem configurados corretamente podem servir como uma porta de entrada para possíveis atacantes e colocar toda a rede em perigo, sendo que as configurações que vem de fábrica ou *default* não implementam restrições de acesso (BEAVER; DAVIS, 2005).

4.2.10.1 Autenticação no Access Point

Na configuração de pontos de acesso podem ser utilizados mecanismos de autenticação (DUARTE, 2003):

a) **Autenticação aberta:** possibilita que qualquer dispositivo que esteja recebendo o sinal possa se conectar a rede sem restrição alguma;
b) **Autenticação compartilhada:** possibilita a conexão de dispositivos que conhecem a chave WEP para fazer a autenticação. O extravio de dispositivos que possuam a chave previamente compartilhada podem por a segurança da rede em risco, para prevenir é necessário trocar a chaves;

c) **Rede-EAP**: autenticação baseadas em algoritmos EAP (*Extensible Authorization Protocol)* que possibilita a utilização de servidores RADIUS.

Além das tecnologias de autenticação disponíveis é possível ampliar o nível de segurança com a utilização de restrições por endereço MAC, SSID *Broadcast disable function*, diminuir a emissão do sinal para que este seja interceptado apenas dentro de um local estipulado, desabilitar o gerenciamento de *Access Point* por meio de redes sem fio, deixando a execução desta tarefa apenas para dispositivos conectados via cabo no *Access Point.*

4.3 S-RES UTINFO 2.0 - TECNOLOGIAS ADOTADAS

Além dos mecanismos de segurança disponibilizados por meio de comunicação sem fio, o qual motivou o desenvolvimento desta pesquisa, aspectos de segurança das ferramentas de desenvolvimento do S-RES UTInfo serão analisados, para garantir de todas as formas e em todos os níveis a integridade das informações.

4.3.1 S-RES - UTINFO 1.0 E UTINFO 2.0

Em uma parceria entre o Laboratório de Informática Aplicada – *Kiron* – do Curso de Ciência da Computação da UNESC e um hospital público da região, foi desenvolvido o S-RES UTInfo 1.0. Foram implementados todos os aspectos indispensáveis a um S-RES para uma UTI. Para o desenvolvimento desta primeira versão, a modelagem foi representada por meio de diagramas *Unified Modeling*

Language (UML) e implementada com a utilização do ambiente de desenvolvimento C++ Builder 5.0 e utiliza o Firebird como Sistema Gerenciador de Banco de Dados Relacional (SGBDR) (CHARNOVSCKI; NASCIMENTO; MACHADO; NICOLEIT; 2004).

Na primeira versão do S-RES, a portabilidade não fora tratada. O S-RES UTInfo 1.0 roda apenas sobre Sistema Operacional *Windows* e possui algumas deficiências tais como problemas relacionados ao processamento de grandes fluxos de informações e dificuldades de expansão e disponibilização destas. A necessidade de um sistema que contemplasse estas carências deu origem à elaboração de um novo S-RES denominado UTInfo 2.0 (MEZAROBA; MENEGON; NICOLEIT, 2008).

O S-RES UTInfo 2.0 abrange funcionalidades que visam oferecer maior segurança, consistência, portabilidade, possibilidades de expansão e maior flexibilidade de apresentação das informações, aspectos estes não eram atendidos na versão 1.0. Um dos destaques desta nova versão é a possibilidade de acesso a informações por meio de DM, sendo que apenas dados gerais do paciente, diagnósticos realizados no hospital e alergias a medicamentos e antibióticos foram disponibilizados. Estas informações são transferidas no formato XML (MEZAROBA; MENEGON; NICOLEIT, 2008).

4.3.1.1 Funcionalidades

O S-RES UTInfo disponibiliza funções tais como cadastro de pacientes, gerenciamento da equipe médica restringindo o acesso de acordo com a função, gerenciamento de leitos, monitoração dos atendimentos prestados ao paciente, consultas e relatórios personalizados. As informações pertinentes ao paciente podem ser divididas da seguinte forma (MEZAROBA; MENEGON; NICOLEIT, 2008):

a) informações gerais que envolvem dados do paciente de caráter pessoal e clínico;

b) condições gerais que englobam informações sobre medicamentos administrados ao paciente e dados relevantes a possíveis transferências;

c) acompanhamento que trata de informações salientes ao comportamento clínico do paciente;

d) resultados dos processos aplicados ao paciente, sendo que somente médicos e enfermeiros autorizados podem editar tais informações;

e) informações referentes a óbitos.

O S-RES é baseado em várias informações para seu correto funcionamento, dentre estas muitas pertencem ao paciente tendo como principal característica o sigilo. Para que seja assimilado corretamente este conjunto de informações, a Figura 8 apresenta algumas tabelas pertencente ao modelo ER do S-RES.

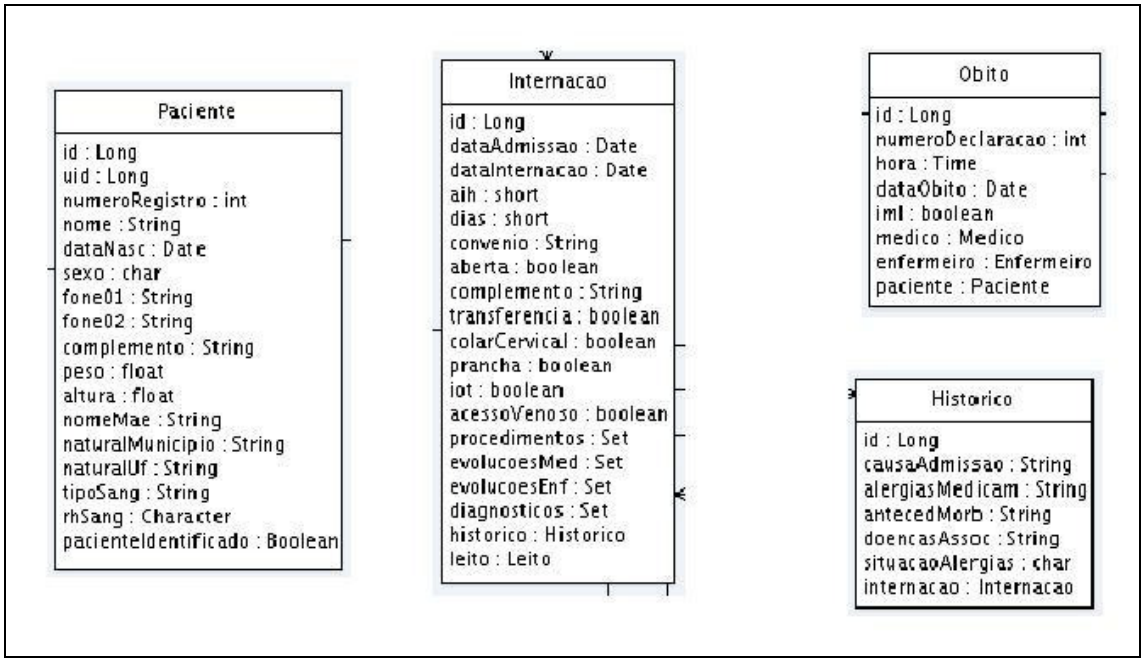

Figura 8: Modelo ER do S-RES UTInfo 2.0
Fonte: KIRON (2008)

4.3.2 Banco de Dados

Grande parte dos bancos de dados armazenam as informações sigilosas pertencentes às organizações. Com isso o servidor no qual estão localizadas, deve oferecer um ou mais mecanismos de segurança para prevenir possíveis falhas que venham a comprometer os dados, garantindo assim sua integridade e a qualidade do sistema. Para prover maior segurança ao servidor de banco de dados, é importante que este seja configurado corretamente, pois ações simples como: desabilitar portas desnecessárias, instalação de um *firewall* na rede, definições de privilégios dos usuários do banco de dados, entre outras, contribuem muito para ampliar a segurança existente.

O S-RES UTInfo 2.0 utiliza o Sistema Gerenciador de Banco de Dados Relacional (SGBDR) *PostgreSQL*[6], que possibilita implementação de aspectos simples de segurança como o par *login* e senha.

4.3.3 Linguagem de Programação

A linguagem *Java* foi apresentada em 1995, pela *Sun Microsystems.* Originalmente, ela buscava a reutilização de códigos e de partes da aplicação, bem como a portabilidade.

A portabilidade é garantida pelo fato dos programas Java serem compilados no formato bytecode, podendo ser executado por qualquer sistema operacional que possua a Máquina Virtual Java (JVM) (LEMAY, 2005). Está característica teve grande influência no crescimento desta linguagem bem como a ampliação do seu alcance que

[6] www.postgresql.org

saiu apenas dos computadores pessoais para dispositivos móveis e até mesmo eletrodomésticos em geral.

Para permitir essa diversidade de equipamentos com suporte a Java, foi dividida em 3 plataformas:

a) *Standard Edition* (J2SE): usado em computadores *desktops* e servidores;

b) *Enterprise Edition* (J2EE): é destinada a aplicações para *web*;

c) Micro *Edition* (J2ME): projetada para dispositivos com limitações computacionais.

A Figura 9 apresenta as divisões da plataforma Java.

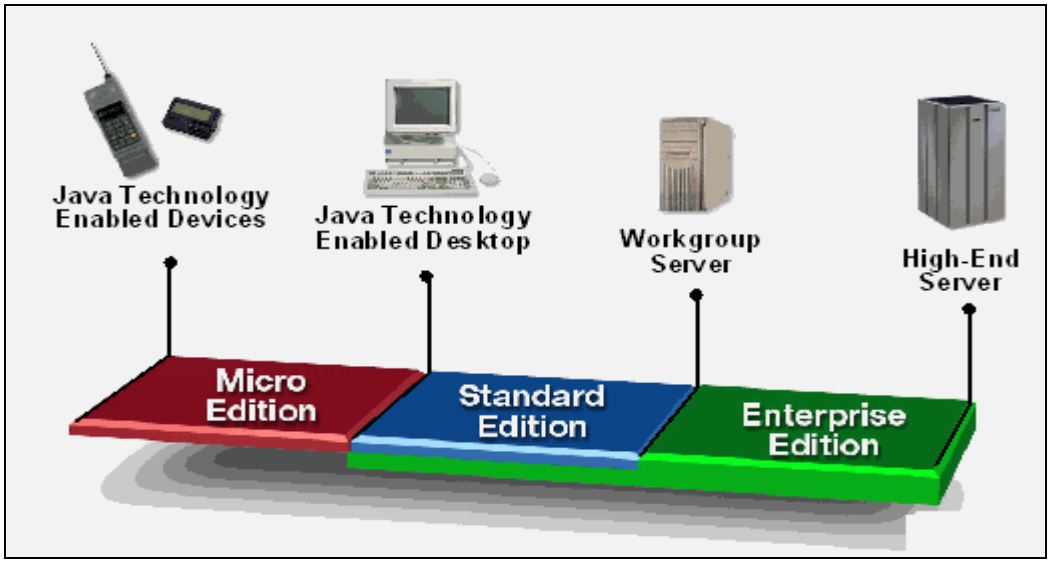

Figura 9: Divisão da Plataforma Java
Fonte: (JAVAMAN, 2008)

Neste trabalho, será abordado com mais detalhes a plataforma J2ME focando principalmente nos aspectos e bibliotecas de segurança.

4.3.3.1 J2ME

O J2ME é a versão da plataforma Java desenvolvida para rodar em dispositivos que dispõem de recursos limitados como o tamanho de tela, armazenamento, processamento entre outras limitações. Busca manter o mesmo padrão aplicado nas outras versões do Java, como orientação a objetos e portabilidade.

A portabilidade pode ser alcançada com a utilização da máquina virtual, chamada de *Kilobyte Virtual Machine* (KVM) que tem o mesmo funcionamento das máquinas mais robustas, mas com recursos limitados e sendo desenvolvidas para configurações especificas (SILVA, 2005).

Com uma quantidade enorme de dispositivos e configurações diferentes, o J2ME define perfis (*profiles*), configurações (*configurations*) e APIs de forma a disponibilizar um ambiente completo de execução compatível com a maioria dos dispositivos disponíveis no mercado atual (MONTEIRO, 2006).

4.3.3.1.1 Configurações (configurations)

Existem hoje duas configurações diferentes que fornecem serviços básicos para alguns dispositivos e são constituídas de APIs e da KVM:

a) ***Connected Device Configuration* (CDC):** destina-se à dispositivos que dispõem de conexões mais rápidas, maior capacidade de processamento e memória, conexões para transferência de dados mais estáveis e com maior largura de banda (MONTEIRO, 2006);

b) ***Connected Limited Device Configuration* (CLDC):** destinada a dispositivos caracterizados pelas restrições de memória, processamento,

largura de banda, interface com o usuário e alimentação (ALBUQUERQUE, 2002).

4.3.3.1.2 Perfil MIDP (profile)

O perfil é utilizado juntamente com a configuração para formar um ambiente Java completo. Disponibiliza serviços mais próximos do usuário, como: interface com o usuário, persistência e entrada de dados, conexões, informações dos aparelhos e aspectos de programação. Muitos aparelhos contem API,s especificas para ele em seu perfil, tornando difícil a portabilidade entre dispositivos de fabricante diferentes. Para manter a portabilidade é recomendado seguir as especificações mínimas disponibilizadas pelo MIDP 1.0 ou MIDP 2.0 (KUHNEN, 2003).

O perfil MIDP 2.0 se diferencia do MIDP 1.0 nas questões de segurança que foram reforçadas, adicionadas APIs para manipulação de som e vídeo, interface com o usuário foi melhorada, suporte a protocolos como HTTP[7] e HTTPS[8] (CARDOSO, 2007).

4.3.4 Vulnerabilidades na Camada da Aplicação

Em todos os elementos que compõe um ambiente móvel podem ser encontradas vulnerabilidades de segurança, tanto de tecnologias como de

[7] Protocolo de transferência de hipertexto, responsável pelo gerenciamento dos pedidos e respostas na WWW (W3C, 2008).
[8] Protocolo seguro de transferência de hipertexto, funciona de forma semelhante ao HTTP, mas as conexões estabelecidas são criptografadas (W3C, 2008).

desenvolvimento, estas por sua vez são as originadas por deslizes cometidos por parte dos envolvidos no processo de desenvolvimento bem como na utilização.

Entre estas vulnerabilidades podemos citar (LEE; SCHNEIDER; SCHELL, 2005):

a) **login e senha fracos:** consiste na má formação de senhas, onde uma senha forte implica em ser formada por no mínimo 8 caracteres e conter maiúsculas, minúsculas, números e caracteres especiais;
b) **permissões excessivas:** quanto menos privilégio o usuário possuir para com a aplicação, mais segura está se encontra, pois em um possível ataque utilizando as credenciais de tais usuários, estes terão dificuldade de causarem maiores danos;
c) **transferência de dados decriptados:** permite aos invasores ler e alterar dados se estes forem interceptados;
d) **login e senha incorporado ao código:** algumas aplicações permitem que as credenciais do usuário fiquem gravadas para um próximo acesso, está prática facilita que invasores analisem o código e obtenham tais credenciais;
e) **falhas de injeção:** permite que os dados informados pelos usuários façam parte de comandos internos a aplicação; entre outras.

Segundo a organização Owasp (2008) as falhas de injeção, em específico o *SQL injection* é uma das vulnerabilidades de segurança que está entre as 10 mais críticas em aplicações WEB.

Consiste na injeção de comandos SQL em campos de entrada de dados o qual não é filtrado corretamente pela aplicação, fazendo com que partes importantes e até mesmo sigilosas da aplicação e do conjunto de informações que a compõe sejam

expostas a terceiros, mesmo que tais conexões tenham sido estabelecidas por vias seguras e os dados transmitidos de forma criptografada (PESSOA, 2007).

5 TRABALHOS CORRELATOS

Neste capítulo são relacionados alguns trabalhos de pesquisas que são correlatos destes. Buscou-se resgatar pesquisas relacionadas com a essência deste trabalho, tais como, dispositivos móveis, aplicação móvel e padrões de segurança.

5.1 PROTOCOLO MOBIS: UMA SOLUÇÃO PARA O DESENVOLVIMENTO DE APLICAÇÕES SEGURAS PARA DISPOSITIVOS MÓVEIS

O artigo chamado Protocolo Mobis: Uma Solução para o Desenvolvimento de Aplicações Seguras para Dispositivos Móveis, foi apresentado por Ringel Filho et al. (2008).

Nesta pesquisa foi verificado que com a grande evolução dos dispositivos móveis com acesso as redes sem fio e a facilidade de se disponibilizar dados nesse meio, surgem novos desafios, como a segurança.

A solução proposta é o desenvolvimento de aplicações utilizando o protocolo, chamado MobiS, que garante a segurança em transmissões de dados utilizando as redes *Wireless.* O protocolo WEP empregado nas redes sem fio 802.11b oferece um esquema forte de segurança, com isso serviu de base para o desenvolvimento deste novo protocolo.

5.2 ANÁLISE DAS VULNERABILIDADES DE SEGURANÇA EXISTENTES NAS REDES LOCAIS SEM FIO: UM ESTUDO DE CASO DO PROJETO WLACA

O artigo chamado Análise das vulnerabilidades de segurança existentes nas redes locais sem fio: um estudo de caso do projeto wlaca, foi apresentado por Coutinho et al. (2005).

Eles analisaram as falhas de segurança das redes sem fio, bem como as ferramentas que exploram essas falhas, e desenvolveram uma fonte de pesquisa.

5.3 UTILIZAÇÃO DOS REQUISITOS OBRIGATÓRIOS DE SEGURANÇA, CONTEÚDO E FUNCIONALIDADES NO REGISTRO ELETRÔNICO EM SAÚDE DA UNIDADE DE TERAPIA INTENSIVA DO HOSPITAL REGIONAL DE ARARANGUÁ

O Trabalho de Conclusão de Curso Utilização dos Requisitos Obrigatórios de Segurança, Conteúdo e Funcionalidades no Sistema de Registro Eletrônico em Saúde (RES) da Unidade de Terapia Intensiva do Hospital Regional de Araranguá, apresentado por Machado (2007) na UNESC, analisa-se a compatibilidade do sistema UTInfo com o manual de requisitos de segurança, conteúdo e funcionalidades para certificação de sistemas de RES.

Entre estes requisitos tem-se itens específicos para a segurança e com a análise feita obteve-se algumas sugestões para adequação do software aos requisitos impostos.

5.4 CONSIDERAÇÕES DE SEGURANÇA NO USO DE PDA COMO TERMINAIS MÓVEIS PARA APLICAÇÕES CONFIDENCIAIS E DE ACESSO RESERVADO

O artigo Considerações de segurança no uso de PDA como terminais móveis para aplicações confidenciais e de acesso reservado submetido ao Spring 2002 por Duartenn (2008) refere-se ao uso dos dispositivos móveis (PDA), e o risco que está abertura pode oferecer.

Diz ainda que, os PDA e as redes móveis as quais esses se conectam estão longe de oferecerem um grau de segurança satisfatório o qual possibilita a utilização deste com segurança. Ressalta ainda que as aplicações de um modo geral estão preparadas para serem utilizadas em ambientes fechados, com isso não possuem infra-estrutura necessária para utilização em ambiente móveis.

O intuito desta pesquisa foi apontar as vulnerabilidades encontradas nestes ambientes, bem como formas de utilização segura destas tecnologias.

6 TRABALHO DESENVOLVIDO

Esta pesquisa busca aperfeiçoar a segurança na transmissão de dados pelas redes sem fio *com a* utilização de aplicações móveis, fazendo isso por meio de um modelo de recomendações que aborda os mecanismos de segurança do padrão das redes sem fio, as falhas de protocolos como WEP, WPA e WPA2 e as ferramentas que exploram tais falhas.

Analisando as vulnerabilidades nas transações entre DM e servidor de informações para a aplicação móvel, o modelo de recomendações busca por meio da junção dos mecanismos de segurança das redes sem fio, os mecanismos e bibliotecas de segurança da tecnologia J2ME, bem como os mecanismos de segurança dos DM garantir em todos os níveis a integridade das informações utilizadas pelas aplicações móveis.

Para realização de testes e a validação das recomendações propostas, foi feito um estudo de caso utilizando a aplicação móvel - mUTInfo 2.0 [9] - para acesso à base de dados do Sistema de Registro Eletrônico em Saúde para UTI - UTInfo 2.0 [10].

6.1 METODOLOGIA

Para atingir os objetivos propostos foi necessário, inicialmente um levantamento das tecnologias utilizadas, com o intuito de identificar vulnerabilidades inerentes a cada uma delas e quais aspectos de segurança estas disponibilizam para corrigir tais deficiências. Houve também a necessidade de se comparar os equipamentos

[9] O sistema mUTInfo 2.0, em sua atual versão, está disponibilizado apenas para consultas à base de dados do sistema UTInfo 2.0, sendo vetada a inserção de novos registros.
[10] Os sistemas UTInfo e mUTInfo são desenvolvidos pelo Grupo de Pesquisa Informática Médica e Telemedicina - Kiron - da Unesc.

utilizados nos ambientes móveis, a fim de comparar quais aspectos de segurança cada um deles trata.

Além disso foram efetuados testes na aplicação móvel desenvolvida para acessar as informações do UTInfo 2.0, com o intuito de analisar as vulnerabilidades abordadas na fundamentação teórica, e verificar se este possui métodos que abrangem estas falhas e com isso disponibilizar algumas sugestões de alterações.

Segue uma relação mais detalhada da metodologia utilizada para realização desta pesquisa:

a) realizar levantamento bibliográfico;
b) compreender os meios de conexão com a Internet nos dispositivos móveis;
c) compreender as técnicas de segurança nas conexões utilizadas;
d) compreender as vulnerabilidades existentes nas redes wireless;
e) compreender a tecnologia J2ME;
f) elaborar um modelo de recomendações para desenvolvimento de aplicações móveis seguras;
g) verificar as recomendações abordadas;
h) realizar testes;
i) validar o estudo proposto.

6.2 CENÁRIOS E RECOMENDAÇÕES PROPOSTAS

Um cenário é formado por um ou mais itens do ambiente móvel analisado, que podem ser compostos de: dispositivos móveis, Access Point, aplicação móvel e pela união de alguns destes cenários. A estrutura de cenários foi utilizada para ilustrar quais

as situações que podem ocorrer e quais os aspectos de segurança devem ser tratados em cada uma destas situações, bem como quais equipamentos podem ser utilizados. Importante ressaltar que os valores dos equipamentos foram baseados em uma média do mercado atual, podendo se diferenciar para mais ou para menos.

6.2.1 Cenário A

Atualmente existem diversos equipamentos que fazem parte deste cenário, sendo essencial a disponibilização de alguns parâmetros que direcionem a escolha do DM que se adéqüe às necessidades dos usuários.

No Capítulo 4 foram apresentados alguns mecanismos de segurança que são essenciais na avaliação de DM e para validação destes, foram analisados alguns *smartphones* disponíveis no mercado atual, sendo escolhidos por marca e funcionalidades.

A Figura 10 apresenta os DM com Wi-Fi que foram analisados.

Figura 10: Cenário A

A Tabela 4 apresenta o resultado da análise feita em dispositivos que possuem conexão Wi-Fi, visando identificar os mecanismos que oferecem segurança, bem como, as características gerais e ressaltar dentre estas as que podem auxiliar no processo de aquisição de segurança.

Tabela 4: Configuração de segurança dos dispositivos móveis com Wi-Fi

Configuração	**E61**	**S620 EXCALIBUR**	**Check Mate**
Solicitação do código PIN	Possui	Possui	Possui
Código de travamento	Possui	Possui	Possui
Bloquear SIM diferente	Possui	Não	Não
Travamento remoto	Possui	Não	Não
Certificados	Possui	Possui	Possui
Sistema Operacional	Symbian OS 9.1	Windows Mobile 5.0	Windows Mobile 5.0
Processador	TI OMAP 235 MHz	TI OMAP 200 MHz	TI OMAP 850 201 MHz
Memória (MB)	64	64	64
Tela	5,9 x 4,5 cm	5,1 x 3,8 cm	41 x 54 mm
Programação	Java MIDP 2.0, Symbian	Java MIDP 2.0	Java MIDP 2.0
Conexão	GSM/EDGE, Wi-Fi, Bluetooth, USB	GSM/EDGE, Wi-Fi, Bluetooth, USB	GSM/EDGE/GPRS, Wi-Fi, IrDA, USB, Bluetooth
Bateria	1500 mAh 715 minutos	960 mAh 475 minutos	1250 mAh 240 minutos
Peso	147 g	130 g	149 g
Fabricante	Nokia	HTC	Elef
Custo[11]	R$ 600,00	R$ 1.054,00	R$ 1.600,00

[11] Preços adquiridos em (http://info.abril.com.br/). Acesso em: 12 nov. 2008

Mesmo não sendo o foco desta pesquisa, optou-se por analisar também os dispositivos que não possuem conexão Wi-Fi, a fim de relacionar quais poderiam ser usados em casos específicos.

A Figura 11 apresenta os DM que não possuem Wi-Fi e foram analisados.

Figura 11: Dispositivos sem Wi-Fi

A Tabela 5 apresenta o resultado da análise feita com estes, visando relacionar os mecanismos de segurança bem como as configurações gerais.

Tabela 5: Configuração de segurança dos dispositivos móveis sem Wi-Fi

Configuração	**A1200i**	**N73**	**SGH-I321N**
Solicitação do código PIN	Possui	Possui	Possui
Código de travamento	Possui	Possui	Possui
Bloquear SIM diferente	Não	Possui	Não
Travamento remoto	Não	Possui	Não
Certificados	Possui	Possui	Possui
Sistema Operacional	Linux	Symbian S60 3.0	Windows Móbile 5.0
Processador	XScale 312 MHz	TI OMAP 200 MHz	XScale 416 MHz
Memória (MB)	8	42	64
Tela	4.0 x 5.0 cm	240 x 320 pixel	4.9 x 3.5 cm
Programação	Java MIDP 2.0	Java MIDP 2.0, Symbian	Java MIDP 2.0
Conexão	GSM/EDGE, Bluetooth, USB	GSM/EDGE/GPRS, Bluetooth, USB	GSM/EDGE, Bluetooth, USB
Bateria	850 mAh 200h Stand-by 4h Ligação	960 mAh 300h Stand-by 6h Ligação	800 mAh 250h Stand-by 5h Ligação
Peso	122 g	100 g	101 g
Fabricante	Motorola	Nokia	Samsung
Custo[12]	R$ 549,00	R$ 600,00	R$ 680,00

[12] Preços adquiridos em (http://info.abril.com.br/). Acesso em: 12 nov. 2008

6.2.1.1 Comentários sobre a Avaliação

Mecanismos como Solicitação de Código PIN e Código de Travamento podem se tornar complicados para alguns usuários, pois implicam na digitação de uma seqüência de dígitos para que o equipamento seja liberado para uso.

O mecanismo de Bloquear SIM diferente tem grande contribuição no quesito segurança, pois impede que o dispositivo seja ligado com um SIM CARD não configurado no mesmo, mas em relação aos aparelhos analisados apenas os modelos da *Nokia* apresentaram está funcionalidade.

Já a opção de travamento remota pode ser considerada interessante, mas se o DM for extraviado e o SIM CARD for substituído não terá efeito algum, mas apenas os dispositivos da *Nokia* oferecem está solução, os demais modelos devem ser verificados com a operadora.

Os certificados digitais podem auxiliar em tarefas de autenticação em servidores, e possibilitam que sistemas desenvolvidos possam fazer uso destes para muitos fins.

O dispositivo A1200i da Motorola possui um item de segurança que não foi encontrado nos demais aparelhos analisados, o qual permite que este seja bloqueado e seu desbloqueio só será possível com uma frase-senha de impressão de voz. Itens deste gênero aumentam consideravelmente a segurança dos dispositivos, pois não depende de algo que o usuário saiba ou possua fisicamente, mas sim dele próprio dificultando possíveis fraudes contra este método de autenticação.

Neste cenário todos estes aspectos podem ser utilizados em conjunto, pois um não interfere no funcionamento do outro sendo que funcionam em camadas diferentes o que não dificulta a utilização dos DM.

Importante salientar que para o ambiente analisado é imprescindível que os dispositivos utilizados possuam conexão Wi-Fi, para usufruir da segurança oferecida por está tecnologia. Os acessos às informações podem ocorrer com a utilização de qualquer dispositivo que possua acesso a internet, independente da tecnologia utilizada, mas para garantir a integridade das informações transmitidas é necessário que as demais camadas do ambiente implementem mecanismo forte de segurança.

Configurações como processador e memória estão relacionados com os mecanismos de segurança implementados na aplicação móvel, ou seja, quanto mais robusto for o *hardware* deste equipamento, melhores soluções podem ser desenvolvidas e/ou aprimoradas, assim como algoritmos de criptografia mais eficientes.

6.2.2 Cenário B

Constituído apenas do *Access Point*, pode ser definido como um dos cenários mais importantes, pois este equipamento é responsável por todas as configurações de segurança que podem ser encontrada nas redes sem fio, é nele que são definidos quais protocolos vão ser utilizados na transferência de dados, bem como a definição das chaves criptográficas utilizadas. Os equipamentos que fazem parte do cenário B são apresentados na Figura 12.

Figura 12: Cenário B

Ultimamente têm surgido vários equipamentos englobando tecnologias diferentes, sendo assim é essencial desenvolvimento de um guia que auxilie os usuários na escolha de aparelhos que mais se possa adequar a suas necessidades.

Para a análise do conjunto ínfimo dos aspectos de segurança levantados no Capítulo 4, foram analisados vários equipamentos disponíveis no mercado atual e os resultados poderão ser visualizados na Tabela 6.

Tabela 6: Configurações de segurança dos Access Point

Equipamentos / Configuração	DWLG700 AP	WRT54 GLA	SE361 WLAN	TLWR 542G	WAP0003	3CRWE454G75
SSID Disable	Sim	Sim	-	Sim	Sim	Sim
Endereço MAC	Sim	Sim	-	Sim	Sim	Sim
WEP	64/128 Bits (RC4)	Sim	64/128 Bits	64/128/152 bits	64/128 bits	40/64/128 bits
WPA	Sim	Sim	Sim	Sim	Sim	Sim
WPA2	Não	Não	Sim	Sim	Não	Sim
Padrão	802.11b 802.11g	802.11b 802.11g	802.11b 802.11g	802.11b 802.11g	802.11b 802.11g	802.11b 802.11g
Velocidade	54 Mbps	54 Mbps	54 Mbps	54 Mbps	108 Mbps	54 Mbps
Alcance	Até 400 m	Até 100 m	Até 300 m	Até 830 m	-	Até 100 m
Fabricante	D-Link	Linksys	GigaSet	TP Link	LevelOne	3COM
Custo[13]	R$ 190,00	R$ 370,00	R$ 160,00	R$ 330,00	R$ 215,00	R$ 350,00

6.2.2.1 Comentários sobre a Análise

Na Tabela 6 foram relacionados os aspectos julgados como sendo imprescindíveis para utilização segura destes equipamentos, nota-se na análise que grande parte das diferenças está relacionada com a distância atingida pelo sinal, mas no quesito segurança, todos compreenderam os requisitos mínimos que são: SSID *Disable*, Endereço MAC, WEP e WPA, já outros apresentam algoritmos mais robustos e chaves

[13] Preços adquiridos em (www.submarino.com.br). Acesso em: 12 nov. 2008

criptográficas maiores o que resultam em maior confiabilidade para com o aparelho, já o preço oscila entre modelos e fabricantes, não se diferenciando muito pela configuração destes.

No decorrer da pesquisa foi verificado que mecanismos considerados simples podem se tornar um incômodo para usuários e administradores, assim como o SSID *Disable* Function que inibe o nome da rede, ou seja, o Access Point não a envia em *broadcast*, fazendo com que usuários que necessitam se conectar a está rede devem saber de antemão o nome desta.

Outro aspecto que dificulta as atividades desempenhadas pelos administradores de redes é a restrição por endereço MAC, onde apenas aparelhos identificados no *Access Point* podem se conectar a rede, com isso cada equipamento a ser utilizado deve ser registrado. Os aspectos de criptografia são os que garantem maior segurança nas conexões e podem ser utilizados em conjunto.

Grande parte dos *Access Points* disponíveis no mercado atual possibilitam restringir o acesso a rede por uma série de configurações. Para ampliar a segurança das redes sem fio é importante configurar estes dispositivos a não permitirem acesso por tecnologias que não oferecem tanta segurança, como é o caso do 802.11b, que é mais lento que o 802.11g e não implementa as mesmas técnicas de segurança.

Em relação ao tamanho das chaves no WEP, quanto maior mais segura já que ao utilizar uma chave de 128 bits dificultará a invasão, mas dependendo do tempo desprendido por parte do invasor, poderá ser quebrada.

Foram comparadas outras especificações dos equipamentos que não possuem elo direto com os aspectos de segurança, com o intuito de prover um resultado mais abrangente.

6.2.3 Cenário C

Este cenário é formado apenas da aplicação móvel, para a constituição deste foram analisados os aspectos de segurança inerentes à lógica de negócio, que trata especificamente da segurança na manipulação dos dados. Este cenário possui muitos mecanismos para prover segurança para a aplicação, e pode ser considerado um dos cenários mais flexíveis, pois pode ser adaptado para suprir as vulnerabilidades encontradas no decorrer do desenvolvimento, bem como depois que a aplicação já estiver concluída. A Figura 13 demonstra este cenário.

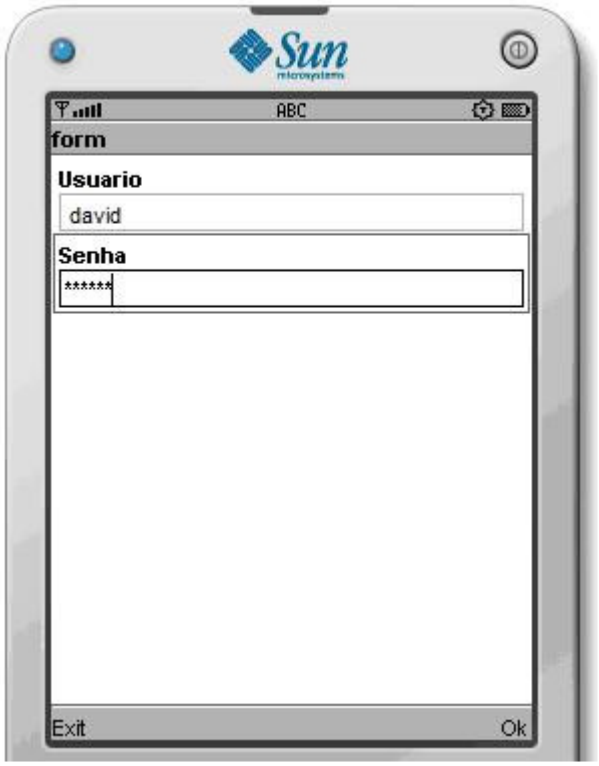

Figura 13. Cenário C
Fonte: Kiron (2008)

Os aspectos de segurança inerentes as aplicações móveis foram relacionados no Capítulo 4, mas foi feita uma análise com o intuito de identificar alguns dos métodos mais eficientes que contribuem para a segurança, bem como sua relação com os

usuários finais. Importante salientar que existem diversos métodos de segurança que não foram abordados nesta análise, pois foi dado foco nos métodos possíveis de implementar nas aplicações móveis e o objetivo desta pesquisa não é esgotar todas as fontes de segurança aplicadas às tecnologias abordadas aqui.

De acordo com os mecanismos identificados no Capítulo 4 seguem:

a) **destruição de dados:** pode ser considerado importante, mas sua implementação é complicada, pois se torna difícil definir em quais casos este deve entrar em funcionamento, por exemplo, se o sistema estiver configurado para se autodestruir ao ser negado por mais de 3 vezes o binômio *login* e senha e o usuário por qualquer motivo o fazer, o sistema deverá ser reinstalado no DM. Já em casos de extravio do equipamento sua utilização é indispensável, pois permite que na próxima conexão ao servidor, após a identificação que o DM foi extraviado, desencadeie funções na aplicação móvel capaz de eliminar quaisquer vestígios de conexão e informações armazenadas nos equipamentos;

b) **criptografia e injeção de SQL:** a implementação destes dois aspectos de segurança são incontestáveis, pois permite diminuir consideravelmente as vulnerabilidades das aplicações móveis mantendo transparência total com os usuários;

c) **autenticação:** é um mecanismo altamente confiável para as aplicações móveis, mas devem ser desenvolvidas corretamente e obedecer a uma política de senha, ou seja, deve solicitar uma nova senha em um curto período de tempo, não permitir senhas simples e estar relacionada a configurações de privilégios na aplicação e banco de dados.

d) **assinatura digital:** pode ser utilizada tanto para permitir que o servidor identifique a autenticidade do usuário que está se conectando no mesmo, e pode ser utilizada também como uma forma de autenticação na própria aplicação, substituindo a autenticação convencional.

Com está análise foi possível definir que a aplicação é a camada mais simples de se prover segurança, pois como é de fácil implementação, pode-se utilizar vários métodos incluindo métodos próprios e métodos já consolidados para prover mecanismos de segurança mais eficientes, atribuindo assim mais qualidade a aplicação.

O desenvolvimento de um algoritmo próprio de criptografia, por exemplo, pode se tornar interessante, pois é um código totalmente novo e proprietário, sendo que somente o responsável pela aplicação terá conhecimento do seu funcionamento, mas por outro lado a utilização de algoritmos já apresentados publicamente se torna mais confiável, pois a possibilidade de existir vulnerabilidades é bem menor, sendo que ele já foi testado várias vezes e por diversos usuários e o fato de ele ser livre não implica que outra pessoa poderá ler seus dados, pois algoritmos desse tipo utilizam chaves públicas e privadas para cifrar as mensagens.

Em termos gerais pode-se afirmar que todos estes aspectos são possíveis de se implementar, e se planejados com cuidado garantirão maior segurança para as aplicações, importante salientar que o ponto C identificado na Figura 1 em muitos casos podem ser uma das ameaças mais críticas, sendo que alguns usuários podem oferecer resistência em aspectos relacionados a política de senha, mas está não deve ser ignorada, fazendo com que os usuário se adaptem a política imposta.

6.2.4 Cenário D

Este cenário é formado pela união dos cenários A e B e trata de aspectos de segurança relevantes a utilização de DM junto as redes sem fio *wireless*. A análise da união de cenários se fez necessária para permitir propor recomendações que além de prover segurança, consiga relacioná-la com a sua utilização no dia-a-dia evitando a utilização errônea de vários métodos dificultando a utilização das tecnologias envolvidas. A Figura 14 ilustra o cenário D.

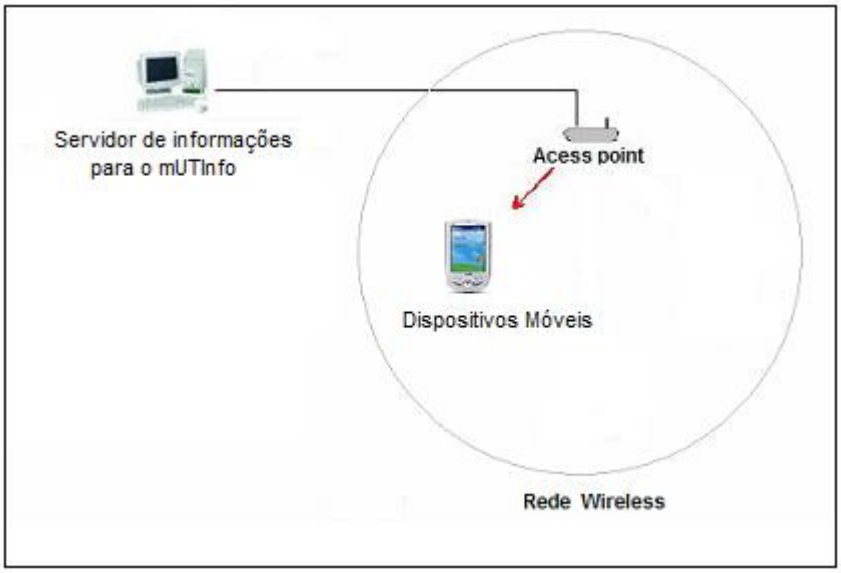

Figura 14: Cenário D
Adaptado de TISAFE. (2008)

Com está análise foi possível identificar que os aspectos de segurança inerentes aos dispositivos móveis são aplicados, em sua maioria, no momento de inicialização destes e os aspectos relacionados com a sua autenticação junto à rede, ocorre no momento que a conexão é efetuada, sendo assim os dois não se conflitam, pois incidem em momentos diferentes.

6.3 ESTUDO DE CASO

O estudo de caso visa identificar, na aplicação móvel desenvolvida para acesso às informações do S-RES UTInfo 2.0, no DM Nokia E61 e no *Access Point* WRT54G-LA da LinkSys, as vulnerabilidades abordadas nesta pesquisa, bem como os aspectos de segurança relacionados às aplicações móveis e sugerir modificações para que estes passem a prover maior segurança na transferência e processamento dos dados.

6.3.1 Metodologia

Para realização do estudo de caso foi analisado na aplicação móvel os itens que são julgados importantes no gerenciamento de riscos, que são:

a) **Utilidade da informação:** as informações manipuladas neste sistema, são útil para o correto funcionamento e andamento de processos clínicos, tal que, informações incompletas ou erradas podem comprometer a vida de um paciente;

b) **Validade da informação**: as informações inerentes ao prontuário médico possuem validade indeterminada, pois tratam especificamente da saúde de um paciente e informações colhidas hoje, podem ser usadas muitos anos depois para fins de comparação;

c) **Valor da informação**: no Capítulo 3 que trata sobre segurança das informações no S-RES, foram abordadas questões que tratam dos aspectos legais das informações manipuladas por sistemas desta índole. Vale lembrar que tais informações possuem um valor inestimável, pois

envolvem a privacidade dos indivíduos e sua utilização e/ou disponibilização inadequada pode ir contra a moral destes.

Baseando-se nesta análise, afirma-se que sistemas de atenção à saúde, em específico o S-RES UTInfo 2.0, devem implementar mecanismos de segurança capazes de garantir a confiabilidade e a integridade das informações. Investimentos em capacitação de profissionais, bem como, aquisição de *hardwares* e *softwares* específicos para o aumento da segurança são requeridos.

O estudo de caso busca identificar se o sistema analisado está em conformidade com as recomendações propostas disponibilizadas nesta pesquisa.

6.3.2 Análise do Dispositivo Móvel

O item Solicitação do código PIN, que diz respeito ao controle de acesso ao DM por meio da digitação de uma seqüência de caracteres não foi atendido pelo dispositivo utilizado para acessar a aplicação móvel, pois o mesmo não solicita o código PIN ao ligar o aparelho e este ainda é o PIN original.

Para que este mecanismo de segurança seja compreendido, deve-se alterar as configurações originais do aparelho modificando o código PIN deste, e habilitar a opção que obriga a digitação do código para que este seja iniciado, vale lembra que está senha deve estar relacionada a uma política de senha sendo alterada ao decorrer do tempo.

O dispositivo utilizado também não contemplou o item de segurança Código de travamento, sendo que indiferente do tempo que o equipamento ficar sem uso este estará sempre habilitado, o que pode implicar em acessos indevidos, devido a possibilidades de roubo, extravio, entre outros.

Deve-se alterar o código de Travamento padrão também seguindo uma política de senha, a escolha deste é mais flexível já que suporta até 255 caracteres.

A função de Bloquear SIM diferente oferecida pelo dispositivo móvel utilizado não está configurada para utilização, possibilitando assim que qualquer SIM CARD inserido no dispositivo seja reconhecido.

Sugere-se configurar o aparelho corretamente a fim de permitir que seja aceito somente o SIM CARD de usuários que tenham permissões para utilizar a aplicação móvel.

A opção de Travamento remoto só foi encontrada nos dispositivos de marca *Nokia*, e o que está sendo utilizado não foi configurado para permitir o travamento remoto.

Sugere-se configurar uma mensagem de travamento remoto no aparelho, possibilitando assim um travamento imediato se este for extraviado, importante ressaltar que algumas operadoras oferecem este serviço.

Todos os aparelhos analisados oferecem a lista de certificado pessoal, e o utilizado no acesso a aplicação móvel esta incluído nesta lista.

Este item está sendo usado corretamente pelo sistema, já que este faz uso dos certificados pessoais para realização da conexão HTTP com SSL. Com o estabelecimento de conexões seguras para a transferência de dados entre o cliente e o servidor, já atende o requisito obrigatório RSEGM7 dos requisitos de segurança NGS1 que são estipulados pelo SBIS-CFM para certificação de software na área da saúde.

6.3.4 Análise do Access Point

O item de segurança SSID *Disable*, que diz respeito ao não envio em *broadcast* da identificação da rede é suportado pelo *Access Point* utilizado pelo *Kiron* para disponibilizar o acesso à rede sem fio, mas este mecanismo de segurança não é utilizado.

Sugere-se configurar o equipamento de modo que, para um cliente se conectar seja preciso informar o nome da rede. Está técnica não agrega muita segurança ao meio, mas dificulta a ação de possíveis invasores.

Todos os *Access Point* relacionados no cenário B, possuem está característica, que permite restringir o acesso a rede apenas a dispositivos previamente cadastrados no *Access Point*, está técnica é denominada restrição por Endereço MAC.

O equipamento empregado no Kiron faz uso deste mecanismo, restringindo assim de forma simples o acesso a rede. Este mecanismo não acrescenta muita segurança às redes, já que existem *softwares* que capturam o endereço MAC de máquinas conectadas para posteriormente emular estes endereços em outras máquinas fazendo se passar por um dispositivo registrado no *Access Point*.

A opção de criptografia WEP, não está sendo utilizada pelo *Access Point* empregado na rede do Kiron, mas devido as problemas que envolvem está técnica, sua utilização é desnecessária, pois existem outros algoritmos de criptografia mais eficientes.

O mecanismo de segurança WPA, que foi criado especificamente para suprir as falhas encontradas no WEP, está sendo utilizado pelo *Access Point* que disponibiliza acesso sem fio a rede do Kiron.

O WPA2, que é uma versão melhorada do WPA não é suportado pelo A*ccess Point* utilizado pelo Kiron, sugere-se adquirir um *Access Point* compatível com está tecnologia com o intuito de maximizar a segurança deste ponto de acesso.

6.3.5 Análise de Aplicação

A autenticação e controle de acesso à aplicação é um requisito de segurança exigido pelo SBIS-CFM o qual deve ser contemplado para que *softwares* na área da saúde possam ser certificados. A aplicação móvel para acesso às informações do S-RES UTInfo 2.0 contemplou parcialmente este aspecto de segurança, já que restringe o acesso apenas a usuários cadastrados na base de dados, mas mostrou deficiência na política de senha, pois não são estipulados prazos para que está expire e nem são exigidos padrões de senha no momento de criação destas.

Sugere-se seguir um padrão no momento de concepção das senhas, possibilitando assim agregar um pouco mais de segurança a está técnica simples que é a autenticação. Um padrão que pode ser empregado é impor que as senhas geradas ou informadas pelos usuários devam possuir ao mínimo quatro itens diferentes, como por exemplo, utilizar caracteres maiúsculos e minúsculos, utilizar números e caracteres especiais.

A criptografia é uma técnica de segurança muito utilizada e que possibilita agregar segurança as aplicações que a utilizam, este item foi contemplado pela aplicação móvel desenvolvida para DM, pois utiliza o algoritmo SHA-1 para criptografar todos os dados que são compartilhados entre cliente e servidor.

Mesmo contemplando este item, sugere-se que sejam efetuados testes utilizando o algoritmo de criptografia SHA-2 a fim de verificar se é possível

implementá-lo e utilizá-lo no DM. O SHA-2 além de oferecer maior segurança que o SHA-1 devido ao tamanho da chave que pode chegar a 512 bits, ate a conclusão desta pesquisa não se obteve relatos de quebras o envolvendo.

A utilização da assinatura digital no ambiente médico possibilita substituir os prontuários em papel pelo prontuário eletrônico, pois os cadastros efetuados podem ser assinados pelos médicos, com a mesma validade que era assinado quando em papel. A aplicação móvel mUTInfo 2.0, de aceso às informações do S-RES, contempla este item parcialmente, já que utiliza o certificado digital para estabelecer a conexão HTTP com SSL.

Mesmo que esteja disponibilizando para a aplicação móvel apenas consulta à base de dados do S-RES UTInfo 2.0, sugere-se que sejam efetuados testes com o intuito de utilizar os certificados digitais homologados, neste caso a infra-estrutura de Chaves Públicas Brasileira – ICP Brasil, que dá validade aos documentos eletrônicos no País, a fim de agregar segurança a autenticação convencional utilizada hoje, e em uma próxima versão possibilitar a inserção de dados que sejam assinados com a utilização do certificado digital.

O problema de injeção de SQL o qual possibilita que dados sigilosos do banco de dados sejam revelados a terceiros, está sendo tratado no servidor o qual disponibiliza os dados para a aplicação móvel utilizada nos DM. O tratamento ocorre pela utilização do *framework Hibernate* que ao utilizar a API *PreparedStatement* elimina tais vulnerabilidades.

A destruição de dados não é contemplada pela aplicação móvel desenvolvida para DM. Sua implementação na aplicação disponível hoje não é necessária já que os dados consultados são apagados assim que a aplicação seja fechada e/ou ficar sem utilização por um curto período de tempo, o qual pode ser configurado.

CONCLUSÃO

A segurança em aplicações móveis e aspectos relacionados com a utilização de DM e das redes W*ireless* são fundamentais para prover segurança em vários níveis tais como nível lógico que envolve os dados manipulados e nível físico que envolve os equipamentos utilizados.

Foram analisados aspectos de segurança relacionados às tecnologias utilizadas no S-RES UTInfo 2.0 bem como na aplicação mUTInfo 2.0 de acesso às informações do S-RES por meio de DM.

A partir do estudo de caso abordado e, de acordo com as recomendações propostas e dos aspectos de segurança envolvendo os DM, foram identificadas vulnerabilidades e classificadas em conjuntos: DM, *Access Point*, aplicação móvel e usuário.

A aplicação móvel mUTInfo 2.0 para acesso às informações do S-RES, requer adequações para oferecer maior segurança. Algumas soluções foram propostas no estudo de caso e nas recomendações de cada cenário. Importante salientar que se as recomendações propostas forem seguidas, grande parte dos requisitos dos Níveis de Garantia de Segurança 1 e 2 do Manual de Certificação para Sistemas de Registro Eletrônico em Saúde (S-RES) SBIS-CFM serão contemplados.

Os itens analisados oferecem vários mecanismos de segurança, possibilitando assim, a implementação de soluções eficientes que ofereçam mais confiabilidade prover integridade às informações manipuladas.

Sugerem-se, para trabalhos futuros, as seguintes abordagens: analisar o desempenho do DM com a utilização de WEP, WEP2; analisar o desempenho dos DM com a utilização de algoritmos mais complexos de criptografia; possibilitar a utilização de certificados para autenticação em servidor RADIUS utilizando DM; implementar o

uso de XML assinado; identificar o ponto de acesso em que se está conectado e definir quais mecanismos de segurança serão utilizados; analisar aspectos de segurança nas demais tecnologias de conexão, como, GSM, GPRS, EDGE, IrDA, *Bluetooth*, entre outras; implementar autenticação da aplicação móvel no servidor por meio do certificado digital disponível nos DM; analisar aspectos relacionados à destruição de dados na aplicação móvel.

REFERÊNCIAS

AGUIAR, P. A. F. **Segurança em Redes Wi-Fi.** 2005. 79 f. Projeto de Conclusão de Curso (Bacharel) - Curso de Sistemas de Informação, Departamento de Ciências da Computação, Universidade Estadual de Montes Claros, Montes Claros, 2005.

ALBUQUERQUE, R. L. **Kagent:** Uma API Java para Agentes Inteligentes em Dispositivos Móveis. 2002. 146 f. Dissertação (Mestre) - Curso de Ciência da Computação, UFPE, Recife, 2002.

BATISTA, C. F. A. **Métricas de segurança de software.** 2007. 103 f. Dissertação (Pós-graduação) - Departamento de Informática, Puc, Rio de Janeiro, 2007.

BEAVER, K.; DAVIS, P. T.. **Hacking Wireless Networks For Dummies.** River Street: Wiley Publishing, Inc., 2005. 387 p.

BURNETT, S.; PAINE, S. **Criptografia e segurança:** O guia oficial RSA. 3ª ed. Rio de Janeiro: Ed. Campus, 2002.

BRASIL. **Código de Ética Médica**. Resolução CFM nº 1.246/88, Capítulo IX Artigo 108. Código de Ética Médica. 5ed. Brasília: Conselho Federal de Medicina, 2003.

CAMINHA, J. **Uma Arquitetura para autenticação de dispositivos móveis.** 2006. 101 f. Dissertação (Mestrado) - Universidade Federal de Campina Grande, Campina Grande, 2006.

CARUSO, C. A. A.; STEFFEN, F. D. **Segurança em informática e de informações.** 2. ed. São Paulo: Senac, 1999.

CARDOSO, J. **Java para Telemóveis MIDP 2.0.** Porto (Portugal): Feup, 2007. 259 p.

CARVALHO FILHO, J. R. L. **UM ESTUDO DE PROTOCOLOS EMPREGADOS NA SEGURANÇA DE DADOS EM REDES SEM FIO – PADRÃO 802.11.** 2005. 106 f. Trabalho de Conclusão de Curso (Bacharel) - Curso de Ciências da Computação, Centro Universitário de João Pessoa, João Pessoa, 2005.

DIAS, C. Segurança e Auditoria da Tecnologia da Informação. Rio de Janeiro: Axcel Books, 2000.

COSTA, C. G. A. **Desenvolvimento e Avaliação Tecnológica de um Sistema de Prontuário Eletrônico do Paciente, Baseado nos Paradigmas do World Wide Web e da Engenharia de Software.** 2001. 288 f. Dissertação (Mestrado) - Curso de Engenharia Elétrica, Departamento de Engenharia Elétrica, Unicamp, Campinas, 2001.

DUARTENN, C. J. **Considerações de segurança no uso de PDA como terminais móveis para aplicações confidenciais e de acesso reservado.** Disponível em: <http://www.juliao.org/pub/CCSW-WP-PDAS-001-A.pdf>. Acesso em: 10 nov. 2008.

DUARTE, L. O. **Análise de vulnerabilidades e ataques.** 2003. 66 f. Projeto Final de Curso (Bacharel) - Curso de Ciência da Computação, Departamento de Ciências de Computação e Estatística do Instituto de Biociências, Letras e Ciências Exatas, Universidade Estadual Paulista Júlio de Mesquita Filho, São José do Rio Preto, 2003.

FARIA, R. A. **Treinamento Avançado em XML.** São Paulo: Digerati, 2005. 128 p.

FARINAZZO, V. M. S., ALMEIDA, F. G. V. F., Aspectos Éticos e de Segurança do Prontuário do Paciente, São Paulo, 2004.

FONSECA, J. C. **Portando a KVM.** 2002. 64 f. Trabalho de Conclusão de Curso (Graduação em Ciências da Computação) – Centro de Informática, Universidade Federal de Pernambuco, Recife.

INTEGRAL SISTEMAS. (Brasil). **FAQ.** Disponível em: <http://www.embeddedworld.com.br/ex03.asp>. Acesso em: 16 jun. 2008.

FRANÇA, G. V. **Telemedicina:** Breves Considerações Ético-Legais. Disponível em: <http://www.la-plaza.com/vdc/index.php?option=com_content&task=view&id=31&Itemid=154>. Acesso em: 02 nov. 2008.

FURUIE, S. S.; REBELO, M. S.; GUTIERREZ, M. A.; MORENO, R.; MOTTA, G.; BERTOZZO, N.; NARDON, F.; FIGUEIREDO, J.; TACHINARDI, U. **Prontuário Eletrônico de Pacientes: Integrando Informações Clínicas e Imagens Médicas.** Revista Brasileira de Engenharia Biomédica, v. 19, n. 3, 2005.

HOWARD, M.; LEBLANC, D. **Writing secure code.** 2. ed. Washington: Microsoft Press, 2002.

JAVAMAN (Brasil). **Site do JavaMan.** Disponível em: <www.javaman.com.br>. Acesso em: 12 nov. 2008.

KUHNEN, A. **Protótipo de uma aplicação LBS utilizando GPS conectado em celular para consultar dados georeferenciados.** 2003. 62 f. Trabalho de Conclusão de Curso (Bacharel) - Curso de Ciência da Computação, Furb, Blumenau, 2003.

LAUREANO, M. A. P. **Gestão de Segurança da Informação.** Disponível em: <www.mlaureano.org/aulas_material/gst/apostila_versao_20.pdf>. Acesso em: 02 nov. 2008.

LEE, V.; SCHNEIDER, H.; SCHELL, R. **Aplicações móveis:** Aquitetura, projeto e desenvolvimento. São Paulo: Pearson Education do Brasil, 2005.

Soares, L. F. G.; Lemos, G.; Colcher, S. **Redes de computadores:** das LANs, MANs e WANs às Redes ATM, 2a. Edição (revisada e ampliada), Ed. Campus 1995.

LEMAY, C. **Aprenda em 21 dias Java 2.** São Paulo: Editora CAMPUS, 2005.

DUARTE, L. O. **Análise de Vulnerabilidades e Ataques Inerentes a Redes Sem Fio 802.11x.** 2003. 66 f. Trabalho de Conclusão de Curso (Bacharel) - Curso de Ciências de Computação, Departamento de Ciências de Computação e Estatística do Instituto de Biociências, Letras e Ciências Exatas, Centro Universitário de João Pessoa, São José do Rio Preto, 2003.

KIRON, Grupo de Pesquisa em Informática Médica e Telemedicina da Unesc.
Disponível em: < http://www.kiron.unesc.net >. Acesso em: 02 nov. 2008.

MACERATINI, R.; SABBATINI, R. M. E. **Telemedicina:** A Nova Revolução. Informédica 1 (6): 5-10, 1994.

MACHADO, G. B. **IMPLEMENTAÇÃO DE ASSINATURA DIGITAL NA EVOLUÇÃO MÉDICA DE PRONTUÁRIO ELETRÔNICO DO PACIENTE:** UM ESTUDO DE CASO NO HOSPITAL REGIONAL DE ARARANGUÁ. 2006. 71 f. Trabalho de Conclusão de Curso (Bacharel) - Curso de Ciência da Computação, Unesc, Criciúma, 2006.

MACHADO, S. D. **UTILIZAÇÃO DOS REQUISITOS OBRIGATÓRIOS DE SEGURANÇA, CONTEÚDO E FUNCIONALIDADES NO REGISTRO ELETRÔNICO EM SAÚDE DA UNIDADE DE TERAPIA INTENSIVA DO**

HOSPITAL REGIONAL DE ARARANGUÁ. 2007. 144 f. Trabalho de Conclusão de Curso (Bacharel) - Curso de Ciência da Computação, Departamento de Ciência da Computação, Unesc, Criciúma, 2007.

MAIA, R. F.; RODRIGUES, V. J. S.; ENDLER, M. **ORB para dispositivos móveis em redes.** 2005. 29 f. Monografia (Bacharel) - Curso de Ciência da Computação, Pontifícia Universidade Católica do Rio De Janeiro - Puc, Rio De Janeiro, 2005.

MATEUS, G. R.; LAUREIRO, A. A. F. **Introdução a computação móvel.** Disponível em: <http://www.dcc.ufmg.br/~loureiro/cm/docs/cm_livro_1e.pdf>. Acesso em: 15 jun. 2008.

MARTINS, R.; ROCHA, J.; HENRIQUES, P. **Segurança dos Web Services no Comércio Eletrônico Móvel**. Braga, 2006.

MASSAD, E.; MARIN, H. F.; AZEVEDO NETO, R. S. **O Prontuário Eletrônico do Paciente na Assistência, Informação e Conhecimento Médico**. São Paulo: H. de F. Marin, 2003.214p. Disponível em: < www.sbis.org.br/site/arquivos/prontuario.pdf > . Acesso em: 10 nov. 2008.

MCDONALD, C. J., BARNETT, G. O., Computer Applications in Health Care, Addison-Wesley Longman Publishing Co., Inc., 1990.

MEZAROBA, W. F., MENEGON, M. P., NICOLEIT, E. R. Registro Eletrônico do Paciente: Comunicação, Interação com Dispositivos Móveis e Previsão de Expansibilidade In: IV Congresso Sul Brasileiro de Computação, 2008, Criciúma. **Anais do IV Congresso Sul Brasileiro de Computação** , 2008.

MICROSOFT (Org.). **Aprimorando a segurança de dados por meio do SQL Server 2005.** Disponível em: <http://technet.microsoft.com/pt-br/library/bb735261.aspx>. Acesso em: 11 nov. 2008.

MONTEIRO, Jane Dirce Alves. **Desenvolvimento de aplicações multi-plataformas para dispositivos Móveis.** 2006. 149 f. Dissertação (Mestre) - Curso de Ciência da Computação e Matemática Computacional, USP, São Carlos, 2006.

NOKIA (Brasil). **Nokia Brasil.** Disponível em: <www.nokia.com.br>. Acesso em: 10 set. 2008.

OWASP (Org.). **Open Web Application Security Project.** Disponível em: <OWASP>. Acesso em: 11 nov. 2008.

PEREIRA JUNIOR, C. A. C. V.; BRABO, G. S.; AMORAS, R. A. S. **Segurança em redes wireless padrão ieee802.11b: protocolos wep, wpa e análise de desempenho.** 2004. 78 f. Monografia (Bacharel) - Curso de Ciência da Computação, Universidade Da Amazônia – UNAMA, Belém, 2004.

PESSOA, M. **Segurança em PHP.** São Paulo: Novatec, 2007. 152 p.

PINTO, V. B. Prontuário eletrônico do paciente: documento técnico de informação e comunicação do domínio da saúde. **Pesquisa Brasileira em Ciência da Informação e Biblioteconomia**, Rio de Janeiro, v. 1, n. 2, p.1-15, 01 jan. 2006. Disponível <http://revista.ibict.br/pbcib/index.php/pbcib/index>. Acesso em: 12 nov. 2008.

PIRES, F. A. et al, **Prontuário eletrônico:** Aspectos legais e situação atual, Artigo apresentado no O CBIS'2004 - IX Congresso Brasileiro de Informática em Saúde, São Paulo, 2004.

PITOMBEIRA, D. K. D. **Uma Arquitetura eficiente para armazenamento, gerenciamento e acesso a Dados em dispositivos móveis com recursos computacionais limitados.** 2006. 137 f. Dissertação (Mestrado) - Universidade De Fortaleza – UNIFOR, Fortaleza, 2006.

RUFINO, N. M. O. **Segurança em Redes Sem Fio.** 2. ed. São Paulo: Novatec, 2005. 224 p.

SCHMITT JUNIOR, A. J. **Protótipo de front end de controle de acesso usando J2Me.** 2004. 70 f. Trabalho de Conclusão de Curso (Bacharelado em Ciências da Computação) – Centro de Ciências Exatas e Naturais, Universidade Regional de Blumenau, Blumenau.

SITTIG, F. (1999), **Advantages of Computer-Based Medical Records.** Disponível em: http://www.informatics-review.com/thoughts/advantages.html. Acesso em: 19 outubro 2008.

SBIS; CFM. (2004), Manual de Certificação para Sistemas de Registro em Saúde. Disponível em: http://www.sbis.org.br/certificacao/Manual_Certificacao_SBIS_CFM_Fase2_v3.1_Consulta_Publica.pdf. Acesso em: 19 outubro 2008.

SILVA, R. L.. **Aplicativo para Representante comercial em dispositivo móvel (PDA) Usando a Tecnologia J2ME e Banco de Dados.** 2005. 73 f. Trabalho de Conclusão de Curso (Bacharel) - Curso de Ciência da Computação, Furb, Blumenau, 2005.

TI SAFE (Brasil). **TI Safe Segurança da Informação.** Disponível em: <www.tisafe.com>. Acesso em: 12 nov. 2008.

TIZIANO, M. G. **Análise e implementação de segurança aplicada à comunicação de mensagens de texto em telefonia móvel.** 2006. 81 f. Dissertação (Pós Graduação) - Curso de Especialização em Segurança da Informação em Redes de Computadores e Sistemas, Universidade do Oeste Paulista, Presidente Prudente, 2006.

TRANSCORTEC INDÚSTRIA E COMERCIO LTDA (Brasil). **Cabeamentos & Conexões.** Disponível em: <http://www.transcortec.com.br/info.htm>. Acesso em: 15 jun. 2008.

VOLPI, M. M. **Assinatura digital:** Aspectos Técnicos, Práticos e Legais . Rio de Janeiro: Ed Excel, 2001.

W3C. **World Wide Web Consortium.** Disponível em: <www.w3c.org>. Acesso em: 11 nov. 2008.