Segurança de Sistemas Ubíquos Baseada em Informações de Contexto

Francisco Gomes Milagres, Rodrigo Felício dos Santos,
Rudinei Goularte, Edson dos Santos Moreira
Universidade de São Paulo – Instituto de Ciências Matemáticas e de Computação
Departamento de Computação e Estatísica – Laboratório Intermídia
Avenida Trabalhador Sancarlense, 400 – 13566-590 – São Carlos – SP
{milagres, felicio, rudinei, edson}@icmc.usp.br

RESUMO

A computação ubíqua, área de pesquisa idealizada por Mark Weiser em 1991, sugere novas formas de interação entre usuário e máquina, desenvolvendo ambientes onde a inserção de tecnologia no cotidiano ocorre de modo transparente. Nesses ambientes, ditos ubíquos, é crescente a presença de mobilidade e informações como identificação, atividade, preferências e histórico de usuários são monitoradas, processadas e armazenadas por diferentes dispositivos e aplicações. O objetivo deste artigo é levantar as questões de segurança e privacidade existentes no paradigma de computação ubíqua utilizando um protótipo de TV interativa (TVI) que possui características de mobilidade e ciência de contexto. As informações de contexto presentes no TVI devem ser mapeadas restringindo-se o acesso de acordo com políticas de privacidade.

ABSTRACT

The ubiquitous computing area, introduced by Mark Weiser in 1991, suggests new ways of interaction between users and machines, towards the development of environments where the technological insertion in the every day life occurs in a transparent way. In these ubiquitous environments, the presence of mobility is increasing and information like user's identity, activity, preferences and history are under monitoring, processing and storing by different devices and applications. This paper aims to raise questions about security and privacy under the ubiquitous computing paradigm using an interactive TV prototype (TVI) which supports both context-awareness and mobility. The context information in the TVI environment are tracked in order to control the access in conformance with privacy policies.

1 INTRODUÇÃO

Com o desenvolvimento de tecnologias cada vez mais transparentes ao cotidiano, muitos conceitos novos têm surgido para definir nichos de mercado e se estabelecerem como as bases de pesquisas que estão em desenvolvimento, para serem naturalmente parte do nosso dia-a-dia no futuro.

Exemplos cada vez mais comuns são os dispositivos portáteis multifuncionais – que substituem as agendas, telefones, *pagers* ou um computador pessoal – até as ainda distantes redes *ad hoc* de micro sensores com capacidade de processamento e comunicação, a *smart dust*, alvo de pesquisas em universidades norte-americanas e com financiamento da agência DARPA (*Defense Advanced Research Projects Agency*), do governo dos EUA. (Stajano, 2001)

A área de pesquisa responsável por abstrair novas formas de interação entre usuário e máquina é a computação ubíqua, que surgiu a partir de protótipos de dispositivos idealizados pelo pesquisador Mark Weiser (1991).

Em ambientes ubíquos onde a presença de mobilidade é crescente, informações sobre o usuário como identificação, preferências e histórico de uso são monitoradas, armazenadas, processadas e intercambiadas entre aplicações em diferentes domínios. Dessa forma, paralelamente ao desenvolvimento de tecnologias inseridas em nosso cotidiano de forma não intrusiva, surgem questões sobre segurança e privacidade dos dados.

O objetivo deste artigo é levantar as questões de segurança e privacidade existentes no paradigma de computação ubíqua utilizando um sistema de processamento e transmissão de TV interativa que possui características de mobilidade e ciência de contexto.

A partir deste ponto, este artigo está organizado da seguinte forma: no capítulo 2 são apresentados os conceitos de computação ubíqua e no capítulo 3, é feito um detalhamento da área de pesquisas de ciência de contexto em computação ubíqua. No capítulo 4 é feita a contextualização de segurança da informação e no capítulo 5 são apresentadas as principais considerações de segurança da informação em computação ubíqua, que justificam este trabalho. No capítulo 6 são apresentados o projeto TVI e as implementações que visam garantir privacidade aos clientes do sistema de TV interativa e no capítulo 7 são apresentadas as considerações finais. Há seções adicionais com os agradecimentos dos autores deste trabalho e as referências bibliográficas citadas nessa publicação.

2 COMPUTAÇÃO UBÍQUA

O termo "computação ubíqua" foi introduzido pelo pesquisador Mark Weiser (1991) quando vislumbrou ambientes acrescidos de recursos computacionais capazes de prover serviços e informações quando e onde sejam desejadas. De acordo com Weiser, deve haver integração contínua entre tecnologia e ambiente de modo a auxiliar os usuários em atividades cotidianas. Portanto, computadores devem ser embutidos de forma implícita ao ambiente do usuário (Weiser, 1993). A interação usuário-computador deve ocorrer de modo não intrusivo, sem impor a utilização de artefatos como teclados e controles-remotos, ficando mais próxima à forma com que os seres humanos gesticulam, falam ou escrevem para se comunicarem.

No entanto, para garantir essa integração, e conseqüentemente, uma expansão no paradigma de interação computacional, Weiser (1991) previu o desenvolvimento de infra-estrutura e aplicações capazes de suportar informações e serviços de computação ubíqua. Houve a proliferação de dispositivos heterogêneos e de escalas variadas, como PDAs (*Personal Digital Assistants*), *tablets* digitais (dispositivos computacionais portáteis semelhantes a uma prancheta com telas sensíveis ao toque), lousas eletrônicas, *laptops*, telefones celulares e, portanto, um enriquecimento na infra-estrutura. Desse modo, a infra-estrutura necessária para o desenvolvimento da computação ubíqua estaria assegurada.

Porém, Weiser (1991) visualizou o desenvolvimento de novas aplicações capazes de explorar o uso desses novos dispositivos. Logo, nos últimos anos o desenvolvimento dessas aplicações tem o seu foco voltado para três tipos principais de interação: aplicações cientes de contexto, interfaces naturais e captura e acesso de atividades humanas (Abowd, 2002).

2.1 Interfaces Naturais

Além da proliferação de dispositivos pelo ambiente, a computação ubíqua envolve também o desenvolvimento de interfaces naturais. Por meio do suporte a formas comuns de expressão humana, as interfaces naturais facilitam a capacidade de comunicação entre usuários e computadores utilizando ações explícitas ou implícitas durante a comunicação.

O objetivo das pesquisas nessa área é aproximar a interação usuário-computador da interação natural que ocorre entre pessoas. Desse modo, a interação usuário-computador seria não-intrusiva, ideal para computação ubíqua. Com isso, projetos voltados para interfaces mais amigáveis investigam técnicas de reconhecimento de escrita e de gestos, interação com canetas, técnicas de voz e percepção computacional, interação com sensores e manipulação de artefatos eletrônicos (Abowd, 2002).

2.2 Captura e Acesso de Atividades Humanas

Grande parte do tempo dos seres humanos é gasto registrando acontecimentos dos quais participam. Para isso, é necessário absorver a informação e depois tentar recuperá-la. No entanto, os humanos não são capazes de registrar todas as informações relevantes, talvez nem mesmo todos os tópicos de interesse. Logo, com o advento de recursos como anotações e gravações de áudio e vídeo, a tarefa de registrar fatos tornou-se menos árdua. Com a utilização de multimídia em ambientes computacionais, o ser humano pode enfim focar sua atenção exclusivamente na atividade que exerce de modo mais eficiente.

Segundo Abowd e Mynat (2000) e Abowd et al. (2002), a área de captura e acesso de atividades humanas é responsável pelo desenvolvimento de aplicações capazes de preservar a gravação de alguma experiência cotidiana para acesso futuro. Várias aplicações relacionadas a aulas, palestras e reuniões foram desenvolvidas nessa área, como o eClass (Abowd, 1999) que enfatiza a transparência dos processos de captura e autoria de hiperdocumentos multimídia disponibilizados por meio da Web (Pimentel et al., 2001, 2000).

2.3 Computação Ciente de Contexto

De acordo com Dey e Abowd (1999), contexto é qualquer informação relevante que possa ser utilizada para caracterizar a situação de uma entidade. Uma entidade pode ser uma pessoa, um lugar, ou um objeto, relevantes para a interação entre o usuário e a aplicação.

A computação ciente de contexto é responsável por obter e utilizar informações de contexto adquiridas de um dispositivo computacional com o objetivo de prover serviços a uma entidade. Informações de contexto são úteis quando se pode interpretá-las. Enriquecendo a interação usuário-aplicação com informações de contexto é possível melhorar os serviços oferecidos. A computação ciente de contexto será detalhada na Seção 3.

3 COMPUTAÇÃO CIENTE DE CONTEXTO

Na interação entre pessoas, muitas das informações são trocadas de forma implícita. Expressões, gestos e tonalidade de voz podem ser utilizados para auxiliar a comunicação entre as pessoas envolvidas na interação. No entanto, na interação usuário-computador raramente há o compartilhamento de informações de contexto devido ao uso de dispositivos tradicionais de interação como o teclado e mouse.

Aplicações cientes de contexto devem ser capazes de adquirir informações de contexto de modo automatizado, disponibilizando-as em um ambiente computacional em tempo de execução. Os desenvolvedores deste tipo de aplicação têm a tarefa de decidir se as informações obtidas são realmente relevantes e como manipulá-las (Dey e Abowd, 1999). Para isso, há a necessidade de definir quais são informações contextuais e o que é contexto.

3.1 Definição de Informação de Contexto

De acordo com Dey, o primeiro trabalho a utilizar o termo “ciente de contexto” foi o de Schilit e Theimer (1994), os quais se referiam a contexto como localização, identidades de pessoas e objetos e mudanças desses objetos (Dey, 2001). Outras abordagens definem contexto como o ambiente ou situação em que uma determinada interação ocorre. Dey ainda argumenta que tanto a definição de Shilit (1994) (os principais aspectos do contexto são: onde você está, quem está com você, e quais recursos estão próximos) quanto à de Pascoe (1998) (contexto é o subconjunto de estados físicos e conceituais de interesse de uma entidade

particular) são muito específicas, já que contexto é toda situação relevante a uma aplicação e seu conjunto de usuários.

Desse modo, Dey e Abowd (1999) definem informação de contexto como qualquer informação que possa ser usada para caracterizar a situação de uma entidade. Uma entidade é uma pessoa, lugar ou objeto que é considerado relevante para a interação entre um usuário e uma aplicação, incluindo ambos. Se uma parte de informação pode ser usada para caracterizar a situação de um participante em uma interação, então tal informação é contexto.

3.2 Categorização de Contexto

Para obter informações de contexto relevantes à aplicação, pode-se utilizar uma categorização de tipos de contexto que auxilie desenvolvedores a construírem aplicações cientes de contexto. Ryan et al. (1997) sugere tipos de informações de contexto como localização, ambiente, identidade e tempo. Segundo Dey e Abowd (1999), é possível obter informações de contexto com base em cinco dimensões conhecidas como "cinco Ws":

- *Who* (quem): Sistemas atuais focam a interação na identidade de um usuário em particular, incorporando raramente informação referente a outras pessoas também presentes ao ambiente. Porém, seres humanos associam atividades à presença de outras pessoas como artifício para se lembrarem do ocorrido. Logo, é importante prover informações não apenas do usuário, mas também de todas as pessoas em uma atividade assistida por computador;
- *Where* (onde): A idéia de localização é a mais utilizada por aplicações cientes de contexto. Na área de computação ubíqua, esta dimensão é muito utilizada em associação com a dimensão de identidade (*who*) e a temporal (*when*) no intuito de fornecer novas funcionalidades às aplicações. Como exemplos de sistemas que exploram esta dimensão podem ser citados guias turísticos capazes de prover informações na localização e na identidade do usuário em um determinado instante;
- *When* (quando): O contexto temporal tem sido utilizado para indexação de registros capturados ou para informar a duração de um usuário em um determinado local ou sessão;
- *What* (o quê): Dimensão responsável por identificar a atividade do usuário, tarefa que em geral é considerada complexa. Dispositivos cientes de contexto devem suportar interpretações de atividades humanas;
- *Why* (por quê): Mais complexo do que inferir a ação do usuário é descobrir o porquê de sua atividade. Obter informações capazes de prover o motivo de uma ação do usuário talvez seja o maior desafio da computação ciente de contexto. Devido à essa complexidade, para a obtenção de informações desta dimensão a combinação das quatro dimensões anteriores pode ser utilizada.

3.3 Definindo Computação Ciente de Contexto

A primeira definição de aplicações cientes de contexto elaborada por Schilit e Theimer (1994) restringiu a definição de aplicações que são simplesmente informadas sobre contexto para aplicações que se adaptam ao contexto. Segundo Dey e Abowd (1999), definições anteriores podem ser classificadas em duas categorias: o uso de contexto e adaptação ao contexto. Ambos ainda acrescentam que nas duas classes as definições são muito específicas e, portanto, definem de maneira geral um sistema consciente de contexto como sendo "um sistema que utiliza contexto para prover informação relevante e/ou serviços ao usuário, onde a relevância depende da tarefa do usuário". Considerando esta última definição, três aspectos

importantes em computação ciente de contexto podem ser identificados (Pascoe, 1998; Dey e Abowd, 1999):

- Apresentação de informações e serviços ao usuário;
- Execução automática de um serviço a um usuário;
- Etiquetar o contexto à informação para suportar recuperações posteriores.

4 SEGURANÇA DA INFORMAÇÃO

Segundo uma pesquisa recente sobre segurança da informação no país, realizada pela Módulo Security Solutions (2003), 78% das empresas no Brasil reconhecem que tiveram perdas financeiras devido a alguma violação de segurança no último ano. Apesar disso, 56% das empresas entrevistadas ainda não conseguem quantificar o valor dos prejuízos causados pelos problemas com a segurança de suas informações. Em 22% das organizações que conseguiram contabilizar estes valores, o total de perdas registradas foi de R$ 39,7 milhões.

A preocupação crescente pela segurança da informação foi redobrada no ano de 2002 em todo o mundo a partir de incidentes como o que se abateu sobre o *World Trade Center* (WTC) e o Pentágono em Setembro de 2001. Na ocasião, muitas empresas sem planos de contingência e continuidade de negócios perderam, além de seus funcionários, todas as suas bases de dados e sistemas de informação devido a um ataque terrorista bem sucedido.

Exemplos recentes do aumento de investimentos na área de segurança podem ser extraídos de pesquisa realizada pelo CSI (*Computer Security Institute*) em conjunto com o FBI com grandes organizações norte-americanas. Segundo Richardson (2003), a grande maioria das organizações entrevistadas afirmou possuir controle contra vírus (99%) e *firewalls* (98%). É crescente também em relação aos anos anteriores da pesquisa a porcentagem de uso de controles para acesso físico (91%). Apesar de serem resultados positivos em relação aos anos anteriores da pesquisa, ainda há uma fatia considerável de entrevistados (15%) que afirmaram sequer saberem, por exemplo, se a empresa foi alvo de tentativa bem sucedida ou não de um ataque durante o ano de 2002. (Whitman, 2003)

4.1 Segurança por definição

É uma prática comum em todos os setores onde podem ser aplicados os conceitos de segurança da informação a máxima que não há um sistema completamente seguro. Pode-se definir então um sistema seguro de acordo com alguns parâmetros, como por exemplo, a análise e o gerenciamento do risco que podem ser aceitos.

Para que o conceito abstrato de risco possa ser mensurado, é preciso inicialmente definir os conceitos a serem considerados para a segurança de um sistema, seja ele computacional ou não. (Tipton e Krause, 2002) Na Figura 1 é ilustrada a integração que deve existir entre estes conceitos, que são explanados resumidamente a seguir.

Fig. 1 - Premissas para garantia de segurança

- Autenticidade: visa garantir a identificação dos usuários e a validade de informações transmitidas e armazenadas;
- Controle de acesso: tem como objetivo garantir que somente usuários autorizados tenham acesso a determinados recursos;
- Integridade: visa garantir que dados não sejam alterados sem permissões explícitas;
- Não repúdio: visa provar sem possibilidade de dúvida que uma ação foi executada e que sua origem ou eventual resposta podem ser contestadas;
- Privacidade: tem como objetivo garantir o segredo dos dados e entre comunicações.

É importante destacar que não há uma definição estabelecida do que seja segurança da informação e há conflitos de conceitos na literatura com relação aos pontos básicos para sua garantia. De acordo com Garfinkel et al. (2003), ainda deve-se incluir conceitos como disponibilidade para que seja garantida a segurança de um sistema – proteção a um sistema de modo que ele não se degrade ou se torne indisponível sem autorização – e auditoria, que visa permitir que ações de usuários e processos sejam eles legítimos ou não, possam ser traçadas.

Há diversas metodologias e ferramentas que, aliados aos conceitos apresentados, permitem uma definição e um estudo mais amplo de riscos e da segurança computacional envolvida (Bishop, 2003), no entanto, a discussão em detalhes destes conceitos está fora do escopo principal deste artigo.

5 SEGURANÇA EM COMPUTAÇÃO UBÍQUA

Apesar da computação ubíqua ser uma área de pesquisas com mais de uma década de desenvolvimento, as considerações de segurança e privacidade em sistemas desta natureza têm sido pouco adotadas como tema de estudos.

Nesta seção serão descritas algumas das principais considerações de segurança e privacidade levantadas para sistemas que façam uso das interações classificadas para sistemas em computação ubíqua: aplicações cientes de contexto, interfaces naturais e captura e acesso de atividades humanas. (Abowd, 2002)

Durante alguns anos, a criptografia e a garantia de integridade de dados foi considerada a premissa para a segurança de um sistema computacional. (Schneier, 2000). Com a evolução dos sistemas computacionais interligados por redes e o surgimento de novas necessidades e, conseqüentemente, novas ameaças à informação, esta preocupação singular ganhou novas

companhias. (Schneier, 2003) A autenticidade e o não repúdio são algumas das premissas que devem ser garantidas para que um sistema seja seguro dentro de um nível de riscos aceitável.

5.1 Autenticidade e não repúdio

A garantia de autenticidade e o não repúdio das partes que se comunicam em um sistema computacional e também da informação, especialmente em sistemas ubíquos, é uma tarefa difícil. Há novas condições que devem ser consideradas na segurança de sistemas desta natureza, por exemplo, a ausência de servidores centralizados para autenticação.

A primeira opção nesses casos é a adoção de criptografia por par de chaves ou de chaves públicas (Garfinkel et al., 2003). Dessa forma, cada entidade móvel e independente possuirá uma chave pública assinada por uma autoridade certificadora e que não necessariamente deverá estar on-line para garantir a autenticação de cada elemento do sistema. Apesar de ser um método de criptografia e assinatura digital que também garante o não repúdio, devido à ausência da figura central, alguns problemas devem ser tratados.

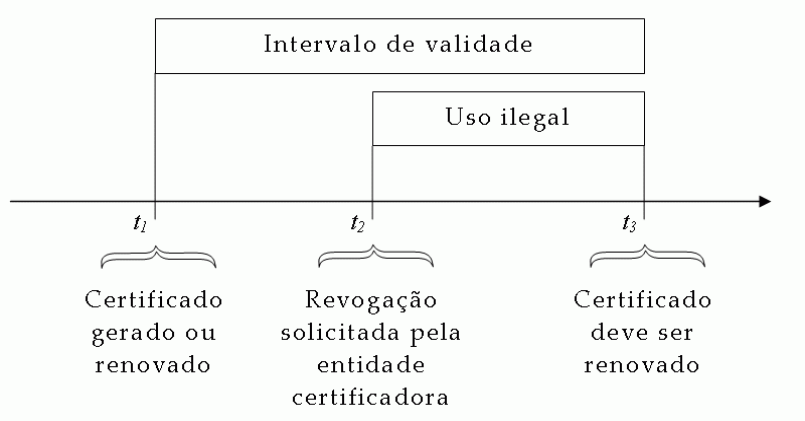

Fig. 2 – O período de validade de um certificado digital

Um dos problemas do uso de par de chaves criptográficas em computação ubíqua é ausência de uma entidade central que garanta a validade das identificações das entidades clientes, por exemplo. Em intervalos de tempo entre a revogação e a emissão de um novo certificado (ou a sua negação), entidades mal intencionadas podem usar a identificação por certificados antigos para atividades teoricamente autênticas (Figura 2) (Stajano, 2002).

Uma solução para este problema é diminuir o prazo de validade dos certificados para um nível de risco aceitável. Deve ser observado também que, nessa solução, as entidades ubíquas devem possuir *clocks* sincronizados, o que adiciona outro item para processamento. Um equilíbrio entre o gasto em processamento na geração de novos certificados, sincronização dos *clocks* e o nível de risco aceitável deve ser analisado para cada caso.

5.2 Sigilo e privacidade

Segundo Schneier (2000), há alguns anos vêm se desenvolvendo protocolos de criptografia que visam garantir, dentro de níveis de risco calculados, a segurança das informações durante o trajeto ou armazenamento. Assim, pode-se dizer que os protocolos de criptografia deixaram de ser *o elo mais fraco* em cadeias que visam garantir a segurança da informação (Stajano, 2001).

Em sistemas ubíquos e móveis, geralmente compostos de dispositivos de tamanho reduzido e de menor capacidade de processamento e armazenamento se comparados com computadores pessoais, há restrições, por exemplo, na complexidade que pode ser usada em algoritmos

criptográficos. É importante destacar também que, além da garantia de sigilo de informações transmitidas, deve ser considerado o tratamento específico das informações que são armazenadas nos dispositivos portáteis.

Uma das premissas de sistemas de computação ubíqua é que, por exemplo, um ambiente dito ubíquo deve ser considerado *inteligente*, *ciente às preferências do usuário e sensível à sua presença* e deve ainda *servir ao usuário como um mordomo*. (Stajano, 2001). Da mesma forma que uma pessoa *responsável por auxiliar nas tarefas domésticas* é habituada com as preferências do seu *patrão*, ela tem conhecimento de informações sensíveis e deve manter segredo delas. Essa visão é análoga se for considerada a quantidade de informação que pode ser inferida no uso de um computador portátil, por exemplo.

Exemplificando algumas variáveis que devem ser asseguradas em sistemas ubíquos, pode-se listar: *quem, com quem* e *quando* (ao contrário de *o quê*, que pode ser assegurado por criptografia).

Há diversas considerações que ainda não foram sequer tema de pesquisa em computação ubíqua e em segurança da informação. Stajano (2001) lista alguns problemas que em pouco tempo devem começar a ser tema de preocupação para todos que utilizam sistemas ubíquos:

- Se a computação ubíqua permite a tecnologia pervasiva e de forma transparente, cada vez mais atividades comuns devem então ser conduzidas através de dispositivos eletrônicos. Desta forma, será mais fácil coletar informações de comportamento e preferências de usuários, facilitando o dia-a-dia, bem como reduzindo a sua privacidade;
- Se sistemas ubíquos permitem que nossos ambientes sejam sensíveis e personalizados, um dos objetivos principais destes sistemas é obter o máximo de informações possível sobre nós e nossas preferências, o que pode ser crítico se não for bem controlado. Um exemplo desta característica pode ser observado no filme *Minority Report – A Nova Lei*, dirigido por Steven Spielberg [1], quando o personagem John Anderton (Tom Cruise) entra em um centro comercial e é recepcionado por sistemas que detectam sua presença e, de acordo com suas preferências, apresentam ofertas direcionadas de produtos;
- A computação ubíqua adiciona a questão da escala de uso das informações. Se forem consideradas as partes de dados pessoais que podem ser coletadas em sistemas computacionais onde os dados pessoais de um usuário são processados, geralmente não é possível inferir muito sobre tal pessoa, por exemplo, em contas de banco e operações com cartão de crédito. No entanto, se houver uma integração entre estes sistemas, com objetivo de criação de um sistema ubíquo, grande parte da informação que precisaria ser inferida em sistemas não monolíticos já estará disponível;
- Não será incomum o uso de tecnologias criadas originalmente para um uso aceitável de forma ilegal, como por exemplo, para espionagem.

As considerações de sigilo e privacidade listadas são apenas exemplos apresentados por Stajano (2001), que apresenta exemplos e algumas soluções em detalhes e que não estão completamente no escopo deste artigo.

Um modelo apresentado pelo mesmo pesquisador e que visa contornar as principais questões de autenticação de dispositivos em computação ubíqua, especificamente em redes *ad hoc*, é o *Ressurrecting Duckling*. Através de uma metáfora, Stajano e Anderson (1999) demonstram um protocolo para a autenticação entre dispositivos em um sistema ubíquo, utilizando o conceito de *associação volátil e segura.*

[1] http://www.imdb.com/Title?0181689

Através de uma associação entre dois dispositivos, por exemplo, um controle remoto e um dispositivo computacional, é necessário que essa associação seja válida durante o período de uso do dispositivo por seu dono. Caso o seu controle remoto precise ser substituído, deve ser possível associar o controle do dispositivo a um novo controle remoto compatível. É importante destacar que, apesar de ser uma associação volátil, ela deve ser segura, não podendo ser desfeita por um usuário mal intencionado.

As premissas de segurança integridade e controle de acesso estão fora do escopo específico deste trabalho e devem ser tratadas em detalhes em trabalhos futuros.

Os conceitos de segurança da informação em computação ubíqua estão sendo validados em nosso sistema de processamento e transmissão de TV interativa (Goularte, 2002), o qual possui características de mobilidade e ciência de contexto. Nesse sistema devem ser mapeadas as informações de contexto dos usuários e, através de um *framework* em desenvolvimento, restringir o acesso a estas informações de acordo com políticas de privacidade definidas de acordo com o perfil dos serviços do sistema TVI.

6 PROJETO TVI

O projeto de TV interativa TVI tem como objetivo desenvolver um protótipo no qual usuários podem interagir com vídeos distribuídos a partir de uma variedade de sistemas, como transmissão terrestre, *streaming* (em redes cabeadas e em redes sem fio) e via redes de telefonia celular. Entre as características do projeto estão a utilização de padrões como MPEG-4 e MPEG-7 no auxílio à personalização de conteúdo de acordo com as preferências do usuário ou condições do sistema.

6.1 Arquitetura do Protótipo de TV Interativa

A arquitetura do servidor (ilustrada na Figura 3) foi originalmente modelada por Santos Jr. (2001) prevendo-se o suporte à descrição de mídias e à consciência de contexto, e está atualmente dividida em: Serviços; um Servidor de Objetos Multimídia (SOM) e um Servidor de Descrições Multimídia (SDM); e um Gerenciador de Serviços que age como interface entre os serviços e os servidores.

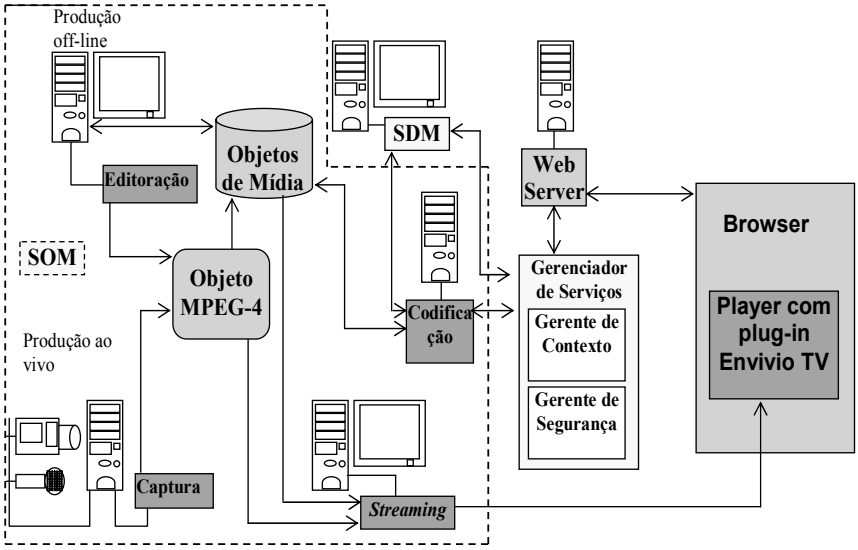

Fig. 3 – Arquitetura do Protótipo TVI

As funções do SOM são, basicamente, codificar, armazenar, e entregar programas de TV Interativa, além de objetos e *streams* de mídia no formato MPEG-4. A produção de conteúdo pode ser feita ao vivo ou *off-line*. Em ambos os casos os objetos MPEG-4 resultantes são armazenados em um repositório. A transmissão desse conteúdo é realizada tanto através de redes cabeadas (*wired*) quanto através de redes sem fio e o acesso pode ser realizado através de dispositivos com alto poder de processamento (como um PC) quanto por dispositivos móveis (como Pocket PCs).

O Gerenciador de Serviços coordena as requisições dos usuários por apresentações de programas e por buscas. Além disso, fornece uma API (*Application Program Interface*) em linguagem Java para que desenvolvedores de aplicações tenham acesso a serviços como codificação MPEG-4, *streaming* de programas, buscas, monitoramento de políticas de segurança e geração automática de programas personalizados (Goularte, 2003). Os serviços de codificação e de *streaming* utilizam, respectivamente, o *Envivio Encoding Station*™ (Envivio 2003a) e o *Envivio Streaming Server*™ (Envivio 2003b). A recepção e exibição dos programas são realizadas através da ferramenta *Envivio TV*™ (Envivio 2003c), na forma de *plug-in* MPEG-4 para alguns *players* mais populares (RealOne, QuickTime e Windows Media).

O SDM é responsável por gerar descrições MPEG-7 sobre programas de TV Interativa e sobre os objetos de mídia armazenados no SOM. As descrições armazenadas no SDM são instâncias XML do modelo de programa para TV interativa, desenvolvido por Faria et al. (2001), e do modelo para representação de objetos de mídia desenvolvido por Goularte e Moreira (2002). O SDM é uma implementação de um *parser* MPEG-7 feita em Java através da API Apache Xerces [2]. O SDM recebe como entrada os esquemas de descrição e os dados sobre o programa ou objeto que se deseja descrever. A saída é uma descrição MPEG-7 que é armazenada em uma base Oracle XDB [3].

As informações sobre os objetos de mídia (programas de TV, por exemplo) são obtidas pelo Gerenciador de Serviços sempre que a codificação de um objeto é realizada. Algumas informações podem ser extraídas automaticamente (como localização, tamanho do arquivo e tipo do arquivo) e outras devem ser fornecidas pelo autor, como quais são os segmentos e quadros de vídeo de interesse e algumas informações contextuais. O modo de representar as informações necessárias para descrever um objeto qualquer está especificado nos esquemas dos modelos, independentemente de os valores para tais informações poderem ser extraídos automaticamente ou não.

6.2 Privacidade e sigilo no Projeto TVI

Como o projeto TVI tem como objetivo adaptar as transmissões de multimídia para diferentes contextos de aplicação, infra-estrutura e preferências de usuários, diversas informações devem ser capturadas, processadas e armazenadas.

As questões críticas de segurança e privacidade envolvidas em computação ubíqua foram descritas em detalhes no Capítulo 5. Os objetivos de pesquisas adicionais em desenvolvimento no projeto TVI são de prover capacidades adicionais de gerenciamento de informações de contexto e de perfis de segurança e privacidade (Santos, 2003; Milagres, 2003), como já foi ilustrado na Figura 3.

A seguir serão descritos os padrões do W3C (*World Wide Web Consortium*) em aplicação no projeto TVI para esses fins e como estão sendo utilizados para controle de informações de contexto e de perfis de segurança e privacidade no TVI.

[2] http://xml.apache.org/xerces-j/
[3] http://oracle.xmlspy.com/

6.3 CC/PP

Composite Capabilities/Preference Profiles (CC/PP) [4] é um *framework* proposto pelo W3C (*World Wide Web Consortium*)[5]. Um perfil CC/PP é uma descrição das capacidades de um dispositivo ou das preferências de um usuário que podem ser usadas para adaptar a apresentação de conteúdo de acordo com o dispositivo utilizado ou com as preferências do usuário.

Baseado em RDF (Resource Description Framework) [6], um perfil CC/PP contém um determinado número de componentes (*Hardware*, Sistema Operacional ou Aplicação) e cada componente possui pelo menos um ou mais atributos (versão, nome, etc). O conjunto de atributos de componentes e seus valores constituem um vocabulário utilizado para validação do perfil CC/PP. Um exemplo de perfil é mostrado a seguir. As linhas 7 e 8 apresentam os atributos referentes à resolução (*displayWidth* e *displayHeight*) suportada pelo dispositivo para a apresentação de conteúdo.

```
1 <?xml version="1.0"?>
2 <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
xmlns:ccpp="http://www.w3.org/2002/11/08-ccpp-schema#"
xmlns:ex="http://www.example.com/schema#">
3 <rdf:Description rdf:about="http://www.example.com/profile#MyProfile">
4 <ccpp:component>
5   <rdf:Description
rdf:about="http://www.algumsite.com.br/profile#TerminalHardware">
6        <rdf:type
rdf:resource="http://www.algumsite.com.br/schema#HardwarePlatform" />
7  <ex:displayWidth>320</ex:displayWidth>
8  <ex:displayHeight>200</ex:displayHeight>
9   </rdf:Description>
10 </ccpp:component>
11 ...
12 </rdf:Description>
13 </rdf:RDF>
```

A troca de perfis CC/PP pode ser efetuada por meio do protocolo HTTP (*Hyper Text Transfer Protocol*). Um programa cliente envia uma requisição HTTP a um servidor *proxy* intermediário. Este por sua vez pode impor restrições ao tipo de conteúdo que pode ser acessado ou pode adaptar outras formas de conteúdo à capacidades do cliente que não foram mencionadas. O *proxy* estende, portanto o perfil CC/PP com possíveis restrições ou adaptações e o envia ao chamado "servidor de origem" (*origin server*), responsável pela geração ou seleção do conteúdo suportado pelo dispositivo do usuário. O *origin server*, então recebe a requisição, a interpreta, seleciona e/ou gera o conteúdo requisitado e o envia de volta ao *proxy*, que por sua vez entrega o conteúdo ao cliente.

O *framework* CC/PP é utilizado no projeto TVI para prover não somente informações relacionadas às características do dispositivo, mas também informações do estado da rede de comunicação. É importante destacar que a especificação CC/PP não abrange aspectos de segurança e privacidade. Portanto, outros artifícios devem ser utilizados para suprir esta abordagem. A Seção 6.3 apresenta o padrão P3P, uma das alternativas para notificação de políticas de segurança e privacidade e a Seção 6.4 apresenta a linguagem EPAL de definição de políticas de privacidade, usadas no presente trabalho.

[4] http://www.w3c.org/Mobile/CCPP
[5] http://www.w3c.org
[6] http://www.w3c.org/RDF/

6.3 P3P

O padrão da W3C, P3P (Projeto para Plataforma de Preferências de Privacidade *ou Platform for Privacy Preferences Project*) [7] permite que *sites* divulguem suas práticas de privacidade em formato padronizado, de modo que seja possível a interpretação destas normas por agentes de softwares heterogêneos bem como por seus usuários.

Classificada como uma recomendação pelo W3C em Abril de 2002, a versão 1.0 do padrão P3P tem como objetivo principal automatizar a tomada de decisão com relação às preferências dos usuários, facilitando a garantia de níveis de privacidade aceitáveis e permitindo que as aplicações troquem informações pessoais somente dentro do especificado por seus proprietários ou responsáveis. Assim, o controle automatizado das preferências de privacidade evita, por exemplo, que o usuário deva conhecer a política de privacidade de cada *site* ou serviço que ele utiliza.

Utilizando o P3P, é possível formalizar em XML [8] as regras da política de privacidade de um *site* ou serviço disponibilizado através da Internet. Um exemplo de código XML de uma política de privacidade em P3P é exibido a seguir: (`http://algumsite.com.br/w3c/p3p.xml`)

```
1 <META xmlns="http://www.w3.org/2002/01/P3Pv1">
2 <POLICY-REFERENCES>
3     <POLICY-REF
about="http://algumsite.com.br/support/policy.p3p#PrivacyMain">
4       <INCLUDE>/*</INCLUDE>
5       <COOKIE-INCLUDE/>
6     </POLICY-REF>
7 </POLICY-REFERENCES>
8 </META>
```

Neste caso, a política P3P armazenada em um arquivo XML indica que está destinada a todo o conteúdo do *site* o qual faz parte (linha 4). A referência à política completa é feita na linha 3 e algumas partes são destacadas a seguir: (`http://algumsite.com.br/support/policy.p3p#PrivacyMain`)

```
1 <?xml version="1.0"?>
2 <POLICIES xmlns="http://www.w3.org/2002/01/P3Pv1">
...
8 <POLICY discuri="http://algumsite.com.br/support/privacypolicy.htm"
opturi="http://algumsite.com.br/support/privacypolicy.htm"
...
11     name="PrivacyMain">
12     <!-- Descricao da entidade responsavel por essa declaracao de
privacidade. -->
13     <ENTITY>
14     <DATA-GROUP>
15 <DATA ref="#business.contact-info.telecom.telephone.number">(123)
ALGUMSITE</DATA>
16 <DATA ref="#business.contact-
info.online.email">privacy@algumsite.com.br</DATA>
17 <DATA ref="#business.contact-
info.online.uri">http://algumsite.com.br</DATA>
18 <DATA ref="#business.contact-info.postal.organization">ALGUMSITE
Ltda.</DATA>
...
```

Neste exemplo em destaque para o TVI, a empresa em destaque que é provedora de serviços de TV interativa é denominada “Algumsite.com.br”, que declara sua política de

[7] http://www.w3c.org/P3P/
[8] http://www.w3c.org/XML/

privacidade de acordo com o padrão P3P e na linha 8 em formato texto, como é feito tradicionalmente no *site* institucional da empresa.

Devem-se declarar no mesmo documento XML as ações que podem ser executadas sobre as informações dos clientes que utilizam o serviço de *streaming* disponibilizado pela empresa em questão.

```
48 <CONSEQUENCE>
49 O servidor web da empresa coleta os logs
50 que contem as informações.</CONSEQUENCE>
...
53 <PURPOSE><admin/><current/><develop/></PURPOSE>
...
56     <RECIPIENT><ours/></RECIPIENT>
...
59     <RETENTION><indefinitely/></RETENTION>
```

Na política de privacidade devem ser declaradas todas as informações do ciclo de uso da informação, por exemplo, a forma de obtenção, as razões, a classificação dessas informações dentro da empresa e a forma de descarte, caso se aplique (linhas 53, 56 e 59).

6.4 EPAL

EPAL (*Enterprise Privacy Authorization*) [9] é uma linguagem formal para definição de políticas de privacidade com objetivo de controle de acesso a informações por meio de regras detalhadas baseadas em modelos de dados e autenticação de usuários.

Em uma política EPAL são definidas hierarquias de categorias de dados (data category), de usuários (user category) e de finalidades (purposes) e conjuntos de ações (actions), obrigações e condições (obligations). Nas categorias de dados são definidas as diferentes informações coletadas de acordo com suas perspectivas de privacidade (por exemplo, informações de contato ou pessoais). Os usuários e seus grupos são definidos em categorias de usuários de acordo com os dados coletados os quais eles possuem acesso e no modelo de finalidades são definidos os serviços associados a cada dado coletado (por exemplo, para processamento de solicitações de clientes ou para auditorias detalhadas).

Em modelos de ações são definidos como os dados são utilizados (por exemplo, para leitura ou divulgação) e em obrigações são definidas as ações que devem ser tomadas pelo sistema que controla os dados (por exemplo, remoção após 30 dias ou retenção indefinida).

As condições são expressões lógicas que avaliam o contexto do sistema de acordo com regras definidas (por exemplo, “os usuários devem ter idade superior a 18 anos” ou “os usuários devem estar localizados fisicamente dentro da empresa”). Esses elementos, que compõem o vocabulário da política de privacidade, são então usados para formular regras de controle de privacidade para, por exemplo, permitir ou negar ações de categorias de usuários em categorias de dados para determinadas ações sob condições e obrigações definidas.

Após a definição da política de privacidade do sistema TVI, foram definidos o vocabulário e a política de privacidade em EPAL. Na Tabela 1 são destacados os elementos do vocabulário EPAL do sistema TVI, que serão explanados a seguir:

[9] http://www.zurich.ibm.com/security/enterprise-privacy/epal

User category	Data category	Purposes	Action	Containers	Obligation
Client Administrator	Audio stream Video stream Control	Research Optimization	Access	Adult Location Service level	Retention

Tabela 1 – Elementos do vocabulário EPAL do sistema TVI

- *User category*: categorias de usuários do sistema TVI (cliente convencional e administrador do sistema;
- *Data category*: tipos de tráfego de dados a serem analisados (*streams* de áudio e vídeo e informações de controle e navegação);
- *Purposes*: razões para coleta e análise de cada informação pessoal (para fins de pesquisa ou para otimização e personalização de serviços);
- *Action*: ação efetuada sobre os dados coletados;
- *Containers*: conjunto de atributos dos usuários e dispositivos que devem ser coletadas para as razões especificadas (idade do cliente, localização física e nível de serviço especificado em Contrato de Nível de Serviço (SLA) entre as partes);
- *Obligation*: condições e obrigações a serem estabelecidas pelo usuário das informações coletadas (tempo de retenção dos dados).

O vocabulário e a política de privacidade nos padrões EPAL são estruturadas em formato XML, para posterior validação nas aplicações que disponibilizam os serviços de acesso de TV interativa TVI.

A seguir é destacada uma regra definida em EPAL para controle de acesso às informações capturadas pelo sistema TVI.

```
1 <condition id="isadult">
2...
3    <xacml:Condition
FunctionId="urn:oasis:names:tc:xacml:1.0:function:any-of"
xmlns:xacml="urn:oasis:names:tc:xacml:1.0:policy">
4       <xacml:Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:IS
EQUAL TO">
5          <xacml:EnvironmentAttributeDesignator
AttributeId="urn:ibm:epal:attribute:context_container:adult"
DataType="http://www.w3.org/2001/XMLSchema#boolean"/>
6       </xacml:Apply>
...
7    </xacml:Condition>
8 </condition>
```

A política de privacidade em EPAL contém basicamente duas seções, além da identificação da entidade emissora da política, que inicia o documento. A primeira seção, listada acima, descreve as condições básicas para acesso. Neste caso, a condição analisada é a maioridade do cliente identificado no sistema, que pode ter informações direcionadas ao conteúdo adulto, por exemplo (linhas 4 e 5).

Após a definição da condição, usando os atributos do vocabulário, deve ser definida a terceira seção da política de privacidade EPAL, a regra de acesso:

```
1 <rule id="basic_access" ruling="allow">
2    <short-description language="en">Access rule</short-description>
3    <long-description language="en">Basic TVI system access rule</long-
description>
4    <user-category refid="client"/>
5    <data-category refid="audiostream"/>
6    <data-category refid="videostream"/>
7    <data-category refid="control"/>
8    <purpose refid="optimization"/>
9    <action refid="access"/>
10   <condition refid="isadult"/>
11   <obligation refid="retention"/>
12 </rule>
```

Neste caso, a regra deve obedecer à condição de maioridade (linha 9), permitindo o acesso (linha 1) de um usuário da categoria *client* (linha 4) aos conteúdos em áudio, vídeo e navegação e otimização do sistema TVI (respectivamente linhas 5, 6 e 7). É importante destacar que a regra padrão do sistema é negar qualquer tipo de acesso e, através da política de privacidade, as restrições a acesso devem ser feitas.

Atualmente na versão 1.1, a linguagem EPAL está em processo de avaliação do W3C, tendo sido submetida para tal pela IBM Research em Novembro de 2003.

É válido destacar também que os excertos da política de privacidade do sistema TVI explanados nesta seção estão em desenvolvimento para aplicações em diversos cenários de testes que estão em desenvolvimento. A integração do projeto TVI desenvolvido e detalhado na Seção 6.1 em conjunto com trabalhos em desenvolvimento para gerenciamento de informações de contexto, de segurança e privacidade será detalhada em publicações futuras (Milagres, 2003; Santos, 2003).

7 CONCLUSÕES E TRABALHOS EM DESENVOLVIMENTO

São cada vez destaque na mídia a necessidade de segurança e a falta de privacidade que é causada pelo uso cada vez mais transparente de tecnologia interconectada por redes em nosso cotidiano.

Este artigo teve como objetivo apresentar os conceitos envolvidos na área de pesquisas de computação ubíqua e contextualizá-los com a necessidade real e crescente de segurança. Com uma revisão das principais considerações apresentadas por pesquisadores da área de segurança da informação e de computação ubíqua, os pesquisadores envolvidos no projeto TVI têm como objetivo assegurar as informações de contexto que são gerenciadas no sistema de TV interativa que possui capacidades de mobilidade e ciência de contexto para personalização de conteúdo.

Foram apresentados os padrões e recomendações W3C aplicados neste projeto e como o uso integrado de gerenciamento de preferências de usuário e perfis de segurança deve garantir um baixo nível de risco para informações pessoais no uso do TVI. Resultados detalhados de testes integrados entre as características de gerenciamento de informações de contexto e de segurança serão apresentados oportunamente em trabalhos futuros.

AGRADECIMENTOS

Os autores agradecem o apoio financeiro das agências de fomento de pesquisas CAPES, CNPq e FAPESP, que financiam individualmente cada um dos projetos envolvidos com o sistema TVI.

REFERÊNCIAS BIBLIOGRÁFICAS

ABOWD, G. D. *Classroom 2000: an experiment with the instrumentation of a living educational environment*. In: IBM Systems Journal, 1999, v. 38, n. 4, pp. 508–530.

ABOWD, G. D., MYNATT, E. D. *Charting past, present, and future research in ubiquitous computing*. In: ACM Transactions on Computer-Human Interaction (TOCHI), 2000, v. 7, n. 1, pp. 29–58.

ABOWD, G. D., MYNATT, E. D., RODDEN, T. *The Human Experience*. In: Pervasive Computing, 2002, v. 1, n. 1, pp. 48–57.

BISHOP, M. *What is Computer Security?* In: IEEE Security & Privacy, v.1, n.1, Janeiro-Fevereiro, 2003. pp. 67–69.

DEY, A. K., ABOWD, G. D. *Towards a Better Understanding of Context and Context-awareness*. Gvu technical report GIT-GVU-99-22, College of Computing, Georgia Institute of Technology, 1999.

ENVIVIO Inc. *Envivio MPEG-4 Encoding Station Software – Overview*. 2003 http://www.envivio.com/products/ees.html.

ENVIVIO Inc. *EnvivioTV MPEG-4 Player – Overview*. 2003. http://www.envivio.com/products/etv/

FARIA, G. B., SANTOS JR, J. B., GOULARTE, R., MOREIRA, E. S. *Uso de perfis em aplicações de televisão interativa conscientes de contexto*. In: Anais do SBMídia 2001 - VII Simpósio Brasileiro de Sistemas Multimídia e Hipermídia, Outubro, 2001. pp. 139–154.

GARFINKEL, S., SCHWARTZ, A., SPAFFORD, Gene. *Practical Unix & Internet Security*. Ed. 3, O'Reilly, 2003.

GOULARTE, R., MOREIRA, E. S. *Representação de objetos de mídia para aplicações conscientes de contexto em TV interativa*. In: Anais do SBMídia 2002 - VIII Simpósio Brasileiro de Sistemas Multimídia e Hipermídia, Outubro, 2002. pp. 150–165.

GOULARTE, R., SANTOS, R. F., MILAGRES, F. G., MOREIRA, E. S. *Um Serviço de personalização automática de conteúdo para TV interativa*. In: Anais do WebMidia 2003 - IX Simpósio Brasileiro de Sistemas Multimídia e Web, Salvador, Novembro, 2003, v.2, n.1, pp. 547-550.

MILAGRES, F. G. *Segurança Baseada em Informações de Contexto para Redes Sem Fio.* Dissertação de Qualificação de Mestrado. Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo. São Carlos, 2003.

MÓDULO Security Solutions S. A. *Nona Pesquisa Nacional de Segurança da Informação*. Rio de Janeiro: Setembro, 2003. http://www.modulo.com.br/pdf/nona_pesquisa_modulo.pdf

PASCOE, J. *Adding generic contextual capabilities to wearable computers*. In: International Symposium on Wearable Computers, 1998, pp. 92–99.

PIMENTEL, M. G. C., ABOWD, G. D., and Ishiguro, Y. *Linking by interacting: a paradigm for authoring hypertext*. In: ACM Conference on Hypertext, 2000, pp. 39–48.

PIMENTEL, M. G. C., KERIMBAEV, Y. I. B., ABOWD, G. D., GUZDIAL, M. *Supporting Long-term Educational Activities Through Dynamic Web Interfaces*. In: Interacting With Computers Journal, 2001, v. 13, pp. 353–374.

RICHARDSON, R. *CSI/FBI Computer Crime and Security Survey*. Computer Security Institute, v.8, 2003. http://www.gocsi.com

RYAN, N. S., PASCOE, J., MORSE, D. R. *Enhanced reality fieldwork: the context-aware archaeological assistant*. In: Gaffney, V., van Leusen, M., and Exxon, S., editors, Computer Applications in Archaeology, British Archaeological Reports, Oxford. Tempus Reparatum, 1997.

SANTOS JR., J. B., GOULARTE, R., MOREIRA, E. S., FARIA, G. B. *The Modeling of Structured Context-Aware Interactive Environments*. In: Transactions of the SDPS Journal of Integrated Design and Process Science, v. 5, n. 4, Dezembro, 2001. pp. 77–93.

SANTOS, R. F. *Gerenciamento de Informações de Contexto para Ambientes Móveis.* Dissertação de Qualificação de Mestrado. Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo. São Carlos, 2003.

SCHILIT, B., THEIMER, M. *Disseminating active map information to mobile hosts*. In: IEEE Network, v.8, n.5, 1994. pp. 22–32.

SCHNEIER, B. *Beyond Fear. Thinking Sensibly About Security in an Uncertain World.* Copernicus Books, Ed. 1. 2003.

SCHNEIER, B. *Secrets and Lies: Digital Security in a Networked World.* John Wiley & Sons, Ed. 1. 2000.

STAJANO, F., ANDERSON, R. J. *The Resurrecting Duckling: Security Issues for Ad Hoc Wireless Networks*. In: Proceedings of the Seventh Security Protocols Workshop – Lecture Notes in Computer Science, v.1796, Springer-Verlag, 1999. pp. 172–182.

STAJANO, Frank. *Security for Ubiquitous Computing*. John Wiley & Sons, Ed. 1, 2002.

STAJANO, Frank. *The Resurrecting Duckling - What Next?* In: Proceedings of the Eighth Security Protocols Workshop – Lecture Notes in Computer Science, v.2133, Springer-Verlag, 2001. pp. 204–214.

TIPTON, H. F., KRAUSE, M. *Information Security Management Handbook*. CRC Press LLC, 2002.

WEISER, M. *Some Computer Science Issues in Ubiquitous Computing*. In: Communications of the ACM, 1993, v. 6, n.7, pp. 75–84.

WEISER, M. *The Computer for the 21st Century*. In: Scientific American, 1991, v. 265, n. 3, pp. 94–104.

WHITMAN, M. E. *Enemy at the Gate: Threats to Information Security*. In: Communications of the ACM, v.46, n.8, Agosto, 2003. pp. 91–95.