Universidade de São Paulo
Instituto de Ciências Matemáticas e de Computação
Departamento de Ciências de Computação e Estatística

Implementação de Segurança no Sistema DEEPSIA

Francisco Gomes Milagres

Prof. Dr. Edson dos Santos Moreira
Orientador

Dezembro de 2002

Monografia apresentada ao Departamento de Ciências de Computação e Estatística do ICMC-USP, como parte dos requisitos para o Exame Final da disciplina SCE-192 – Projeto de Graduação II.

Resumo

O objetivo do DEEPSIA (*Dynamic On-line Internet Purchasing System Based on Intelligent Agents*) é desenvolver uma infra-estrutura computacional que auxilie empresas como compradoras em processos de *e-procurement* no comércio eletrônico, utilizando um sistema multi-agentes. Por ser um sistema que utiliza a Internet e lida com informações críticas, um alto nível de segurança é necessário. O objetivo deste trabalho é, utilizando análises de segurança e modelo proposto em trabalho anterior (Milagres, 2002b), demonstrar as implementações de segurança em desenvolvimento na atual arquitetura do Sistema DEEPSIA.

Agradecimentos

Agradeço a Deus pela força em todos os momentos durante toda a minha graduação em São Carlos, no ICMC – USP.

Agradeço imensamente a Andréa.

Obrigado aos meus pais e irmãos.

Agradeço a meu orientador, Prof. Edson Moreira, pelo incentivo e pelo conhecimento compartilhado desde o início de minha graduação, bem como a todos os professores e funcionários do ICMC que colaboraram, direta ou indiretamente, para minha formação.

Obrigado aos amigos do Laboratório Intermídia pela ajuda e troca de conhecimentos (e festas!) compartilhadas desde a minha entrada no grupo.

Agradecimentos também ao CNPq por ter financiado a minha pesquisa no Projeto DEEPSIA, no qual está inserido este trabalho.

Sumário

1 Introdução

O projeto DEEPSIA (*Dynamic on-linE IntErnet Purchasing System based on Intelligent Agents*)[1] (DEEPSIA – IST-1999-20483) foi desenvolvido por um consórcio no âmbito do programa europeu de pesquisa denominado *Information Society Technologies* (IST), formado por empresas e institutos de pesquisa de vários países, dentre eles: empresa *ComArch* (Polônia), *Universidade Nova de Lisboa* – UNINOVA (Portugal), *Université Libre de Bruxelles* (Bélgica), *University of Sunderland* (Inglaterra), empresa *Zeus* (Grécia) e empresa *Atlante* (Espanha). O Brasil é o colaborador externo à União Européia do projeto DEEPSIA, sendo representado pelo ICMC – Instituto de Ciências Matemáticas e de Computação [2] e pelo NUMA – Núcleo de Manufatura Avançada da Escola de Engenharia de São Carlos [3] e fomentado pelo CNPq (Conselho Nacional de Desenvolvimento Científico e Tecnológico) (DEEPSIA – CNPq-68.0236/01-2). A participação do Brasil está ligada a uma parceria direta com a UNINOVA e se encerrará oficialmente em Março de 2003, apesar do projeto DEEPSIA já ter sido concluído oficialmente na Europa em Outubro de 2002.

O objetivo do DEEPSIA é desenvolver uma infra-estrutura computacional que auxilie a atuação das Pequenas e Médias Empresas (PMEs) como compradoras no comércio eletrônico em processos de *e-procurement.* Esta infra-estrutura deve estar disponível para a entidade (pessoa ou departamento) responsável pelas compras e deve ser adaptável aos requisitos particulares da empresa em questão. Os modelos tradicionais de comércio eletrônico têm como característica focarem-se nas PMEs como fornecedores, normalmente dentro de centros comerciais ou mercados virtuais. No entanto, as PMEs são também compradoras de bens e serviços.

A infra-estrutura computacional em desenvolvimento pelo DEEPSIA visa tornar o processo de compra mais eficiente em termos de tempo e custo, fornecendo uma interface amigável baseada em um catálogo de compras personalizado que será automaticamente atualizado com a informação sobre os produtos, informação essa obtida dos portais eletrônicos existentes na Internet ou diretamente de bancos de dados das empresas parceiras do sistema. Este catálogo personalizado fornecerá ao comprador um conjunto de ofertas apropriadas em termos de qualidade, diversidade e aplicabilidade.

---

[1] DEEPSIA *Consortium web site:* http://www.deepsia.com

[2] Instituto de Ciências Matemáticas e de Computação (ICMC): http://www.icmc.usp.br

[3] Núcleo de Manufatura Avançada da Escola de Engenharia de São Carlos (NUMA): http://www.numa.org.br

O processo de busca e processamento de informação no sistema DEEPSIA é suportado por um conjunto de agentes inteligentes que analisam informações sobre produtos na *web* e processam seus resultados, com o objetivo de obter informações referentes aos produtos vendidos como, por exemplo, custo, descrição, etc. (Garção, 2001).

No âmbito do projeto DEEPSIA, a Universidade de São Paulo (USP) contribui em duas áreas distintas: a área sócio-econômica e a de desenvolvimento da infra-estrutura tecnológica do DEEPSIA.

2 Objetivos e Resultados Esperados

O objetivo deste trabalho é, utilizando resultados de análise de segurança já realizada (Milagres, 2002b), apresentar as implementações e estudos em desenvolvimento na atual arquitetura do sistema DEEPSIA. Para mais informações sobre as pesquisas em andamento no grupo Intermídia, vide Anexo A ou visite o site do projeto DEEPSIA no Brasil, http://www.deepsia.com/br

Dentre os resultados esperados, pode-se listar:

- Apresentação do atual cenário nacional e internacional de segurança da informação, visando à implementação de melhorias em sistemas de comércio eletrônico, por exemplo, como o DEEPSIA;
- Definição de novas ferramentas a serem utilizadas em futuras versões do sistema DEEPSIA, como a *Web* Semântica, de modo que este tenha como segurança uma característica de projeto;
- Estudo e definição de um padrão de gestão de segurança da informação a ser utilizado para modelagem de sistemas seguros como o DEEPSIA, por exemplo.

A seguir é apresentada a organização deste trabalho:

No capítulo 3 será feita uma descrição da arquitetura do sistema DEEPSIA, destacando o funcionamento de seus agentes e da forma de comunicação entre eles. No capítulo 4 serão apresentadas as implementações feitas para a segurança na comunicação dos agentes em linguagem KQML. No capítulo 5 será apresentado o conceito de *Web* Semântica e de representação de informação com semântica em documentos hipertexto.

No capítulo 6 é apresentado um breve cenário de segurança da informação no Brasil, com as pesquisas mais recentes realizadas no país e também no exterior e no capítulo 7, são apresentados padrões para gestão segura em sistemas de tecnologia da informação.

No capítulo 8 são apresentados os resultados parciais do trabalho no projeto DEEPSIA, as publicações e apresentações relevantes dos resultados e os temas que ainda estarão em desenvolvimento até o fim do projeto DEEPSIA.

No capítulo 9 são listadas as referências deste texto e no anexo A é apresentado um breve histórico do grupo de pesquisas Intermídia.

3 O Sistema DEEPSIA

Um dos mais importantes tipos de serviços na *web* atualmente relaciona-se ao desenvolvimento de sistemas on-line aplicados a negócios, ou *e-business*. A atual onda de globalização da economia encontrou na Internet um meio apropriado para a divulgação e comercialização de bens e serviços. Nichos de mercado, antes inacessíveis por limitações geográficas, agora podem ser alcançados pela vasta abrangência da “rede mundial de computadores”.

A fim de solucionar o problema da divulgação de negócios, muitos portais ou *market places* começaram a surgir. Tais portais estabelecem associações com *sites* de venda, mediante contrato e possibilitam a realização pelos usuários da Internet da busca por produtos oferecidos naquele domínio restrito. Pelo fato de divulgarem os seus produtos, torna se um bom negócio para os fornecedores de bens e serviços.

Porém, tal solução não satisfaz todas as necessidades do usuário, pois a principal intenção de uma pessoa ou empresa, ao buscar por ofertas de bens e serviços é avaliar qual negócio oferecido melhor lhe favorece em uma relação custo e benefício. A limitação do domínio na busca reduz as opções de escolha, constituindo a desvantagem do comprador em relação ao fornecedor nesse tipo de negócio proposto pelos *market places*.

Sistemas como o DEEPSIA visam apresentar uma solução mais adequada ao comprador, através de processos de classificação de páginas *Web* em um catálogo, que representa uma ontologia de produtos à venda. A correta extração de informação de produtos à venda depende de métodos otimizados de recuperação e classificação de conteúdos das páginas na Internet.

No sistema DEEPSIA, a busca e classificação de produtos em páginas da Web são feitas por três agentes distintos e com papéis bem definidos. O *Web Crawler Agent* busca páginas com produtos a venda, o *Miner Agent* extrai as informações sobre os produtos nas páginas e o *Dynamic Catalogue* armazena as informações sobre os produtos. Há basicamente dois métodos de busca independentes que podem ser adotados, de acordo com a escolha dos parceiros ou do cenário onde o sistema é aplicado. A busca direta é feita diretamente no catálogo das empresas parceiras e a busca autônoma, que é feita em sites na Internet, utilizando recursos de busca e classificação de informação de forma inteligente.

A Figura 1 ilustra como ocorre a integração entre os principais agentes do DEEPSIA, que formam o Sistema Multi-Agentes e que se integram com os catálogos das empresas parceiras no projeto. É importante destacar que o foco de trabalho da equipe brasileira no consórcio

DEEPSIA é na busca autônoma e não na busca direta nos catálogos dos parceiros cadastrados pelo projeto:

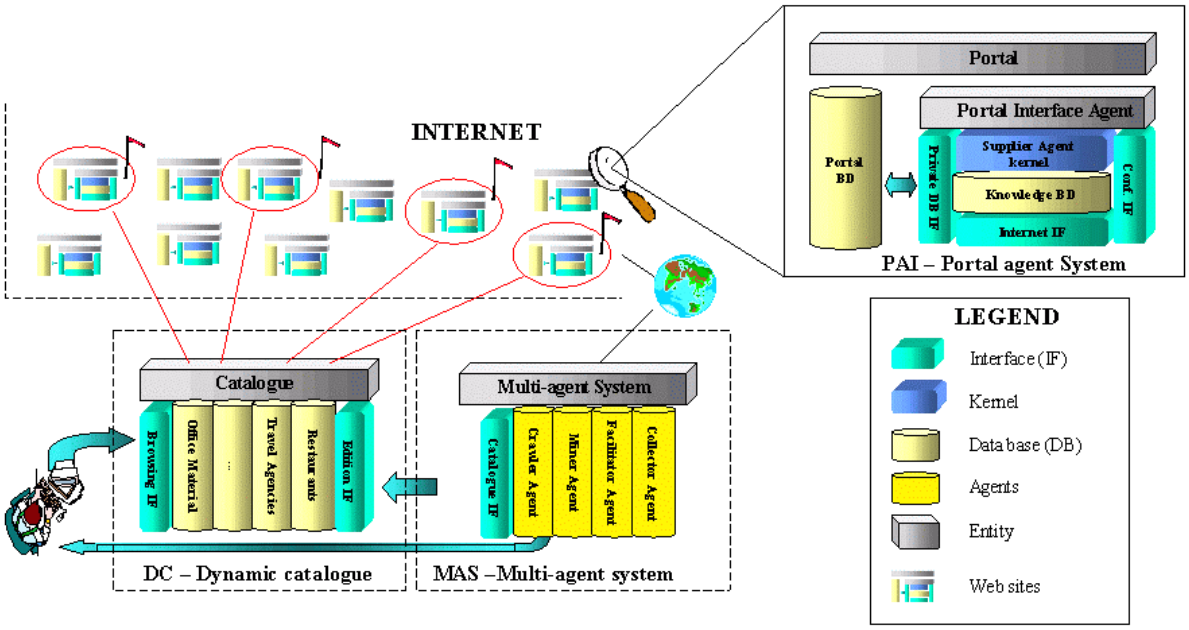

Figura 1: Os componentes da arquitetura DEEPSIA (Garção, 2002)

- *Portal Interface Agent* (PIA): Cria uma interface privilegiada entre os portais da *Web* e o *Multi-Agent System* (MAS). O agente atuará como um facilitador ao acesso a dados contidos nos *sites* e bancos de dados de fornecedores, permitindo um acesso privilegiado e direto às informações dos parceiros. Sua utilização opcional pelos fornecedores garante que as informações sobre seus produtos serão acessadas pelo sistema DEEPSIA, independente dos resultados das buscas efetuadas pelo *Web Crawler Agent* em sites na Internet. A empresa Atlante (Espanha) detém a responsabilidade de seu desenvolvimento e o PIA não foi foco de desenvolvimento pela equipe brasileira;
- *Dynamic Catalogue* (DC): Consistirá da interface do usuário e será responsável pela manutenção e apresentação dos dados coletados pelos agentes contatados, com base nas preferências do usuário fornecidas. Além de tais dados, o sistema possibilitará o acesso a informações de *sites* visitados, e a configuração da ontologia (representando o perfil individual da expectativa de compra) pelo usuário. A empresa ComArch detém a responsabilidade de seu desenvolvimento e este catálogo atualmente está recebendo adições na equipe brasileira, com objetivo de inserção de características que permitam a mineração de dados nas informações armazenadas no catálogo;

- *Multi-Agent System* (MAS): Sistema autônomo para coleta de dados e um processo semi-automático de atualização do catálogo, composto de um conjunto de agentes, com tarefas específicas. A responsabilidade de seu desenvolvimento é da UNINOVA e é o foco principal de trabalho do Brasil, através da USP, no consórcio DEEPSIA. Os módulos internos deste sistema, que caracterizam os tipos especialistas de agentes, são descritos como:

    - *Web Crawler Agent* (WCA): Busca por páginas *Web* com dados de interesse pelo usuário, baseando-se em um processo recursivo a partir de um ponto inicial, sendo previamente treinado em um processo *off-line*. Executa a primeira seleção e classificação das páginas, separando em *páginas de venda* e *páginas que não são de vendas*, para posterior processamento do agente *Miner;*

    - *Miner Agent* (MA): De posse das páginas de ofertas de produtos, o *Miner Agent* se encarrega de obter informações sobre o tipo de produto que está sendo vendido na página e também de classificar este produto segundo uma ontologia definida;

    - *Human Agent* (HA*):* É a interface do usuário do sistema e integra o DEEPSIA para validação de informações sobre produtos e suas classificações, enviando estas informações para o *Facilitator Agent,* e possibilitando também a adição de *sites* pelo usuário ao *Miner*. É o único agente a estabelecer contato direto com o usuário, já que os demais serão executados através da interface com o catálogo.

    - *Facilitator Agent* (FA): Delimita a interface entre o catálogo e o conhecimento obtido pelos agentes *Miner* ou *Collector*. Possibilitará a configuração da periodicidade da produção e atualização de dados para o catálogo, com objetivos de obtenção de dados para armazenamento e futura mineração.

    - *Collector Agent* (CA): É a interface direta com o banco de dados que mantém os sites inscritos pelo PIA, para acesso privilegiado às bases de dados dos parceiros do sistema DEEPSIA. Ele recebe mensagens do catálogo com solicitações por atualização e mantém a relação de usuários on-line, possibilitando também o acesso a informação de fornecedores inscritos.

No capítulo seguinte são apresentadas as implementações realizadas na plataforma de agentes JATLite modeladas por Milagres (2002b).

4 Implementação S-KQML

Após análise da segurança do sistema de multi-agentes do DEEPSIA (Milagres, 2002b; 2002c; 2002d), a etapa que se seguiu foi a implementação do modelo proposto na plataforma de agentes JATLite (Jeon *et al*, 2000), que foi a escolhida pelo projeto para a base de comunicação entre os agentes móveis em linguagem KQML.

Dentre as principais características que, de acordo com a análise realizada, devem ser garantidas com esta implementação, pode-se listar:

- Privacidade: deve ser garantida a privacidade das informações trafegadas nos agentes e nas plataformas dos agentes móveis;
- Sigilo: deve ser garantido o sigilo das partes em comunicação através dos agentes móveis;
- Integridade: deve ser garantida a integridade da informação em trânsito através dos agentes móveis do sistema multi-agentes;
- Autenticação: deve ser disponibilizado um sistema de autenticação dos agentes que se comunicam através das plataformas de agentes do sistema DEEPSIA, de modo a evitar acesso não autorizado aos recursos das plataformas de agentes;
- Controle de Acesso: o controle de acesso dos agentes a cada plataforma de agentes é feito pela própria plataforma, neste caso, a JATLite. Esta característica de segurança não é tratada diretamente neste projeto já que é inerente à definição da plataforma de agentes.
- Disponibilidade: a disponibilidade do serviço de agentes através das plataformas também é uma característica inerente das próprias plataformas, não sendo escopo deste trabalho tratar este item.

Para tal análise e considerando as quatro primeiras características de segurança dentre as listadas anteriormente (privacidade, sigilo, integridade e autenticação), o modelo utilizado para descrever as vulnerabilidades é o da figura 2.

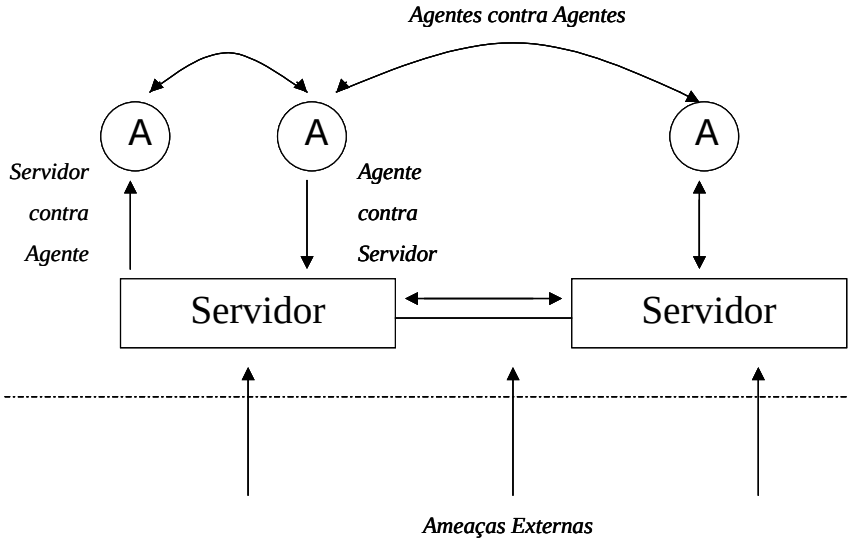

Figura 2: Os principais tipos de ataques e ameaças ao sistema multi-agentes (Milagres, 2002b)

A implementação das funções de segurança foi feita no JATLite, a plataforma de agentes que se comunicam com linguagem KQML. Para tal, um estudo inicial da plataforma de agentes em questão foi feito (Jeon *et al*, 2000). Na figura 3 é ilustrada a implementação da plataforma JATLite em camadas, para posteriormente serem definidas quais alterações foram feitas nesta implementação.

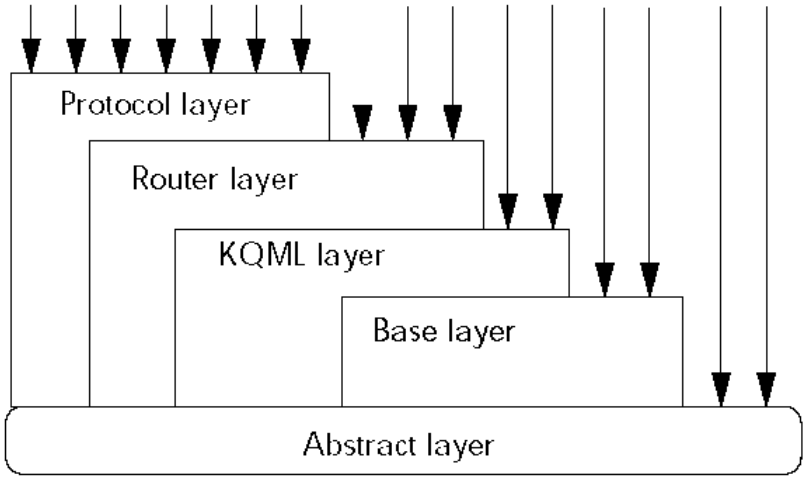

Figura 3 : A implementação em camadas do JATLite (Jeon *et al*, 2000)

Utilizando o código fonte disponibilizado pelos desenvolvedores da plataforma de agentes KQML JATLite e o modelo proposto para segurança S-KQML em Milagres (2002a), modificações foram feitas essencialmente nas camadas de base do sistema de comunicação (*Base Layer*) e na interface entre os agentes que se comunicavam por linguagem KQML (*KQML Layer*). Modificações adicionais na camada de roteamento dos agentes não foram

exigidas nesta etapa, visto que os agentes somente utilizavam uma plataforma de agentes para sua *saída* e *retorno*, o que não requer implementação de segurança nesta camada (*Router Layer*). Modificações também na camada de protocolo de comunicação não foram efetuadas, já que os agentes, como já citado, neste sistema de testes, ficam confinados em uma única plataforma de agentes, sem a necessidade de protocolos de comunicação entre plataformas.

Para tais implementações na *Protocol Layer*, podem-se utilizar, de acordo com a necessidade, protocolos seguros já consolidados na Internet, como redes privadas virtuais (VPNs) para tunelamento e canais seguros de comunicação ou SSL (*Secure Sockets Layer*), por exemplo.

Chave de comunicação segura

Para que uma comunicação entre dois ou mais agentes possa ser segura, a implementação de uma nova função em KQML foi feita de modo a permitir o estabelecimento de uma chave para comunicação segura. Esta chave pode ser a mesma entre toda a sessão de comunicação entre dois agentes, no caso, denominada chave simétrica ou pode ser parte de um par de chaves, através de criptografia assimétrica.

Devido à quantidade reduzida de informação armazenada em cada agente e à razoável capacidade computacional para *quebrar* diversas chaves para cada sessão de comunicação, caso um atacante tenha como alvo o sistema multi-agentes DEEPSIA, foi escolhido o método mais rápido e simples de criptografia, o de chaves simétricas.

É importante destacar que, no entanto, para o estabelecimento da chave de comunicação que será usada durante toda a comunicação, a criação de uma chave de sessão é necessária. Esta chave de sessão é única e somente válida para o processo de conexão inicial e acordo da chave entre dois agentes que irão se comunicar. A definição em KQML da chave de comunicação segura é a seguinte:

```
(key          <sending-agent>
              <receiving-agent>
              <master-key?>
              <key-type>
              <encrypted-key>)
```

Em KQML, a diretiva **key** define a chave que será usada para codificar a informação trocada por dois agentes em uma comunicação segura. Os dois agentes que fazem parte da comunicação são identificados pelos campos **<sending-agent>** e **<receiving-agent>**. O tipo de chave que será trocada na comunicação é definido no campo **<master-key?>** e caso o valor deste campo seja verdadeiro (*true*), a chave trocada é a principal, caso contrário é uma chave de sessão, usada somente no estabelecimento inicial da comunicação e na definição de uma chave principal.

O tipo de chave de comunicação, ou seja, o algoritmo de criptografia escolhido, é definido pelo campo **<key-type>**, que pode ser, por exemplo, IDEA ou SHA. (Milagres, 2002b). O valor que identifica a chave de comunicação propriamente dita é inserido no campo **<encrypted-key>.**

Comunicação criptografada

Após a troca de chaves para uma comunicação segura entre dois agentes, as informações podem ser trocadas de forma codificada (ou criptografada), de modo a dificultar ataques contra o conteúdo das mensagens, o sigilo das partes comunicantes ou mesmo ao sistema de agentes por completo. Para tal, foi definida uma diretiva especificamente para tal função, implementada na interface da camada KQML (*KQML Layer*), em destaque na figura 3.

```
(auth-private
      :sender Agent_A
      :receiver Agent_B
      :auth-key K
      :auth-digest (<digest-type> <encrypted-digest>)
      :content <KQML-msg>)
```

A diretiva **auth-private** foi definida para permitir a comunicação segura entre duas partes, no caso dois agentes que se comunicam utilizando linguagem KQML, identificados unicamente nos campos **Agent_A** e **Agent_B**. A chave de comunicação segura, definida na diretiva **key** é utilizada no campo **auth-key**, na variável **K**.

Opcionalmente, a mensagem codificada pode ser assinada digitalmente para futura verificação, através de uma função *hash*. A sub-diretiva que permite esta característica é a **auth-digest**, que tem como parâmetros a função utilizada para a assinatura (por exemplo, SHA ou MD5) e a assinatura digital, respectivamente nos campos **<digest-type>** e **<encrypted-digest>.**

O conteúdo da mensagem original KQML codificado pela chave K e assinado digitalmente pelo campo auth-digest na comunicação entre os dois agentes é o valor da variável **<KQML-msg>** da diretiva **content**, que substitui a função tradicional da linguagem KQML de troca de mensagens por uma comunicação segura e garantida, por criptografia e assinatura digital.

É importante destacar que a implementação realizada tem objetivo de tratar as premissas básicas de segurança e não é uma garantia completa de ausência de vulnerabilidades do sistema de multi-agentes DEEPSIA.

De acordo com estudos publicados a partir da análise inicial de segurança do sistema multi-agentes (Milagres, 2002c; 2002d), a implementação dos agentes em um novo formato em substituição a linguagem de comunicação de agentes KQML é essencial para que seja possível a implementação de novos padrões de segurança e a comunicação dos agentes DEEPSIA com agentes de outras plataformas em funcionamento, em especial, na Europa.

As fases de implementação e testes dos novos agentes em formato FIPA, bem como os resultados já alcançados e os esperados até o fim do projeto DEEPSIA no Brasil estão em destaque no capítulo 8.

No capítulo seguinte é apresentado o conceito de *Web* Semântica e dos padrões *WWW Consortium* para expressão semântica em hipertexto.

5 Web Semântica

Durante o evento “XML2000”, Tim Berners-Lee (2000), diretor do *WWW Consortium*[4] anunciou a instituição do projeto *Web* Semântica (2001). O principal objetivo desse trabalho está relacionado à implantação, nos próximos dez anos, de uma nova filosofia para o desenvolvimento e utilização da *Web* tradicional.

Na *Web* tradicional, os conteúdos de hipertextos expressos em HTML possuem significado apenas para a interpretação humana mas não representam apropriadamente a semântica de conceitos manipuláveis por computadores. Para suprir tal deficiência foram desenvolvidos os padrões XML (*Extensible Markup Language*) (2002) e RDF (*Resource Description Framework*) (2002).

O padrão XML estabelece uma linguagem que oferece ao usuário a possibilidade de adicionar estruturas arbitrárias com a criação de suas próprias *tags* (etiquetas ou rótulos), mas não especifica nada sobre o significado dessas estruturas.

O padrão RDF, por sua vez, tenta expressar os significados sobre coisas ou objetos codificados por um conjunto de triplas na linguagem XML. Cada tripla consiste de: um sujeito (*subject*), um verbo (*verb*) e um objeto (*object*) que formam uma sentença elementar. Assim, um documento RDF descreve que coisas individuais (por exemplo, pessoas, páginas da *Web*) têm propriedades (como “é irmã de” ou “é autor de”) com certos valores (outra pessoa, outra página da *Web*). Sujeitos, objetos e verbos são identificados individualmente por um URI (*Universal Resource Identifier*), o que possibilita a definição de um novo conceito, um novo verbo, com a associação de um novo URI em algum lugar na *Web*.

Outro componente básico da *Web* Semântica (2002), cuja arquitetura é mostrada na Figura 4, é a ontologia, que pode expressar classes de objetos e as relações existentes entre elas. Tanto as classes e suas subclasses, quanto às relações entre elas constituem uma ferramenta muito poderosa para uso na *Web*.

[4] http://www.w3c.org/

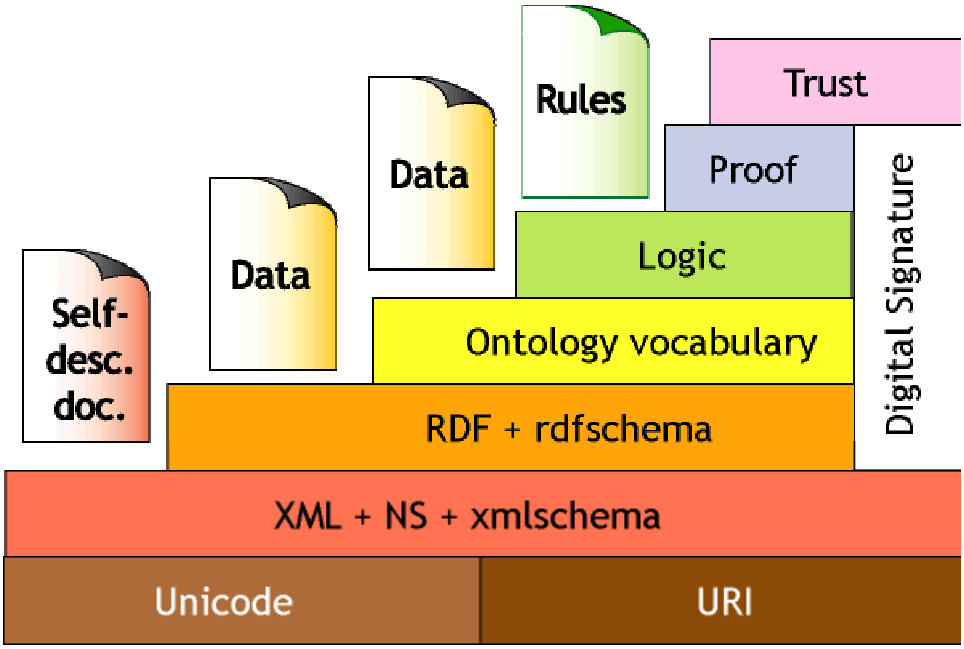

Figura 4 – Arquitetura da *Web* Semântica *(2000)*

Segundo Berners-Lee (2001), o poder real da *Web* Semântica será atingido quando programas que coletam conteúdo *Web* de fontes diversas processarem a informação e trocarem resultados com outros programas.

Muitos trabalhos foram desenvolvidos na definição de aplicações utilizando os padrões propostos pela arquitetura da *Web* Semântica como, por exemplo, por Klapsing (2001) e Chaves (2001). O grande problema encontrado atualmente é que a maior parte do conteúdo da *Web* não segue a padronização XML/RDF na composição e representação de seus conteúdos.

No capítulo seguinte é apresentado o cenário brasileiro de segurança da informação com resultados das pesquisas mais recentes no país e no exterior.

6 O Cenário Atual de Segurança da Informação

Resultados de estudos recentes de institutos de pesquisa que têm como tema principal a segurança da informação mostram a crescente preocupação com o tema, seja no Brasil ou no exterior.

Segundo pesquisa mais recente realizada no Brasil pela Módulo *Security Solutions* (2002), 78% das empresas reconhecem que tiveram perdas financeiras apesar de que 56% das entrevistadas ainda não conseguem quantificar o valor dos prejuízos causados pelos problemas com a segurança da informação. Em 22% das organizações que conseguiram contabilizar estes valores, o total de perdas registradas foi de R$ 39,7 milhões. De acordo com o *Computer Security Institute* (CSI) na pesquisa realizada nos EUA em conjunto com o *Federal Bureau of Investigation* (FBI) (Power, 2002), 98% das corporações que participaram da pesquisa possuem *web site*, sendo que 52% deste total usam os seus *sites* como ferramenta de comércio eletrônico.

A necessidade de proteger seus ativos e assegurar a continuidade das operações tem levado as corporações a desenvolverem um sistema de gestão de segurança da informação e implementar controles baseados em análise dos riscos ao negócio e em requisitos legais compatíveis com a natureza da sua atividade.

Nos últimos meses, importantes organismos internacionais como Banco Mundial, FBI e CIA têm alertado sobre a importância de se investir em segurança da informação para evitar prejuízos que muitas vezes produzem alto impacto nos negócios, essencialmente em treinamento especializado. Os resultados das pesquisas em questão demonstram que, a cada ano, o assunto tem sido tratado pelos altos executivos com mais importância e com respectivo aumento de investimentos focados na efetiva redução dos riscos operacionais.

Esse aumento significativo, especificamente no cenário brasileiro, pode ser notado na figura 5, extraída da pesquisa nacional feita pela Módulo *Security Solutions* (2002).

Figura 5 – Plano de investimentos em segurança no Brasil (Módulo, 2002)

De acordo com um relatório divulgado recentemente pelo *The Meta Group Inc*.[5], 41% das companhias estão gastando pelo menos 5% de suas verbas de tecnologia em segurança, mundialmente, o que representa um incremento de 33% no setor, em relação a 2001. No final de 2003, o *Meta Group* espera que este nível de investimentos em segurança seja praticado por 55% das companhias, no mundo. De acordo com Chris Byrnes, vice-presidente de programas de segurança no *Meta Group*, áreas como os sistemas de *Customer Relationship Management* (CRM) e armazenamento, para as quais se previa um crescimento explosivo, também ficarão em segundo plano diante das iniciativas de segurança de dados.

No capítulo seguinte são apresentados padrões de gestão de segurança para tecnologia da informação, dentre eles, o nacional NBR/ISO 17799.

[5] http://www.metagroup.com/

7 Código de Prática ISO 17799

Atualmente, a segurança da informação é preocupação de todos que integram as organizações e sua cadeia de valor e a ausência de processos e controles de segurança pode acarretar diversos impactos que podem resultar, por exemplo, em perda de faturamento, aumento de custos e conseqüente perda de valor da empresa. Por isso, uma dúvida que sempre acompanha os profissionais responsáveis pela administração de segurança da informação nas organizações é: como medir e verificar se as recomendações e controles usados são efetivos e completos.

Com base nessa necessidade, o BSI (*British Standard Institute*) criou a norma BS 7799 (1998), considerada o mais completo padrão para o gerenciamento da Segurança da Informação no mundo. Com ela é possível implementar um sistema de gestão de segurança baseado em controles e práticas definidos por norma e práticas internacionais. Até o momento, 143 empresas de variados segmentos de negócios em todo o mundo, já foram certificadas pela BS 7799, demonstrando confiança e promovendo publicamente o compromisso da organização com a segurança de suas informações e de seus clientes.

Em dezembro de 2000, a Parte 1 da BS 7799 se tornou norma oficial da ISO (*International Organization for Standardization*), sob o código ISO/IEC 17799 (2000), o mais recente padrão internacional de gerenciamento de segurança da informação que já está sendo utilizado em mais de 20 países. Em agosto do ano seguinte, o Brasil adotou esta norma ISO como seu padrão, através da ABNT, sob o código NBR ISO/IEC 17799 (2001).

O objetivo da ISO 17799 é fornecer recomendações para gestão da segurança da informação para uso por aqueles que são responsáveis pela introdução, implementação ou manutenção da segurança em suas empresas. A norma estabelece uma base comum para o desenvolvimento de normas de segurança organizacional e das práticas efetivas da gestão da segurança, facilitando testes e medições dos processos e provendo confiança nos relacionamentos entre as organizações.

A norma BS 7799 é dividida em duas partes:

Parte 1 - Código de Prática para Gestão da Segurança da Informação

Esta parte contém recomendações de segurança, divididas em dez seções com requisitos gerais de vários grupos de controles:

1. Política de Segurança
2. Segurança Organizacional

3. Classificação e Controle dos Ativos de Informação

4. Segurança em Pessoas

5. Segurança Física e do Ambiente

6. Gerenciamento das Operações e Comunicações

7. Controle de Acesso

8. Desenvolvimento e Manutenção de Sistemas

9. Gestão de Continuidade do Negócio

10. Conformidade

É importante salientar que somente a primeira parte da BS 7799 compõe a norma ISO 17799 e consequentemente, suas versões. Esta norma original recentemente passou por nova revisão que em breve deverá originar adaptações também na ISO correspondente.

Parte 2 - Especificação de Sistema de Gestão de Segurança da Informação

Esta parte da norma define um SGSI – Sistema de Gestão de Segurança da Informação, que é objeto de certificação. A adoção da BS 7799 Parte 2 como norma ISO está em estudo inicial e não há previsão para conclusão desse trabalho em curto prazo.

Diversas empresas no mundo já foram certificadas na norma BS 7799, como bancos, empresas de telecomunicações, indústrias, prestadores de serviços, consultorias e organizações governamentais. São empresas que optaram pela certificação por vários motivos e benefícios que variam desde a redução de prêmios de seguro, até uma estratégia de marketing utilizando a certificação como diferencial competitivo e como demonstração pública do compromisso da empresa com a segurança das informações de seus clientes. É válido destacar que a norma original e suas versões são documentos que constantemente passam por revisões e adaptações de acordo com políticas locais dos países onde são aplicadas.

No capítulo seguinte são apresentados os resultados alcançados na etapa atual de trabalho e os resultados esperados até o fim do projeto DEEPSIA.

8 Resultados Alcançados

Este trabalho é um resultado parcial de um projeto de pesquisa para especificação e implementação de segurança no sistema DEEPSIA. Os resultados aqui apresentados são intermediários e devem ser refinados até o fim do projeto, que será em Março de 2003.

Dentre os principais resultados nesta fase de projeto, pode-se citar:

- Análise do atual cenário nacional e internacional de segurança da informação, visando à implementação de melhorias em sistemas de comércio eletrônico, por exemplo, como o DEEPSIA;
- Definição de novas ferramentas a serem utilizadas em futuras versões do sistema DEEPSIA, como as que compõem a *Web* Semântica (XML e RDF), de modo que este tenha como segurança uma característica de projeto;
- Estudo e definição de um padrão de gestão de segurança da informação a ser utilizado para modelagem de sistemas seguros como o DEEPSIA.

Trabalhos futuros

Há alguns pontos que estão em estudo e desenvolvimento e utilizarão os resultados deste trabalho e de outros já publicados, como base para a continuidade no desenvolvimento do sistema DEEPSIA e da colaboração da USP à Universidade Nova de Lisboa (UNINOVA), em Portugal.

- Especificação de uma política de gestão de segurança da informação do sistema DEEPSIA de acordo com a norma internacional ISO 17799;
- Implementação de agentes utilizando novo padrão de linguagem de comunicação de agentes FIPA (*Foundation for Intelligent Physical Agents*) [6];
- Implementação de uma representação semântica na *web* da norma NBR/ISO 17799 de gestão de segurança para aplicação em processos de desenvolvimento e testes de software;
- Avaliação e comparação de testes de softwares ou processos seguros de acordo com a norma ISO 17799 que sejam desenvolvidos sem o uso da representação semântica em desenvolvimento;
- Adição de novos conceitos de segurança da norma ISO 17799 ao projeto DEEPSIA, em desenvolvimento atualmente pelo grupo de pesquisadores do Laboratório Intermídia e do Núcleo de Manufatura Avançada (NUMA);

[6] http://www.fipa.org/

- Publicação dos resultados em periódicos e anais de conferências nas áreas de pesquisa relacionadas.

Publicações

Após conclusão da primeira etapa de trabalho de "Especificação de Segurança na Comunicação de Agentes" (Milagres, 2002b), este foi publicado como um trabalho acadêmico no portal da Módulo *Security Solutions* e divulgado em boletim eletrônico da empresa à comunidade de segurança da informação brasileira. Foram publicados em eventos internacionais também dois artigos de autoria do autor deste trabalho, em conjunto com seu orientador e pesquisadores da Universidade Nova de Lisboa. (Milagres 2002b; 2002c)

Além das publicações, é importante destacar o convite de Monique Calistri, da Whitestein Technologies [7] e organizadora do grupo de discussão "*AgentCities Security Workgroup*" [8] para uma apresentação sobre as pesquisas em segurança do projeto DEEPSIA no evento "*AgentCities.NET Information Day 2*" [9] em Lisboa, nos dias 9 e 10 de Setembro de 2002. A apresentação em questão foi feita por João Paulo Pimentão (UNINOVA).

Todos os artigos publicados e apresentações feitas em eventos podem ser encontrados no *site* do autor, no endereço http://milagres.com/papers/

[7] http://www.whitestein.com

[8] AgentCities Security Workgroup: http://www.agentcities.org/Activities/WG/Security/

[9] AgentCities iD2, Lisboa: http://www.agentcities.org/EUNET/ID2/

9 Referências

AMBRÓSIO, D. R. *Alternativas de Implementação de Reconhecimento de Padrões para Agentes Móveis em Ambiente de Segurança Computacional.* São Carlos, 2002. Dissertação (Mestrado) - Instituto de Ciências Matemáticas e de Computação de São Carlos, Universidade de São Paulo.

BERNARDES, M. C. *Avaliação do uso de agentes móveis em segurança computacional*. São Carlos, 1999. 105 p. (Dissertação de Mestrado). Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo.

BERNERS-LEE, T.; HENDLER, J.; LASSILA, O. *The Semantic Web*. Scientific American. Maio 17, 2001.

BONIFÁCIO JR., J. M. *Sistemas de segurança distribuído: integração de firewalls com sistemas de detecção de intrusão*. São Carlos, 1998. 79 p. (Dissertação de Mestrado). Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo.

BS 7799 Revision 1. *British Standard Code of Practice for Information Security Management*. British Standard Institute. 1998.

CANSIAN, A. M. *Desenvolvimento de um sistema adaptativo de detecção de intrusos em redes de computadores*. São Carlos, 1997. 153 p. (Tese de Doutorado). Instituto de Física de São Carlos, Universidade de São Paulo.

CHAVES, M. S.; VIEIRA, R.; RIGO, S. *Uso de ontologias para gerenciamento e acesso a documentos na Web.* Universidade do Vale do Rio dos Sinos. 2001.

CICILINI, R. *Desenvolvimento de um agente SNMP para plataformas rodando DOS.* São Carlos, 1994. 107 p. (Dissertação de Mestrado). Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo.

Extensible Markup Language 1.0 (XML) 2002. <http://www.w3.org/XML/>

FININ, T.; LABROU, Y. *A Proposal for a new KQML Specification*. University of Maryland Beltimore Count - UMBC, 1997.

GARÇÃO, A. S.; SOUSA, P. A.; PIMENTÃO, J. P.; SANTOS, B. R.; BLAZQUÉZ, V.; OBRATANSKI, L. *Annex to Deepsia's Deliverable 4 – System Architecture*. Janeiro 2002. 135p. Report. IST PROJECT-1999-20483.

GOULARTE, R. *Utilização de meta-dados no gerenciamento de acesso a servidores de vídeo*. São Carlos, 1998. Dissertação (Mestrado) - Instituto de Ciências Matemáticas e de Computação de São Carlos, Universidade de São Paulo.

HERRERA, J. F. A.; MARTINS JR., J.; MOREIRA, E. S. *A Model for Data Manipulation and Ontology Navigation in DEEPSIA Project. In* First Seminar on Advanced Research in Electronic Business, PUC-RJ, Rio de Janeiro, Novembro 2002. A ser publicado.

HERRERA, J. F. *Uso de Data Warehousing e Data Mining na busca de Relações e Conhecimento em um Ambiente de Comércio Eletrônico*. São Carlos, 2002. Monografia de Qualificação (Mestrado) - Instituto de Ciências Matemáticas e de Computação de São Carlos, Universidade de São Paulo.

ISO/IEC 17799:2000 *Information Technology – Code of Practise for Information Security Management*. ISO – International Organization for Standardization. 2000.

JEON, H., PETRIE, C., CUTKOSKY, M. R. *JATLite: A Java Agent Infrastructure with Message Routing*. In IEEE Internet Computing. Stanford Center for Design Research. March-April 2000. p. 87-97.

KLAPSING, R.; NEUMANN, G.; CONEN, W. *Semantics in Web Engineering Applyning the Resource Description Framework.* In: IEEE Multimedia. Abril-Junho 2001.

LIEIRA, J. F. *Utilização de áudio e vídeo em sistemas gerenciadores de redes de computadores*. São Carlos, 1995. 111 p. (Dissertação de Mestrado). Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo.

MILAGRES, F. G.; MOREIRA, E. S. *Detecção de Intrusões com Auxílio de Agentes Móveis*. *In* Revista Eletrônica de Iniciação Científica, Porto Alegre, RS, v. I, n. II, 2001 <http://www.sbc.org.br/reic/>

MILAGRES, F. G.; MOREIRA, E. S. *Especificação de Segurança na Comunicação de Agentes In* Módulo Security News número 251 e on-line no *site* da Módulo Security Solutions S. A., como Trabalho Acadêmico. Módulo Security Solutions S.A. <http://www.modulo.com.br/pdf/milagres-deepsia_security.pdf>. São Carlos. Julho 2002.

MILAGRES, F. G.; MOREIRA, E. S.; PIMENTÃO, J. P.; SOUSA, P. A. C.; GARÇÃO, A. S. *Dealing with Security within DEEPSIA Project In*. WSEAS International Conference on Information Security. Rio de Janeiro. Outubro 2002 WSEAS Press, 2002, p. 2431-2439.

MILAGRES, F. G.; MOREIRA, E. S.; PIMENTÃO, J. P.; SOUSA, P. A. C. *Security Analysis of a Multi-Agents System in EU's DEEPSIA Project. In.* First Seminar on Advanced Research in Electronic Business, PUC-RJ, Rio de Janeiro, Novembro 2002. p. 155-162.

MÓDULO *Security Solutions* S. A *Oitava Pesquisa Nacional de Segurança da Informação.* São Paulo. Outubro 2002. <http://www.modulo.com.br>

MORAES, S. *Voz em sistemas computacionais: projeto e implementação de módulos de processamento de voz em gerenciamento de redes*. São Carlos, 1995. 103 p. (Dissertação de Mestrado). Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo.

MOROSHITA, F. T. *Uma avaliação evolutiva dos protocolos de gerenciamento da Internet: SNMPv1, SNMPv2 e SNMPv3*. São Carlos, 1997. 68 p. (Dissertação de Mestrado). Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo.

NBR ISO/IEC 17799:2000 *Tecnologia da Informação – Código de Prática para a Gestão da Segurança da Informação*. ABNT – Associação Brasileira de Normas Técnicas. Agosto 2001.

ODA, C. S. *Desenvolvimento de um sistema monitor gráfico baseado em protocolo de gerenciamento SNMP*. São Carlos, 1994. 111 p. (Dissertação de Mestrado). Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo.

ODEH, M. M.; MOREIRA, E. S.; MADEIRA, T. L. *Electronic Commerce and Its Socio-Economic Implications in Brazilian Small and Medium Enterprises*. *In.* IEEE 2002 International Symposium on Technology and Society. Proceedings p. 45-50. Social Implications of Information and Communication Technology Symposium. Junho 6-8, 2002.

OLIVEIRA, F. A. *Extração de Informação sobre Produtos Comercializados em Páginas Brasileiras para a Alimentação de Catálogos Eletrônicos*. São Carlos, 2002. Monografia de Qualificação (Mestrado) - Instituto de Ciências Matemáticas e de Computação de São Carlos, Universidade de São Paulo. A ser apresentada.

PEREIRA FILHO, S. F. *Avaliação para ambientes servidores para agentes móveis*. São Carlos, 2001. 100 p. (Dissertação de Mestrado). Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo.

POWER, R. *2002 CSI/FBI Computer Crime and Security Survey*. Computer Security Institute (CSI) and Federal Bureau of Investigation (FBI). V. 8, n. 1. 2002. <http://www.gocsi.com>

REAMI, E. R. *Especificação e prototipagem de um ambiente de gerenciamento de segurança apoiado por agentes móveis*. São Carlos, 1998. 82 p. (Dissertação de Mestrado). Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo.

Resource Description Framework (RDF) 2002. <http://www.w3.org/RDF/>

SANTA EULÁLIA, L. A; MOREIRA, E. S., CARVALHO, A. P. L. F.; ROZENFELD, H. *Using Ontologies for Intelligent Agent Training and Information Retrieval in a E-Commerce* Application Case Study In ECCPPM — European Conference on Product and Process Modeling, Portoroz, Slovênia, Setembro, 2002.

TAVARES, D. M. *Avaliação de técnicas de captura para sistemas detectores de intrusão.* São Carlos, 2002. (Dissertação de Mestrado). Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo.

TAVARES, D. M.; CASTEJON, E. F.; ROSSI, G. B.; CANSIAN, A. M.; MOREIRA, E. S. *ACME! (Advanced Counter-Measures Environment) - Um Mecanismo de Captura e Análise de Pacotes para Aplicação em Detecção de Assinaturas de Ataque*. *In.* Anais do Primeiro Simpósio de Segurança, em Informática, p. 39-46, São José dos Campos 1999.

Web Semântica (*Semantic Web*) 2001. <http://www.w3c.org/2001/sw/>

Anexo A: Histórico do Grupo de Pesquisa Intermídia

O grupo de pesquisas do Laboratório Intermídia no Instituto de Ciências Matemáticas e de Computação da Universidade de São Paulo (USP) vem desenvolvendo projetos em duas frentes importantes na área da computação: segurança computacional e sistemas multimídia distribuídos.

Tendo iniciado seus trabalhos no início da década de 1990 com projetos relacionados ao gerenciamento de redes de computadores (Oda, 1994; Cicilini, 1994; Lieira, 1995; Moraes, 1995; Moroshita, 1997), o grupo de pesquisa do Laboratório Intermídia desenvolve atualmente pesquisas na área de Segurança Computacional com sistemas detectores de intrusões que utilizam redes neurais para o reconhecimento de padrões de ataques (Bonifácio Jr., 1998; Cansian, 1997; Tavares, 1999) e aplicam a tecnologia de agentes móveis para o gerenciamento da segurança (Reami, 1998) e a verificação de anomalias (Bernardes, 1999; Milagres, 2001). Também foram desenvolvidas, pelo grupo, pesquisas sobre ambientes servidores para agentes móveis (Pereira Filho, 2001) e tecnologias que podem conferir inteligência a tais agentes (Ambrósio, 2001) bem como estudos para implementação de sistemas detectores de intrusão em dispositivos de segmentação de redes (*switches*) (Tavares, 2002).

A segunda frente de trabalho desenvolve atualmente pesquisas em sistemas multimídia distribuídos aplicando estudos em padrões para a representação de informações e meta dados na identificação de fluxos de mídia contínua e técnicas adequadas para transmissão e distribuição de vídeo na Internet (Goularte, 1998).

A partir do segundo semestre de 2001, o Laboratório Intermídia, juntamente com o NUMA[10] (Núcleo de Manufatura Avançada) e fomentados pelo CNPq [11] (Conselho Nacional de Desenvolvimento Científico e Tecnológico) (DEEPSIA – CNPq-680263/01-2), passou a integrar a iniciativa brasileira pela cooperação com o projeto internacional DEEPSIA[12].

O projeto DEEPSIA foi estabelecido por um consórcio entre diversas instituições e empresas européias com o apoio da *Information Society Technologies* (IST), tendo como objetivo principal promover o ingresso das Pequenas e Médias Empresas (PMEs) no comércio eletrônico, utilizando uma solução centrada no comprador, tratando as PMEs não somente

[10] http://www.numa.org.br/

[11] http://www.cnpq.br/

[12] http://www.deepsia.com/

como fornecedoras de produtos, mas também como consumidoras de bens e serviços. (Garção, 2002)

A participação em tal projeto motivou o grupo a instituir uma nova frente de trabalho relacionada ao estudo e ao desenvolvimento de soluções otimizadas para sistemas de Comércio Eletrônico, com a aplicação de técnicas apropriadas para as tarefas de busca, classificação, armazenamento e extração de informações sobre os produtos.

Os principais projetos correlatos que estão em desenvolvimento pelo grupo são:

- Segurança para o sistema Multi-Agentes DEEPSIA: análise de segurança do sistema multi-agentes e proposta de um modelo para segurança de comunicação no protocolo de comunicação entre agentes KQML - *Knowledge Query and Manipulation Language* (Finin, 1997; Milagres, 2002a; Milagres 2002b);
- Impacto sócio-econômico do DEEPSIA: estudo das mudanças promovidas com a utilização do sistema DEEPSIA pelas Pequenas e Médias Empresas (Odeh, 2002);
- Mineração de dados nas informações do catálogo: visando a descoberta de dados que não estejam apresentados explicitamente (Herrera, 2002a);
- Implementação de técnicas de extração de informação sobre produtos em páginas da *web* brasileira para inclusão em catálogos eletrônicos como o usado no DEEPSIA (Oliveira, 2002);
- Navegação na Ontologia: visando facilitar a interação do usuário com a ontologia dos produtos, através de mecanismos como busca, *bookmarks* e outros. (Herrera, 2002b; Santa Eulália, 2002)