Projeto Ralnet: avanços e resultados

SIDCLEY DA SILVA SOARES[1]
ALEX DA ROSA MEDEIROS[2]
ADRIANO PETRY[3]
ADRIANO ZANUZ[4]

RESUMO

Este trabalho apresenta os principais avanços e resultados obtidos no Projeto RALNET: Desenvolvimento e Aplicação de Tecnologias de Reconhecimento Automático de Locutor para Autenticação de Usuários em Redes de Computadores, desenvolvido junto ao laboratório de Redes e Hardware da Universidade Luterana do Brasil, com apoio do CNPq.

Palavras-chave: *reconhecimento de locutor, criptografia, redes de computadores, autenticação de usuários, processamento de voz.*

ABSTRACT

This work presents the main results and advances obtained with RALNET Project: Development and Application of Automatic Speaker Recognition Technologies for User Authentication in Computer Networks, developed in Networks and Hardware Laboratory of Universidade Luterana do Brasil, with sponsor of CNPq.

Key words: *speaker recognition, cryptography, computer networks, user authentication, speech processing.*

[1] Acadêmico do Curso de Ciência da Computação/ULBRA – Bolsista do CNPq

[2] Acadêmico do Curso de Ciência da Computação/ULBRA – Bolsista PROICT/ULBRA

[3] Professor – Orientador do Curso de Ciência da Computação/ULBRA (adpetry@ulbra.tche.br)

[4] Professor do Curso de Ciência da Computação/ULBRA

INTRODUÇÃO

Uma das técnicas mais utilizadas para garantir a segurança de transações em redes de computadores envolve a identificação e a autenticação de usuários. A identificação e a autenticação são os processos de reconhecimento e de verificação da identidade de usuários válidos. Uma nova forma de identificação e autenticação de pessoas pode ser realizada através da análise de sua voz. Desse modo, técnicas de Reconhecimento Automático de Locutor (RAL) podem ser utilizadas para validar a identidade de um usuário através de uma medida biométrica vocal. Como o sinal de voz gerado por uma pessoa nunca será igual a outro já gerado, o sistema de verificação vocal será capaz de identificar tentativas de fraude, caso a senha vocal apresentada para análise seja coincidente com outra já utilizada. A utilização de senhas vocais aumentará a confiabilidade do sistema como um todo, possibilitando a implementação prática de uma autenticação robusta.

A Internet é uma rede de alcance mundial de computadores que utiliza o protocolo TCP/IP para suas comunicações. O uso dessa rede fornece uma série de benefícios em termos de aumento ao acesso à informação para diversos tipos de instituições (educacionais, governamentais, comerciais, etc.). Porém, o acesso a redes de computadores apresenta diversos problemas significativos relacionados à segurança. Os problemas inerentes do protocolo TCP/IP, a complexidade da configuração de servidores, as vulnerabilidades introduzidas no processo de desenvolvimento de software e uma variedade de outros fatores tem contribuído para tornar computadores despreparados abertos à ataques de intrusos.

O projeto RALNET: Desenvolvimento e Aplicação de Tecnologias para Reconhecimento Automático de Locutor em para Autenticação de Usuários em Redes de Computadores, vem sendo desenvolvido junto ao Laboratório de Redes e Hardware da Universidade Luterana do Brasil (ULBRA), com apoio do Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq). Dentre os objetivos propostos nesse projeto, salientam-se o estudo de tecnologias de RAL aplicáveis em sistemas de segurança de redes de computadores, o planejamento de um sistema capaz de integrar as tecnologias de RAL e sistemas para transações pela Internet, e a construção e validação de um protótipo capaz de efetivamente utilizar tais tecnologias e efetuar a autenticação por voz de usuários localizados remotamente. Este trabalho apresenta os resultados já alcançados no projeto, assim como o desenvolvimento técnico obtido.

MATERIAL E MÉTODOS

A autenticação de usuários em sistemas digitais quaisquer pode apresentar diferentes graus de confiabilidade. Inicialmente, podemos imaginar sistemas onde o usuário é autenticado utilizando uma informação secreta de seu conhecimento (senha). Esse tipo de sistema apresenta vulnerabilidades relacionadas ao roubo da informação secreta. Isso muitas vezes acontece através da utilização de programas que recebem todas informações inseridas no sistema e as enviam para seu criador. Outras vezes, as pessoas escolhem senhas que podem ser mais facilmente descobertas, como data de nascimento, seu próprio nome, etc. Nesses casos, tentativas sistemáticas de acesso poderão resultar na descoberta dessas senhas.

Outra forma de tentar dificultar a ação de fraudadores é a utilização de elementos físicos para permissão do acesso a sistemas. Muitas vezes, os elementos utilizados são cartões magnéticos que armazenam informações do usuário. Assim, para que um intruso consiga acesso ao sistema ele necessariamente deverá roubar o cartão magnético da vítima. A fim de aumentar ainda mais a confiabilidade de sistemas que utilizam dispositivos físicos de acesso, por vezes esse tipo de segurança é combinado com a necessidade de conhecimento de uma senha secreta. Assim, um sistema que exige uma informação que apenas o usuário saiba associado a um dispositivo físico que apenas o usuário possua, garante uma maior confiabilidade ao sistema. Esse tipo de proteção atualmente é adotado em muitos sistemas que exigem um certo grau de segurança, como o sistema bancário. Ainda assim, esses sistemas podem ser fraudados pelo extravio do dispositivo de acesso e a descoberta da senha secreta.

Em um terceiro nível de segurança, podemos imaginar um sistema que não requeira informação secreta do usuário (que pode ser descoberta), nem mesmo a posse de um cartão magnético (que pode ser roubado), mas forneça o acesso ao usuário apenas se ele puder provar que ele é realmente o usuário com direito de acesso, através de uma medição biométrica. A possibilidade de utilização de técnicas para RAL em sistemas reais é uma das grandes motivações dos trabalhos desenvolvidos na área. Outras técnicas também poderiam ser utilizadas para a confirmação automática da identidade de uma pessoa através de medidas biométricas, sem intervenção humana. Alguns exemplos são o reconhecimento da íris, reconhecimento de face, análise da impressão digital, verificação das características geométricas da mão, avaliação da forma do caminhar, análise da assinatura, etc. Por outro lado, a autenticação biométrica através da voz possui várias vantagens intrínsecas, quando comparadas às outras técnicas biométricas, como:

- Facilmente adquirida, sem a necessidade de hardware específico. Apenas um microfone de custo reduzido é capaz de adquirir a voz do locutor com precisão.
- Não intrusiva, isto é, não existe a necessidade de contato físico do usuário com o sistema de captação da voz.
- Natural e de fácil aceitação. As maioria das pessoas se comunicam através da voz, que é um método extremamente difundido e utilizado, excetuando-se as pessoas com necessidades específicas.
- Não requer treinamento, ou seja, os usuários podem ser autenticados sem que necessitem aprender a lidar com o sistema.
- Pode ser facilmente utilizada em redes telefônicas, permitindo a autenticação remota, sem a necessidade de qualquer equipamento extra, uma vez que o próprio aparelho telefônico já possui o transdutor para a captação do sinal de voz.

Pode-se identificar muitas aplicações práticas para os sistemas de RAL. De uma forma geral, os sistemas de autenticação de usuários através de senhas ou cartões poderiam ser substituídos por (ou agregados a) sistemas de RAL, estabelecendo-se uma confiabilidade superior.

SISTEMA PROPOSTO

O sistema construído funciona através de uma arquitetura cliente-servidor. O lado servidor conta com o acesso a um banco de dados para armazenamento e consulta de informações de usuários e padrões vocais. Além disso, a geração dos padrões de voz e a autenticação das informações extraídas a partir do sinal de voz do usuário é realizada também no lado servidor. A comunicação se dá através da Internet, utilizando técnicas de criptografia para troca de dados. No lado cliente, a interação com o usuário e captura do sinal de voz se dá pela manipulação de uma placa de som comum, que deverá estar presente no computador cliente. Parte do processamento digital do sinal de voz é realizado já no lado cliente, que envia apenas as informações extraídas a partir do sinal de voz, reduzindo assim o tráfego da rede e a carga de processamento no computador servidor. A figura 1 ilustra os principais blocos constituintes do protótipo desenvolvido, que são detalhados a seguir.

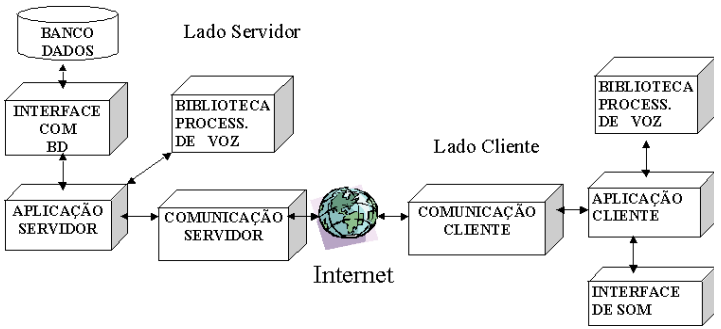

Figura 1 - Ilustração da arquitetura utilizada na construção do protótipo de autenticação remota por voz.

A linguagem de programação Java foi adotada para a construção do protótipo por oferecer recursos poderosos de programação para comunicação entre computadores, além de suportar diversas arquiteturas de hardware e sistemas operacionais. O ambiente de desenvolvimento utilizado foi o NetBeans IDE 3.5.1, com o kit de desenvolvimento Java 2 SDK standard edition versão 1.4.1. Apenas a biblioteca de processamento de voz foi implementada utilizando uma linguagem de programação diferente, a linguagem C++, através da ferramenta Visual Studio 6.0. Essa escolha foi feita principalmente pela maior velocidade de processamento oferecida e possibilidade de reutilização de código já construído ao longo de trabalhos anteriores (PETRY, 2002). O acesso à base de dados foi feito através de Java Database Connectivity (JDBC), utilizando um servidor de banco de dados MySQL (HORSTMANN & CORNELL, 2001).

TÉCNICAS PARA RAL EM UMA ARQUITETURA CLIENTE-SERVIDOR

As técnicas empregadas para o RAL são objeto de estudos e aperfeiçoamentos de pesquisadores há vários anos. Atualmente os algoritmos dis-

poníveis oferecem taxas de reconhecimento elevadas, permitindo a construção de sistemas bastante confiáveis. Um sistema para RAL é composto basicamente pelas etapas de treinamento e reconhecimento. A etapa de treinamento normalmente é realizada antes de se tentar reconhecer qualquer amostra de voz. Essa etapa abrange a aquisição do sinal vocal dos locutores que serão cadastrados no sistema, extração de informações úteis dessas amostras, geração dos padrões de voz que serão utilizados como referência na etapa de reconhecimento e identificação dos limiares de similaridade associados aos padrões gerados, para o caso de verificação de locutor. A etapa de reconhecimento ou autenticação abrange a aquisição do sinal de voz que será avaliado, extração de informações úteis e comparação dessas informações com os padrões gerados na etapa anterior. Nesse momento, o limiar de similaridade indicará se a identidade foi ou não aceita. A figura 2 ilustra as etapas de treinamento e reconhecimento para um sistema genérico de RAL.

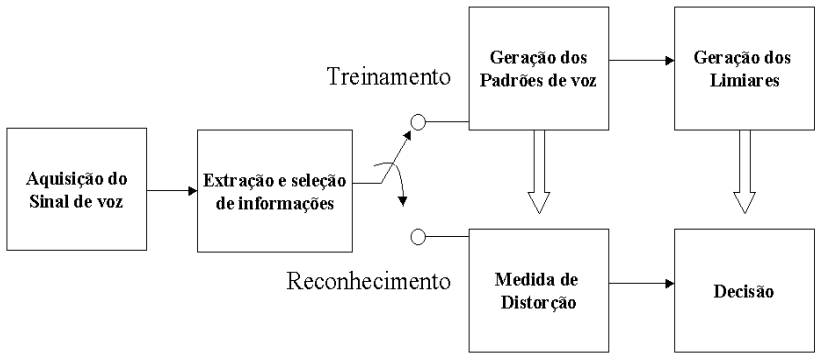

Figura 2 - Ilustração das etapas de treinamento e reconhecimento para um sistema genérico de RAL.

Neste trabalho, o processamento dos sinais de voz foi feito de acordo com resultados obtidos a partir de diversos experimentos práticos, que também são similares a vários outros trabalhos dos autores na área (PETRY, ZANUZ & BARONE, 1999; PETRY, 2002; PETRY & BARONE, 2002; PETRY & BARONE, 2003). Os algoritmos foram implementados utilizando a linguagem de programação C++, objetivando principalmente a redução no tempo de processamento requerido. Eles foram disponibilizados ao programa principal (escrito em linguagem Java) através de uma biblioteca de vínculo dinâmico.

No sistema proposto, as amostras de voz utilizadas são gravadas a uma freqüência de amostragem de 8000 Hz, com resolução de 16 bits por amostra em apenas um canal (mono). A seguir, um filtro digital de pré-ênfase com resposta em freqüência de +6 dB/oitava é aplicado ao sinal de forma a atenuar as componentes em baixa freqüência, nivelando o espectro do sinal. Posteriormente o sinal é dividido em janelas de curta duração, dentro das quais o sinal de voz pode ser considerado estacionário. As janelas do tipo hamming foram utilizadas com duração de 45 ms. Essas janelas são sobrepostas, sendo aplicadas a cada 10 ms do sinal de voz, de forma a suavizar a

extração das informações. As janelas de voz que contiverem apenas silêncio são descartadas, baseado na análise da energia do sinal contido na janela. A partir de cada janela de voz são extraídos 16 coeficiente mel-cepstrais e 16 coeficientes delta mel-cepstrais, que serão utilizados para a caracterização do locutor. Os procedimentos de aquisição da voz, pré-ênfase e extração de informações úteis são detalhados em diversos trabalhos, como em (DELLER, PROAKIS & HANSEN, 1987; RABINER & JUANG, 1993). O classificador utilizado é baseado em modelos de mistura de gaussianas (GMM), tendo sido empregadas 80 gaussianas adaptadas a partir de um modelo universal (UBM) para representação de cada padrão de voz. Maiores detalhes relativamente à implementação das técnicas empregadas na classificação podem ser obtidos em (REYNOLDS, QUATIERI & DUNN, 2000; PETRY & BARONE, 2003).

Ao se trabalhar com uma arquitetura cliente-servidor, é importante definir-se onde será realizado o processamento da voz adquirida no computador cliente. É possível transmitir-se todo o sinal de voz adquirido para o computador servidor. Entretanto, essa alternativa imporia um alto tráfego na rede, uma vez que os dados brutos de voz ocupam muitos bytes. Por exemplo, um sistema de cadastramento de um usuário que requerer 12 repetições de uma senha vocal composta de 5 dígitos, como sugerido em (CHIRILLO & BLAUL, 2003) em um produto comercialmente disponível, pode facilmente obter um minuto de fala. Se os dados brutos forem gravados a uma taxa de amostragem de 8000 Hz, 16 bits por amostra em apenas um canal, o espaço ocupado pelo sinal completo chegaria próximo a 1 MB. Além disso, o processamento de todo esse sinal (pré-ênfase, janelamento, extração de informações e geração do padrão de voz) seria realizado no computador servidor, elevando a carga de processamento requerida. Por outro lado, se a geração completa do padrão de voz fosse feita no computador cliente, que então enviaria ao servidor apenas o padrão gerado, poderiam haver sérios problemas relativos à segurança, como o envio de um padrão não confiável. Isso porque o computador cliente disporia dos algoritmos utilizados e dos padrões gerados, que poderiam ser utilizados para testes de padrões de autenticação, visando a quebra da segurança imposta pelo sistema. A situação seria pior se a fase de autenticação também fosse feita no computador cliente. Uma autenticação negativa poderia ser facilmente desprezada através de poucas mudanças no código do sistema. Assim, é importante que o computador servidor não sirva apenas como um repositório de padrões de voz e receptor de uma decisão sobre autenticação tomada em outro lugar, mas que o padrão de voz em si seja gerado assim como a comparação de padrões na autenticação sejam feitos lá.

No sistema proposto, as etapas de aquisição da voz, pré-ênfase, janelamento e extração de informações são realizadas no computador cliente, tanto no treinamento quanto no reconhecimento. Apenas as informações úteis extraídas são enviadas ao computador servidor, que gera o padrão de voz na fase de treinamento ou autentica o usuário, liberando o acesso a algum serviço restrito, na fase de reconhecimento.

BASE DE DADOS

Visando uma ágil e robusta forma para o armazenamento e consulta das informações utilizadas no sistema proposto, foi construído um banco

de dados para armazenar os padrões de voz e informações do usuário, assim como um conjunto de dados relativos à utilização do sistema, tais como: Internet Protocol (IP) do computador cliente, data de conexão, ações tomadas pelo cliente durante o decorrer da conexão. Foram utilizadas as tecnologias de acesso à base de dados Java Database Connectivity (JDBC) e servidor de banco de dados MySQL (HORSTMANN & CORNELL, 2001). Deve-se salientar que o sistema proposto não está atrelado a nenhum banco de dados específico, visto que é disponibilizada na aplicação servidora a opção de conexão com os servidores de banco de dados mais utilizados atualmente no mercado.

Informações como nome de usuário, padrões de voz, informações sobre aquisição da voz e extração de informações úteis, e a data em que o último padrão de voz foi atualizado são guardados na tabela Users. A Tabela Historic armazena informações a respeito de conexões realizadas por cada um dos usuários da aplicação. São armazenadas as informações que identificam o usuário, o IP do computador cliente, a data de conexão e as informações úteis extraídas a partir da voz do usuário. Esses dados podem ser usados para uma possível avaliação futura de desempenho do sistema.

COMUNICAÇÃO

A possibilidade de dispor de uma comunicação segura é de importância fundamental para qualquer sistema de autenticação. A partir do estabelecimento da comunicação segura, todo o tráfego de informações entre o computador cliente e servidor deve ser realizado utilizando técnicas criptográficas para garantir o sigilo e a integridade dos dados.

Neste projeto, optou-se por utilizar um algoritmo de chave única para cifrar e decifrar os dados, o Data Encryption Standard (DES) (SCHNEIER, 1996; TANENBAUM, 1997; STALLINGS, 1999). Um dos fatores que contribuiu para a escolha desse algoritmo refere-se à disponibilidade do cifrador junto ao kit de desenvolvimento utilizado (Java 2 SDK standard edition versão 1.4.1). Outro fator importante diz respeito à rapidez de execução do DES na cifragem e decifragem, quando comparado com algoritmos de chave assimétrica. O desafio para a perfeita utilização de algoritmos de chave única foca na troca segura da chave criptográfica entre os computadores cliente e servidor. Uma vez que inicialmente a comunicação segura ainda não existe enquanto a chave não é conhecida pelo lado cliente e pelo lado servidor, deve-se buscar meios para que ambos lados conheçam a chave que será utilizada. O envio "em aberto" de uma chave pode ser interceptado, invalidando assim toda a segurança da comunicação. Para resolver o problema de definição de uma mesma chave criptográfica no computador cliente e servidor, sem ter que envia-la de forma não segura, foi implementado o protocolo mostrado na figura 3. Nesse protocolo, foram utilizadas classes que tratam especificamente da parte de criptografia - classes CriptoClient e CriptoServer - e classes utilizadas no gerenciamento da aplicação e comunicação via Transmission Control Protocol (TCP) - classes Cliente e Servidor.

Inicialmente, o computador cliente solicita uma conexão ao computador servidor, que estabelece a conexão. A partir de então, o computador cliente gera um par de chaves assimétricas, utilizando o algoritmo Diffie-Hellman com extensão de 1024 bits (SCHNEIER, 1996), enviando para o servidor apenas a chave pública.

Da mesma forma, o computador servidor gera um par de chaves assimétricas e envia ao cliente sua chave pública. Nesse momento, tanto o lado cliente quanto o lado servidor possuem seu par de chaves assimétricas, e a chave pública do outro lado. O lado cliente gera então uma informação (segredo) utilizando sua própria chave privada (de conhecimento exclusivo e nunca transmitida) e a chave pública do computador servidor. A seguir o cliente envia ao servidor o tamanho do segredo gerado. O mesmo segredo gerado no cliente pode ser agora gerado no lado servidor. Isso é feito utilizando a chave pública do computador cliente, a chave privada do servidor (de conhecimento exclusivo e nunca transmitida) e sabendo-se o tamanho do segredo que deve ser gerado. Dessa forma, ambos lados cliente e servidor compartilham o mesmo segredo (utilizado como chave de extensão de 56 bits para o algoritmo DES), que foi gerado utilizando dados nunca transmitidos (chave privada).

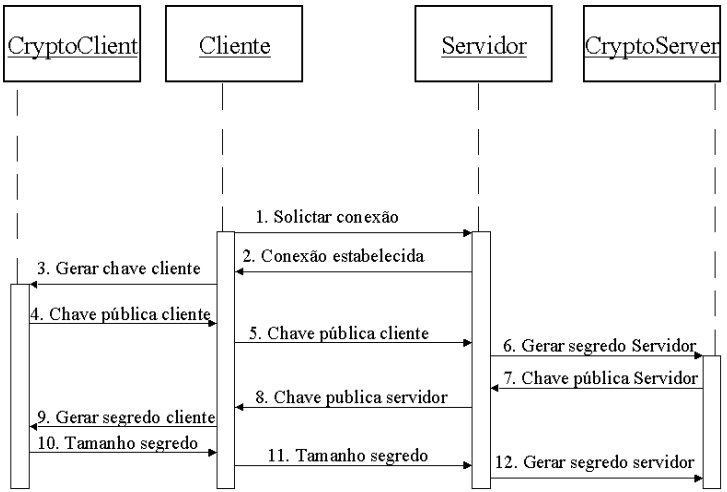

Figura 3 - Protocolo para estabelecimento de chave criptográfica.

APLICAÇÃO CLIENTE E SERVIDOR

As técnicas apresentadas devem ser utilizadas de acordo com a evolução da interação entre o computador cliente e servidor. Assim, foram desenvolvidas as chamadas aplicação cliente e aplicação servidora. Elas são responsáveis basicamente por implementar um protocolo de comunicação previamente definido para que se possa efetivamente realizar um cadastramento ou autenticação por voz. Além disso, devem ser capazes de utilizar os outros módulos disponíveis para acessar a base de dados, processar sinais de voz, comunicar-se com o outro lado de forma segura e interagir com o usuário a fim de adquirir amostras de sua voz.

A aplicação cliente e a aplicação servidora também são responsáveis pela interação com o usuário através de interface gráfica. Na janela construída para o lado cliente é possível: configurar parâmetros

como nome do usuário que utiliza o sistema, definir se será realizado um cadastramento ou autenticação, inserir dados sobre o computador servidor e ajustar controles de áudio.

DISCUSSÕES

Após a construção do protótipo foram conduzidos alguns testes iniciais para averiguação do perfeito funcionamento e possível correção de problemas. Os experimentos realizados foram executados inicialmente apenas entre os pesquisadores envolvidos na construção do sistema. Um dos fatores críticos que foi identificado refere-se a parte de aquisição do sinal de voz no computador cliente. Ficou clara a dificuldade que poderá surgir se não houver uma prévia calibração dos recursos de áudio no computador cliente. Coisas como ajuste automático do volume de gravação do microfone, desabilitação de qualquer dispositivo de reprodução durante a gravação da voz, e uma clara orientação ao usuário para o momento exato que deverá iniciar sua fala, poderão facilmente resultar na má utilização do sistema. Várias dessas características já foram incorporadas ao protótipo desenvolvido, mas acredita-se ser possível facilitar ainda mais a utilização do sistema em estudos futuros.

Outra questão que deve ser levada em consideração refere-se às brechas de segurança que esse tipo de sistema pode apresentar. Pode-se imaginar que a pré-gravação da voz de uma pessoa e sua reprodução para o sistema de RAL possa acarretar a aceitação incorreta de impostores. Isso é especialmente verdade com a utilização de recursos de gravação e reprodução sofisticados. Os sistemas para RAL pouco podem fazer contra esse tipo de erro. Os métodos mais eficientes que se pode conceber seriam uma vigilância permanente do dispositivo de aquisição de voz, ou o sistema requerer uma palavra pseudo-aleatória específica. Uma vigilância permanente, a fim de garantir que aparelhos de reprodução sonora não sejam utilizados, normalmente não é algo desejado em um sistema. Para o aspecto de o sistema requerer uma palavra pseudo-aleatória, palavras diferentes da requerida apresentariam um valor superior de distorção, impedindo uma falsa aceitação. O fato de a palavra ser pseudo-aleatória dificulta o sucesso de uma pré-gravação (PETRY, 2002).

CONCLUSÕES

Este trabalho apresentou os avanços obtidos no projeto RALNET, que resultaram em um protótipo desenvolvido para autenticação de usuários por voz em redes de computadores. O funcionamento geral do sistema construído foi descrito, assim como foram detalhados seus principais blocos constituintes. Diversos desafios foram encontrados ao longo do desenvolvimento deste protótipo, relacionados a problemas específicos de construção de alguma parte ou integração e teste do sistema completo. O protótipo construído deve servir apenas como intermediador para acesso a algum serviço remoto, como por exemplo comércio eletrônico, internet banking ou acesso a e-mails. Assim, deve haver uma preocupação também sobre formas para disponibilizar tal serviço com segurança.

AGRADECIMENTOS

Os autores agradecem ao Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) pelo apoio financeiro disponibilizado dentro do programa CT-INFO.

REFERÊNCIAS BIBLIOGRÁFICAS

CHIRILLO, J. ; BLAUL, S. **Implementing Biometric Security**. Wiley Publishing Inc., 2003.

DELLER, J. R.; PROAKIS J. G.; HANSEN, J. H. L. **Discrete-time Processing of Speech Signals.** Prentice-Hall Inc., 1987.

HORSTMANN, C. S.; CORNELL, G. **Core Java 2**: Recursos Avançados. Makron Books, 2001.

PETRY, A.; ZANUZ, A.; BARONE, D. A. C. Utilização de Técnicas de Processamento Digital de Sinais para a Identificação Automática de Pessoas pela Voz. In: SIMPÓSIO SOBRE SEGURANÇA EM INFORMÁTICA, São José dos Campos, 1999. **Anais...** São José dos Campos: ITA, 1999.

PETRY, A. **Reconhecimento Automático de Locutor Utilizando Medidas de Invariantes Dinâmicas Não-Lineares**, 2002. Tese (Doutorado em Informática) - Instituto de Informática, Universidade Federal do Rio Grande do Sul, Porto Alegre, 2002.

PETRY, A.; BARONE, D. A. C. Speaker Identification Using Nonlinear Dynamical Features. **Chaos Solitons and Fractals**, v. 13, p. 221-231, 2002.

PETRY, A. ; BARONE, D. A. C. Preliminary Experiments in Speaker Verification using Time-dependent Largest Lyapunov Exponents. **Computer Speech and Language**, v. 17, p. 403-413, 2003.

RABINER, L. ; JUANG, B. **Fundamentals of Speech Recognition.** Prentice-Hall Inc., 1993.

REYNOLDS, D. A.; QUATIERI, T. F.; DUNN, R. B. Speaker Verification Using Adapted Gaussian Mixture Models. **Digital Signal Processing**, v. 10, p. 19-41, 2000.

SCHNEIER, B. **Applied Cryptography:** Protocols, Algorithms, and Source Code in C.John Wiley & Sons Inc., 1996.

STALLINGS, W. **Cryptography and Network Security**: Principles and Pratice. Prentice-Hall Inc., 1999.

TANENBAUM, A. S. **Redes de Computadores.** Editora Campus Ltda, 1997.