Computação Pervasiva Aplicada a Mecanismos de Segurança em Ambientes Computacionais Utilizando Java e Dispositivos Móveis.

Leandro F. Cardoso[1], **Liliane N. Vale**[1]

[1]Universidade Federal de Goiás – Departamento de Ciência da Computação (UFG)
Campus Catalão – Caixa Postal 56 – 75.705-020 – Catalão – GO – Brazil

leandrofc514@gmail.com, lili_malman@yahoo.com.br

Abstract. *Pervasive computing is a recent paradigm that leaves your computer "invisible"in a computing environment. The user does not realize, directly, the existence of actions of the computer acting to do a task. Although a current technology, security in this approach is not much discussed by researchers. This work shows a study and creation of forms of security in computing environments using the Pervasive Computing. This will be represented by a prototype that by looking the number Bluetooth Device Address (BD-ADDR) of Bluetooth devices (cell phones, smart phones) for a user will access the same computing environment. BD-ADDR function as password.*

Resumo. *A Computação Pervasiva é um paradigma recente que deixa o computador "invisível"em um ambiente computacional. O usuário não percebe, diretamente, a existência de ações do computador atuando para fazer uma tarefa. Apesar de ser uma tecnologia atual, a segurança nessa abordagem não é muito discutida por pesquisadores. Este trabalho vem mostrar um estudo e criação de formas de segurança em ambientes computacionais usando a Computação Pervasiva. Isso será representado por um protótipo que por meio da procura do número Bluetooth Device Address (BD-ADDR) dos dispositivos Bluetooth (celulares, Smartphones) de um usuário, fará com que o mesmo acesse um ambiente computacional. O BD-ADDR funcionará como senha de acesso.*

1. Introdução

No início da década passada, foi observado um movimento em direção à Computação Pervasiva (CP), sendo a mesma uma proposta de um método computacional que deixa livre ao usuário o acesso a ambientes computacionais em qualquer hora e lugar. Cria-se a possibilidade do usuário interagir com equipamentos de diferentes perfis de *hardware*, tendo suporte móvel ou não [Yamin 2004].

O termo CP vem sendo associado a IBM desde a edição intitulada *Pervasive Computing* do *IBM System Journal* [IBM 1999], onde foi feita uma divulgação sobre os aspectos promissores da CP. Essa idéia alcança destaque no cenário das tecnologias atuais. O método se mostra promissor na linha da mobilidade física (de equipamentos e/ou usuários) e do *software* (componentes a aplicação e serviços) [Yamin 2004].

Vários elementos da CP aparecem inseridos no cotidiano de pessoas que exigem cada vez mais pela disponibilidade de informação em qualquer lugar e hora. Neste

cenário, observa-se que muitos usuários abrem mão de, por exemplo, visualizar as informações sobre a tela de um monitor em alta definição para acessar os dados na tela de um celular e com recursos limitados. Tudo isso se remete a flexibilidade, a rapidez e comodidade para acesso aos dados de maneira rápida [Preece, Rogers e Sharp 2005]. Entretanto, em meio a alta flexibilidade, não devemos deixar de lado a segurança dos dados inerentes ao uso de recursos que a CP oferece.

Dessa forma, é apresentada uma análise da CP aplicada à segurança para ambientes computacionais, aliada a dispositivos móveis que tenham suporte a tecnologia Bluetooth. É apresentado um aplicativo que possa interagir com dispositivo Bluetooth e através deste, o usuário possa acessar serviços computacionais com segurança.

O objetivo em questão é a construção de um protótipo que funcione como meio de acesso a usuários em um Sistema Operacional. Este tem como funcionalidade a procura de dispositivos móveis Bluetooth, como celulares e smartfones, e relaciona o *Bluetooth Device Address* (BD-ADDR) desse dispositivo com algum usuário do Sistema Operacional.

2. Trabalhos Relacionados

Em [Campbell, Al-Muhtadi e Naldurg 2002] discutiu-se que na construção de sistemas pervasivos o critério de segurança é um assunto brevemente abordado. Entretanto faz-se uma análise de pesquisas atuais em CP que se concentram na construção de infraestrutura para a gestão de espaços ativos para o paradigma pervasivo, a conexão de novos dispositivos, ou a construção de aplicações úteis para melhorar a funcionalidade. No contexto de segurança e privacidade em tais ambientes, no entanto, não foram exploradas em profundidade. De fato, vários pesquisadores admitem que a segurança e privacidade nesse tipo de ambiente são problemas reais. Nesse trabalho é descrito formas de melhorar a segurança nestes ambientes.

Em [Kagal, Finin e Joshi 2001] foi proposto aplicações de segurança de sistemas distribuídos, voltado a ambientes de CP. Inicialmente faz-se uma análise sobre métodos tradicionais apontando que os mesmos não são tão eficientes em ambientes pervasivos e ambientes distribuídos. Para tal foi proposto uma solução baseada em gerenciamento de confiança que envolve o desenvolvimento de uma política de segurança. A atribuição de credenciais para entidades, destina-se a verificar que as mesmas devem cumprir a política, delegando confiança a terceiros, e raciocinando sobre os direitos de acesso dos usuários. Esta arquitetura é geralmente aplicável a sistemas distribuídos, voltado para ambientes de CP.

É apresentado em [Venkatasubramanian e Gupta 2006] formas de melhorar a segurança em ambientes de sistemas de saúde pervasivos. Neste trabalho afirma-se que a segurança é muito importante nos sistemas de saúde pervasivos para proteção de informações relativas à saúde que são coletadas e gerenciadas. É apresentada também uma visão geral de soluções de segurança para os sistemas de saúde pervasivo, concentrando-se principalmente em três aspectos: proteção de dados coletados por sensores médicos; controlar o acesso à informação de saúde gerenciados pelo sistema pervasivos e quadro legislativo para proteger sistemas de saúde.

É necessário salientar que a preocupação com a inserção de mecanismos de segurança em ambientes pervasivos se faz presente. Entretanto, não se encontrou até

o momento relatos que relacionam a segurança para o acesso a aplicativos oriundos da CP com dispositivos móveis. Em vista da grande demanda por disponibilidade de informações de forma rápida e fácil por meio de dispositivos móveis, é importante destacar sobre a necessidade de inclusão de técnicas de segurança durante a manipulação de dados.

3. Fundamentação Teórica

Uma tendência atual da CP tem sido a promoção de aplicativos presentes além do Desktop. Com a inserção de tecnologias (móvel, sem fio e portátil), os desenvolvedores criaram portanto aplicações utilizadas de variadas formas, ao invés de manter seu usuário apenas ao Desktop [Preece, Rogers e Sharp 2005].

O conceito de CP implica que o computador esta inserido no ambiente de forma ”invisível”para o usuário. Nestas condições, o computador tem a capacidade de captar informações do ambiente no qual se insere e depois utilizá-las para constituir dinamicamente modelos computacionais, controlando, configurando e ajustando a aplicação para melhor atender as necessidades do dispositivo ou do usuário. O ambiente poderá e deverá ser capaz de detectar outros dispositivos que venham a fazer parte dele. Desta interação, nasce a capacidade de computadores agirem de forma ”inteligente”, um ambiente repleto de sensores e serviços computacionais [Araujo 2005].

Usuários interagem com informações a qualquer instante e localização. Assim a idéia é que exista uma interação de tecnologias. Na linha domestica são prototipadas geladeiras que avisam ao usuário quando o estoque chega ao nível de ressuprimento, microondas interativo que permite ao usuário acessar a web enquanto cozinha e panelas que através de um ”bip”avisam quando o alimento esta pronto [Preece, Rogers e Sharp 2005].

É de extrema importância salientar a distinção entre CP e computação Ubiqua (CUb) e computação móvel (CM), pois é fácil confundi-las. A CUb tem em sua composição a mobilidade em grande escala, unida a funcionalidade da CP, ou seja, a CP é uma parte da CUb. A idéia da CUb é de a computação locomover-se para fora de terminais de trabalho ou computadores pessoais e tornar-se pervasiva em nosso cotidiano. A CM é baseada no crescimento da capacidade de locomover-mos fisicamente em ambientes computacionais, ou seja, o computador torna-se um dispositivo que expande a capacidade de usuários utilizar serviços que até então eram oferecidos por um computador de mesa, não importando sua localização [Araujo 2005]. A Figura 1 representa um comparativo entre as tecnologias abordadas.

Conforme na Figura 1, a CUb utiliza CP e CM na sua constituição. No protótipo é utilizada a idéia de CM juntamente com a CP. O mesmo não pode ser confundido com CUb , pois a mobilidade não será seu principal foco e sim quais dispositivos fazem parte dessa mobilidade, no caso da rede Bluetooth [Araujo 2005]. Este utiliza a idéia de mobilidade apenas para identificar o dispositivo.

Como se percebe, existem várias aplicações sendo empregadas em torno da CP, ou seja pode-se criar várias aplicações que vão facilitar e melhorar a vida das pessoas que utilizam tais tecnologias para o acesso a dados. A esta tendência a CP pode ser englobada no conceito de novas formas de interface homem-computador. O computador é inserido

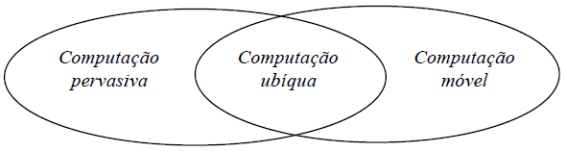

Figura 1. Comparativo entre Computação Pervasiva, Computação Móvel e Computação Ubíqua [Araujo 2005].

de forma ”escondida”no ambiente, mas sempre se comunicando com o usuário seja de forma direta ou indireta [Preece, Rogers e Sharp 2005].

É habitual usar interfaces diretas como teclados, mouses, tela do computador, entre outros. A CP, por ser eclética na questão de áreas de atuação, pode ser uma forma de segurança em ambientes computacionais. Uma das pontes usadas pela CP no protótipo apresentado neste trabalho é a tecnologia Bluetooth, através da pesquisa do BD-ADDR ou endereço Bluetooth de um dispositivo. Essa tecnologia surge da necessidade de criar uma comunicação curta entre dispositivos sem a utilização de fios.

O dispositivo Bluetooth do computador consegue distinguir os tipos de aparelhos através do BD-ADDR, citado anteriormente, através de uma sequência de 48 bits que dispositivos conseguem enxergar a identidade de cada um na rede. Essa sequência é definida pela *Institute of Electrical and Electronics Engineers* (IEEE) [Vainio 2000]. Isso será de grande importância para o protótipo abordado que utiliza essa sequência de bits única em cada dispositivo Bluetooth, como uma identificação de um usuário. Essa idéia é semelhante à das placas de rede para acesso a internet. Ela utiliza um número *MAC Address* ou endereço de MAC para identificá-la como única na rede.

Como se pode observar, podemos unir tecnologias para a construção de um paradigma, no caso o ambiente pervasivo. Na próxima seção, será descrito a estrutura utilizada para a construção de um exemplo que possa ilustrar a abordagem em questão. Este exemplo é um protótipo que, juntamente com a CP irá funcionar como uma nova forma de acesso a ambientes computacionais. Ele será capaz de identificar dispositivos Bluetooth e com essa identificação, o usuário poderá ou não acessar um Sistema Operacional.

4. Arquitetura Geral do Protótipo

O protótipo proposto, tem ênfase na segurança de sistemas computacionais, que utiliza maneiras não tradicionais de acesso. Uma das maneiras mais tradicionais de acesso em um ambiente computacional é por meio de senhas inseridas manualmente pelo usuário, por exemplo. Também nos preocupamos muito com o nível de segurança que senhas possuem, através de criptografias com melhor eficiência, entre outros. A idéia principal é trazer isso de uma maneira simples e automática de uma forma inovadora, não esquecendo a segurança. É apresentada a arquitetura geral do protótipo na Figura 2.

O protótipo funcionará em um computador e o mesmo deverá ter suporte a tecnologia Bluetooth e ao iniciar o sistema ele tentará localizar um dispositivo para determinado usuário que tentar logar no sistema. Na Figura 3 é apresentado o funcionamento do sistema.

Para que certo usuário consiga ter acesso a um Sistema Operacional, ele terá que

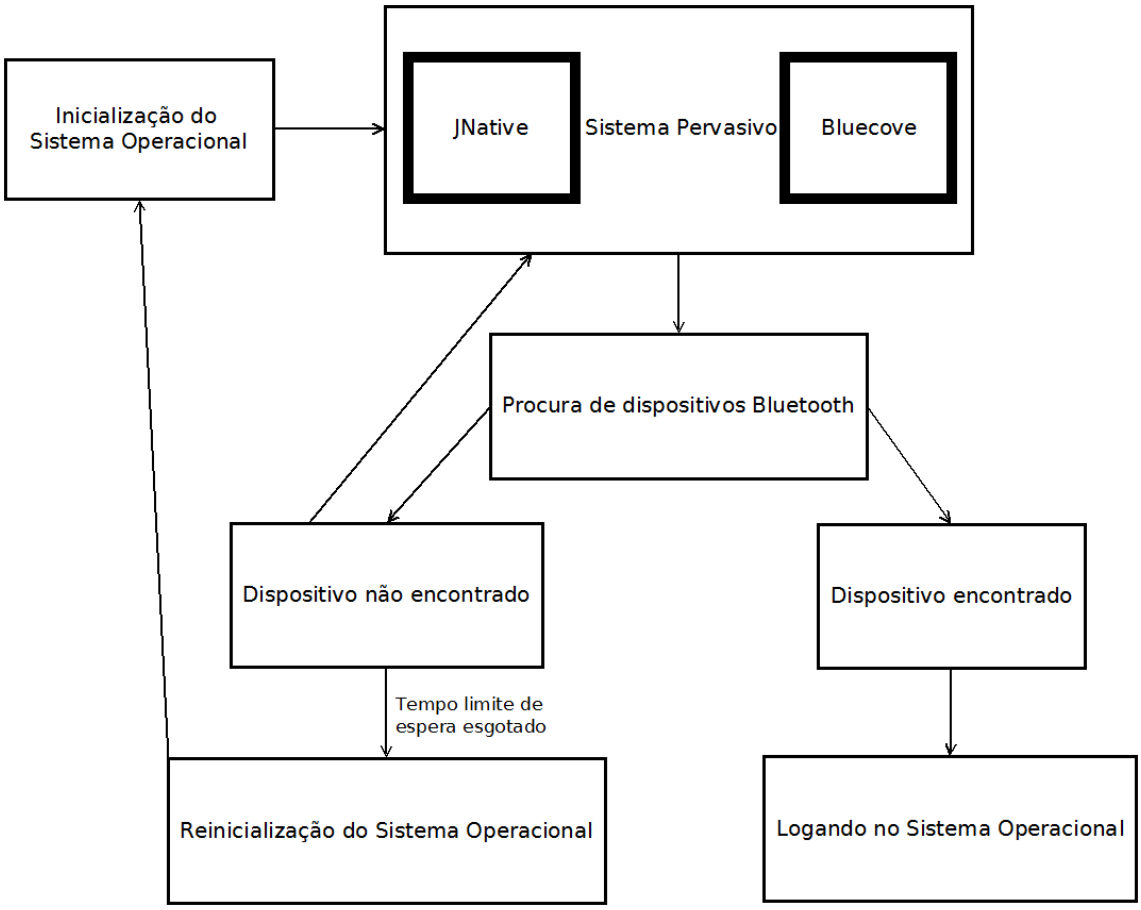

Figura 2. Arquitetura geral do protótipo.

cadastrar seu dispositivo Bluetooth, através da informação do BD-ADDR de seu dispositivo. Em relação à segurança, o protótipo terá a capacidade de localizar o dispositivo de rádio Bluetooth que terá que estar em um raio de alcance visível a ele e o mesmo terá a capacidade de comparar o BD-ADDR do dispositivo móvel do usuário com seu banco de dados. No banco de dados, teremos este número que estará referenciado para determinado usuário do Sistema Operacional. Se não existir um número BD-ADDR para determinado usuário, ou se esse número não for compatível para aquele usuário, o mesmo não conseguirá ter acesso ao sistema.

Em relação ao funcionamento interno do protótipo, ele possui duas partes integrantes muito importantes que dão a idéia de CP ao mesmo. São as APIs *Application Programming Interface* Java, BlueCove [BlueCove 2011] e JNI(*Java Native Interface*) [Liang 1999].

A JNI é uma API que está acoplado à máquina virtual Java e tem como função, a comunicação com recursos específicos em um determinado Sistema Operacional. Ela permite que um código Java entenda uma biblioteca C/C++, Assembler, e muitas outras linguagens de programação. O Sistema Operacional não entende a linguagem Java e esta ferramenta constrói formas para que o mesmo entenda [Liang 1999]. Para que o protótipo consiga bloquear entradas do usuário, seja por teclado ou mouse, tem que ser utilizado esta API pois se não utilizarmos a mesma, o próprio Java não consegue manipular eventos

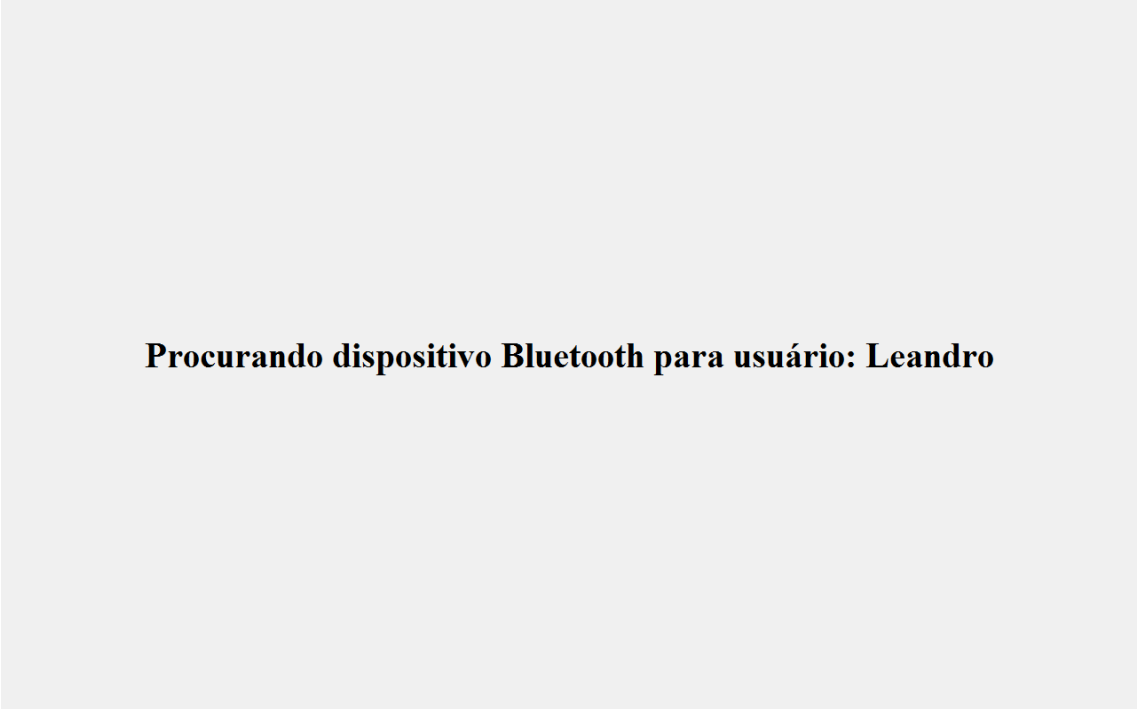

Figura 3. Protótipo em funcionamento.

que o Sistema Operacional faz diretamente.

A API BlueCove é parte integrante da plataforma Java J2SE e dá suporte a computadores para que os mesmos possam trabalhar com dispositivos Bluetooth de forma simples. O mesmo tem em sua arquitetura a API JNI. [BlueCove 2011]

Em nossa abordagem foi utilizada a tecnologia JNI, porque é preciso bloquear qualquer tipo de entrada do usuário, seja por teclado ou mouse. Isso deve ocorrer pois durante a procura de um BD-ADDR (que será feito pelo BlueCove) é necessário barrar qualquer tipo de acesso do usuário. Dessa maneira, o usuário terá que possuir um dispositivo Bluetooth relacionado a ele para que consiga ter acesso ao Sistema Operacional. É apresentado na Figura 4 o algoritmo do protótipo que explica o funcionamento geral do mesmo de acordo com o descrito anteriormente.

5. Estudo de Caso

Apesar de serem formas eficientes de segurança de dados e informações formas tradicionais de acesso a ambientes computacionais precisam de um estímulo direto do usuário, ou seja, o computador necessita diretamente de eventos do usuário para conseguir liberar as suas funcionalidades. A diferença crucial na abordagem defendida é que não existirá contato direto do usuário com o computador, ou seja, defende a idéia de CP, que adere pela abstração de eventos tradicionais de dados como senhas digitadas manualmente.

Para ilustrar a abordagem proposta foi construído um cenário de casos de uso. Foi utilizado para avaliação do protótipo os sistemas operacionais Windows Seven (Windows 7) da Microsoft e o Linux Ubuntu 10.04. Por ser desenvolvido na plataforma Java, não foi preciso grandes alterações na adaptação do mesmo. Quem prefere, essa abordagem pode

```
//Algoritmo seguraça pervasiva

Método Inicia_prototipo
Início
    bloquer_entrada_dados(true);
    contador;
    //Enquanto o Bluetooth Adrress(BA) for diferente a do Bluetooth Adrress
    //do banco de dados(BA-DB) ou o BA nao existir...
    Enquanto BA != BA-DB
    Início Enquanto
        Busca_Dispositivo_Bluetooth();
        contador++;
        Se contador > limite_contagem_busca();
        Início Se
            sair_do_sistema();
        Fim Se
    Fim Enquanto
    //Se for encontrado o BA para determinado usuario do sistema operacional,
    //iniciar o sistema...
    bloquer_entrada_dados(false);
    inicia_Sistema_Operacional();
Fim
```

Figura 4. Algoritmo do protótipo.

funcionar juntamente com formas tradicionais de acesso a meios computacionais, como senha digitada manualmente.

O computador, através protótipo busca o número BD-ADDR que está cadastrado para um determinado usuário. Como dispositivos móveis foram utilizados para teste os celulares Nokia 5130 e o Sony Ericsson k550im. Na Figura 5 é mostrado estes dispositivos.Este número funcionará como senha de acesso para determinado usuário em um Sistema Operacional. Se o nenhum dispositivo não for encontrado ou se determinado dispositivo não estiver referenciado ao usuário logado, o mesmo não conseguirá ter acesso ao Sistema Operacional.

Figura 5. Celulares com Bluetooth testados

O que o usuário perceberá que com a aproximação de seu dispositivo móvel, ele conseguirá ter acesso a um sistema computacional desde que esteja cadastrado com seu BD-ADDR. Ele não perceberá nada do que está acontecendo por trás do sistema. O sistema será inteligente o suficiente para perceber se o dispositivo está perto o bastante

para efetuar o acesso ao ambiente computacional. Essa é a idéia principal de CP, abstrair ao máximo, as funcionalidades ao usuário.

6. Conclusão

O protótipo conseguiu demonstrar com eficiência o bloqueio de usuários que não possuem um BD-ADDR cadastrado no sistema. A única dificuldade encontrada até o momento foi no caso do usuário perder ou se existirem defeitos em seu dispositivo Bluetooth. Se acontecer tal fato,o mesmo não conseguirá, de maneira alguma, entrar em um ambiente computacional. Esta exceção terá que ser analisada para que o usuário não tenha dificuldades caso ocorra tal problema.

Como trabalhos futuros será construído outro protótipo que reconhece voz de um usuário e com este reconhecimento poderá falar suas senhas. Este protótipo vai trabalhar com o *software* ViaVoice 5.0 da IBM, uma versão *free* e com API Java Speech serão utilizadas para o reconhecimento de voz. Este *software* vai ser construído para trabalhar como eventual forma de escape para quem não conseguir logar no sistema através de um dispositivo Bluetooth.

Referências

Araujo, R. (2005). *Computação Ubíqua: Princípios, Tecnologias e Desafios.* Departamento de Computação - Universidade Federal de S. Carlos (UFSCar). XXI Simpósio Brasileiro de Redes de Computadores.

BlueCove (2011). *The Official Web Site.* Disponível em: http://www.bluecove.org . Acessado em: ago.2011.

Campbell, R., Al-Muhtadi, J. e Naldurg, P. (2002). *Towards Security and Privacy for Pervasive Computing.*

IBM (1999). *Pervasive Computing*. IBM System Journal. New York, v.38, n4, 1999. Disponível em: http://www.research.ibm.com/journal/sj38-4.html. Acessado em: ago.2011

Kagal, L., Finin, T. e Joshi, A. (2001). Trust-Based Security in Pervasive Computing Environments. Comunications, *University of Maryland, Baltimore County.* dez.2001.

Liang (1999). *The $Java^{TM}$ Native Interface (1999).* Programmers Guide and Specification Impresso por: Addison Wesley Longman, Inc.

Prece, J., Rogers, Y. e Sharp, H. (2005). *Design de interação: além da interação homem-computador.* Editora: Bookman,2005.

Vainio (2000). *Bluetooth Security.* Department of Computer Science and Engineering. Helsinki University of Technology.

Venkatasubramanian, K. e Gupta, S. (2006). *Security Solutions for Pervasive Healthcare. Part IV - Security in Pervasive Computing.* out.2006.

Yamin, A. (2004). *Arquitetura para um Ambiente de Grade Computacional Direcionado às aplicações Distribuídas, Móveis e Conscientes do Contexto da Computação Pervasiva*. Tese de Doutorado.