CARTA DO PROF. DR. JORGE STOLFI (TITULAR DA UNICAMP), DESMENTINDO O "RELATÓRIO DA UNICAMP" QUE APROVA AS URNAS ELETRÔNICAS, TRANSFORMADAS EM LEI EM 2003

From: Amilcar Brunazo Filho
To: voto-eletronico@pipeline.iron.com.br
Sent: Saturday, September 06, 2003 10:32 AM
Subject: [VotoEletronico] Carta do Prof. Jorge Stolfi

Para efeito de registro estou reenviando para o Fórum do Voto-E a carta originalmente enviada em 22 de outubro de 2002 pelo professor Jorge Stolfi, Professor Titular do Ins-tituto de Computação da Unicamp.

Amilcar Brunazo Filho

Caros colegas,

Em 29 de maio de 2002, uma comissão de docentes da Unicamp entregou ao Tribunal Superior Eleitoral (TSE) um relatório de 48 páginas, com título "Avaliação do Sistema Infor-matizado de Eleições (Urna Eletrônica)" [1]. Esse relatório tem sido interpretado e divulgado pelo TSE como sendo uma confirmação, por parte desta Universidade, da segurança do sistema de voto eletrônico.

Em primeiro lugar, é preciso esclarecer que esse relatório nunca foi examinado, muito menos aprovado, pelos órgãos colegiados da Unicamp ou das unidades envolvidas. Pelo contrário, a avaliação foi realizada apesar de recomendação contrária da Comissão de Perícias da Unicamp, que havia alertado a Universidade sobre o perigo dos resultados virem a ser mal interpretado e mal utilizados[2]. Portanto, o relatório e suas conclusões não po-dem ser tomados como a opinião institucional "da Unicamp", mas apenas de seus auto-res.

Além disso, deve-se observar que a avaliação foi feita sobre o hardware e software usado nas eleições de 2000, e portanto não pode ser usado para respaldar o sistema de 2002 - que difere daquele em detalhes de natureza e extensão desconhecidas.

Por fim, é no mínimo estranha a conclusão principal do relatório (na página 45), incondicional e categórica, de que

"o sistema eletrônico e votação implantado no Brasil desde 1966 é um sistema ro-busto, seguro e confiável atendendo a todos os requisitos do sistema eleitoral brasileiro"

Acontece que esta conclusão é contrária não apenas ao bom senso e à experiência de qual-quer profissional minimamente competente do ramo, mas inclusive às próprias constata-ções da comissão - que, no corpo do relatório, aponta várias falhas de segurança que possibi-litariam fraudes generalizadas e indetectáveis. Sem contar que as falhas realmente gra-ves da urna não foram sequer mencionadas no relatório.

Após ler esse texto, e alguns testemunhos sobre a fiscalização feita pelos partidos [4,5,6], confesso que perdi até mesmo a pouca confiança que eu tinha na urna eletrônica. Assim como vários outros especialistas bem mais competentes e informados do que eu (como o Prof. Pedro A. D. Rezende, da UnB), acredito que uma avaliação imparcial e completa da mesma deveria concluir exatamente o contrário.

Não sou, de modo algum, perito em segurança; mas creio que entendo o suficiente de computação para avaliar os argumentos dos críticos e defensores da urna eletrônica. E, no meu entender, os críticos têm vários argumentos lógicos (óbvios, até), que os defensores apa-rentemente nem tentam responder. (Infelizmente, declarações em defesa da urna eletrôni-ca muitas vezes se reduzem a simples afirmações de autoridade, ou apelos ao patriotis-mo ingênuo[8] - ou mesmo argumentos "ad hominem", em que os críticos são tachados de retrógrados, inimigos do progresso, derrotistas, etc..)

Na análise desta questão, é importante notar que nossa imagem mental do que seria uma tentativa "típica" de violação de segurança é baseada na população geral de "hackers", que na maioria são vândalos juvenis atacando por "esporte", ou vigaristas aplicando fraudes co-merciais.

Nos dois casos, os atacantes geralmente são pessoas sem conexões especiais com a vítima, que operam sozinhos ou em pequenas quadrilhas, com recursos relativamente limitados, e têm que se esquivar da polícia como marginais comuns. Nos dois casos, o atacante não tem uma vítima determinada; de modo que mesmo uma barreira parcial pode ser efetiva, por desviar os ataques para vítimas mais fáceis.

Em contraste, no caso de fraude eleitoral, o maior risco vem de partidos e outros gru-pos organizados e poderosos, com recursos abundantes, amplo apoio político e social, e contatos e simpatizantes em todos os setores do governo - inclusive dentro da polícia e da Justiça Eleitoral. Grupos que, por exemplo, conseguem obter dezenas de exem-plares da urna eletrônica (legítimos ou imitações, pouco importa), sem que ninguém consiga explicar onde ou como; ou que podem exigir que um funcionário sênior quebre o sigilo de uma votação secreta do Senado, sem temor de que este venha a revelar o fato à justiça. Para atacantes desse calibre, o ganho potencial é muito maior, e o risco de punição é muito menor. Por isso, infelizmente, não faltam pessoas, em todos os níveis do governo e da sociedade, dispostas até a matar (ou a arriscar a própria vida) por um cargo político, para si ou para o candidato "certo".

Portanto, para ser considerado seguro, um sistema de votação deve ser capaz de resistir, não apenas aos ataques típicos de hackers adolescentes ou de fraudadores bancários, mas também a ataques bem planejados, por grupos que têm conhecimento detalhado do software e hardware da urna eletrônica, e estão determinados a quebrar esse sistema, a qualquer custo.

Uma avaliação séria da segurança de qualquer sistema deve partir do princípio de que, se o sistema tem algum ponto fraco, é justamente nele que se concentrarão os ataques. A presunção de inocência e integridade deve valer para o indivíduo, sem dúvida; mas, ao nível de sistema, deve-se aceitar como fato dado que uns poucos funcionários em posição es-tratégica podem ser intimidados ou subornados. Deve-se supor que materiais falsificá-veis podem ser falsificados, chaves e lacres podem ser duplicados, telefones podem ser grampeados, e assim por diante. Deve-se supor também que os atacantes terão opor-tunidade de testar previamente o ataque, numa urna eletrônica legítima ou clonada. Um sistema eleitoral que não pode resistir a ataques desse nível não pode ser, de modo al-gum, considerado "seguro".

Neste aspecto, o relatório "da Unicamp" é extremamente insatisfatório, pois parece supor, implicitamente, que todos os programadores e operadores com algum tipo de acesso ao software e hardware da urna e da rede do TSE - incluindo não só os funcionários do TSE e dos TREs, mas também todos os funcionários da ABIN, da Microbase, da Módulo, e da Procomp - são íntegros, incorruptíveis, inintimidáveis, e incapazes de qualquer erro ou distração que possa ter comprometido o software da urna.

Acredito que uma avaliação mais realista dos riscos de fraude - que leve em conta o que pode acontecer, e não apenas o que o TSE gostaria que acontecesse - seria algo como o "relatório alternativo" abaixo:

Em todos os modelos da Urna Eletrônica, o software que a opera inclui um siste-ma operacional com centenas de milhares de instruções, cujo código-fonte não não é acessível ao TSE, e cujo comportamento nunca foi analisado pelos técnicos do Tribunal, pelos fiscais de partido, ou por peritos independentes. A mesma situação se verifica nos computadores utilizados pelo TSE para a montagem do software e inseminação da urna.

Mesmo que fosse feita uma análise minuciosa do código-fonte do sistema operacional (e de todos os demais programas excutados com privilégios equivalentes), sua complexi-dade é tal que não seria possível excluir a existência nele de vulnerabilidades, intencionais ou acidentais, suficientes para permitir a introdução e execução de instruções maliciosas.

Instruções executadas com os privilégios do sistema operacional podem efetuar alterações arbitrárias no conteúdo das principais unidades de memória da máquina (RAM, "flash cards" e discos internos) - inclusive alterando outros programas, curto-circuitando senhas e permissões, neutralizando rotinas de assinatura digital e outros testes de integridade, falsificando logs, e por fim apagando a si próprias.

Portanto, uma única vulnerabilidade desse tipo poderia permitir a introdução e execução de código malicioso nos computadores do TSE e/ou na urna eletrônica, capaz de alterar in-devidamente os votos digitados e/ou os totais acumulados, sem acionar alarmes ou criar inconsistências. Esse código poderia ser facilmente programado para agir apenas na votação real, e não nos testes dos fiscais. Usando os pró-

prios sensores de segurança da urna, ele poderia também detectar facilmente tentativas de abertura ou auditoria da mesma, e apagar a si próprio nesse caso. Uma vez que a urna eletrônica não mantém nenhum registro permanentes e inalterável dos votos lançados, fora os totais armazenados nos "flash cards", tal fraude seria praticamente impossível de detectar - quer durante a votação, quer a posteriori.

A elaboração de um código malicioso com essas características não exigiria conhecimentos especializados de computação ou criptografia, apenas habilidades elementares de pro-gramação, e alguns dados específicos sobre o software e hardware da urna (endereços ou código objeto das rotinas de segurança, formato das tabelas de totais, e assim por dian-te). Tal código poderia ser facilmente programado de modo a funcionar com versões dife-rentes do software da urna, mesmo versões não disponíveis ao autor.

A introdução do código malicioso na urna eletrônica provavelmente precisaria da colaboração (consciente ou inconsciente) de alguma pessoa com posição especial dentro do esque-ma; mas não necessariamente com privilégios administrativos, conhecimento de senhas ou chaves criptográficas, ou acesso físico aos ambientes do TSE. Esta pessoa poderia ser, por exemplo, um programador ou operador do TRE ou do TSE, ou de qualquer das empresas e instituições que contribuem para o software da urna ou dos computadores usados na compilação e inseminação (incluindo Microbase, Módulo, Procomp, ABIN e Micro-soft).

A introdução do "vírus" poderia ser feita de muitas maneiras. Ele poderia já estar embutido no sistema operacional, no BIOS, ou nas rotinas da ABIN; poderia ser enxertado no software da urna durante a compilação ou inseminação; ou poderia estar escondido em programas secundários, arquivos de dados ou áreas supostamente virgens dos disquetes e flash cards, e ativado graças a alguma vulnerabilidade do software da urna. Em qual-quer destes cenários, a adulteração do software da urna poderia ser consumada numa fra-ção de segundo, por um programa "cavalo de tróia" ou alguma outra vulnerabilidade do software. Essa operação não exigiria a presença física do atacante ou acesso remoto, e po-deria ocorrer sem que operadores, fiscais, ou usuários presentes se dêem conta do fato.

A complexidade e dificuldade de tal ataque não seria maior que a dos vírus e outros pro-gramas maliciosos que periodicamente invadem computadores no mundo todo, mesmo os mais bem-protegidos (incluindo, aliás, os nossos aqui na Unicamp). Portanto, tal co-mo nesses casos, o ataque poderia ser perfeitamente planejado e excutado por uma única pessoa. E, com um único ataque desse tipo, seria perfeitamente possível alterar em vários pontos percentuais os totais de todas as urnas do país, ou de um determinado es-tado.

Conclui-se portanto de tudo isto que ninguém - nem o TSE, nem os peritos e fiscais, nem os fornecedores do software - tem razões para crer que não houve fraude generali-zada nas eleições passadas, ou meios efeitvos de impedir que ocorram fraudes generali-zadas neste segundo turno.

Ou seja, as afirmações do relatório e do TSE, de que a urna é 100% segura, não têm nenhu-ma base racional; são apenas declarações de fé cega na integridade de todas as centenas de programadores e operadores envolvidos com o sistema.

Ressalto que esta minha avaliação baseia-se em informações públicas, extraídas do relatório "da Unicamp" disponibilizado no site do TSE [1] (e portanto implicitamente confirmadas pelo mesmo), e de alguns outros testemunhos públicos[4,5,6]. Quanto à minha conclusão, acredito que ela pode ser confirmada por qualquer profissional com um mínimo de ex-periência em questões de segurança - mesmo que apenas na qualidade de vítima.

Inexplicavelmente, o relatório "da Unicamp" nem sequer menciona os pontos fracos mais óbvios e perigosos do sistema - como por exemplo a possivel presença de "cavalos de Tróia" nos computadores do TSE, a quantidade absurda de software aplicativo carre-gado na urna (segundo outro relato[4], são 3 milhões de linhas de código-fonte - ou seja, mais de 400.000 linhas para cada membro da comissão!), e o fato de nem os peritos, nem os fiscais, nem o TSE terem acesso ao código fonte do sistema operacional da mesma.

Outras falhas igualmente sérias - como a ativação das rotinas secretas da ABIN antes da impressão dos totais, a impossibilidade de se examinar o conteúdo da urna após a carga, e a execução de um script

carregado localmente pelo disquete - mal são mencionadas no relatório, e apenas para serem desconsideradas com afirmações otimistas sem fundamen-to. Por exemplo, lê-se na página 38 que:

"A combinação dessas formas de proteção tem como resultado a criação de uma bar-reira de segurança de difícil transposição. Mesmo que cada uma das formas de pro-teção possa ser individualmente superada, a superação do conjunto é pouco provável, dados a extensão e a profundidade de conhecimento necessário e o grande número de participantes cujo envolvimento seria requerido para sua realização."

Ora, esta afirmação simplesmente não procede. Em particular, não é preciso entender uma rotina de autenticação criptográfica ou validação de senha para curto-circuitá-la. Não é preciso entender todo o sistema operacional para inserir nele uma rotina de alteração dos votos. Não é preciso examinar o código de um aplicativo para imitar sua interface. Não é preciso roubar senhas, arrombar fechaduras, ou grampear redes para conseguir acesso irres-trito e indetectável a um computador. E a história mostra que não é preciso mais do que um único "hacker" adolescente para implementar tudo isso!

Inexplicavelmente, também, a seção de recomendações do relatório nem sequer menciona a proposta de impressão do voto, com verificação imediata pelo eleitor e depósito em urna lacrada. pelo que sei, essa proposta constava do projeto original da urna, e é a única que pode dar um mínimo de segurança contra fraudes generalizadas - e, por isso mesmo, é tema obrigatório em qualquer discussão séria sobre voto eletrônico[7].

Na verdade, minha avaliação acima pode ser resumida a dois parágrafos:

A urna eletrônica é um computador autônomo que, no início do dia, é carregado com alguns milhões de instruções e dados diversos, preparados por centenas de pessoas parcialmen-te desconhecidas e potencialmente mal intencionadas. A maior parte dessas instruções, incluindo as mais usadas e as mais poderosas, nunca foram analisadas - muito menos certificadas - por inspetores confiáveis, e talvez nem mesmo pelos seus autores.

Ora, nessas condições, é matematicamente impossível extrair do estado final qualquer in-formação significativa, mesmo que probabilística, sobre a seqüência de teclas digitadas du-rante o dia.

Ou seja, é inútil analisar detalhes como as técnicas criptográficas ou procedimentos de in-seminação, pois a falta de segurança é uma propriedade fundamental dessa arquitetura. A validação desse tipo de urna exigiria uma validação rigorosa de todo o software que poderia modificar os totais, incluindo especialmente o sistema operacional, BIOS, e outros pro-gramas que rodam em modo privilegiado. Validação essa que nunca foi feita - e que, da-do o volume de código envolvido, não pode nem ser cogitada.

Mas, naturalmente não estou pedindo que confiem nas minhas conclusões. Por favor, lei-am os muitos documentos disponíveis - como o relatório da Unicamp[1], os artigos de Rezende e Maneschy[3,4,5,6], e o artigo recente na IEEE Spectrum[7] - e tirem suas próprias conclusões.

Lamentavelmente, a estas alturas, não sei o que poderia ser feito para garantir um míni-mo de segurança nas eleições do segundo turno. Se de fato há código malicioso na urna (e, repito, *ninguém* neste planeta tem base para afirmar o contrário), ele pode facilmente se esconder de uma auditoria física da urna - quer esta seja realizada antes, durante, ou após a votação. Ainda mais que neste ano foram eliminadas as últimas urnas tradicionais, que poderiam servir como uma (fraca) confirmação estatística (por amostragem) dos to-tais gerais.

No que tange à eleição presidencial, ao menos, podemos confiar que haverá pouco espaço para fraude - desde que sejam mantidas as projeções atuais até o fim da semana. Porém, nos estados onde a disputa por governador está mais equilibrada, não se podem excluir pequenas "ajudas eletrônicas" - transferindo, digamos, 3-4% dos votos de um candidato para outro. Nesse caso, a discrepância entre os resultados e as pesquisas de boca de urna possivelmente levantaria suspeitas - mas parece pouco provável que o TSE, em vista do seu óbvio entusiasmo pela urna eletrônica, aceitaria essas diferenças como evidên-cia de fraude.

Pelo visto, o jeito é rezar para que ambos os candidatos tenham conseguido inserir seus vírus na urna, de tal modo que um cancele o efeito do outro...

Estou surpreso e preocupado com a indiferença com que os acadêmicos da área, que teri-am "ex officio" a responsabilidade de esclarecer a sociedade sobre as implicações e peri-gos da tecnologia, tenham no geral ignorado esta controvérsia vital para o futuro do país. (Mas confesso que eu também dei pouca atenção ao assunto quando o relatório foi noticia-do nos jornais, e nem sequer tentei procurar obter o texto - só li agora, depois que ele foi, por assim dizer, esfregado na minha cara.) Infelizmente, parece que nossa

omissão foi interpretada pelo TSE como aprovação do relatório e de suas conclusões, e auto-rização para continuar ignorando os argumentos dos críticos.

Creio que o mínimo que nós, acadêmicos de computação, podemos fazer agora, para cum-prir nossa obrigação social, é espalhar o alerta, da maneira mais ampla e responsável pos-sível. Por favor, interes-se-se, forme sua opinião, manifeste-se, e procure interessar seus colegas. Afinal, os vampiros - reais ou imaginários - que ainda assombram a nossa de-mocracia não podem ser exorcisados com crucifixos, colares de alhos ou expedições furti-vas em cemitérios eletrônicos. Como bem sabem os peritos *desse* ramo, eles só podem ser eliminados escancarando as janelas e expondo-os à luz do dia.

Sinceramente,

Jorge Stolfi
Professor Titular
Instituto de Computação, Unicamp

---

[1] "Avaliação do Sistema Informatizado de Eleições (Urna Eletrônica)" Relatório de convênio Unicamp-Funcamp-TSE, 29/maio/2002

http://www.tse.gov.br/servicos/download/rel_final.pdf

[2] Roberto Romano. "Urnas Eletrônicas, ABIN e Unicamp", Folha de São Paulo 11/jun/2002.

[3] Pedro Antonio Dourado de Rezende. "Análise do Relatório da Unicamp"

http://www.cic.unb.br/docentes/pedro/trabs/relunicamp.htm

[4] Pedro Antonio Dourado de Rezende. "Voto Eletrônico - Fiscalização e cineminha no TSE", Observatório da Imprensa, Caderno da Cidadania, 21/08/2002

http://www.observatoriodaimprensa.com.br/cadernos/cid210820021p.htm

[5] Pedro Antonio Dourado de Rezende, "Mundo Digital - Informática, arma e panacéia" Ibidem, 24/08/2002

http://www.observatoriodaimprensa.com.br/artigos/eno240420024p.htm

[6] Osvaldo Maneschy. "Urna Eletrônica - Sigilo oficial e a segurança do voto" Ibidem, 28/08/2002

http://www.observatoriodaimprensa.com.br/cadernos/cid280820021p.htm

[7] Rebecca Mercuri. "A Better Ballot Box?", IEEE Spectrum Online - Weekly feature - 02/oct/2002

http://www.spectrum.ieee.org/WEBONLY/publicfeature/oct02/evot.html

[8] Carta-corrente eletrônica recebida em 25/set/2002. (Vejam o item 4 da lista)

http://www.ic.unicamp.br/~stolfi/urna/VivaOBrasil.msg