Auditoria de Sistemas Eleitorais: o Caso São Domingos

Autores:

Evandro Luiz de Oliveira
Auditor de Informática da Empresa da Informática e Informação do Município de Belo Horizonte S/A - PRODABEL
Professor Substituto do Centro Federal de Educação Tecnológica de Minas Gerais - CEFET-MG
Av. Presidente Carlos Luz, 1275 - Bairro Caiçara - CEP 31230-000 - Belo Horizonte - Minas Gerais
e-mail - pyxis@gold.com.br ou evandro@pbh.gov.br

Cláudio Andrade Rego
Perito Judicial em Informática da Antecipar - Inteligência Aplicada Ltda.
Membro Associado do Instituto dos Auditores Internos do Brasil - AUDIBRA
e-mail - claudio.rego@antecipar.com.br

Resumo

A partir da realização das eleições municipais de 2000, o Brasil adquiriu a condição inédita de nação com todos os procedimentos de voto integralmente informatizados. Os objetivos principais, segundo o Tribunal Superior Eleitoral - TSE, foram: dar rapidez ao processo eleitoral e eliminar os problemas de segurança na votação manual, passando-se a utilizar de *hardware* (equipamentos) e *software* (programas de computador) em todas as etapas.

O mecanismo adotado, com identificação do eleitor na Urna Eletrônica (UE) e a não verificação prévia dos códigos de todos os programas atentam contra requisitos de privacidade e de confiabilidade. A teoria e a prática de auditoria no sistema eleitoral brasileiro são incompatíveis com o discurso de infalível e 100% seguro, realizado pelo TSE.

No caso São Domingos-GO, foi aberta a hipótese de realização de auditoria nos equipamentos utilizados naquela cidade. Na abertura da sessão o juiz eleitoral, a pedido dos representantes do TSE, impugnou cada solicitação de procedimento técnico que era solicitada pelos auditores, fazendo com que as conclusões fossem parciais e subjetivas, demonstrando que ao TSE não interessa abrir completamente a caixa-preta denominada Urna Eletrônica (UE).

Palavras-chave:
Auditoria, segurança, voto, voto eletrônico, confidencialidade, integridade, sistemas de informação.

1) Introdução

A ilusão vendida pela mídia de massa e, principalmente, pelas grandes empresas fornecedoras de produtos e serviços de tecnologia, atribuindo infalibilidade e total segurança às máquinas, provoca conclusões do senso comum que podemos considerar precipitadas. Essas conclusões levam o cidadão, que utiliza qualquer tipo de tecnologia, a acreditar e confiar na mesma como perfeita e infalível. O caso da urna eletrônica brasileira não foge a esse padrão de comportamento.

Num país onde existem muitos analfabetos e gente sem intimidade com tecnologia avançada, poderia parecer um contra-senso a adoção de computadores como máquinas de receber votos para todos os eleitores brasileiros. O ponto positivo da idéia é a possibilidade de colocar uma tecnologia avançada a serviço do processo democrático, no intuito de minimizar as fraudes e manipulação dos eleitores, as quais ocorreram durante décadas nos mais diversos municípios sob a complacência das mais diversas instituições.

Os problemas com a UE começam na sua origem, pois, em se tratando da coisa pública e que deveria atender aos mais diversos interesses políticos, técnicos e administrativos, seria necessário uma ampla discussão entre os segmentos da sociedade envolvidos, para que fossem delineadas as especificações técnicas necessárias e que se implantasse um sistema informatizado do porte das eleições brasileiras, o qual não poderia ter sido instituído sem debate, testes e normalização mínima necessária.

A realização de uma auditoria posterior à eleição, caso fosse integralmente realizada, poderia dar legitimidade mínima aos processos e tecnologias utilizadas. A não realização de procedimentos

internacionalmente aceitos invalida a possibilidade de que o sistema seja totalmente confiável e seguro. Agrava-se o fato de que qualquer programa poderia se auto-destruir às 17 horas do dia da eleição, deixando as urnas sem vestígios do que aconteceu durante o período de votação.

Mesmo com esses pré-requisitos sendo desconsiderados, a máquina eletrônica de votação foi sendo gestada em ambientes de acesso restrito, e depois de vários protótipos e experimentos teve sua primeira versão utilizada em 1996, por um terço do eleitorado brasileiro. Depois de mais dois pleitos, em 1998 e 2000, a discussão em pauta é sobre a confiabilidade da máquina de votar, que foi imposta para o eleitor, e qual o tratamento que o TSE dá às sugestões e questionamentos técnicos sobre a segurança da mesma.

Essa discussão já fora apresentada no Simpósio de Segurança em Informática, promovido pelo Instituto Tecnológico da Aeronáutica, ITA (Brunazo, 2000). O Eng. Amílcar Brunazo indica que *"Uma polêmica estabeleceu-se sobre a impossibilidade de se conferir a apuração dos votos na urna eletrônica brasileira.."*. A referência é conseqüência do fato da urna eletrônica brasileira não permitir recontagem e conferência da apuração, recaindo o problema de sua confiabilidade diretamente sobre a auditoria do sistema eleitoral, mais especificamente sobre a validação e certificação dos programas das urnas.

Para fundamentar esta polêmica nos valemos do relato da tentativa de auditoria em parte do sistema eleitoral, mais especificamente nas urnas eletrônicas utilizadas nas eleições de 2000 em São Domingos-GO. Nesse caso, avaliamos o sistema a partir dos procedimentos de auditoria necessários e que permitiriam uma avaliação da segurança e das vulnerabilidades a que o sistema de voto eletrônico no país está submetido. Uma descrição breve deste caso de São Domingos foi feita pelo jornalista Oswaldo Maneschy (Maneschy, 2001).

Nas seções 2 e 3, são apresentadas condições do voto eletrônico no Brasil e alguns aspectos técnicos próprios do nosso sistema eleitoral, relevantes para a análise feita na seção sobre o Caso São Domingos. Ao final apresenta-se as conclusões.

2) O Voto Eletrônico no Brasil.

Em 1982, no início da informatização do processo de totalização dos votos, ficou bastante conhecido o chamado "Caso Proconsult" (Mineiro, 2000), um problema de totalização a partir de programas desenhados e construídos de forma não auditada. Mesmo que naquela época houvesse fiscalização, mesmo que os responsáveis pelo processo eleitoral tenham garantido que os programas não tinham vícios nem defeitos, uma apuração paralela simples foi suficiente para demonstrar que havia erros grosseiros para uma cidade como o Rio de Janeiro. Nenhuma constatação foi feita em municípios menores do que a ex-capital federal, que constatassem que os erros ali verificados foram mais abrangentes. Parecia ter ficado claro, para todos, que a possibilidade de ocorrer uma fraude, ou mesmo um erro não intencional, é permanente quando os programas existentes nos computadores são construídos por seres humanos e quando o processo eletrônico não têm fiscalização, situação que piora quando esses procedimentos não podem ser auditados e conferidos nos momentos devidos.

Em 1986, o recadastramento eleitoral foi realizado com a adoção da informatização em mais esta etapa.

Em 1996, iniciou-se a informatização da própria votação, num processo que foi concluído no ano 2000 e cujo orçamento gasto foi superior a 500 milhões de dólares, segundo o secretário de informática do TSE (Camarão, 1997).

A máquina de votar introduzida em 1996 imprimia o voto de cada eleitor, o qual era automaticamente depositado numa urna convencional, sem que o eleitor visse a impressão, para que, em caso de problemas com a urna ou com a contagem dos votos, o mesmo ainda fosse aproveitado e o processo informatizado pudesse ser auditado através da recontagem de votos. Em 1998 a impressão do voto foi suprimida, sob o argumento de que os mecanismos de impressão apresentavam defeitos excessivos, sendo desconsiderada a premissa de que a impressão atendia ao preceito de dirimir dúvidas, permitindo assim uma recontagem da vontade expressa do eleitor. Nas versões mais recentes da máquina de votar, a recontagem e auditoria da votação efetuada tornam-se tecnicamente impossíveis pois não existe contraprova material para auditoria e recontagem.

O projeto atual da UE impõe que toda a confiança no processo deve ser depositada na palavra dada pelos projetistas, de que os programas em sua totalidade são absolutamente seguros e confiáveis. Neste sentido é importante ressaltar que, apesar do artigo 66 da Lei Eleitoral 9504/97 permitir que os representantes dos partidos políticos verifiquem o código fonte de todos os programas utilizados no processo eleitoral brasileiro, o TSE não tem permitido a verificação da totalidade dos programas, sob a alegação de possibilidade de quebra dos direitos

autorais dos fabricantes. Deve-se lembrar porém que, segundo Stang (1994), nenhum sistema de informática é totalmente e integralmente seguro, contrariando parte das argumentações do TSE. Não é permitido aos representantes partidários participar, ou melhor, nem presenciar qualquer etapa do processo de criptografia e assinatura eletrônica dos programas, fazendo com que nenhum desses partidos tenha certeza de que aquilo que foi colocado em funcionamento no dia da eleição é realmente o mesmo conjunto de programas vistoriados anteriormente, agravando-se pelo fato de que, mesmo depois de vistoriados, os programas podem ser alterados, e nas eleições de 2000 eles efetivamente foram modificados depois de vistoriados, conforme entrevista publicada pelo jornalista Marcelo Soares, da Folha de São Paulo (Soares, 2000).

É possível que o grande problema sejam os vácuos existentes na legislação eleitoral, os quais permitem interpretações variadas e decisões unilaterais sobre a análise de todo o processo. O trabalho que pretendíamos fazer em São Domingos pode ser considerado violação de segredo da UE. Têm-se, adicionalmente, um Código Eleitoral o qual quase ignora a máquina de votar eletrônica, apresentando parte da legislação como se a eleição fosse completamente manual. Freqüentemente, solicitações de perícia ou auditoria de urnas eletrônicas são negadas com o simples argumento de que o Código Eleitoral, escrito em 1965, não prevê tal coisa. Parte dos representantes do judiciário não têm noções básicas de técnicas de segurança e auditoria em ambientes informatizados, além de não lançarem mão de técnicos especializados para realizarem auditoria e perícias judiciais em assuntos de informática e que sejam independentes dos Poderes diretamente envolvidos.

Os legisladores dão pouca atenção quando esses técnicos fazem alertas sobre vulnerabilidade existentes na construção de programas de computador. Desta forma, cabe ao órgão executor da eleição, quase a totalidade da legislação, execução e julgamento do processo eleitoral informatizado sem a crítica provida pela sociedade organizada e meio acadêmico. A ele é dado a prerrogativa de construir os programas, ou mandar construí-los, verificar suas condições técnicas, controlar absolutamente os equipamentos em todas as etapas, indicar para o Poder Legislativo o que se deve, ou não, colocar na legislação eleitoral e, caso ocorram dúvidas ou questionamentos, por mais inadequado que possam parecer, cabe também ao próprio órgão julgar sua procedência e pertinência. Esse amplo poder deveria ser, ao menos, submetido a uma auditoria externa, mas essa também não é permitida, por determinação, do próprio TSE. Tal proibição fere um dos preceitos básicos da auditoria, o qual preconiza que o auditor e o auditado devem manter independência completa, e deve inexistir qualquer subordinação entre eles (Russel, 1991).

3) Aspectos Técnicos.

O processo eleitoral brasileiro adotou a tecnologia da informática de ponta a ponta. Desde o momento em que o eleitor utiliza-se da máquina de votar até a divulgação do resultado final, todas as etapas são realizadas utilizando-se de recursos tecnológicos de informática, de criptografia e de telecomunicações.

Para que estes recursos funcionem a contento, é essencial a adoção de procedimentos de segurança adicionais aos já existentes nos processos de votação com etapas eminentemente manuais. Uma das vantagens da utilização de recursos tecnológicos foi a eliminação das possibilidades de fraudes exploradas no processo manual. A inserção de recursos tecnológicos não pode, ou pelo menos não deveria, ensejar a criação de novas vulnerabilidades, até então impensáveis. Assim, não deve ser permitido a um programa de computador na UE que desvie votos do candidato "A" para o candidato "B", e isso só é possível se não existirem mecanismos e procedimentos de validação e certificação que:

1) Verifiquem a idoneidade do código fonte do programa de votação;
2) Verifiquem todo o processo de transformação do código fonte em executável;
3) Verifiquem e confirme a veracidade de que o executável seja idêntico ao que diz o código fonte;
4) Certifiquem que o programa que será executado em cada uma das máquinas de votar sejam o mesmo que foi certificado em todas as etapas.

Acrescenta-se a complexidade devido ao porte deste sistema, com mais de 320 mil urnas a serem certificadas, e o fato de que não existe somente o *software* de votação, são muitos os programas (sistema operacional, candidatos, totalizadores, de criptografia, identificadores de eleitores etc.) presentes na urna e no processo de totalização dos votos, e todos eles, sem exceção, deveriam estar submetidos aos mesmos procedimentos de garantia da confiabilidade desde a criação, implementação, funcionamento e auditoria.

Deve-se sempre considerar a possibilidade de que, pessoas com conhecimento de informática, obtendo acesso aos programas das urnas, poderiam adulterar qualquer um desses programas para fazer com que atuem de forma diferente daquela para qual os mesmos foram previstos. Um exemplo simples dessa possibilidade é a mensagem que aparece na Figura 1, retirada da tela de uma das urnas de São Domingos, e indica que o processador está fazendo uma determinada atividade quando poderia realizar muitas outras funções como, por exemplo, destruir indícios de programas hostis ou não homologados.

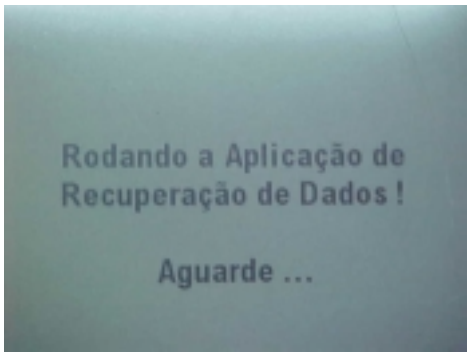

Figura 1

Toda essa babel tecnológica deveria ser acompanhada, obrigatoriamente, em todas as suas etapas, por representantes qualificados da sociedade. No processo eleitoral implementado no Brasil, isso não é permitido, e o exemplo que trataremos adiante demonstra que possíveis questões de vulnerabilidades inerentes a sistemas informatizados estão presentes e as quais estão submetidos todos os eleitores brasileiros. A partir da utilização integral da informática no sistema de votação as vulnerabilidades aparecem e ainda são encaminhados procedimentos de forma imprecisa e deficiente, do ponto de vista de padrões e normas internacionais de segurança e auditoria.

4) O Caso São Domingos.

Os autores foram convidados a compor a equipe executiva do processo denominado como "auditoria das urnas eletrônicas" no dia 8 de janeiro de 2001, na cidade de São Domingos, no Estado de Goiás, com aproximadamente 10 mil habitantes e 7 mil eleitores, onde, em Outubro último, foram usadas urnas eletrônicas pela primeira vez – num total de 23 seções eleitorais.

O candidato a prefeito, Gervásio Silva, alegando suspeita de fraude na eleição apresentou pedidos de perícia nas urnas eletrônicas junto ao Cartório Eleitoral da cidade e ao TRE de Goiás, tendo seus pedidos indeferidos. Com o apoio de políticos levou seu pedido diretamente ao Presidente do TSE e conseguiu o que afirmava ser "*… o primeiro processo de auditoria nas urnas realizado no país…*". Ainda segundo o candidato, entre 4 ou 5 urnas, das 23 utilizadas na votação do dia 1º. de outubro de 2000, naquele município goiano, seriam auditadas com critérios tecnicamente e juridicamente aceitos.

Porém, ao chegarmos ao município, fomos informados que as instruções superiores da Justiça Eleitoral não permitiriam tais procedimentos, e que somente técnicos especializados do TSE poderiam atuar sobre as urnas, sendo que os ritos processuais entre auditores e auditados não seriam realizados.

A sessão foi aberta pelo Juiz Eleitoral da comarca que confirmou a inexistência de auditoria e identificou a sessão como de "*…de caráter pedagógico para demonstração e esclarecimento…*", constando essas afirmações na ata do evento. Mesmo não podendo atuar nas urnas eletrônicas, seus complementos e acessórios, acompanhamos todos os passos dados pelos técnicos do TSE, os quais procuravam demonstrar que o equipamento não é passível de erros e que os votos lá totalizados correspondiam exatamente à vontade popular.

Algumas distorções, incompatíveis com procedimentos de auditoria, apresentaram-se durante a sessão. Nossa solicitação, de que fosse feita cópia do conteúdo das memórias (*flash-cards* interna e externa) antes de que qualquer procedimento fosse realizado, foi negada. Nenhuma cópia do conteúdo das memórias poderia ser feita ou apresentada, sob nenhum pretexto, por técnicos que não fossem do TSE. Um procedimento de auditoria, minimamente correto, trataria de colocar uma cópia do conteúdo dos programas e dados a serem auditados em ambiente distinto do objeto da auditoria, lacrada, sob as rubricas de auditado e auditor, podendo trabalhar etapas

de auditoria livremente em qualquer outro espaço. Essa solicitação e orientação foi negada e desconsiderada pelos representantes do TSE e condutores do processo de demonstração do funcionamento da urna eletrônica.

Figura 2

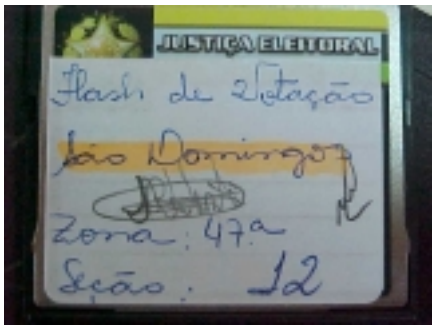

Figura 3

A Figura 2 mostra disquetes, memórias (*flash-cards*) de votação, também denominadas de *flashes* externas, e relatórios obtidos após os processos e programas executados pelos técnicos do TSE. A Figura 3 reproduz uma *flash* externa de uma seção eleitoral, os técnicos do TSE determinaram que todos os presentes deveriam acreditar que o conteúdo das memórias é aquilo que eles diziam ser, não permitindo que os auditores independentes fizessem quaisquer testes e verificações de conteúdo naquela mídia, mesmo sabendo-se que é impossível de se conferir qualquer conteúdo a olho nu.

Os técnicos do TSE apenas permitiam procedimentos externos de testes padrão, como uma possível recuperação do disquete do boletim de urna, procedimentos de limpeza do equipamento e uma simulação de nova votação, mesmo assim operado exclusivamente por eles, com os programas inseridos pelo TSE, sendo que a maioria deles não foram fiscalizados e auditados.

Destaca-se durante este processo de simulação conduzido pelo TSE alguns itens:

1) No processo de simulação de eleição alguns eleitores erraram o voto, como acontecido na eleição de 1º. de outubro, proporcionando a troca dos candidatos majoritários e proporcionais, fato que reforça a necessidade da discussão do processo informatizado. A lógica de processamento dos idealizadores do programa não coincide com a lógica do eleitor usuário do sistema;

2) Não foi permitido o acesso aos registros (*log*) de utilização individual de cada urna, mas no registro consolidado verificamos que, entre a lacração oficial das urnas e o dia anterior às eleições, as 24 (vinte e quatro) urnas daquele município foram religadas 51 (cinqüenta e uma) vezes, sem qualquer explicação plausível, além de 19 (dezenove) religações no dia da eleição antes do horário estipulado, fato que não pode ser considerado "normal" conforme argumentação do TSE;

3) Afirmações contraditórias foram feitas pelos técnicos do TSE e TRE-GO, quando perguntados sobre a forma (texto aberto ou criptografado) na qual os dados ficam armazenados nas memórias, não sendo permitida a conferência das informações, outras perguntas específicas obtiveram respostas dúbias ou divergentes;

4) Os conteúdos das *flashes* (interna e externa), entre o momento da liberação para voto, por parte do mesário, e o término da votação através do "Confirma" acionado pelo eleitor, não é bem esclarecido, fazendo com que permaneçam dúvidas sobre a possibilidade de erro e suas conseqüências durante esse período, provocados, por exemplo, pela utilização de equipamentos de rádio-frequência entre os dois momentos descritos.

5) Na simulação da votação, os técnicos do TSE sentiram a necessidade, para efeito de credibilidade e convencimento dos presentes, técnicos e leigos, de anotar em um papel os votos que estavam sendo sufragados, para que posteriormente pudessem conferir o resultado, sendo esse importante detalhe uma representação definitiva da existência de uma prova material que permita a conferência posterior, recurso adotado pelo próprio TSE na demonstração efetuada.

6) Ao serem questionados sobre a utilização da norma ISO/IEC 15408-1, os técnicos do TSE admitiram que utilizam somente partes da mesma, em função do interesse deles próprios e ressaltaram ainda que várias partes da norma não são consideradas.

5) Conclusão.

O caso do município de São Domingos é somente um exemplo de como todo processo informatizado precisa de mecanismos para conferência e auditoria. A implementação de sistemas automatizados sem a devida e ampla discussão de parâmetros de segurança coloca em risco a credibilidade do projeto. Simples evidências devem ser colocadas à disposição de qualquer interessado para que os dados de entrada, assim como todo o processo possam ser auditados.

Neste sentido, a informatização do processo eleitoral brasileiro consiste num avanço sem paralelo em qualquer nação do mundo, e que serviria de exemplo para muitas delas, ditas desenvolvidas mas que tropeçam em processos simples e democráticos como o ato de votar. Alguns defeitos apresentados no processo eleitoral brasileiro não são de ordem técnica, mas de natureza procedimental, como por exemplo: a) Precária discussão do processo com a sociedade; b) Auto-suficiência dos técnicos do TSE, no sentido de não reconhecer possíveis vulnerabilidades, ignorando propostas de melhoria e menosprezando a capacidade técnica externa ao TSE e seus contratados; e c) Omissão da classe política, desprezando, durante a elaboração e votação da legislação, a adoção de procedimentos simples mas vitais à condução de uma eleição informatizada.

Cabe apresentar algumas diretrizes básicas, as quais poderiam contribuir para que o projeto da urna eletrônica seja mais confiável e que não onerariam o projeto mais do que o necessário, quais sejam:

1) Adoção de mecanismos de impressão do voto, o qual pudesse ser observado pelo eleitor, sem qualquer contato manual, propiciando a possibilidade de recontagem ou auditoria do processo de votação;

2) Adoção de mecanismos de assinatura eletrônica que possam ser verificadas pelos representantes dos partidos, para que se garanta, numa possível auditoria, a origem e fidelidade dos programas e dados inseridos em cada uma das mais de 300 mil urnas do país;

3) Adoção, em caráter obrigatório, de programas de computador considerados como "*software* aberto" nos processos e etapas eleitorais, fazendo com que não exista a possibilidade de programas deixarem de ser verificados e auditados em função da argüição de direitos autorais.

Essas contribuições são, efetivamente, o que aparentam ser, simples e de custo reduzido. Bastaria a determinação de tornar o processo cada vez mais democrático e correto tecnicamente. Técnicos em produção de *software* e profissionais de auditoria têm maior facilidade no entendimento dessas argumentações; resta fazer entender aos legisladores a necessidade de colocar tais procedimentos em lei para que sejam cumpridos. Passada esta etapa de legalização, o processo de discussão e implementação técnica detalhada deveria ser aberto pelo TSE para implementar as alterações, de forma que não fiquem dúvidas quanto as melhorias a serem adotadas.

Espera-se ainda ter contribuído para a disseminação do debate sobre o tema Segurança, e ampliação da visão de que as vulnerabilidades e erros em sistemas informatizados são mais reais e possíveis de acontecer do que efetivamente se propaga.

6) Bibliografia.

BRUNAZO F., A. Avaliação da Segurança da Urna Eletrônica Brasileira. In: Simpósio de Segurança em Informática, SSI'2000, Anais, São José dos Campos: Instituto Tecnológico da Aeronáutica, 2000, http://www.votoseguro.org/textos/SSI2000.htm

CAMARÃO, P. C. B., O Voto Informatizado: Legitimidade Democrática. São Paulo, Brasil, Ed. Empresa das Artes, 1997.

ISO - International Organization for Standardization. Information technology - Security Techniques - Evaluation criteria for IT security. ISO/IEC 15408-1. Genebra, Suiça,1999.

MANESCHY, O., Palm Beach Versus Araçoiaba da Serra. Site Jus Navegandi, 2001, http://www.jus.com.br/doutrina/urnael19.html

MINEIRO, P., Proconsult – Um Caso Exemplar. Cadernos do Terceiro Mundo, Rio de Janeiro, Ed. Terceiro Milênio, n. 219, p. 17, Abril/Maio 2000, http://www.votoseguro.org/noticias/cad3mundo1.htm

RUSSEL, Deborah. GANGEMI, G.S. Computer Security Basics. 2ª. Ed. Sebastopol - CA: O'Reilly. 1991.

SOARES, M., Entenda a Questão da Segurança. São Paulo, Folha de São Paulo, 15/10/2000, http://www.uol.com.br/fsp/brasil/fc1510200018.htm

STANG, David J. Segredos de Segurança em Rede / David J. Stang, Sylvia Moon. Tradução: Cláudio Lobo. 1ª Ed. Rio de Janeiro : Berkeley Brasil, 1994. 986p.