Utilização de Agentes em um Modelo de Autorização para Acessos a Dados Médicos em Ambiente de Computação Móvel

Erico M. H. do Amaral[1], Gerson A. Soares[2], Raul C. Nunes[1,2], Roger C. Machado[2]

[1]Curso de Ciência da Computação – Universidade Federal de Santa Maria
Av. Roraima – Bairro Camobi – Santa Maria - RS - Brasil

[2] Programa de Pós Graduação em Engenharia de Produção – Centro de Tecnologia
Universidade Federal de Santa Maria
Av. Roraima – Bairro Camobi – Santa Maria - RS - Brasil

{erico,gerson,ceretta}@inf.ufsm.br, cavilhas@gmail.com

Resumo. *A crescente disponibilização eletrônica de dados médicos salienta a necessidade de mecanismos de controle de acesso efetivos. Este artigo descreve um modelo de autorização para acesso a dados médicos utilizando agentes em um ambiente sem fio. O objeto de estudo e conseqüente proteção configura-se em um sistema de monitoramento de curvas cardíacas em pós-operatório, denominado CardioMonitor, onde questões como segurança de informações em prontuário eletrônico são essenciais.*

Abstract. *The increasing of the electronic patient data claims by effective access control mechanisms. This paper describes an authorization model that uses agents on controlling health information on wireless environment. The goal is to protect the cardiac waves collected from a net of peacemakers. The monitoring system is called CardioMonitor and it is used on post-operative step. The collected waves are saved on an electronic way and its access must be protected.*

1. Introdução

Marca-passos cardíacos são equipamentos que começam a ser utilizados em redes [HUTTEN, 1997] e [BRAECKLEIN, 2004]. Entretanto, a segurança do sistema é um desafio. Equipamentos que monitoram pacientes e coletam dados para diagnósticos necessitam dar garantias que o acesso aos equipamentos com informações do paciente (telemetria) e/ou aos seus dados somente sejam realizados por pessoal autorizado. Este artigo explora questões de autenticação no âmbito do projeto CardioMonitor [MAZZUTTI, 2003], um sistema de monitoramento de curvas cardíacas em pós-operatório.

De acordo com a Resolução 1.639 do CFM [CFM, 2002], o sistema de informações e a qualidade do serviço referente a dados de prontuário eletrônico em atividade médica deverá manter a integridade da informação para segurança dos processos de sistema. Conforme a norma ISO/IEC 15408, a integridade da informação é

obtida através do controle de vulnerabilidades, de métodos fortes de autenticação, de restrições de acesso e métodos de processamento dos sistemas operacionais.

Baseado nestas legislações, neste artigo determina-se uma política de segurança mínima capaz de abranger estes requisitos. Para tal, desenvolveu-se um modelo de autenticação que utiliza agentes e que deverá prover os níveis de segurança desejados.

O artigo está estruturado da seguinte forma: na seção 2 descreve-se o projeto CardioMonitor; na seção 3 avalia-se à tecnologia *wireless*, especificamente no que se refere às normas IEEE 802.11x e IEEE 802.15; a seção 4 avalia questões quanto à política de segurança, que servem de base para a definição do modelo de autenticação proposto; e, finalmente, na seção 5 estabelece-se as considerações finais.

2. Projeto CardioMonitor

Segundo [MAZZUTTI, 2003], o sistema de monitoramento cardíaco CardioMonitor destina-se ao monitoramento de pacientes internados em unidades de tratamento intensivo (UTI). O *software* do sistema controla os dados coletados nos equipamentos de monitoramento cardíaco e repassa esta informação à uma central, onde pode-se visualizar, processar e/ou armazenar os dados.

Os coletores de sinais são integrados a *palmtops* providos de dispositivos *bluetooth* capazes de transmitir e receber dados via ondas eletromagnéticas. Os dados coletados nos dispositivos são tratados e transformados em curvas graficamente contínuas, permitindo o acompanhamento do estado dos pacientes. Após a coleta os dados são transmitidos, via rede sem fio *bluetooth,* para uma central de monitoramento equipada com um microcomputador capaz de receber o sinal de vários emissores e mostrá-los em gráficos independentes, possibilitando assim, uma análise médica individual de cada paciente a partir desta central.

Descrição Técnica

O Sistema em análise, segundo [NUNES, 2002], consiste em um *handheld* atuando como eletrocardiógrafo e marca-passo de demanda, com transmissão *wireless* dos sinais por intermédio de uma conexão *bluetooth.* O *handheld* é ligado a um circuito para condicionamento dos sinais obtidos através de eletrodos ligados ao coração de um paciente em fase pós-operatória. O sinal amplificado é filtrado para a redução de ruídos e convertido do modo analógico para o modo digital. O sinal digitalizado é então transmitido em protocolo serial para o *handheld.* Um *software* executa no *handheld* para a exibição dos sinais cardíacos na tela do mesmo e para o controle das funções do marca-passo. Ao mesmo tempo em que isto é realizado, o sinal é transmitido pela conexão *bluetooth* para um computador central.

O Sistema funciona como uma rede de sensores monitorada local e remotamente, e é composto por nós responsáveis pelo sensoriamento e pelo envio das informações coletadas (PDA's) a um nó que agrega informações. Este nó pode ser um nó comum da rede ou um nó de maior capacidade. Em todo o caso, a informação concentra-se na direção de um ponto centralizador. Observa-se que este ponto centralizador é de fundamental importância para a segurança da rede e que a comunicação *wireless* torna-se um ponto crucial para garantir a privacidade e confidencialidade dos dados do paciente e o sigilo profissional.

3. Tecnologias de Comunicação sem fio

É necessário que se faça uma breve descrição da norma IEEE 802.15, utilizada no escopo do projeto CardioMonitor, bem como da norma IEEE 802.11x, que trata sobre redes *wireless* em geral, uma vez que a proposta apresentada neste trabalho não restringe-se apenas à comunicação entre dispositivos *bluetooth.*

A especificação de WPAN, segundo [IEEE, 2002], determina que fazem parte de uma rede pessoal sem fio todos os dispositivos capazes de se conectar entre si, utilizando dispositivos *bluetooth*, conforme preconiza a norma IEEE 802.15, onde os mesmos podem formar redes utilizando conexões através de radio freqüência, através da licença ISM (*Industrial, Scientific, Medical*), de 2.4 Ghz de banda, com modulação FM, e utilizando um esquema TDD (*Time-Division Duplex*) para emular uma transmissão *full duplex,* sobre este canal, a informação e transmitida em pacotes que são agrupados em *slots* de tempo, e cada um deles pode ser enviado em saltos de freqüência.

O padrão IEEE 802.11x é definido em 6 métodos de modulação, e as técnicas de segurança estão implementadas no padrão 802.11i. O padrão 802.11b foi o primeiro modelo amplamente aceito e utilizado em conexões *wireless,* o padrão sugerido para a aplicação no projeto é o 802.11g, aprovado em junho de 2003, que trabalha sobre uma banda de 2.4 Ghz, com o diferencial de operar a uma taxa de transmissão de até 54 Mbps. Esta taxa de transferência pode ser influenciada pela interferência de vários produtos que utilizem ondas de radio freqüência, devido à banda utilizada. O método de detecção de colisões no meio de transmissão, adotado neste padrão é conhecido como CSMA/CA que diminui a capacidade de transmissão por este canal. O padrão 802.15 oferece interferência na comunicação do padrão 802.11g, ambos adotados no escopo deste trabalho, devido a esta característica, cuidados especiais na implementação do ambiente *wireless* sobre o padrão 802.11g devem estar bem claros e definidos na especificação do projeto.

4. Modelo de Autenticação

Nesta seção descreve-se a especificação da política de segurança implementada e, com base nesta, a arquitetura sistema de autenticação.

4.1. Política de Segurança

Todo modelo de autenticação necessita de uma política de segurança. No Brasil, a norma NBR/ISO 17799 define um “código de prática” para a gestão de segurança da informação e, na área médica, o CFM regula a utilização de sistemas informatizados. Especificamente no que diz respeito a modelos de autenticação, a resolução 1.639/2002 do CFM define as "Normas Técnicas para o Uso de Sistemas Informatizados para a Guarda e Manuseio do Prontuário Médico". Quando armazenados, os sinais cardíacos coletados em equipamentos cardíacos tornam-se parte integrante do prontuário médico, logo, no âmbito do CardioMonitor, a política de segurança deve considerar tanto a norma NBR/ISO 17799 quanto a resolução 1.639/2002 do CFM.

Para atender a norma NBR/ISO 17799 e a resolução 1.639/2002 do CFM, o sistema CardioMonitor adota uma política de segurança que define um modelo de autenticação que: (1) possibilite a criação de diferentes perfis de usuários; (2) utilize mecanismos de acesso restrito e limitado a cada perfil; (3) identifique cada usuário

através de um método de autenticação seguro; e (4) possua um certificado digital que autentique a transmissão remota de dados do prontuário.

4.2. O Serviço

Para atender a política de segurança, o serviço de autenticação de acesso a dados médicos deve definir perfis de usuários e prover níveis de acesso diferenciados a cada um deles. Além disto deve definir um mecanismo simples e eficiente que habilite o acesso aos dados. A existência de um agente conectado a um servidor de autenticação é a opção adotada no CardioMonitor para prover dinamicidade ao serviço.

O agente estabelece comunicação com três repositórios mantidos pelo serviço a fim de garantir confidencialidade e integridade. Os repositórios armazenam informações especificas dos clientes que acessam a rede, tal como: a lista de clientes autorizados a conectar-se a rede, os perfis de usuário e o histórico de acesso dos clientes. Desta forma, o agente possibilita manter a integridade do perfil preestabelecido para os usuários.

O uso de agentes no modelo de serviço é um instrumento efetivo para o gerenciamento da segurança das informações e atende de forma rápida e eficiente as necessidades de um ambiente computacional sem fio, respeitando a política de segurança pré-estabelecida.

4.3. O Agente

A função do agente é monitorar requisições de acesso e detectar a conexão de dispositivos ao ambiente de rede, mantendo registros relativos às atividades realizadas por estes equipamentos.

A figura 1 ilustra o diagrama de caso de uso do serviço de autenticação por um dispositivo/usuário. Inicialmente o usuário conecta-se com o serviço de autenticação, e este tenta instalar o agente de autenticação no dispositivo (Mensagem Aut./Val.). O usuário então responde aceitando ou rejeitando a instalação do agente. Caso o usuário aceite o agente o acesso é liberado, caso contrário bloqueado.

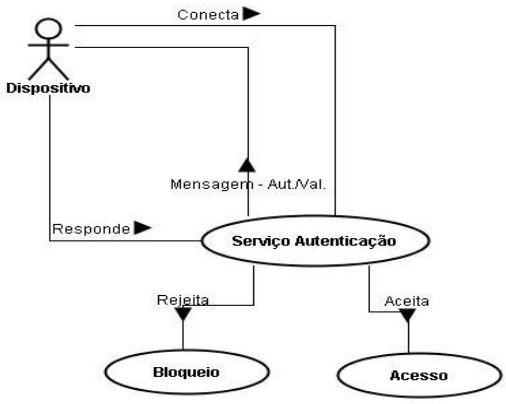

Figura 1. Diagrama Use-case

Salienta-se que para garantir integridade e confidencialidade o agente carrega a chave que possibilita o acesso. Neste processo o quesito segurança da informação é levado em consideração desde o inicio do projeto, o que garante uma facilidade maior no desenvolvimento prático do sistema proposto, permitindo que requisitos indispensáveis para a proteção das informações deste modelo não sejam omitidos.

O diagrama de seqüência descrito na figura 2 descreve as possíveis iterações de um usuário com o serviço de autenticação. Na primeira iteração o usuário aceita o agente e o acesso é liberado. Na segunda iteração o usuário rejeita a instalação do agente no dispositivo e conseqüentemente tem o acesso negado. Observa-se que sempre que um novo dispositivo efetua uma requisição de acesso, o serviço de autenticação envia um agente solicitando a habilitação do mesmo. A referência de cada dispositivo é determinada pelo seu ID, que é identificado pelo MAC *address* de sua placa de rede, ou conector *bluetooth,* em conjunto com o *login* e senha, informados pelo usuário e previamente armazenados em uma tabela. Caso o usuário do equipamento não responda ao agente, os recursos da rede não serão habilitados para este dispositivo.

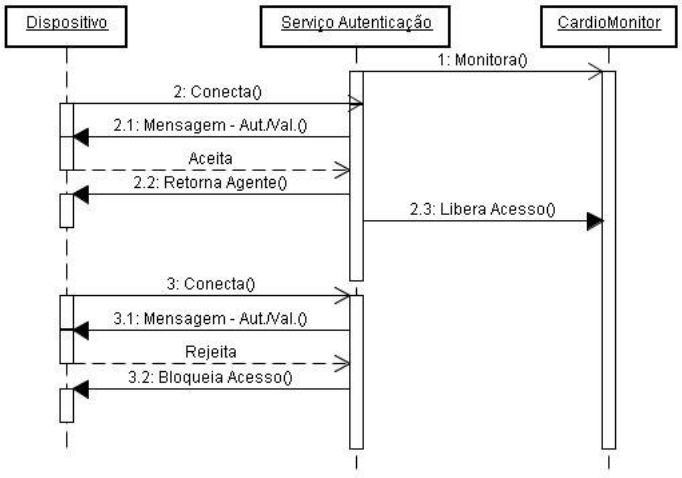

Figura 2. Diagrama de Seqüência do Sistema de Autenticação

O nível de acesso de cada usuário é determinado por um modelo de hierarquia de papéis predefinido, onde a confidencialidade aos recursos é garantida. O perfil mínimo permite ao usuário a utilização apenas de serviços como Internet, vinculados à porta 80. Isto garante a utilização do serviço por qualquer usuário que esteja no ambiente da rede e que possua um equipamento *wireless* habilitado. Desta forma, o controle de acesso à aplicação do CardioMonitor restringe-se aos usuários com nível de acesso adequado à este serviço. Todos os requisitos e regras destinados a este modelo são baseados na política de segurança previamente estabelecida.

5. Considerações Finais

Fatores importantes são considerados críticos na implantação de sistemas de segurança de informação em uma organização. Itens como política de segurança, enfoque de implementação, comprometimento, gerenciamento e treinamento são de extrema necessidade. O objetivo deste trabalho foi desenvolver uma ferramenta capaz de complementar os requisitos estabelecidos para obtenção de um ambiente seguro.

O fato do modelo proposto estar de acordo com as normas de segurança vigentes, e obedecendo os requisitos definidos pela política de segurança, o caracteriza como uma boa solução para a gestão do problema apresentado.

Referências

CFM. (2002), "Resolução 1.639/2002 do Conselho Federal de Medicina". Disponível em http://www.arnaut.eti.br/ResoCFM.htm.

IEEE 802.15. (2002), "*Standard for Information technology*" *- Telecommunications and information exchange between systems — Local and metropolitan area networks — Specific requirements.*

ISO/IEC JTC 1/SC 27. (1998), "*Glossary of IT Security Terminology. Information Technology – security techniques.*".

Mazzutti, Cristiano; Nunes, Raul Ceretta. (2003), "CardioMonitor: Ferramenta para Visualização de Curvas de Batimentos Cardíacos.**"** CRICTE, Univali, Itajaí.

NBR/ISO/IEC 17799. (2002), "Tecnologia da informação: Código de prática para a gestão da segurança da informação". Associação Brasileira de Normas Técnicas ABNT, 55pp.

Nunes, Raul Ceretta; et all. (2002), "Sistema Integrado para Aquisição, Conversão e Visualização Remota de Sinais Cardíacos Utilizando PDA's". Universidade Federal de Santa Maria, Santa Maria.

Pfleeger, Charles P.; Pfleeger, Shari L.(2003), "*Security in Computing.*" Prentice Hall: 3 ed. New Jersey.

SUN Microsystems. (2005), "*How to develop a network security policy an overview of internet working site security.***"** Disponível em http://www.sun.com/software/white-papers/wp-security-dedvsecpolicy.

Hutten, H.; Schreier, G.; Kastner, P.; Schaldach, M. (1997), "Cardiac Telemonitoring by Integrating Pacemaker telemetry within Worldwide Data Communication Systems." In Proc. of the IEEE International Conference EMBS, Chicago, Oct.30-Nov.2.

Braecklein, M.; et all. (2004), "*New System Cardiological Home Monitoring With Integrated Alarm Function.*" OpenECG Worshop, Berlin.