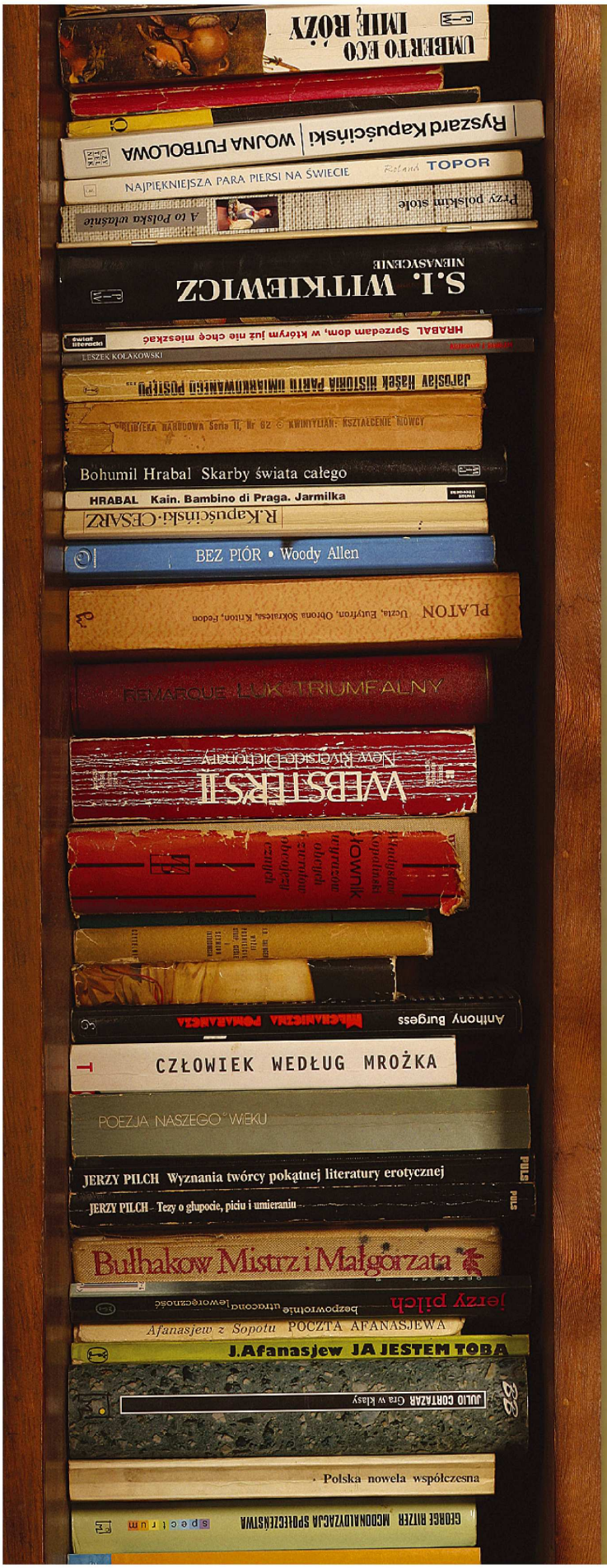


ISSN: 1980-0193

PERSPECTIVAS CONTEMPORÂNEAS

Revista eletrônica de ciências sociais aplicadas.

V.2, N.2, 2007

EDITORIAL

Perspectivas Contemporâneas
Faculdade Integrado
Campo Mourão – Paraná – Brasil
Av. Irmãos Pereira, 670, Centro
Fone: 55 44 3523 1982
CEP: 87301-010

Editor Chefe
Patrícia Regina Cenci Queiroz

Editor de Revisão e Correção
Ana Paula Previate Widerski

Editor de Língua Estrangeira
Aparecida da Penha dos Santos
Fernanda Scheibel Bispo

Editor de normalização
Vinicius Ortiz de Camargo

Editor Externo
Luciana Aparecida Bastos
Emanulle Torino

Editor de Layout
Márcia Regina Ferri

Projeto Gráfico e Edição Final
Emanuelle Torino
Márcia Regina Ferri
Patrícia Regina Cenci Queiroz

Suporte Técnico
José Leandro Xavier
xavier@grupointegrado.br

Perspectivas Contemporâneas

"*It's a brave new world*", diria Aldous Huxley em sua célebre obra, e certamente admirável é, este mundo. Este novo mundo, modificado de forma acelerada nos dois últimos séculos, tornou-se, ao mesmo tempo, uma arena de desafios e oportunidades tanto para as ciências quanto para os empreendimentos humanos. É lícito afirmar que a ciência tem modificado o mundo e os efeitos destas mudanças trouxeram simultaneamente soluções e problemas para a humanidade.

É uma era de paradoxos, parafraseando Charles Handy, na qual pode-se, ao mesmo tempo, verificar os benefícios inegáveis da tecnologia nas áreas da saúde, comunicações, educação e transportes e, em contraposição, os problemas causados nas mesmas áreas têm igual ou maior impacto.

Para explicar as relações existentes entre os artigos do presente número da revista, preferi classificá-los em três eixos principais: i) problemática sócio-ambiental; ii) negócios; e iii) tecnologia.

No primeiro eixo, sócio-ambiental, enquadram-se o artigo de SILVA e CORONEL, sobre os movimentos ambientais e o artigo "Desenvolvimento humano em municípios gaúchos [...]" de FROEHLICH e NEUMANN, que demonstram dois campos de estudos que, embora muito abordados ultimamente, ainda carecem de contribuições como estas para o entendimento desta interação entre sociedade e ambiente, tão antiga na convivência, mas grande novidade como área de estudos nas ciências sociais.

Como representantes do segundo eixo, estão os artigos de SANTOS e SAAVEDRA, sobre negociações, GONÇALVES e RAIHER, sobre concessões rodoviárias, MACIEL, da área de estratégia, GALEANO e MATA, representante da área de finanças. Estes artigos, quando lidos e classificados como presentes em uma linha de raciocínio, têm o grande mérito de demonstrar a grande diversidade de temas que podem ser discutidos na área de organizações e, mais especificamente, sobre empresas. Esta diversidade que depõe a favor do, já antigo, alerta sobre o aumento da complexidade das operações dos setores produtivos, e em última instância, impactando em inevitável aumento da complexidade da vida humana na sociedade de consumo atual.

Restam ainda os artigos de JESUS e PERIOTO, que mesclam os dois eixos anteriores, apresentando uma visão sobre a interface existente empreendedorismo e meio-ambiente, mediada pela tecnologia e o artigo de RIBEIRO, ZABADAL e FREITAG, sobre os custos de emprego de tecnologias de segurança no mundo virtual, como respostas às ameaças que diariamente rondam este ambiente.

Desta forma, novamente, a revista *Perspectivas Contemporâneas* faz jus a seu título e a sua linha editorial, apresentando artigos de qualidade e que efetivamente contribuem para o fomento às discussões e ao esclarecimento dos temas que concernem a estes assuntos.

Boa leitura.

Rogério Silveira Tonet

Coordenador de Extensão da Faculdade Integrado, administrador com especializações em Recursos Humanos e Marketing, Mestre em Administração pela Universidade Federal do Paraná (2004).

ARTIGOS COMPLETOS/COMPLETS ARTICLES

QUAL É O CUSTO DO EMPREGO DAS TECNOLOGIAS DE SEGURANÇA NO MUNDO VIRTUAL?

Vinicius Gadis Ribeiro (1)
Centro Universitário Ritter dos Reis, Porto Alegre – RS

Jorge Rodolfo Silva Zabadal (2)
Universidade Federal do Rio Grande do Sul, Porto Alegre – RS

Victor H. Freitag (3)
Centro Universitário La Salle, Canoas – RS

RESUMO

Este artigo apresenta a análise do resultado da condução de um conjunto de experimentos, no sentido de se quantificar o custo computacional para prover os serviços de segurança necessários em um sistema de informações - para que os usuários o considerem como um sistema confiável. Para tanto, foram empregadas equipamentos em condição de laboratório, e foi realizada a tomada de tempos, considerando-se aplicações simples que efetuavam comunicação de dados - simulando as mensagens entre as partes componentes de um sistema de comércio eletrônico – e para o emprego de Biometria. Buscou-se empregar as tecnologias atuais para prover serviços de segurança, e realizar medições com a ausência/presença desses serviços. Os resultados obtidos nos experimentos - considerando-se apenas as condições de laboratório - possibilitam afirmar que o impacto, em termos de tempo, não é significativo.

PALAVRAS-CHAVE: Comércio Eletrônico, Segurança Computacional, Análise de Desempenho.

HOW MUCH IS A JOB OF TECHNOLOGY OF SECURITY IN THE VIRTUAL WORLD?

ABSTRACT

This paper presents the analysis of some experiments on processing and communication times among machines that simulate an electronic commerce system and employing a biometric device. The object of this work is measure the impact of using security technologies in electronic commerce and in biometric systems. The results of the experiments allow asserting the impact the usage of these technologies is not elevate, considering the experiments conditions.

KEYWORDS: Electronic Commerce, Computer Security, Performance Analysis.

INTRODUÇÃO

A sociedade atual é altamente dependente de tecnologia – em especial, das tecnologias de informação. Tais tecnologias proporcionam maiores facilidades e conforto a diversas atividades do ser humano.

Contudo, não apenas há apenas benesses em se tratando da tecnologia. Essa mesma pode ser empregada com propósitos maliciosos, vindo a se obter vantagens particulares. Por essa razão, é comum que sistemas de informação sejam dotados de serviços de segurança. O presente trabalho apresenta os resultados da condução de experimentos para medir o impacto do emprego de tecnologias de segurança. Assim, esperava-se que se o custo fosse elevado, poderia inviabilizar atos que são realizados no mundo virtual – como comércio eletrônico, consultas bancárias ou até eleições seguras pela Internet. Mas de nada adianta a tecnologia por si, se não houver a cooperação do elemento humano.

O presente artigo está estruturado na seguinte forma: a próxima seção trata da virtualização dos serviços; a seção seguinte define o que se entende por segurança, tratando a seção posterior das técnicas que fornecem serviços que garantem a segurança no mundo virtual. Posteriormente, são apresentados os experimentos realizados e resultados obtidos para, na última seção, analisar e discutir tais resultados.

2. VIRTUALIZAÇÃO DOS SERVIÇOS NA SOCIEDADE ATUAL

A sociedade presente não prescinde da tecnologia; ao contrário, torna-se cada vez mais dependente da mesma. Surge um conceito novo: a dependabilidade – isto é, o maior grau de dependência da tecnologia. Assim como a eletricidade, não se cogita atividade humana produtivo sem o emprego de alguma tecnologia. Na verdade, há atividades que têm seus procedimentos alterados em relação à vida real, graças à tecnologia (envio do Imposto de Renda Pessoal Física, movimentações bancárias, marcação de exames, etc.).

O grupo de tecnologias mais ativas atualmente é, sem dúvida, o que Pierre Lévy chamou de "tecnologias da inteligência" (LEVI, 1993). Na obra citada, ele

descreve o impacto e facilidades fornecidas por diversas tecnologias – partindo de considerações históricas, e adequando aos conceitos por ele propostos. Coloca que, assim como a imprensa criou diversos impactos sobre a sociedade, da mesma forma as tecnologias da informação estão criando novas situações – algumas que visam à facilidade e ao conforto na realização de atividades humanas; outras, baseadas nas primeiras, que expõe a confiança dos usuários, colocando em risco a sua produção, ou mesmo seus bens. Tais tecnologias, outrora aparentemente tão distantes - quando da elaboração daquela obra – são hoje de tal forma naturais e transparentes aos usuários, sendo que esses nem cogitam o não-emprego daquelas, nas atividades cotidianas.

3. O QUE É SEGURANÇA

Normalmente, ao se tratar de aspectos de segurança e se considerarmos a Internet, tem-se como padrão a preocupação de não permitir que alguma pessoa não autorizada tenha acesso à informação a nós destinada ou de nós originada. Contudo, o conceito de segurança abrange os chamados serviços (SCHNEIER, 1994, p.2; STALLINGS, 1998, p.5), apresentados a seguir:

- **Privacidade**: também conhecido como o serviço de confidencialidade, trata de oferecer condições para impedir-se que pessoas não autorizadas, caso venham a obter a informação, não a possam utilizar. Normalmente, tal serviço é oferecido por intermédio de técnicas criptográficas - isto é, a informação é transformada de tal forma que apenas a pessoa que dispõe de outra informação específica1, que permite recuperar a informação original sem perdas.
- **Autenticação**: esse serviço torna-se fundamental para a comunicação na Internet. Como se pode garantir que uma determinada página da Internet é realmente da instituição que buscamos - por exemplo, um banco? O serviço de autenticação busca impedir que entidades - sejam pessoas ou instituições - passem por outra entidade. Assim, garante-se a identidade das partes envolvidas em uma comunicação são quem afirmam. Da mesma forma que o serviço anterior, emprega-se a criptografia para que um sistema disponha desse serviço.
- **Integridade**: a informação, uma vez produzida, não pode ter o seu conteúdo alterado. Esse é o conceito do serviço de integridade, também conhecido por confiabilidade. Para que se possa dispor desse serviço, empregam-se técnicas de tolerância a falhas.

- **Disponibilidade**: determinados sistemas não podem deixar de oferecer seus diversos serviços. Assim, têm-se os chamados sistemas de alta disponibilidade, conhecidos na área de Sistemas de Informação como 7/24 - ou seja, sete dias por semana, vinte e quatro horas por dia disponíveis para uso.
- **Acesso**: a entrada no sistema, seja de modo físico, seja de modo virtual, deve ser planejada de tal forma que apenas possam usar os recursos de um sistema, os legítimos participantes autorizados.
- **Não-Repúdio**: partes envolvidas em um acordo ou acerto não podem negar atos realizados. Em tempos de comércio eletrônico, esse serviço é vital: é inconcebível que uma pessoa contrate um produto pela Internet e, ao receber o produto, negue a sua solicitação; do mesmo modo, o comerciante não pode se eximir de entregar o produto, tendo recebido a solicitação de compra.

Como se pode observar, não é razoável tratar segurança por apenas um aspecto, mas por todos os serviços acima. Se cada sistema que fosse desenvolvido buscasse oferecer todos os serviços, teriam sua complexidade ampliada - sem considerar que minimizariam o impacto dos serviços específicos que seu sistema deveria oferecer - e o seu desempenho certamente seria minimizado.

A própria Internet não foi concebida com tais preocupações. Em seus primórdios, baseava-se na confiança mútua, não prevendo a maioria desses serviços (SMITH, 1997, p. 97). Na verdade, a grande preocupação era a perda de mensagens - assim, o serviço de integridade foi previsto inicialmente. Ademais, não fora projetada com preocupações comerciais, mas tão somente para fins militares e acadêmicos.

Assim, por meio de padrões e convenções, buscam-se oferecer alguns desses serviços já em outros níveis. Alguns dos serviços de segurança já são providos pela Internet. Por exemplo, o conjunto de regras que define a comunicação entre duas máquinas na rede – ou seja, o protocolo TCP/IP - já oferece o serviço de integridade. Cabe, então, ao desenvolvedor do sistema integrar esses serviços, considerando-se as necessidades do usuário. Quanto mais automatizado por o sistema, em relação as suas defesas, mais transparente ao usuário ele será.

4. CONSIDERAÇÕES TÉCNICAS – AUTOMATIZANDO AS DEFESAS

O que pode acontecer quando as preocupações colocadas acima não são atendidas?

Os sistemas podem ficar expostos a vulnerabilidades inerentes a projeto, ao próprio desenvolvimento dos programas, a falhas humanas etc. Busca-se, então, empregar ferramentas ou técnicas que possibilitem a oferta de tais serviços.

Contudo, tal tarefa não é facilitada, visto o conjunto de necessidades que atualmente são exigidas pelos usuários. O ambiente Windows, com todas as falhas de segurança e diversos aspectos técnicos questionados pela comunidade acadêmica de Informática, é o sistema operacional mais usado por usuários de computadores pessoais, e popularizou um padrão de amigabilidade e de interface nem sempre admitido por outras comunidades de usuários. Esse padrão foi tal que se observa, hoje, notável incremento das características e funcionalidades desse padrão em outros sistemas operacionais dirigidos a usuários finais – como o Linux, por exemplo, onde encontramos as facilidades de interfaces gráficas cada vez mais incorporadas em seu ambiente.

Ademais, as ameaças computacionais tendem a aumentar, em se tratando do emprego de serviços da Internet – sendo que problemas de autenticação tendem a se intensificar (BERNSTEIN et al, 1997; BLOOMBECKER, 2005; MINOLI, 1998).

A opção por um sistema operacional com maiores facilidades dirigidas a usuários finais aumenta a responsabilidade pelos serviços de segurança. Geralmente, tem-se uma opção a ser feita: ou são inseridos os serviços de segurança no sistema operacional, tornando-os transparentes ao usuário, ou é permitido que o usuário os configure e visualize as ações deles decorrentes. Essa última opção obriga que o usuário detenha maior conhecimento sobre recursos da máquina em uso, comunicação de dados etc.

Dentre as principais defesas, podem ser citadas:

- **Criptografia:** traduzida livremente como sendo "escrita oculta", a criptografia não esconde a informação – mas tão somente a altera para que

apenas usuários que possuam alguma informação – como uma senha, por exemplo – possa vir a torná-la novamente inteligível (SCHNEIER, 1994, p. 12; STALLINGS, 1998, p. 36). Assim, o emprego de técnicas criptográficas em sistemas de informação ou mesmo em sítios da Internet possibilita evitar que pessoas não-autorizadas tenham acesso legível a tal informação. É uma defesa direta no que se refere aos ataques ao serviço de privacidade. Quando empregada como parte de um protocolo, permite a realização de serviços de nível mais elevado, como votação eletrônica, comércio digital, pôquer virtual etc.

- ***Firewall*:** programa, equipamento ou sistema com o objetivo de impedir o acesso ao sistema – ou a parte do sistema (STALLING, 1998, p. 518; STANLEY, 2002, p. 47). Assim, é uma das possíveis defesas contra ataques ao serviço de acesso.
- **Sistemas de detecção de intrusão**: tendência mais recente em termos de segurança computacional, tais sistemas não buscam impedir invasões, mas tão-somente a identificação de uma provável invasão. Podem ser orientados a arquivos – ou pastas ou diretórios -, ou ser orientados ao comportamento dos usuários – assumindo-se que se houver uma tentativa de acesso em horário diferente daquele costumeiramente registrado pelo usuário, pode ser um indício de invasão. Da mesma forma que um *firewall*, possibilita defesa contra os ataques ao serviço de acesso.
- ***AntiSpam*:** verdadeira praga virtual, os *spams* – ou abuso do protocolo SMTP – é oficialmente conhecido como mensagem em massa não solicitada - mensagens comerciais não solicitadas -, tornou-se rapidamente um dos maiores problemas na Internet atualmente. "[...] a proliferação de *spams* alcançou um ponto que se transformou em um dos problemas para o desenvolvimento do comércio eletrônico e a sociedade da Informação" (UNIÃO EUROPÉIA *apud* MEDEIROS; GADIS, 2005, p. 37). Defesas que existiam há pouco tempo limitavam-se ao conhecimento de especialistas em gerenciamento de redes. Recentemente, técnicas de filtragem de mensagens de correio eletrônico têm sido implementadas em programas mais amigáveis, os quais vêm a deixar esse trabalho facilitado, graças a interfaces mais naturais. Ainda que *spam* não seja um ataque de fato, pode vir a comprometer o serviço de disponibilidade, vindo a possibilitar uma situação de negação de serviço – ainda que apenas afetando o desempenho do sistema cliente de correio eletrônico.
- **Tolerância à falhas:** assume-se que falhas podem ocorrer, sendo até esperados, em algum momento. Assim, podem-se dotar os sistemas de certas características ou mesmo empregar sistemas específicos de tolerância à falhas. Tais sistemas buscam continuar oferecendo as funcionalidades originais, mesmo na ocorrência dessas falhas. Para tanto, esses sistemas devem efetuar diversas atividades: devem identificar que estão em um estado errôneo; conter a falha, para evitar a contaminação do

ISSN: 1980-0193

sistema. Ataques ao serviço de integridade podem ser minimizados com o emprego dessas técnicas.

- **Prevenção a plágio ou cópias:** há ao menos um site de prestação de serviços na qual é possível verificar, automaticamente, o quanto determinado artigo em língua inglesa é plágio, paráfrase ou cópia. Este site é chamado *Turn-it-in*. Dentre suas diversas funcionalidades proporcionadas, a mais interessante realiza análise em diversas bases de artigos, e informa, em diferentes cores, que partes do artigo em análise é plágio, paráfrase ou cópia – apresentando, ainda, a origem de cada parte componente. Há uma demonstração disponível, sendo o serviço comumente cobrado. Não direcionado a usuários finais, pode ser uma alternativa de valor em eventos acadêmicos, quando do momento da seleção de trabalhos.

Como se pode deduzir, sempre que houver a necessidade de algum serviço de segurança, haverá um custo associado. Seja o emprego de *backup*, seja por tomar mais tempo de processamento, a preocupação com segurança traz como conseqüência a redundância – seja de mais carga, mais tempo, mais memória.

5. METODOLOGIA DOS EXPERIMENTOS CONDUZIDOS: DEFININDO O CUSTO DE TECNOLOGIA

Entende-se por custo do uso de Tecnologia ao uso de recurso computacional. Ou seja, qual é a quantidade suficiente de recurso, para que uma tecnologia tenha condições de ser oferecida. Como recurso computacional, entende-se o consumo de memória, emprego necessário de disco, uso de CPU, ou mesmo número de mensagens, quando houver a necessidade de comunicação entre duas máquinas.

Assim, foram conduzidos experimentos em condição de laboratório, para medir a necessidade de recursos computacionais de alguns dos serviços de segurança (RIBEIRO; WEBER, 2001, p. 5). Assim, um dos experimentos contemplava o serviço de autenticação, por meio da biometria de impressões digitais; em outro, buscou-se atender aos serviços de privacidade, integridade, não-repúdio e autenticação, pelo emprego da criptografia e outras tecnologias aplicadas a ambientes restritos – por exemplo, uma aplicação que simula equipamentos servidor e clientes de comércio eletrônico.

ISSN: 1980-0193

5.1. Biometria de Impressões Digitais

Sem dúvida, excetuando-se a biometria de face – que é comumente associado à fotografia -, o mais empregado meio de efetuar autenticação dá-se por meio da Biometria de Impressões Digitais (FIGINI et al, 2003; GONZALEZ et al, 2002; KIM; 1995), empregando-se diversas formas de casamento de padrões (CHAMPOD, 1995) – sendo a principal, a identificação de pontos notáveis chamados minúcias ou minutas, que podem ser automatizados (CARVALHO, 2001).

Para realizar o experimento 1, foi implementado uma aplicação *AFIS* - (*Automatic Fingerprint Identification System)*. Para a coleta de dados do aplicativo desenvolvido, houve a necessidade de que utilizar hardware leitor de impressões digitais. Contudo, a aplicação está limitada às funcionalidades oferecidas pelo *software* fornecido pelo fabricante do leitor e suas particularidades, o qual efetua os seguintes processos:

a) **captura da impressão digital:** *driver* de comunicação com o leitor e rotinas de baixo nível, responsável pelo acionamento dos dispositivos físicos e conversão da imagem em dados digitais;

b) **processamento e geração do *template*:** geração do modelo biométrico por algoritmos patenteados que efetuam a análise qualitativa das impressões digitais, classificação datiloscópica e geração do *template*.

Estes processos são executados por um conjunto de rotinas, parâmetros, estruturas de dados, objetos e outros componentes que são proprietários, implementados pelo fabricante do dispositivo de leitura e interagindo com o sistema operacional e o *hardware* através de rotinas de nível de máquina.

Muitos dos fornecedores encapsulam os processos de maneira a criar funções que recebam e retornem parâmetros e informações para as aplicações desenvolvidas. Isso ocorre em uma aplicação *AFIS,* usando *API´s (Application Program Interface)* que englobam métodos que atuam na camada de gerenciamento do *hardware* e nas

funções básicas do sistema operacional (HONG LIN et al, 1998; MALTONI et al, 2003), conforme modelo de arquitetura apresentado na figura 1.

Neste contexto, o protótipo desenvolvido respeitou as limitações impostas pelo *software* fornecido junto do leitor utilizado, fabricado pela *SecuGen*, quanto ao aspecto de manipulação de parâmetros tais como níveis de resolução de imagem, seleção da área de mapeamento de imagens, quantidade de minúcias usadas no cadastramento de usuários e demais parâmetros pertinentes ao ambiente adotado.

5.1.1 Considerações Técnicas

O objetivo do protótipo era efetuar o cadastramento de usuários e suas digitais para posterior identificação e autenticação dos mesmos. Para tanto, é necessário a captura das respectivas impressões digitais, podendo ser escolhidos diferentes níveis de resolução e diferentes parâmetros de configuração, de acordo com as possibilidades permitidas pelo *software* básico utilizado pelo leitor biométrico. O protótipo do sistema de identificação de impressões digitais implementado permite as seguintes operações:

a) cadastrar usuários e efetuar a leitura de suas impressões digitais dos dedos das mãos, até o limite de doze (12) para cada usuário – considerando problemas congênitos -, capturadas a partir de um leitor óptico;
b) definir diferentes parâmetros de segurança quanto aos diferentes níveis de *threshold* disponíveis no leitor utilizado, de forma a aumentar ou diminuir o nível de acurácia do protótipo;
c) criar e manter de forma individualizada, em tabelas específicas para tal, os resultados da captura e verificação de impressões digitais dos dedos das mãos, efetuadas pelo sistema;

d) associar o conjunto de impressões digitais às informações de cada indivíduo cadastrado no sistema (nome, departamento, sexo, foto, função, etc.);
e) efetuar a comparação entre um *template* existente e a captura de uma imagem da impressão digital pelo leitor, de forma a obter ou não a identificação do usuário;
f) efetuar o armazenamento dos registros de identificação e autenticação pelo protótipo (*match*), bem como as ocorrências de rejeição de cada indivíduo, o que permite a aferição do protótipo;

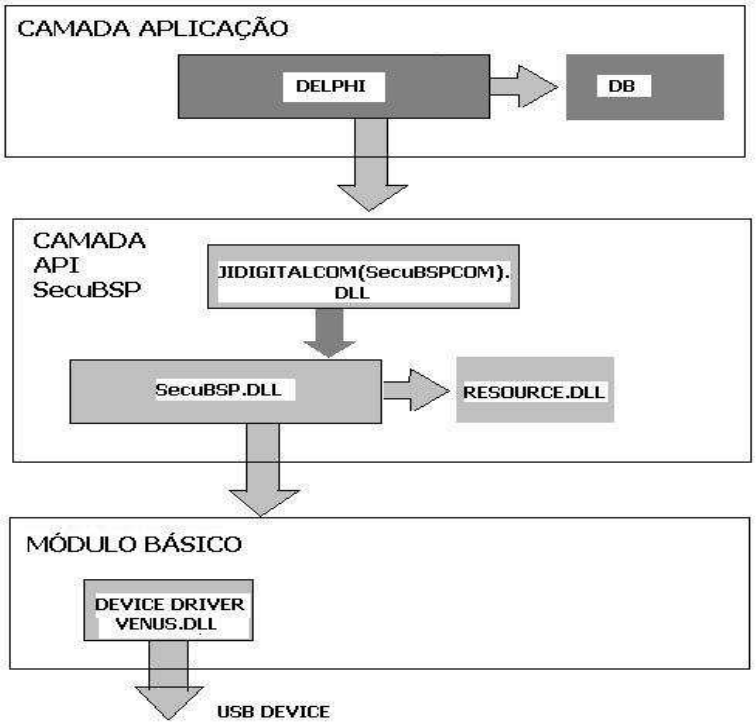
O projeto de desenvolvimento utilizou uma arquitetura composta de *API´s* em diferentes níveis, nos padrões *COM (Component Object Model)*, permitindo desta forma a utilização do ambiente de desenvolvimento *Borland Delphi Enterprise*, da linguagem de programação *Object Pascal* e do Banco de Dados *Interbase* 6.0.1.6, também da *Borland*.

Os componentes referentes ao leitor biométrico modelo *FDU01* da empresa *SecuGen Corporation* que compõem o software *SDK* da mesma, utilizados do presente trabalho foram respectivamente:

a) *SecuBSP.dll* – *DLL* de baixo nível com biblioteca principal;
b) *JIDigitalCOM.dll* – *DLL* de alto nível no padrão COM *(Component Object Model)* que utiliza os métodos da *DLL SecuBSP*;
c) *FpLibX.ocx* – Componente *OCX* para visualização da digital capturada pelo leitor biométrico, usa a *DLL SecuBSP.dll*.

Na versão obtida para o desenvolvimento do protótipo, não são suportados todos os métodos da *DLL SecuBSP*, e os dados da impressão digital *(fingerprint)* estão disponíveis apenas no modo texto. De acordo com a documentação obtida da *SecuGen Corp.*, o *SecuBSP* atende às especificações do *BioAPI 1.1* definida pela *BioAPI Consortium*.

Figura 1: Modelo de arquitetura do sistema protótipo



Fonte: elaborado pelos autores.

O modelo de arquitetura pode ser visualizado na figura 1, onde são apresentadas as diferentes camadas de *software* que formam o projeto. O protótipo foi desenvolvido em ambiente *GUI (Graphic User Interface)*, em módulos, os quais são distintos entre si no aspecto da funcionalidade para com o usuário.

A seguir, são apresentados os resultados do experimento 1.

5.1.2. Resultados Obtidos e Considerações sobre o Experimento 1

Para fins de validação do protótipo desenvolvido, efetuou-se a coleta de dados mediante o cadastramento de usuários, os quais foram distribuídos entre as nove funções cadastradas na tabela de funções, de forma a melhor colocar aleatoriamente o número de usuários entre estas funções, permitindo o uso das diferentes métricas cadastradas na tabela de métricas. Durante a coleta de dados, foram observados os principais erros – o que pode implicar problemas de reconhecimento -, sendo destacados os principais no final da presente seção.

Cada código de métrica corresponde a um nível de segurança, representado pelo nível de *threshold*, variando de 1 a 9, conforme disponibilidade do modelo de leitor utilizado.

O resultado das leituras feitas pelo módulo de acesso e identificação é registrado na tabela de movimento, sobre a qual são obtidos os índices percentuais de *FAR* (*False Acceptance Rate)* e *FRR (False Reject Rate)* para cada um dos nove níveis de segurança. Estes resultados são apresentados no módulo de avaliação e estatísticas, através do relatório de *FAR Vs. FRR* .

Através destes valores é possível comparar os resultados desta coleta de dados com os índices referenciados nas especificações do fabricante do leitor, para o modelo e ambiente utilizado no protótipo.

Foram cadastrados 75 usuários, sendo feitas 407 verificações de acesso e autenticação, sempre com o resultado validado pelo módulo "Árbitro", que demandou a conferência humana sobre os resultados obtidos em cada identificação.

A distribuição dos resultados obtidos entre os diferentes níveis de *threshold* podem ser observados no quadro 1.

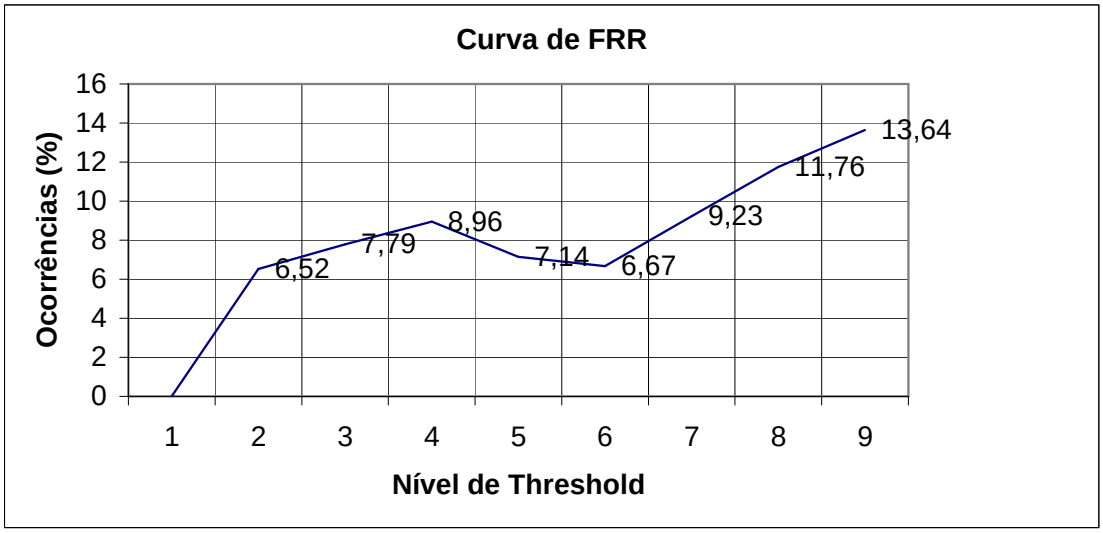
Quadro 1: Distribuição dos resultados

Nível Threshold	Leituras	Correto		FRR		FAR	
		Ocorr.	%	Ocorr.	%	Ocorr.	%
1	4	4	100,00	0	0	0	0
2	92	86	93,48	6	6,52	0	0
3	77	71	92,21	6	7,79	0	0
4	67	61	91,04	6	8,96	0	0
5	14	13	92,86	1	7,14	0	0
6	15	14	93,33	1	6,67	0	0
7	65	59	90,77	6	9,23	0	0
8	51	45	88,24	6	11,76	0	0
9	22	19	86,36	3	13,64	0	0
Total	**407**						

Fonte: elaborado pelos autores, com base nos dados da pesquisa realizada.

No que diz respeito à ocorrência de *FRR (False Acception Rate)*, obtiveram-se índices que variaram de zero até 13,64%, conforme indicado no gráfico da figura 2.

Figura 2 : Gráfico da curva de *FRR*



Fonte: elaborado pelos autores, com base nos dados da pesquisa realizada.

No caso da ocorrência de *FAR (False Acceptance Rate)* não foi possível identificar nenhuma ocorrência neste universo de leituras - o que mostra que o leitor está dentro do parâmetro apresentado pelo fabricante, de cerca de 0,001% para um nível de *threshold* igual a 5 para este tipo de problema, potencialmente mais sério, pois significa que um usuário indevido é aceito no lugar de outro, comprometendo a segurança deste tipo de solução.

Houve a necessidade de um módulo que coletasse automaticamente determinadas métricas para avaliação da funcionalidade pretendida – ou seja, minimizar as taxas de falsos positivos e falsos negativos - e do desempenho – ou seja, o custo computacional. Neste módulo foram efetuadas as operações de manutenção sobre as métricas possíveis de serem utilizadas quanto ao nível de *threshold*, o qual compreende o nível de segurança do sistema. No conjunto leitor/*software SDK* utilizados, estes níveis de segurança variam de 1 a 9. O conceito básico é de que quanto maior o nível de segurança, menores as taxas de *FAR* (Taxa de Falsa Aceitação) e maiores as taxas de *FRR* (Taxa de Falsa Rejeição).

O Cadastro de Métricas foi formado pelos campos código da métrica, nome da métrica e nível de *threshold*. A razão de não serem definidos os níveis de segurança diretamente no código fonte do programa, está na liberdade de poder manipular apenas os níveis desejados de forma dinâmica no banco de dados, inclusive

prevendo a utilização futura de mais de um dispositivo, com diferentes níveis de *threshold*.

As operações possíveis neste módulo foram as seguintes:

- Inclusão de novas métricas (até o limite de 9 para o leitor utilizado);
- Alteração das métricas existentes quanto aos seus respectivos campos;
- Exclusão de métricas existentes;
- Consulta as métricas cadastradas.

Em algumas leituras onde houve repetidas ocorrências de *FRR,* verificou-se que o cadastramento das impressões digitais do usuário ocorreu com níveis de baixa qualidade no que diz respeito à imagem da impressão digital usada como matriz.

Figura 3 : Níveis de qualidade impressões digitais: a) alta e b) baixa

Fonte: SecuGen Corporation

Verificou-se que a maior pressão do dedo no leitor gera imagens mais escuras e com pouca definição, enquanto que usuários que mantiveram o dedo encostado levemente sobre o leitor resultaram em imagens muito fracas – como é possível observar na figura 3.

Mesmo com uma baixa qualidade de imagem, o leitor efetuou a captura das minúcias, gerando o respectivo *template*; porém este possui um número menor de minúcias devido à qualidade da imagem, o que leva a uma maior incidência de ocorrências de *FRR*.

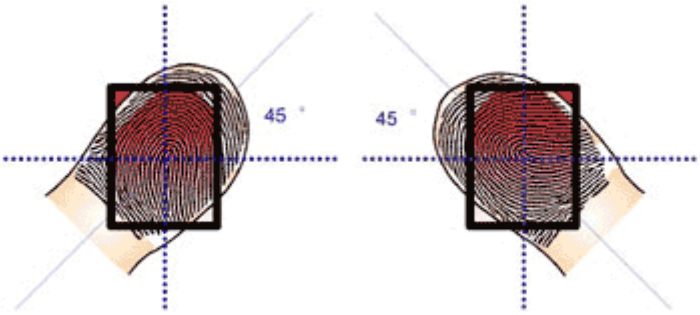
Averiguou-se que um dos fatores da geração de imagens de baixa qualidade foi o posicionamento incorreto do dedo na área de captura do leitor. A figura 4 ilustra erros freqüentes de posicionamento do dedo no leitor, observados na fase de coleta de dados.

Figura 4 : Maneiras incorretas de uso do leitor

Fonte: Elaborado pelos autores.

Outro fator gerador de ocorrências de *FRR* foi posicionamento do dedo de forma incorreta quanto ao angulo em relação ao plano horizontal, pois o modelo testado suporta variações de até 45°.

Figura 5 : Grau de rotação do dedo no leitor



Fonte: Elaborado pelos autores.

A figura 5 ilustra o grau máximo de inclinação do dedo no leitor.

5.2. Comércio eletrônico

Pretende-se, no experimento 2, identificar e medir qual o impacto do emprego de tecnologias de segurança em aplicações de comércio eletrônico? Entende-se aqui, ao contrário da Biometria, que há diversas considerações a serem levantadas, com maior ênfase no software a ser desenvolvido – ao contrário da Biometria, que detém alta dependabilidade de hardware.

O objetivo do trabalho conduzido está ligado diretamente ao impacto, no desempenho, de se utilizar tecnologias de segurança no comércio eletrônico, uma vez que todas as transações eletrônicas nesse segmento exigem serviços de segurança - como privacidade, integridade, autenticidade e não-repúdio (ADAM et al, 1999; GARFINKEL; SPAFFORD, 1999; STALLINGS, 1998). Há a necessidade de se dotar tais serviços; contudo, sabe-se qual será o impacto no desempenho desses sistemas?

Haverá aumento significativo no custo tempo de operações?

Para responder a essa questão, conduziu-se um experimento, considerando os dados coletados na execução de um protótipo cliente/servidor desenvolvido com base nas principais tecnologias de segurança para o comércio eletrônico e a conseqüente análise do impacto do uso das mesmas (FLORES; RIBEIRO, 2006).

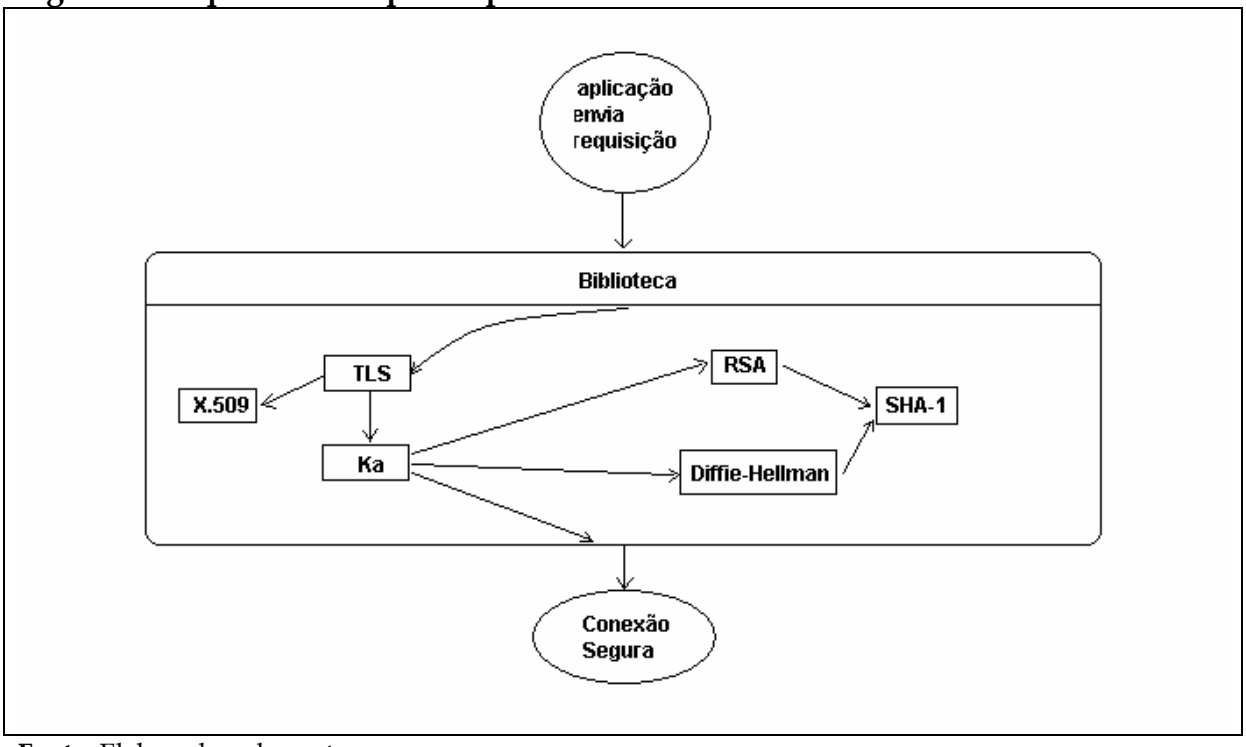
O experimento foi conduzido sob condições de laboratório - isto é, embora tendo sido considerados protocolos empregados pela Internet, os tempos de espera e

outros fatores poderiam demandar análises mais complexas, possibilitando que esse trabalho possa ser conduzido, brevemente, em condições de campo.

5.2.1. Considerações técnicas

O protótipo foi desenvolvido em arquitetura cliente - em número de dois - e servidor, tendo sido possível verificar como funcionou a troca de mensagens e o comportamento e eficácia de algumas tecnologias de segurança empregadas - considerando-se uma rede exclusivamente projetada para o experimento. Os equipamentos da rede tinham a mesma configuração: 15 computadores PC Pentium 4 2.2GHz, com 256 MB de memória RAM e disco rígido de 40 GB, com conexão via "switch", com placas de rede com protocolo Fast Ethernet 100Mbps. Essas máquinas passam a ser conhecidas como servidor, cliente 1 e cliente 2. As considerações sobre medição temporal já levam em conta o tempo de latência dessa sub-rede.

Figura 6 : Arquitetura do protótipo desenvolvido



Fonte: Elaborado pelos autores.

Para a arquitetura representada pela figura acima referida, foi desenvolvido um protótipo em "Object Pascal" - Delphi - para a plataforma Windows; tendo sido executado no ambiente de rede local para a coleta dos dados, conforme já citado.

Conforme é possível inferir, essa arquitetura propõe o emprego de chaves públicas, gerência das últimas, cifragem e decifragem de mensagens, assim como assinatura e verificação das mensagens, vindo, assim, a fornecer os serviços de segurança de autenticação, não repúdio, e privacidade – essenciais quando se trata de comércio eletrônico.

A arquitetura acima propõe a utilização TLS, X.509, RSA/Diffie-Hellman, SHA-1. Entretanto, este trabalho fez algumas restrições na utilização das tecnologias. Por exemplo, os algoritmos que empregam criptografia que este protótipo trabalha são RSA/Diffie-Hellman e SHA-1. A tecnologia conhecida como padrão X.509 não foi implementada, porque não foi possível encontrar um servidor de certificado digital disponível para realizar a implementação desse servidor. Entretanto, prevendo futuros trabalhos, o servidor já dispõe de uma classe preparada para trabalhar com o X.509.

TLS: ou "Transport Layer Security", é um protocolo criptográfico que buscar prover comunicação segura na Internet. Foi derivado do Secure Sockets Layer – ou SSL -, da Netscape, e padronizado pela Internet Engineering Task Force. Após o estudo teórico do mesmo, foi implementado baseando-se na RFC2246. O TLS foi empregado em todas as mensagens com ou sem segurança e sem a necessidade do uso de todos os recursos descritos na RFC que a propõe (DIERKS, 2004).

X.509: Padrão que serve de base para a infra-estrutura de chaves públicas pela "Internet Engineering Task Force". Esse padrão foi considerado no presente trabalho, mas não implementado foi estudada essa tecnologia; entretanto, conforme já citado, não foi implementada por questão de custo econômico. As RFCS que tratam do X.509 são as RFC2459 e RFC3039 (BLAKE-WILSON et al., 2004,; IBM, 2006; TUECKE; WELCH, 2004).

RSA/Diffie-Hellman: são clássicos esquemas de chave pública, necessários para fornecer os serviços de privacidade e não-repúdio. Ambos os esquemas foram implementados, a fim de obter o serviço de privacidade na troca de mensagens. O servidor fornece dois parâmetros ("g" e "n") para os clientes que conectarem ao servidor. O cliente informa uma chave privada ("x/y") e o sistema calcula a chave pública que é trocada entre os clientes. Depois da troca, é calculada a chave pública comum entre os dois clientes. A chave pública é empregada no momento de cifrar a mensagem, enquanto que a chave privada é usada para decifrar a mensagem no

momento em que há a troca de mensagens entre os clientes (JAIN, 1997; NICKOLS, 1998; SCHNEIER, 1994; STALLINGS, 1998).

SHA-1: é um esquema para assinatura digital, necessário para fins de prover o serviço de autenticação, ou validar uma mensagem. A validação, no protótipo desenvolvido, é necessária para trabalhar a mensagem que foi cifrada pelo cliente 1 e decifrada pelo cliente 2. Quando o cliente 2 recebe a mensagem, ele decifra a mensagem e, aplicando o SHA-1 na mensagem decifrada, pode realizar a comparação das assinaturas. Caso forem iguais à mensagem, então esta é considerada válida (SCHNEIER, 1994; STALLINGS, 1998). Deve ser lembrado que, durante a condução do presente estudo, não havia notícias de ataques a essa última tecnologia. Há trabalhos que indicam possíveis ataques ao RSA e, recentemente, ao SHA-1. No entanto, tais ataques limitam-se a realidades acadêmicas – nem sempre presentes no cotidiano.

Contudo, tais algoritmos foram escolhidos para o desenvolvimento do protótipo, em função da simplicidade, o que permite manter o foco do trabalho nas questões de desempenho e sua medição.

O módulo servidor opera da seguinte forma: o servidor disponibiliza alguns parâmetros para os clientes, faz o gerenciamento da troca de mensagens entre os clientes e possibilita salvar o "log" em um arquivo do tipo texto. Primeiramente o servidor é inicializado, para que sejam informados parâmetros - no caso, os valores de "g" e "n" e escolher o tipo de criptografia que será usada pelos clientes. Se nenhum tipo de segurança foi selecionado, então a troca mensagens será feita de modo padrão - Diffie-Hellman. Esse servidor também trabalha como um "midleware" entre os clientes, porque ele recebe e envia mensagens de dados e confirmação. Os parâmetros "g" e "n" devem respeitar a definição do método Diffie-Hellman, podendo o valor n ser empregado, também, no método RSA – também respeitando as suas definições.

Com relação ao módulo cliente, suas funcionalidades englobam o estabelecimento da conexão com o servidor, geração das chaves (pública e privada), envio e recebimento de mensagens e manutenção de um "log" em um arquivo tipo texto. Quando da inicialização do módulo cliente, é necessário informar dois parâmetros: computador escolhido e nome, para que se possa conectar ao servidor. Quando ativado o botão CHK ao lado do nome, é estabelecida a conexão com o servidor e se recebe uma mensagem de resposta.

Após receber os parâmetros "g" e "n" e apresentar ao usuário as possíveis tecnologias de segurança (TLS, RSA, SHA-1 e X.509) que podem ser utilizadas, é apresentada a mensagem no rodapé: "Conectado a <servidor> - Versão <protocolo TLS>". Se estiver somente marcado o TLS, pode-se enviar a mensagem sem fazer a troca de chaves, porque o servidor escolheu a forma que os clientes estão trabalhando sem nenhuma outra opção de uso de tecnologia de segurança. O cliente calcula a chave pública que será enviada para o outro cliente através do método criptográfico RSA, utilizando a chave privada, e os parâmetros "g" e "n". O resultado desse cálculo é enviado para o servidor, que envia para outro cliente.

O servidor recebe a mensagem e aguarda que o próximo cliente requisite a mensagem para que ele possa enviá-la. Ao receber a mensagem, o cliente calcula através do RSA para obter as chaves pública e privada que serão utilizadas por ele.

Nesse momento, os clientes e o servidor estão prontos para fazer a troca de mensagens com segurança, de acordo com as tecnologias adequadas que foram selecionadas no servidor. Quando um dos usuários digita a mensagem e aciona a funcionalidade escolhida, o sistema aplica todas as tecnologias de segurança que o servidor tiver escolhido - o que permite analisar o impacto individual de cada uma delas, considerando cada opção escolhida.

Se estiver utilizando RSA/Diffie-Hellman e SHA- 1, o sistema cifra a mensagem, utilizando a chave pública e aplica a assinatura digital na mensagem original, para que o usuário que recebe a mensagem possa verificar a autenticidade e a integridade da mesma.

Após acionado, iniciando a troca de mensagens, o sistema busca a mensagem e a decifra, utilizando a chave privada e, se necessário, aplica a assinatura digital na mensagem decifrada para poder validar a assinatura da mensagem que havia recebido. O conteúdo que o cliente recebe contém a mensagem cifrada e a assinatura digital quando solicitado, sendo essa assinatura digital da mensagem recebida que é comparada com a assinatura da mensagem decifrada, para fins de verificação.

A vantagem de se empregar os módulos clientes descritos na forma acima é que o emprego de tal módulo tanto pode representar um consumidor, quanto um negociante – simulando uma situação real de emprego.

5.2.2 Resultados Obtidos e Considerações sobre o Experimento 2

As condições de experimentação foram as seguintes, considerando as três situações exploradas para posterior análise de dados:

- no primeiro caso, cada protótipo cliente/servidor foi executado sem nenhum tipo de serviço de segurança disponível.
- no segundo caso, cada protótipo cliente/servidor foi executado, utilizando Diffie-Hellman/RSA na segurança da troca de mensagens.
- e no terceiro e último caso, cada protótipo cliente/servidor foi executado na combinação de Diffie-Hellman/RSA e SHA-1 para troca de mensagens com segurança.

O TLS foi utilizado nos três casos: observou-se mínimo impacto - provavelmente, por já vir incorporado em diversas tecnologias. Em todos os casos, foram utilizadas as mesmas mensagens para tornar possível a avaliação do impacto no desempenho.

Para fazer essa verificação no protótipo, foram definidas trinta e quatro mensagens, que têm tamanhos diferentes, para que se possa coletar o tempo utilizado por cada processo e, além disso, possa visualizar as mensagens com criptografia e assinatura digital. Cada mensagem foi submetida quarenta vezes, e os tempos apresentados nas tabelas é o tempo médio para cada variável tempo. Assim, por exemplo, o tempo mínimo apresentado na tabela representa o tempo mínimo médio, considerando a média dos tempos mínimos das quarenta execuções. Em todos os três casos, foi usada a mesma informação nos parâmetros, para que se tenha o mesmo cenário nas três verificações. Após executar os testes, nos três casos, foi possível analisar os tempos de cada mensagem e identificar qual o impacto dessas tecnologias na troca de mensagens.

Essa verificação foi feita em dois momentos: no primeiro momento, utilizando uma máquina com plataforma Windows 2000 e, no segundo, utilizando três

máquinas com plataforma Windows XP. Nesse último caso, uma máquina era o servidor e as outras duas operaram como máquinas clientes.

Um ponto importante é que o servidor também é utilizado como um "middleware", fornecendo os parâmetros *g* e *n*, e repassando as mensagens de um cliente para outro. Nos testes, um cliente somente enviava as mensagens e outro só as recebia.

Como já citado, três foram as situações exploradas na experimentação, cujas condições se seguem.

Caso 1 - Protótipo Sem Serviço de Segurança

Nesse experimento, o cliente/servidor não utilizou nenhuma opção de emprego de tecnologia de segurança, a fim de obter o maior desempenho nas trocas de mensagens, servido como controle. Essa verificação foi feita para se obter um tempo base médio e apresentar, de forma objetiva, o impacto do Diffie-Hellman/RSA e SHA-1 no desempenho da troca de mensagens (comércio eletrônico). Os "logs" dos módulos clientes e do módulo servidor, nessa situação, estão divididos em máquina local e máquinas em rede.

Caso 2 - Protótipo com Diffie-Hellman/RSA

Já nesse experimento, o cliente/servidor utilizou o Diffie-Hellman/RSA na configuração de segurança, para fazer a criptografia das mensagens. Nesse caso, foi necessária a troca de chaves entre os clientes para gerar a chave pública comum entre eles e gerar a chave privada de cada um deles. Os "logs" dos dados das máquinas de clientes e do servidor desse caso estão divididos em máquina local e máquinas em rede.

Caso 3 - Protótipo com Diffie-Hellman/RSA e SHA-1

Finalmente, nesse experimento, o cliente/servidor utilizou Diffie-Hellman/RSA e SHA-1 na configuração de segurança, para fazer a criptografia e assinatura digital das mensagens. Nesse caso, também foi necessário realizar a troca

das chaves entre os clientes para gerar a chave pública comum entre eles e gerar a chave privada de cada um deles. Os "logs" dos clientes e do servidor desse caso estão divididos em máquina local e máquinas em rede.

Os testes foram executados com mensagens que tinham tamanhos que variam de 10 bytes até 1339 bytes, em dois ambientes: numa máquina com Windows 2000 e em uma rede com três máquinas, com Windows XP.

Os dados coletados nestes testes foram analisados e parametrizados. A seguir, são apresentados dois quadros que contém os tempos máximo, mínimo e médio das mensagens enviadas e recebidas para os três casos descritos acima. A unidade de medida de tempo utilizada foi milésimos de segundos.

Tabela 1: Resultados do teste em Rede (tempo em milésimos de segundos)

Tempos (ms)	Caso 1			Caso 2			Caso 3		
	Env.	**Rec.**	**Total**	**Env.**	**Rec.**	**Total**	**Env.**	**Rec.**	**Total**
Mínimo	62	16	**93**	62	31	**93**	62	31	**93**
Máximo	125	47	**157**	79	63	**141**	93	140	**218**
Médio	73	36	**109**	74	46	**119**	74	50	**123**

Fonte: Elaborado pelos autores.

Analisando a tabela 1 do teste rede, é possível observar que o tempo mínimo foi igual nos casos dois e três, em relação ao caso 1 que não possuía configuração de qualquer tecnologia de segurança e que realizou o protocolo de modo mais rápido - como seria de se esperar. O tempo máximo mostrou que, cada vez que era incorporada uma tecnologia de segurança, aumentava o tempo de envio e recebimento de uma mensagem. Já o tempo médio mostrou que os casos 2 e 3 têm praticamente o mesmo tempo para envio e recebimento de mensagens. Contudo, o caso 3 emprega outra tecnologia de segurança, além da empregada no caso 2: o SHA-1. Assim, pode-se inferir, em um primeiro momento, que a tecnologia SHA-1 não incorre em impacto sensível com a tecnologia de medição empregada para o tempo.

A seguir, são apresentados os resultados dos tempos obtidos no teste 2, em situação de máquina local.

Tabela 2: Resultados do teste - local (tempo em milésimos de segundos)

Tempos (ms)	Caso 1			Caso 2			Caso 3		
	Env.	Rec.	Total	Env.	Rec.	Total	Env.	Rec.	Total
Mínimo	60	30	**90**	60	30	**90**	60	30	**90**
Máximo	80	40	**120**	81	131	**201**	81	130	**210**
Médio	67	34	**101**	70	41	**111**	69	41	**109**

Fonte: Elaborado pelos autores.

Analisando a tabela 2 do teste local, é possível verificar que o tempo mínimo foi igual nos três casos. Os valores de tempo máximo mostraram que, cada vez que era incorporada uma tecnologia de segurança, aumentava o tempo de envio e recebimento de uma mensagem – como esperado. Já os valores de tempo médio mostram que os casos 2 e 3 têm praticamente o mesmo tempo para envio e recebimento de mensagens; entretanto, o caso 3 emprega outra tecnologia de segurança, além da empregada no caso 2: o SHA-1.

A análise dos resultados apresentados nas tabelas 1 e 2 possibilitou constatar que a utilização de segurança é viável em termos de desempenho e necessária para que haja privacidade, confiabilidade, autenticidade e integridade das partes que utilizarão as aplicações para Comércio Eletrônico. Entretanto, é preciso levantar algumas considerações: certamente, para realizar uma implementação em condições de campo, devem ser empregados algoritmos otimizados para criptografia, assinatura digital e certificados digitais; ademais, lembra-se que é imprescindível que a rede e máquinas encontrem-se corretamente configuradas para as comunicações necessárias.

6. LIMITAÇÕES DO EXPERIMENTO DO PRESENTE TRABALHO

Uma limitação que se deve destacar é que o trabalho foi conduzido exclusivamente em situação de laboratório – isto é, as condições não são reais, mas atendendo aos requisitos de controle em uma experimentação. Certamente, ao se realizar experimento em campo, poder-se-á obter resultados diversos daqueles aqui apresentados. Há ainda, como limitações desse trabalho, o tamanho máximo das

mensagens (em torno de 1.400 bytes), e o número de clientes que o servidor comportou (limitado a 2). Alguns fatores que provavelmente vieram a afetar o tempo de envio e recebimento de mensagens, foram:

> • a pequena capacidade da memória dos computadores envolvidos em cifrar e decifrar as mensagens – visto que, dependendo do tamanho usado para as chaves (privada ou pública) é necessário o emprego de mais memória, para que não haja perda de desempenho; e
> • os algoritmos de criptografia, assinatura digital e certificação – a lógica aplicada no desenvolvimento desses algoritmos pode afetar no desempenho, visto que implementações comerciais que já empregam tais algoritmos utilizam técnicas de otimização desses algoritmos.

Uma outra limitação que deve ser considerada é o não emprego da tecnologia X.509, por motivos de não disponibilidade, no momento da condução do experimento, de um servidor público que viabilize a utilização dessa tecnologia.

Em termos de consumo de tempo, a tecnologia SHA-1 não se apresentou onerosa. Contudo, deve-se ter em vista reservas, visto haver recentes comunicações técnicas sobre ataques – até o momento, de cunho acadêmico, visando diminuir o número de chaves possíveis para a realização de um ataque de força bruta - a essa tecnologia.

De forma geral, considerando-se a análise dos dados obtidos, pode-se concluir que o emprego dessas tecnologias não incorreu em demanda de tempo sensível ao usuário – consideradas as condições de laboratório.

7. CONSIDERAÇÕES FINAIS – ONDE A ÉTICA E A SEGURANÇA PODEM FALHAR

Apenas tecnologia não é suficiente para garantir serviços de segurança no mundo virtual. Atividades simples, como a má seleção ou mesmo a ausência de política de troca periódica da senha para acesso a rede ou correio pode ser o início de problemas. A escolha da senha – com caracteres especiais, letras, números, minúsculas e maiúsculas -, bem como a sua troca a cada três meses – assim como a sua não-divulgação – fazem parte de uma cultura na qual nem sempre se reconhece o

valor da sigilosidade. Diversos usuários empregam senhas fáceis, não as trocam periodicamente, ou mesmo a anunciam – julgando pequena a importância de se manter em sigilo. A questão não é o risco individual: uma atitude dessas põe em risco todos os usuários da rede.

Graças a situações como essa, em 1988, a própria Internet ficou fora de serviço nos Estados Unidos. Algo talvez inconcebível, mas real. Pela primeira vez na história, um programa daninho havia atingido proporções enormes. O autor? Robert Tappan Morris – um estudante de 18 anos do curso de Ciência da Computação da Universidade de Cornell, New York. Em 12 horas, tal programa – atualmente conhecido como "Verme da Internet" havia atingido a costa oeste dos Estados Unidos. Um levantamento inicial acusou perdas de cerca de U$ 100 milhões – principalmente, devido a centros de pesquisa haver perdido seus trabalhos. Esse programa baseava-se nas falhas do sistema operacional Unix – na época, na versão 3. Talvez a grande causa de seu sucesso em invadir uma máquina em rede e impedir um usuário de usar essa mesma máquina tenha sido o emprego incorreto de senhas. Em levantamento que realizara previamente, Morris identificou um fato relevante: até então, grande parte das pessoas empregava, como senha, o próprio nome de usuário na rede, ou a inversão do mesmo. Essa situação mostra o quanto o usuário de computador, na época, preocupava-se com segurança, relegando o segredo da senha para um valor secundário.

Ainda sobre os riscos individuais, os anos 1990 receberam o impacto do caso Kevin Mitnik. Típico hacker, fora descrito por muitos como um indivíduo anti-social, e empregava o codinome "Condor". Mitnik obteve enorme sucesso graças ao que se chama hoje de engenharia social – ou seja, obtinha dados que possibilitavam seu acesso físico ou virtual a instalações diversas, empregando recursos de outros usuários para proveito próprio. Com disfarces simplórios, ele conseguia informações de pessoas sobre outras pessoas, e até mesmo dados que posteriormente expunham as senhas dessas mesmas pessoas.

Não apenas a despreocupação com relação à gerência de senhas de usuários contribui para problemas de exposição dos sistemas computacionais a situações de

falha, erro ou mesmo defeitos. Desde os anos 80, têm sido comuns as pragas virtuais conhecidas como vírus de computador. Considerando-se a grande quantidade de usuários de programas da Microsoft, as facilidades de integração dos aplicativos da suíte Office dessa *softwarehouse*, bem como a facilidade de emprego de macros nesses programas, foi apenas questão de tempo até que se desenvolvesse um vírus específico. Um exemplo recente foi o vírus Melissa; contudo, pela primeira vez na história, uma pessoa foi presa assumindo ser o autor de um programa daninho: David L. Smith, de 30 anos, de Aberdeen, em New Jersey. Até então, jamais se viu um vírus com replicação tão rápida, pois ele afetava os documentos do Microsoft Word versões 97 e 2000 e, empregava o programa de correio eletrônico Microsoft Outlook para comunicar-se – destinando mensagens para todos os que constavam na agenda do usuário.

Pode-se observar, assim, que a participação do usuário é de vital importância para o emprego seguro da tecnologia. O emprego de senhas ditas seguras, a atualização de programas antivírus, não ler documentos anexados a mensagens sem ter empregado antes um programa verificador, não executar programas sem o conhecimento de suas reais funcionalidades, não confiar nem empregar *links* para sites onde é solicitada a senhas ou outras informações pessoais, etc. são atitudes que um usuário pode tomar e que são de grande valia para todos os usuários de um sistema computacional – evitando problemas como indisponibilidade de todos ou parte dos serviços.

Talvez o emprego mais curioso da tecnologia em termos de fraude não tenha sido desenvolvido com intenções malignas. É a geração automática de *papers:* três estudantes do *Massachussets Institute of Technology* desenvolveram um programa que gera, de forma automática, artigos da área de Ciência da Computação. Por enquanto, restrito a apenas essa área, e em inglês. A preferência se deve ao fato de haver diversas bases de dados disponíveis nessa língua, na rede e nessa área. O programa desenvolvido é tão refinado, que gera também os objetos freqüentemente empregados em artigos dessa área, tais como figuras, citações, gráficos, etc. O propósito inicial declarado pelos estudantes era gerar material para submeter a

ISSN: 1980-0193

eventos ditos indesejáveis e, cujas chamadas, são reconhecidas tradicionalmente como spam. Eles submeteram dois artigos gerados pelo programa a uma dessas conferências e o resultado foi à aceitação de um como um artigo "não-revisado", e a rejeição do outro – sendo que, para esse último, foi solicitado revisão, e o presidente da conferência respondeu desculpando-se pela avaliação. Maiores detalhes podem ser avaliados no site <http://www.pdos.lcs.mit.edu/scigen>.

Os resultados dos experimentos conduzidos permitem afirmar que, em condições de laboratório, o custo computacional não é elevado – o que favorece a disseminação dessas tecnologias, visto que o grau de segurança oferecido possibilita melhores condições de confiabilidade no sistema.

Certamente, a tecnologia por si não é suficiente para conter as diversas ameaças. O aspecto humano, no que tange à educação, ou mesmo a motivação em um ambiente de trabalho, é extremamente relevante. Não é cabível dotar um sistema automatizado de defesa, considerando que usuários podem expor a segurança de toda uma rede, mesmo que de forma não consciente. O emprego de técnicas automatizadas possibilita minimizar o trabalho de quem gerencia os recursos comunitários; permite identificação de pontos fracos, entre outras facilidades. Assim, não se deve prescindir de ferramentas – entenda-se programas.

Contudo, a educação e a parceria do usuário ainda são as melhores políticas.

REFERÊNCIAS

ADAM, N. R.; DOMAGRACI, O.; GANGOPADHYAY, A. **Electronic Commerce**. Upper Saddle River: Prentice Hall PTR, 1999.

BERNSTEIN, Terry et al. **Segurança na Internet.** Rio de Janeiro: Campus, 1997.

BLAKE-WILSON, S.; NYSTRON, M.; HOPWOOD, D; MIKKELSEN, J. **RFC 3546 (Draft) Transport Layer Security (TLS) Extensions**. 2004. Disponível em: <www.ietf.org/rfc>. Acessado em 02 ago. 2006.

BLOOMBECKER, J. **Spectacular Computer Crimes**. Disponível em: <http://www.kevinmitnick.com/compcri.html> Acessado em 12 fev. 2005.

CARVALHO, C. R. de. **Detecção automática de minúcias em impressões digitais**, [S.l.], 2001. Disponível em: <http://www.cpdee.ufmg.br> Acessado em: 12 Set. 2003.

CHAMPOD, C. E. L. Numerical Standards & Probable Identifications**. Journal of Forensic Identification Philadelphia**. v. 45, n. 2, p.136-163. (1995).

COSTA, S. M. F. **Classificação e Verificação de impressões Digitais.** 2001. Dissertação (Mestrado em engenharia Elétrica). Escola Politécnica, Universidade de São Paulo, 2001.

DIERKS, T.; RESCORLA, E. **RFC 2246 (Draft) The TLS Protocol Version 1.1**. 2004. Disponível em: <www.ietf.org/rfc> Acessado em 21 fev. 2006.

FIGINI, A. R. da L.; SILVA, J. R.; JOBIM, L. F.; SILVA, M. **Identificação Humana.** 2. ed. São Paulo: Millenium, 2003.

FLORES, R. T.; RIBEIRO, V. G. Medindo o Custo de Serviços de Segurança em Sistemas de Informação Orientados a Comércio Eletrônico. **RESI Revista Eletrônica de Sistemas de Informação**, v. 5, p. 1-7, 2006.

GARFINKEL, S.; SPAFFORD, G. **Comércio e Segurança na WEB**. São Paulo: Market Press, 1999.

GONZALEZ, R. C.; WOODS, R. E. **Processamento de imagens digitais**. Tradução de Roberto Marcondes César Filho e Luciano da Fontoura Costa. São Paulo: Edgar Blucher, 1992.

HONG LIN, JAIN, A., WAN YIFEI. Fingerprint Image Enhancement: Algorithm and Performance Evaluation. **Proocedings of the IEEE**, New York, v. 20, n. 8, p. 777-789, Aug. 1998. Disponível em em: <http://www.researchindex.com> Acessado em 21. set. 2006.

IBM. **iKP.** Disponível em: <http://www.zurich.ibm.com/security/pastprojects/ecommerce/iKP.html> Acessado em 20. maio 2006.

JAIN, A. K. Et. An Identity-Authentication System Using Fingerprints. **Proocedings of the IEEE**, New York, v. 85, n. 9, p.1365-1388, 1997.

JONSSON, J.; KALISKI, B. **RFC 3447 Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1**. 2003. Disponível em: <www.ietf.org/rfc>. Acessado em 20 maio 2006.

KIM, H-J. Biometrics, is it a viable proposition for identity authentication and access control? **Computers & Security**, Oxford, v.14, p. 203-213, 1995.

LÉVY, P. **As Tecnologias da Inteligência**. Rio de Janeiro: Editora 34, 1993.

MALTONI D., D. MAIO, A.K. JAIN, S. PRABHAKAR. **Handbook of Fingerprint Recognition.** New York: Springer, 2003, p. 3-53.

MEDEIROS, T. dos S.; RIBEIRO, V. G. Um estudo comparativo para análise de filtros de spams. **Revista do CCEI**, Bagé, v. 9, n. 15, p. 36-45, 2005.

MENEZES, A. J.; VAN OORSCHOT, P. C.; VANSTONE, S. A. **Handbook of Applied Cryptography**. Boca Raton: CRC Press, 1996.

MINOLI, D.; MINOLI, E. **Web Commerce Technology Handbook**. New York: McGraw-Hill, 1998.

NICHOLS, R. K. **ICSA - Guide to Cryptograph.** New York: McGraw-Hill, 1998, p. 650-675.

RIBEIRO, V. G. ; WEBER, R. F. Um estudo sobre os métodos de pesquisa utilizados em segurança computacional - Criptografia. In: VII Congreso Argentino de Ciências de la Computacion, 2001, El Calafate. **Anais do VII Congreso Argentino de Ciências de la Computacion**. El Calafate: Universidad Nacional de la Patagonia Austral, 2001.

SCHNEIER, B. **Applied Cryptography:Protocols, Algorithms and Source Code in C**. New York: John Wiley, 1994.

SMITH, R. E. **Internet Cryptography**. Massachussets: Addison-Wesley, 1997.

SPOFFORD, E. H. The Internet Worm Program: An Analysis. **Computer Communication**. Purdue University. 8 Dez. 1988.

STALLINGS, W. **Cryptography and Network Security**. Upper Saddle River: Prentice-Hall, 1998.

STANLEY, W. D. **Network Analysis with applications**. Upper Saddle River: Prentice Hall, 2002.

TUECKE, S.; WELCH, V. E. **RFC 3820: Internet X.509 Public Key Infrastructure (PKI).** 2004. Disponível em: <www.ietf.org/rfc> Acessado em: 25 maio 2006.

NOTAS

(1) Possui graduação em Ciências da Computação pela Universidade Federal do Rio Grande do Sul (1994), graduação em Bacharel em Ciências Náuticas pelo Ministério da Marinha (1984), mestrado em Administração pela Universidade Federal do Rio Grande do Sul (1997) e doutorado em Ciências da Computação pela Universidade Federal do Rio Grande do Sul (2005). Atualmente é professor da Faculdade Cenecista Nossa Senhora dos Anjos e professor assistente do Centro Universitário Ritter dos Reis. Tem experiência na área de Ciência da

Computação, com ênfase em Segurança da Informação, atuando principalmente nos seguintes temas: segurança computacional, criptografia, redes de computadores, criptografia de chave pública e sistemas de detecção de intrusão. Suas áreas de interesse incluem ainda a Computação Simbólica. E-mail de Contato: vinicius@uniritter.edu.br. Endereço profissional: Rua Orfanotrófio, 555 – Alto Teresópolis – Porto Alegre/RS - Brasil.

(2) Possui graduação em Engenharia Química pela Universidade Federal do Rio Grande do Sul (1987), mestrado em Engenharia Mecânica pela Universidade Federal do Rio Grande do Sul (1990) e doutorado em Engenharia Mecânica pela Universidade Federal do Rio Grande do Sul (1994). Atualmente é Professor Adjunto da Universidade Federal do Rio Grande do Sul. Tem experiência na área de Engenharia Mecânica, com ênfase em Fenômenos de Transporte. Atuando principalmente nos seguintes temas: transporte de nêutrons, Método Nodal, Equação SN. E-mail de Contato: zabadal@ufrgs.br. Universidade Federal do Rio Grande do Sul – Av. Osvaldo Aranha, 99 – 4º andar – Centro – Porto Alegre/RS – Brasil

(3) Graduou-se em Ciência da Computação pelo Centro Universitário La Salle (2004). Atualmente, trabalha com sistemas de biometria. E-mail de Contato: victor@ditech.com.br. Rua Dom Pedro II, 891/605 – São João – Porto Alegre/RS - Brasil.

Enviado: 15/03/2007
Aceito: 13/09/2007
Publicado: 12/12/2007