Tecnologia Eleitoral e a Urna Eletrônica

Relatório SBC 2002

Jeroen van de Graaf
Laboratório de Computação Científica
Universidade Federal de Minas Gerais
Belo Horizonte - MG
jvdg@lcc.ufmg.br

Ricardo Felipe Custódio
Laboratório de Segurança em Computação
Universidade Federal de Santa Catarina
Florianópolis - SC
custodio@inf.ufsc.br

À memória de José Gorgonha de Miranda, Túlio Yuchi Sakamoto e Fagner Oliveira da Costa, alunos da Universidade do Amazonas e estagiários do TRE-AM, e Comandante Celso Reinaldo Salmozzo, piloto: vítimas do acidente fatal da aeronave que os transportava para atuar nas Eleições 2002 no município de São Gabriel de Cachoeira.

Agradecimentos

Agradecemos à Sociedade Brasileira de Computação – SBC pela oportunidade de representá-la neste importante trabalho; ao Secretário de Informática do Tribunal Superior Eleitoral Doutor Paulo César Behring Camarão; ao Doutor Osvaldo Catsumi Imamura; a cooperação e hospitabilidade do TRE-MG e TRE-SC; a Márcio Teixeira pelas importantes informações técnicas; a Amílcar Brunazo pela sua incansável busca pelo aprimoramento do sistema informatizado e eleições; ao professor Pedro Antônio Dourado de Rezende pelas críticas e sugestões; ao professor Jorge Stolfi; a Moacir Casagrande; ao Sr. Carlos Rogério Camargo, Secretário de Informática do TRE-SC pelo pronto atendimento das informações solicitadas; à acadêmica Débora Cabral; à Doutora Lúcia Helena de Oliveira dos Santos Miranda, Secretária de Informática do TRE-MG pela cooperação, ao professor Claudionor Coelho, Wilton Caldas e Daniel Borges por uma assessoria sobre memória *flash*; e a Hao Chi Wong, Cláudia Bauzer, Ana Paola Amaral Duarte e Ana Lúcia Amaral por ajudar com a redação final.

Resumo

Este texto contém um relatório dos trabalhos de cooperação realizados para o TSE por especialistas da SBC no ano de 2002. Este relatório descreve as principais tecnologias eleitorais, de forma a contextualizar o Sistema Informatizado de Eleições Brasileiro e apresenta críticas e sugestões para melhorar a confiabilidade e a confiança no sistema como um todo.

Lista de Siglas

ABIN	Agência Brasileira de Inteligência
AES	*Advanced Encryption Standard*
BIOS	*Basic Input Output System*
BU	Boletim de Urna
CALTECH	*California Institute of Technology*
CD	*Compact Disc*
CEPESC	Centro de Pesquisas e Desenvolvimento para a Segurança das Comunicações
DNS	*Domain Name Service*
FC	cartão de memória *Flash* de Carga
FI	cartão de memória *Flash* Interna
FV	cartão de memória *Flash* de Votação
GM	Gerador de Mídias
MIRACL	*Multiprecision Integer and Rational Arithmetic C/C++ Library*
MIT	*Massachusetts Institute of Technology*
SBC	Sociedade Brasileira de Computação
SHA	*Secure Hash Algorithm*
SIE	Sistema Informatizado de Eleições
SIEB	Sistema Informatizado de Eleições Brasileiro
STF	Supremo Tribunal Federal
SVCFE	Sistemas de Votação com Cédula em Formato Especial
SVCP	Sistemas de Votação com Cédula em Papel
SVECC	Sistemas de Votação Eletrônica Com Comprovação física
SVESC	Sistemas de Votação Eletrônica Sem Comprovação física
SVM	Sistemas de votação mecânica
SVP	Sistema de Votação Paralela
TRE	Tribunal Regional Eleitoral
TSE	Tribunal Superior Eleitoral
UE	Urna Eletrônica
UNICAMP	Universidade Estadual de Campinas
ZE	Zona Eleitoral

Sumário

Capítulo 1

Introdução

O Brasil tem dedicado considerável esforço e recursos financeiros na informatização do processo eleitoral brasileiro, promovido pelo Tribunal Superior Eleitoral – TSE. É talvez o único país no mundo que realiza suas eleições oficiais de forma quase inteiramente eletrônica. Pode-se estabelecer dois períodos principais, em termos do foco de atenção da comunidade interessada, neste processo de informatização. O primeiro período começou no início da década de 1980 e estendeu-se até as eleições de 1996. Neste período o foco de atenção foi projetar e construir um sistema informatizado de eleições robusto e adequado à realidade brasileira. Robusto no sentido de minimizar a quantidade de possíveis falhas de hardware e software e adequado à realidade brasileira no sentido de ter o menor custo possível. Uma vez estáveis os sistemas, nos últimos anos a preocupação tornou-se muito mais a questão de *segurança*.

1.1 Objetivos deste relatório

O objetivo geral deste relatório é descrever os esforços e contribuições do Comitê de Tecnologia Eleitoral da SBC para o Sistema Informatizado de Eleições (SIE) brasileiro no ano de 2002.

Deve-de entender que o SIE é um sistema muito grande, de que a urna é apenas uma parte, mas uma parte importante. Especificamente, o relatório visa descrever a urna brasileira, comparando-a com outras tecnologias existentes, e relatar a nossa participação, como representantes da SBC, no processo de avaliação do Sistema Informatizado de Eleições.

1.2 Histórico da cooperação SBC-TSE

Ao final do ano 2001, o TSE procurou a SBC para estabelecer uma cooperação técnica-científica com a comunidade universitária brasileira. O então Presidente da SBC, Flávio Wagner, visitou o TSE duas vezes. Membros da comunidade acadêmica foram convidados a participar do Comitê Técnico de Tecnologia Eleitoral. As únicas pessoas que aceitaram o convite fomos nós, Prof. Jeroen van de Graaf, da Universidade Federal de Minas Gerais, e Prof. Ricardo Felipe Custódio, da Universidade Federal de Santa Catarina.

Durante o ano de 2002, nós pudemos participar das sessões de avaliação do Sistema Informatizado de Eleições em três oportunidades: duas antes do primeiro turno e uma antes do segundo turno das eleições oficiais brasileiras. A SBC, durante o ano 2002, atuou exclusivamente como observadora através de seus respresentantes.

O trabalho consistia em participar das sessões públicas no TSE (com passagens e diárias pagas pelo TSE), em que os partidos políticos têm o direito de analisar os programas a serem usados nas eleições: programas da urna, programas para configurar as urnas, programas para receber os resultados das urnas e totalizar os

resultados, etc. Também acompanhamos o trabalho no TRE: a preparação da urna e as atividades na véspera e no dia da eleições.

Em setembro houve a primeira sessão de uma semana, em que o TSE montou uma sala com computadores e mostrou os códigos-fonte dos programas. No final desta semana houve uma compilação dos programas, geração de resumos criptográficos dos arquivos, gravação dos arquivos em CDs e lacração dos mesmos.

Nosso papel não era o de um fiscal de partido, mas o de testemunha e observador imparcial. No TRE-MG isto resultou em acesso privilegiado a lugares onde os fiscais normalmente não entram. A nossa missão era:

> *Estudar ao máximo o sistema eleitoral e a urna brasileira em geral, e as questões de segurança e auditabilidade em particular, para depois podermos sugerir possíveis cooperações (pesquisas, estudos, desenvolvimento de protótipos, etc) entre a SBC (representando a comunidade de Computação) e o TSE, visando melhorar o processo eleitoral a curto, médio, e longo prazo.*

Nossa missão não foi limitida por ninguém, nem é nosso trabalho confidencial. Foi possível incluir em nossos estudos o que considerávamos relevante, falar com quem quiséssemos, estudar outras tecnologias eleitorais para sugerir alternativas, etc. Fomos tratados com toda cortesia e respeito pelos funcionários do TSE e do TRE, e também interagimos com representantes de diversos partidos políticos.

O único pedido do TSE foi que não divulgássemos detalhes sobre o software que poderiam ajudar pessoas mal-intencionadas a comprometer a segurança da urna. Já que nossa intenção era ajudar o TSE, não tínhamos problemas com esta restrição. Assinamos um termo de compromisso absolutamente incompreensível (seu texto aparece no apêndice C), mas a explicação dada pelo Secretário de Informática do TSE nos tranqüilizou. Em suma, atendendo ao pedido do TSE, o termo não impediu de forma alguma a execução de nosso trabalho, e tampouco a redação deste relatório.

1.3 Limitações

Para se ter uma idéia da complexidade envolvida numa eleição oficial, relatamos a seguir uma amostra das atividades que são realizadas para uma eleição:

- divulgar o processo eleitoral através de publicidade;
- providenciar tratamento preferencial à Justiça Eleitoral pelas companhias de eletricidade no dia do eleição;
- sortear uma urna por Estado, buscá-la, e fazer uma eleição simulada nela no dia de eleição;
- definir uma interface amigável;
- combater a coação de votos por dinheiro, ameaças e promessas;
- desenvolver firewalls e proteção do DNS[1] para proteger as páginas web dos TREs e do TSE na noite da eleição;
- treinar aproximadamente dois milhões mesários;
- preparar, transportar e entregar aproximadamente 400.000 urnas em todo o território brasilerio;
- preparar, transportar e entregar aproximadamente 50 urnas em embaixadas do Brasil em diversos países;
- julgar e decidir penalidades aos infratores da legislação eleitoral;
- armazenar e manter 400.000 urnas;
- alistar 110 milhões eleitores;

[1] DNS - Domain Name Service

- disponibilizar urnas de contingência, nos inevitáveis casos de falhas técnicas;
- preparar um ambiente com computadores e telões para divulgar os resultados à imprensa em cada TRE e no TSE;
- manter uma rede de comunicação de dados privativa durante as eleições;
- tratar os assuntos jurídicos.

Diante desta quantidade de informações, um relatório feito por uma equipe de duas pessoas tem necessáriamente suas limitações.

1.4 Relatório dos especialistas da UNICAMP

Durante o escândalo de painel do Senado em maio de 2001, especialistas da UNICAMP fizeram uma perícia para apurar o que aconteceu exatamente. Nesta época, surgiu no Senado a idéia de fazer uma avaliação semelhante da urna eletrônica. Foi proposta uma lista de perguntas a ser respondidas nesta avaliação; veja Apêndice B.

Segundo Brunazo [2], o TSE não achou adequado que a possível avaliação fosse feita sob a responsabilidade do Senado, e o pressionou para desistir da idéia. Em vez disso, o TSE contrataria a UNICAMP para avaliar a segurança da urna.

Desconhecemos os detalhes do contrato entre o TSE e os especialistas da UNICAMP, ou qual tipo de perguntas o TSE gostaria que estes especialistas investigassem, mas as questões levantadas no pedido original do Senado não foram todas resolvidas. O relatório dos especialistas da UNICAMP formulou sua missão assim:

> *"**1.2 Objetivo e escopo** O objetivo do trabalho aqui relatado foi a análise do Sistema Informatizado de Eleições visando detectar a existência de eventuais vulnerabilidades, avaliar o seu impacto e recomendar medidas para eliminá-las ou atenuá-las. Em especial, a análise visou as vulnerabilidades que pudessem comprometer os requisitos fundamentais de um sistema informatizado de eleições, ou seja, o sigilo do voto e o respeito à expressão do voto do eleitor. Adicionalmente, buscou-se avaliar a auditabilidade das funções e da operação do sistema.*
>
> *Deve-se salientar que o trabalho realizado não constituiu uma auditoria do Sistema Informatizado de Eleições e, sim, uma avaliação do sistema utilizado nas eleições de 2000 e a proposição de medidas para a sua melhoria." [8]*

Quando este relatório foi publicado no final de maio de 2001, não era possível qualquer avaliação do Comitê de Tecnologia Eleitoral da SBC, porque não tinha ocorrido nenhuma reunião técnica entre o TSE e nós. Contudo, algumas observações foram possíveis:

- O SIE não é igual ao painel do Senado em termos de segurança. Existem alguns mecanismos de segurança no projeto da urna e nos procedimentos associados às eleições, embora não sejam perfeitos;
- Embora dando uma visão global, o relatório também é demasiadamente simples, escondendo muitos detalhes importantes do sistema eleitoral e da urna propriamente dita. As afirmações não são verificáveis e não há referências ou fatos que qualificam o relatório como documento científico. O leitor não pode formar sua própria opinião, mas deve confiar nas opiniões dos autores;
- Apesar de avaliar a auditabilidade e o sigilo do voto ser uma parte explícita da missão da UNICAMP, acreditamos que a urna atual não é auditável, e tampouco protege adequadamente o sigilo do voto. Nestes aspectos, que serão discutidos amplamente neste documento, discordamos veementemente das conclusões do relatório dos especialistas da UNICAMP.

Na semana anterior ao segundo turno, o Dr. Jorge Stolfi, professor de computação da UNICAMP, mas não um dos autores do relatório, escreveu uma carta [14] com duras críticas ao relatório dos especialistas da UNICAMP. Embora não concordemos com todas as opiniões do Prof. Stolfi, a carta faz algumas observações que correspondem às nossas, especificamente sobre a dificuldade de construir software seguro (veja 2.7).

Após ter estudado o sistema eleitoral em maior profundidade, podemos atestar que, apesar de diferentes opiniões, o relatório dos especialistas da UNICAMP faz uma excelente descrição global do sistema eleitoral informatizado, especificamente no Capítulo 3: “Visão geral do Sistema Informatizado de Eleições”. Sugerimos ao leitor que deseja entender os detalhes técnicos deste relatório que leia aquele Capítulo.

1.5 Conteúdo deste Documento

O capítulo 2 apresenta uma visão geral sobre tecnologias eleitorais. Apresentamos várias tecnologias eleitorais, e vemos como tecnologias diferentes mudam a questão de transparência. Explicamos a noção de comprovação física do voto. Depois listamos os requisitos de segurança e aplicamos estes requisitos nas tecnologias.

O capítulo 3 apresenta nossas constatações sobre a segurança e auditabilidade da urna eletrônica. A maior parte é dedicado à corretude e integridade do software antes e durante o dia de eleições, e a como garantir que os resultados de uma urna cheguem sem modificações ao TRE.

O capítulo 4 lista as principais conclusões deste relatório.

Adicionalmente, no Anexo A tem-se uma pequena visão sobre a dificuldade de se implantar um sistema informatizado para o registro de votos, como o realizado hoje no Brasil; no Anexo B tem-se o pedido original do Senado para realizar uma auditoria no sistema informatizado de eleições; e finalmente no Anexo C tem-se uma cópia do termo de compromisso que tivemos que assinar para poder ter acesso à sala preparada pelo TSE com vistas ao processo de verificação dos códigos-fonte dos programas de computador no sistema informatizado de eleição.

Capítulo 2

Tecnologias eleitorais e segurança

2.1 Introdução

Neste capítulo apresentaremos as tecnologias eleitorais que existem hoje, e discutiremos a questão de segurança no processo eleitoral. Começaremos (§2.2) com uma eleição convencional com cédulas em papel que serve como nossa referência principal. Depois (§2.3) apresentaremos outras tecnologias que são utilizadas atualmente. Em seguida, discutiremos a segurança em geral (§2.4), a questão da transparência do processo em particular (§2.5), explicando como uma comprovação física poderia ajudar (§2.6), e quais são as dificuldades de um sistema cuja segurança se baseia no software (§2.7). Na seção 2.8 apresentaremos os requisitos formais de segurança de uma votação, e os aplicaremos às tecnologias eleitorais (§2.9).

2.2 Uma eleição com cédulas em papel

Antes de discutir tecnologias eleitorais e a sua segurança, é ilustrativo descrever uma eleição utilizando tecnologia convencional. Pensamos numa eleição com um número pequeno de eleitores, usando cédulas em papel. Pode-se distinguir as seguintes etapas (compare [3], pg. 58):

Etapa 1 Existe uma lista com todos os nomes das pessoas que têm o direito de votar;

Etapa 2 Antes de começar a eleição, o presidente mostra que a urna está vazia;

Etapa 3 O eleitor recebe uma cédula, entra numa cabine de votação e escreve sua opção na cédula;

Etapa 4 O eleitor confere e confirma seu voto;

Etapa 5 O eleitor deposita sua cédula na urna. A partir deste momento ele não pode mais voltar atrás e modificar seu voto;

Etapa 6 Após a expiração do prazo para votar, o presidente abre a urna e os votos são apurados. Isto é feito numa sessão pública; quem quiser, pode acompanhar a contagem dos votos;

Etapa 7 Quem discordar do resultado, pode solicitar uma recontagem. Na presença de todos, os votos serão recontados (talvez várias vezes) até que haja consenso.

Uma eleição nacional por cédulas nada mais é que uma generalização desta idéia. Contudo, por razões de escala, há modificações:

- Não existe apenas uma urna, mas milhares, cujos resultados parciais são públicos e totalizados para obter o resultado final. (Como é costume, usa-se *apurar* para contar os votos de uma urna, e *totalizar* para agregar os resultados de várias urnas.)

- Algumas responsabilidades na fiscalização das eleições são delegadas e reservadas aos partidos políticos. Eles, representando os candidatos, têm direitos e privilégios específicos, como acompanhar a apuração e totalização dos votos, impugnar uma urna, etc.

O princípio de uma eleição por cédula é simples, mas na prática há vários problemas, destacando-se:

- No Brasil, o eleitor votava escrevendo o número ou o nome do candidato preferido na cédula. Como a letra de cada eleitor nem sempre é muito clara, as incertezas eram resolvidas pelos mesários, resultando em interpretações. Isto levava, em muitos casos, a uma certa ambigüidade (e até arbitrariedade) sobre a validade de um voto. O formato da cédula é diferente em cada país. Na Holanda, os nomes de todos os candidatos cabem na cédula, e o eleitor vota enchendo um círculo (○) em frente do nome do candidato preferido.
- A totalização dos votos é feita manualmente, o que pode levar vários dias (até semanas) e está sujeita a muitos erros. Muitas vezes uma recontagem dá resultados diferentes, e é muito difícil determinar o resultado final com exatidão.
- Tirar cédulas ou colocar cédulas adicionais numa urna é relativamente fácil.

2.3 Outras tecnologias eleitorais

Devido a estes problemas, vários países vêm buscando outras soluções para executar uma eleição. Dependendo da tecnologia empregada, dividimos estas soluções nos seguintes grupos[6, 1]:

Sistemas de votação com cédula em papel (SVCP) Este é o sistema descrito na seção anterior.

Sistemas de votação com cédula em formato especial (SVCFE) No ato de votar o eleitor cria uma cédula num formato que permite que ela seja lida mecanicamente. Por exemplo, a cédula na forma de um cartão perfurado, ou uma faixa de papel com um código de barra. Isto possibilita a contagem dos votos com máquinas (leitoras de cartões perfurados, leitoras de código de barra), o que permite a automatização e a conseqüente aceleração do processo de contagem dos votos.

Sistemas de votação mecânica (SVM) Esta tecnologia, bastante comum em outros países, nunca foi usada no Brasil. Pense numa calculadora mecânica de 40 anos atrás, e pode-se imaginar como uma máquina grande adiciona os votos mecanicamente. O eleitor aperta alguns botões que representam seu voto, gira uma alavanca e o voto é contabilizado.

Sistemas de votação eletrônica sem comprovação física(SVESC) Chamados DREs (Direct Recording Electronic Devices = dispositivos eletrônicos de registro direto) nos Estados Unidos, são essencialmente computadores com uma interface especial (tela sensível ao toque, teclado especial) para registrar o voto. No final da votação, o equipamento fornece os resultados. A urna brasileira pertence a este grupo.

Sistemas de votação eletrônica com comprovação física(SVECC) A única diferença em relação ao grupo anterior é que neste grupo a vontade do eleitor é "gravada" e guardada numa forma física, por exemplo por impressão do voto. Veja seção 2.6 para uma explicação sobre esta propriedade.

2.4 Segurança no processo eleitoral

A seguir, enumeramos alguns fatos gerais sobre segurança:

- Na prática, não existe algo como 100 % seguro ou 100 % infalível.

- Para aperfeiçoar a segurança, é necessário supor que o adversário sempre ataca o ponto mais fraco. Portanto, o processo de melhorar a segurança sempre envolve todo o sistema, e os custos crescem exponencialmente.
- Segurança está sempre associada a custo, embora o custo não seja sempre medido em dinheiro: um político pode estar mais interessado em poder do que em dinheiro, um fraudador pode avaliar a probabilidade de ser preso;
- Na área da segurança não é uma boa prática confiar na boa fé de todas as pessoas envolvidas. Dinheiro ou pressão podem fazer com que as pessoas ajam de má fé. Por isso é sempre bom dividir grandes responsabilidades entre várias pessoas.

A fraude eleitoral é como a sonegação de impostos ou o excesso de velocidade: existe no mundo inteiro, e quem acredita poder agir sem ser detectado, vai tentar. Mesmo se 99,99 % da população brasileira seja honesta, ainda restam milhares de pessoas que podem estar dispostas a manipular uma eleição. Temos que nos preparar contra este pequeno grupo.

Analisando possíveis fraudes eleitorais, temos que comparar o escopo da fraude com o número de pessoas necessárias para executar a fraude. Comparando o sistema com cédulas convencionais com a urna eletrônica, observa-se o seguinte: fraudar ficou mais difícil. No entanto, uma fraude bem sucedida poderia ter um impacto muito maior, modificando o resultado em dezenas ou centenas de urnas de uma só vez, talvez modificando o resultado final da eleição. Aliás, note que neste sentido eleições municipais são muito mais sensíveis a fraudes que eleições nacionais, porque modificando 5-10 urnas em bairros estrategicamente escolhidos é possível modificar o resultado final de uma eleição.

Pensando em segurança em geral, é sempre bom pensar como os bancos ou os militares lidam com este assunto. Estratégias convencionais de segurança são: separar conhecimento (apenas quem precisa tem acesso às informações), separar e dividir responsabilidades, e auditar. Porém, guardar tudo em segredo também não é bom. Esta postura, conhecida como *Security by obscurity*, não permite uma avaliação crítica por terceiros, podendo resultar (como já resultou) em desastres de segurança. É importante achar o equilibro entre uma postura fechada e uma aberta. Veja [15] para uma discussão sobre este assunto.

No entanto, eleições são um caso particular, que não pode ser tratado da mesma forma que os problemas de segurança dos bancos ou ambientes militares. Além da segurança, há a questão da transparência. A transparência leva a uma maior confiança do eleitor no processo eleitoral.

2.5 Transparência no processo eleitoral

Como explicado antes, do ponto de vista da segurança pode parecer uma boa estratégia limitar o conhecimento sobre a segurança a um pequeno grupo de pessoas, dificultando assim as possibilidades de fraudes. Mas ao mesmo tempo isto deixa espaço para dúvidas, suspeitas e teorias de complô e conspiração, por ser pouco transparente. O consenso geral entre especialistas na área de tecnologia eleitoral é que um sistema que elimina estas dúvidas é considerado superior. Por exemplo, num relatório escrito por um grupo de professores do CalTech e MIT [3], constam, entre outras, as seguintes recomendações (pagina 42):

- *Move away from complex, monolithic machines;*
- *Make source code for all vote recording and vote counting machines processes open source and source code for the user interface proprietary;*[1]
- *Adapt equipment so that* voters *can create a record of the vote that they can examine directly, and that can be used to audit equipment and elections;*
- *Conduct audits of votes and equipment, even without a recount [requested by some party];*
- *Design equipment that log all events (votes, maintenance, etc.) that occur on the machine.*

[1] Veja a discussão sobre códigos-fonte aberto em §2.7.

Em suma, recomenda-se tecnologias cuja segurança e auditabilidade sejam fáceis de entender para qualquer pessoa, ao mesmo tempo permitindo uma apuração rápida e confiável dos votos. Estes requisitos contraditórios não são fáceis de conciliar.

Para explicar a noção de transparência, damos primeiro um exemplo num contexto diferente. Quem paga em dinheiro vivo pode simplesmente contar o dinheiro, depois dar à outra parte, que conta o dinheiro e concorda ou não. Porém, se se trata de uma quantia elevada, é melhor que uma das partes pegue o dinheiro e o coloque na mesa ou balcão de maneira que o outro pode facilmente conferir se a quantia está certa, por exemplo agrupando as notas em grupos que somam 100 reais. Assim, disputas podem ser resolvidas facilmente, porque é mais fácil descobrir e apontar onde está o erro. Na realidade, quem age de forma transparente está dizendo o seguinte: você não precisa confiar em mim, use seus próprios olhos e ouvidos e convença-se de que estou sendo honesto com você.

Consideramos a segunda maneira de executar a transação mais *transparente*, porque *a parte passiva é capaz de acompanhar o processo com facilidade e pode se convencer de que ele é executado de maneira honesta*. Adotaremos isto como nossa definição de transparência.

Uma eleição serve para determinar a vontade do povo, assim dando a legitimidade aos candidatos eleitos para assumir seus cargos. Ou seja, para uma democracia é de suma importância que as eleições tenham credibilidade em todos os seus aspectos. Portanto, é desejável executar as eleições de uma forma transparente, porque aumenta sua credibilidade.

Em eleições com cédulas convencionais já existem costumes associados à transparência:

- Antes do início, o presidente mostra que a urna está vazia;
- Observadores podem assegurar a integridade da urna durante a eleição;
- A apuração dos votos acontece em sessão pública;
- As cédulas são mostradas para provar que não foram marcadas;

Também é costume registrar o que acontece, para que no caso de um recurso tal como um pedido de recontagem, seja possível reconstruir o que aconteceu. Dizemos que um processo é *auditável* quando vários registros de eventos são guardados, que garantem que posteriormente seja possível verificar se o processo funcionou corretamente, ou se houve um erro.

Comparando-se as tecnologias apresentadas na Seção 2.3, observa-se que elas diferem muito em termos de transparência e auditabilidade: no sistema de votação com cédula em formato especial (SVCFE) e sistema de votação eletrônica com comprovação (SVECC), a tecnologia permite que não-especialistas em tecnologia, tais como mesários, eleitores, fiscais de um partido, acompanhem e verifiquem a criação do voto e/ou a apuração; também existe a opção de uma auditoria posterior. No caso de sistema de votação mecânica (SVM) e sistema de votação eletrônica sem comprovação (SVESC), estas propriedades estão ausentes: a tecnologia empregada é muito complexa, impossibilitando uma avaliação precisa da segurança do sistema por um não-especialista. Apenas especialistas são capazes de fazer esta avaliação, exigindo do eleitor a necessidade de confiar nas autoridades eleitorais e seus assessores e fiscais. Discutiremos este assunto detalhadamente em seção 2.9.

2.6 Comprovação física do voto

Como já dissemos, tecnologias eleitorais não são iguais nas suas capacidades de registrar eventos importantes. Porém, uma característica merece atenção especial. Em algumas tecnologias, a vontade do eleitor é “gravada” e guardada numa forma física, por exemplo, as marcas de um lápis numa cédula convencional, ou a tinta num papel se houver impressão do voto. Isto é chamado *comprovação física do voto*, e a sua existência facilita muito uma auditoria. Em outras tecnologias esta comprovação física do voto não existe. O voto do eleitor já é contabilizado imediatamente no momento da votação, ou seja, o voto é adicionado ao registro (mecânico ou eletrônico) do candidato correspondente, mas não há um registro independente do voto.

No caso de eleições usando máquinas mecânicas, não existe uma cédula. Como explicado, o eleitor aperta alguns botões que representam seu voto. Depois, aciona uma alavanca para confirmar seu voto, e mecanicamente o voto é totalizado. Com esta tecnologia não é possível verificar se foi criado um voto válido, verificar se ninguém mal-intencionado é capaz de modificar um voto, convencer-se que o voto pertence ao conjunto, ou recontar os votos. O eleitor deve acreditar que a tecnologia empregada fornece estes requisitos, ou seja, ele deve ter fé nas autoridades eleitorais, que devem ser fiscalizadas pelos partidos. Com esta tecnologia, é difícil vincular um voto a um eleitor, e a apuração dos votos se reduz a ler o estado final da máquina.

Como [1] menciona, sistemas de votação eletrônica "são a versão eletrônica de máquinas de alavanca". Tampouco há uma cédula, e eles satisfazem as mesmas propriedades de segurança que os sistemas mecânicos. Porém, o quadro muda completamente quando se acrescenta ao sistema uma comprovação do voto, por exemplo, imprimindo o voto. Tendo uma comprovação física do voto, as propriedades de transparência e auditabilidade que sistemas mecânicos e eletrônicos normalmente não satisfazem, são recuperadas.

2.7 Segurança através de software

Se não houver comprovação do voto ou uma plataforma computacional segura, é muito difícil –senão impossível– garantir a integridade de um equipamento rodando um programa, quando supomos que o adversário tem acesso a ele.

Por exemplo, num sistema de votação com cédula em papel o presidente da mesa mostra que a urna está vazia. Da mesma forma é necessário mostrar que o equipamento que conta os votos está no seu estado inicial. Num sistema de votação mecânica, verifica-se que todos os contadores estão na posição representando zero votos[2]. Num sistema de votação eletrônica imprime-se os valores armazenados nos registros que representam o número de votos por candidato. No Brasil este relatório é chamado de *zerésima*.

No entanto, num sistema de votação eletrônico, quem garante que o relatório impresso representa o verdadeiro estado daqueles registros? Se alguém quisesse fraudar, não seria um dos primeiros passos criar um arquivo falso, de zerésima, garantindo sua impressão quando for solicitado, independente do verdadeiro estado da máquina?

É claro que neste tipo de fraude há mudanças de alguns arquivos: foi colocado um arquivo a mais (contendo a zerésima pré-construída), e foi mudado o programa atendendo à solicitação de impressão da zerésima. Então, para dificultar este ataque podemos escrever um meta-programa, que tem como tarefa verificar a integridade de todos os arquivos, por exemplo comparando os resumos criptográficos calculados com os valores armazenados no equipamento. Teoricamente este esquema descobre qualquer modificação em um dos arquivos, dificultando a modificação dos programas.

Mas se alguém consegue modificar este meta-programa? Modificações, por exemplo, podem fazer com que o meta-programa nunca reclame sobre discrepâncias entre os resumos criptográficos ou mesmo emita um resumo criptográfico padrão para um determinado arquivo. Na realidade, para quem já sabe como modificar programas executáveis, não é muito difícil achar a função responsável pela comparação dos resumos criptográficos calculados com os valores armazenados. Tampouco é complicado descobrir o comando onde se faz esta comparação; deve ser algo parecido com:

```
if (res_calculado==res_armazenado) continuar;
else abortar;
```

e tampouco é complicado modificar a condição para sempre ser verdade:

```
if (TRUE) continuar;
else abortar;
```

Não será em linguagem C, é claro. É preciso conhecimento de *assembly* e talvez um pouco de paciência.

Podemos até pensar em técnicas criptográficas mais avançadas (como *message authentication codes*), mas o problema é que não é claro que estas resolvem todos os possíveis ataques no nível mais baixo de software: firmware, BIOS, sistema operacional, drivers, etc.

[2] Em [9] é descrita uma fraude em que o estado inicial não foi zero.

A conclusão é que estas técnicas dificultam ataques e aumentam a integridade, mas nunca os impossibilitam completamente: para qualquer providência em software contra fraude, é sempre possível conceber um contra-ataque que o burle. Por isso, basear a segurança de um sistema eleitoral apenas no software é, em nossa opinião, um caminho inviável. Abrir o código-fonte não resolveria o problema, porque com uma quantidade enorme do código-fonte fica impossível *provar* que o executável corresponde ao código-fonte, e que não há um software malicioso no equipamento que gera e soma os votos.

Na proposta de [3] há um meio termo interessante. Os autores propõem separar o equipamento que gera os votos daquele que soma os votos. O primeiro equipamento pode ter uma complexidade arbitrária, já que ele gera o voto num formato padronizado. Mas o equipamento que soma os votos deve ser, segundo os autores, um equipamento muito simples, com hardware e software completamente aberto. Poderiam até existir equipamentos de vários fabricantes capazes a somar os votos a partir do voto padronizado, possibilitando uma verificação independente.

2.8 Requisitos de Segurança

Introduzimos a eleição por cédulas em papel por duas razões. Primeiro, quando se discute a tecnologia de eleição através de urnas eletrônicas, é bom ter uma referência. Especificamente, quando se discute a urna e afirma-se que uma coisa é boa ou ruim, deve-se fazê-lo em relação a algo. Em segundo lugar, com uma eleição por cédulas em mente, podemos com mais facilidade apresentar os requisitos de segurança que uma votação deve obedecer.

Procuramos aqui formular uma lista concisa de requisitos de segurança, definindo o que quer dizer uma eleição honesta. Não achamos na literatura um documento simples e conciso definindo estes requisitos, a única exceção sendo [7]. Contudo, optamos por listá-los na ordem cronológica de uma eleição, o que facilita verificar se não há falta de requisitos.

Sobre quem pode votar

Requisito 1: *Apenas pessoas autorizadas, chamadas eleitores, podem criar e depositar uma cédula na urna.*
Explicação: Cada votação tem seu conjunto de pessoas que têm o direito de votar. É necessário verificar que apenas estes votem.

Requisito 2: *Cada eleitor pode emitir apenas um voto.*
Explicação: ”One man, one vote”. Não se pode votar duas vezes.

Sobre o ato de votar — a criação e o depósito do voto

Requisito 3: *O preenchimento de uma cédula e seu deposito na urna é um ato confidencial, e sob hipótese nenhuma deve ser possível deduzir em que(m) o eleitor votou.*
Explicação: Este requisito, o sigilo do voto, é o mais importante de todos. É importante entender que o sigilo de voto tem dois lados. Primeiro, o eleitor deve ter a liberdade de expressar sua vontade sem correr o risco de sofrer represálias. Para garantir isto, ninguém deve ser capaz de descobrir em que(m) ele votou.

Por outro lado, é necessário evitar a compra e venda de votos. Conseqüentemente, não deve ser possível, nem com a cooperação ou conivência do eleitor, deduzir qual foi seu voto. Por isto é de suma importância que, durante a criação da cédula, não seja criado um comprovante que pode ser vinculado a um voto ou a uma cédula na urna, pois isto possibilitaria a coação e a venda/compra de votos.

Para proteger a confidencialidade do eleitor existe um espaço privativo onde ele pode preencher sua cédula. Pode-se reformular este requisito dizendo que a única informação que pode sair da cabine de votação é a cédula preenchida, mais nada.

Requisito 4: *O eleitor pode verificar que criou um voto válido.*
Explicação: Terminado o processo de criar seu voto mas antes de liberá-lo, o eleitor deve ter o direito de conferir seu voto para que ele tenha certeza que votou certo: no candidato certo/alternativa certa e que seu voto é válido.

Sobre a integridade dos votos — da emissão até a apuração

Requisito 5: *O eleitor pode se convencer de que seu voto estará incluído no conjunto para ser apurado.*
Explicação: Este requisito é o mais difícil a ser realizado. Gostaríamos que fosse possível entregar um comprovante ao eleitor para que ele possa verificar que seu voto consta do conjunto de votos apurados[3]. No entanto, este requisito contradiz um outro requisito mais importante: o sigilo de voto. No caso de eleição por cédula, este requisito é teoricamente atendido da seguinte maneira: depois que o eleitor tiver depositado a cédula na urna, ele espera até o encerramento da eleição e quando a urna é aberta para apuração dos votos, ele tem certeza de que sua cédula pertence ao conjunto, mesmo não sabendo qual cédula corresponde àquela que ele preencheu. É interessante notar que, no fundo, a fé do eleitor se baseia numa noção de bom-senso: um objeto depositado num lugar permanece lá e não desaparece sozinho.

É esta tensão entre a auditabilidade e o sigilo de voto que dificulta o projeto de sistemas eleitorais que atendem a ambos os requisitos sem usar cédulas ou outros objetos físicos. Implícito em cada eleição há um sub-procedimento para misturar os votos. Este processo, trivial quando se trata de objetos físicos como cédulas ou cartas de baralho, é extremamente difícil de simular no mundo virtual. Mesmo usando os melhores protocolos e técnicas de criptografia, esta questão não tem uma solução satisfatória.

Requisito 6: *Não deve ser possível modificar um voto ou removê-lo do conjunto, uma vez depositado na urna, ou adicionar ao conjunto votos inválidos, isto é, votos criados em violação ao Requisito 1 e 2.*
Explicação: Os votos representam a vontade (anônima) dos eleitores (até aquele momento), e qualquer modificação alteraria esta vontade. Este requisito explica porque antes do início o presidente mostra que a urna está vazia, porque a urna deve ficar num lugar público e visível a todo mundo, ou porque se usam urnas de plástico transparente em votações.

Requisito 7: *Todos os votos permanecem em segredo até o fim da votação.*
Explicação: Além de obviamente quebrar o sigilo do voto de quem já votou, saber quais votos já foram depositados poderia mudar o voto de quem vota depois. Isto seria injusto para com quem votou primeiro.

Sobre a apuração dos votos

Requisito 8: *A apuração dos votos ocorre numa sessão pública e é verificável.*
Explicação: Para dar maior credibilidade ao resultado é necessário que a presença de fiscais de partidos ou observadores neutros seja permitida.

Requisito 9: *Todas as cédulas válidas, e apenas estas, serão incluídas na apuração.*
Explicação: Este requisito, óbvio em si, está intimamente ligado ao Requisito 6: se ele foi atendido, seria suficiente contar os votas na urna.

Sobre a auditabilidade

Requisito 10: *É possível recontar os votos.*
Explicação: Qualquer pessoa pode contestar o resultado e exigir uma recontagem dos votos, que ocorreria também numa sessão pública. Em princípio este processo deve convergir para um resultado com que todos concordam.

Observe que Requisitos 4, 5, 6, 8, 9 e 10 são ligados à transparência e auditabilidade.

É importante lembrar que os requisitos listados aqui não são os únicos critérios para avaliar um sistema eleitoral. Existem outros, como por exemplo, tempo para obter o resultado, eficiência, custo/benefício, facilidade de uso, etc. Veja por exemplo [10].

[3] O novo protocolo do Chaum[5], de cuja existência ficamos sabendo recentemente, resolve exatamente isto. O sistema gera dois comprovantes, que juntos comprovam o voto. Depois um dos dois, escolhido aleatoriamente, é destruído, e o eleitor fica com o outro, que serve para verificar se seu voto consta no conjunto apurado. Porém, entender porque o comprovante não divulga nenhuma informação sobre o voto exige um conhecimento avançado de criptografia, o que pode ser estar fora do alcance do cidadão comum.

2.9 Aplicando os requisitos de segurança às tecnologias

Na seção 2.3 dividimos as tecnologias eleitorais existentes em cinco grupos:
SVCP: Sistemas de votação com cédula em papel
SVCFE: Sistemas de votação com cédula em formato especial
SVM: Sistemas de votação mecânica
SVESC: Sistemas de votação eletrônica sem comprovação física
SVECC: Sistemas de votação eletrônica com comprovação física.

Na seção anterior formulamos os principais requisitos de segurança. Então é interessante listar todos os requisitos, e comparar em qual medida as tecnologias satisfazem os requisitos, o que é o objetivo desta seção.

Requisito 1 : apenas eleitores autorizados podem votar
Para grandes eleições existe uma lista com os nomes de todos eleitores: um cadastro eleitoral. Este cadastro independe da tecnologia empregada. Observe que a divisão em seções eleitorais serve para facilitar a verificação deste requisito.

Requisito 2 : um eleitor pode votar uma vez só
Este requisito é muito ligado ao Requisito 1: quase todos os sistemas têm um procedimento manual para registrar quem votou, que independe da tecnologia usada para votar. No caso da urna eletrônica, este registro é feito através da própria urna (além da lista de presença que todo eleitor deve assinar): o presidente da mesa digita o título do eleitor na urna para autorizar o eleitor a votar; a urna responde mostrando o nome do eleitor no *display* do presidente. Isto se torna uma grande preocupação nossa; veja o próximo requisito.

Requisito 3 : sigilo do voto
O sigilo do voto durante o preenchimento é preservado em SVCP, em SVCFE e em SVM. No caso de sistemas de votação eletrônica (SVESC ou SVECC), o sigilo do voto depende da implementação: se o equipamento para registrar a identidade é separado daquele de votar, podemos supor que o sigilo é preservado (desde que não exista um programa de log, registrando todas as tecla.) Porém, se é o mesmo equipamento, existe uma possibilidade de vincular o voto à identidade do eleitor. Este é o caso na urna brasileira.

Requisito 4: verificar se a cédula é válida
Em geral, em SVCP e em SVCFE o próprio eleitor pode verificar que criou uma cédula válida. Porém, deve-se observar que não existe nenhuma possibilidade de feedback se o eleitor errar, e que, dependente do leiaute da cédula, a taxa de votos inválidos pode ser considerável.

Em SVM, SVESC e SVECC a tecnologia restringe as opções do eleitor, eliminando vários tipos de erro que um eleitor pode cometer. Porém, não existem cédulas e portanto não há um mecanismo para verificar o voto: o eleitor deve confiar na tecnologia. Em SVECC o eleitor pode verificar a cédula, se a ele é permitido inspecionar a comprovação.

Requisito 5: a cédula será apurada
Em SVCP, SVCFE e SVECC, a cédula e a respectiva comprovação são físicas e o eleitor é capaz de verificar este requisito. Nos casos de SVM e SVESC o eleitor não é capaz de verificar este requisito, ele precisa confiar na tecnologia.

Requisito 6: integridade do conjunto de votos
Em SVCP, SVCFE e SVECC existe um objeto físico e verificar este requisito é mais fácil. Em SVM e SVESC este requisito deve ser fornecido pela tecnologia usada.

O dilema aqui é o seguinte: com um objeto físico verificar é mais fácil, mas também é mais fácil fraudar. Com uma tecnologia avançada, fraudar pode ser mais difícil, mas verificar que não houve fraude também é mais difícil.

Requisito 7: votos ficam em segredo durante a votação
Na prática, este requisito está incorporado no Requisito 6 e não é uma grande preocupação.

Requisito 8: a apuração é verificável

	SVCP	SVCFE	SVM	SVESC	SVECC
1 (apenas eleitores autorizados podem votar)	I	I	I	I	I
2 (no máximo um voto por eleitor)	I	I	I	I	I
3 (sigilo do voto)	A	A	A	D	D
4 (eleitor criou cédula valida)	V	V	N	N	V
5 (voto será apurado)	V	V	N	N	V
6 (integridade do conjunto dos votos)	V	V	N	N	AU
7 (votos ficam segredos até final)	V	V	V	V	V
8 (a apuração somente contém cédulas válidas)	V	V	N	N	AU
9 (a apuração é verificável)	A	V	N	N	AU
10 (uma recontagem é possível)	A	A	N	N	A

Legenda: I=independe da tecnologia;A=atendido;
N=não verificável;V=verificável;AU=auditável;D=Depende

Tabela 2.1: Aplicando os requisitos de segurança aos cinco grupos de tecnologias eleitorais.

Em SVM e SVESC não há cédulas, a apuração já acontece quando o eleitor confirma seu voto, e não há uma apuração posterior.

Requisito 9: a apuração contém apenas cédulas válidas
Em princípio, em SVCFE todo eleitor pode verificar a apuração. Porém, em SVM e SVESC é "a tecnologia" que conta os votos, um método que não pode ser verificado (apesar de ser menos sensível a erros do que SVCFE). Em SVECC, este requisito é auditável.

Requisito 10: recontagem é possível
Obviamente, recontagem é possível em SVCFE e SVECC, mas não em SVM e SVESC.

A situação é resumida na Tabela 2.1.

2.10 Conclusões

Apresentamos neste capitulo várias tecnologias eleitorais. Discutimos os requisitos de segurança que um sistema eleitoral deveria ter. Mostramos que, dependendo da tecnologia empregada, obtém-se propriedades de segurança diferentes, especificamente com relação à transparência e à auditabilidade.

Capítulo 3

A segurança e a auditabilidade da urna brasileira

3.1 Introdução

Depois de ter descrito a tecnologia eleitoral do ponto de vista global e mais teórico, queremos dedicar este capítulo à urna brasileira. Nossa abordagem será a seguinte: queremos aplicar os requisitos de segurança à urna. Especificamente trataremos as perguntas:

- A urna eletrônica é segura?
- A urna eletrônica é auditável?

3.2 Cadastro de eleitores

Todo cidadão brasileiro que reúne as condições necessárias para ser um eleitor deve se alistar em um cartório eleitoral. Após o alistamento, o eleitor recebe seu título de eleitor que contém a zona e seção eleitoral onde o eleitor deverá votar. O atual formato do título contém exclusivamente o nome do eleitor, sua assinatura, um código de identificação do título e a zona e seção eleitoral. O cartório eleitoral se preocupa em alocar um determinado número máximo de eleitores por seção eleitoral. A seção é escolhida também em função da localização do domicílio do eleitor.

3.3 Vincular o Voto ao Eleitor

O presidente da mesa digita o título do eleitor num equipamento chamado *micro-terminal* fisicamente conectado à urna. Com isto é muito simples relacionar eleitores com votos. É só registrar, em separado, as teclas do micro-terminal e da urna. Contudo, trata-se somente de uma possibilidade. Em nossas investigações não foi encontrado qualquer vestígio desta possibilidade ter sido implementada. No entanto, este é um desconforto que o eleitor não precisaria ter.

3.4 A Impressão do Voto

Como foi explicado no capítulo anterior, o voto impresso é um espécie de comprovação física do voto, e sua presença ou ausência determina se as eleições são auditáveis ou não. Com a impressão, a urna cai na coluna SVECC da Tabela 2.1; sem impressão, na coluna SVESC.

Estudando os documentos sobre a concepção, projeto e desenvolvimento do sistema eleitoral informatizado no Brasil, observa-se que um tipo de comprovação do voto era previsto desde o início:

> "b) Deverá ser resguardado o direito à fiscalização da votação e da apuração, bem como garantir a conferência do resultado de cada Seção por meio de auditagem ou recontagem;" ([4], pg. 72)

> "4 – A comprovação física do voto deverá conter pelo menos o número do candidato e será impressa ou grafada, de forma que seja possível a leitura de seu conteúdo sem a necessidade de qualquer tipo de equipamento eletro-eletrônico ou mecânico;" ([4], pg. 75)

A primeira eleição com a urna, a de 1996, foi efetuada com a impressão do voto. Porém, a impressão deu tantos problemas que foi abolida. Nas eleições de 2002 a impressão foi re-introduzida como um teste em aproximadamente 25.000 urnas (3% das urnas). A legislação atual (janeiro de 2003) prevê a impressão do voto para todas as urnas nas eleições de 2004. Mas de novo houve problemas, e aparentemente o TSE pensa em desistir da idéia de imprimir o voto em 2004.

A impressão do voto empregada nas eleições de 2002 é assim: depois de ter apertado a tecla `confirma` pela última vez, confirmando o voto para presidente, a urna imprime os números e nomes dos candidatos escolhidos numa unidade de impressora separada da urna. A impressão acontece numa caixa de plástico com um visor transparente. Desta forma, o eleitor poderia ver o papel com seus candidatos através de uma lente, sem poder tocá-lo.

Vendo os candidatos escolhidos, o eleitor aperta na tecla `confirma` ou `corrige`. No primeiro caso, a palavra VÁLIDO é impressa no papel, o papel é cortado e cai numa sacola de plástico preta, que funciona com uma urna convencional e o procedimento de votar encerra-se. No segundo caso, a palavra CANCELADO é impressa no papel, o papel é cortado e cai na sacola de plástico, e o eleitor pode votar novamente. Se o eleitor cancela duas vezes, ele é conduzido para votar numa cédula convencional de papel.

Desconhecemos a natureza exata dos problemas que ocorreram com a impressão do voto. Mas é obvio (1) que o processo de votação é mais demorado: o eleitor pode conferir seu voto, e refazer se quiser. Aliás, nem todos os eleitores se esforçam para conferir seu voto. (2) A impressora é mais um equipamento que pode ter falhas técnicas. (3) Aumenta os custos.

Várias pessoas acham que a re-introdução da impressão do voto é um retrocesso. Elas acreditam que a urna seja segura, e que a impressão apenas convida os candidatos vencidos a entrar com recursos, solicitando uma nova recontagem. Nós discordamos, porque sem impressão ou outra comprovação do voto é muito difícil, senão impossível, de se provar que a urna seja segura. Se houvesse impressão do voto, isto implicaria auditabilidade, e poderíamos declarar sem ressalva que a urna é segura e auditável. Qualquer leigo poderia entender como esta segurança é estabelecida. Contudo, sem impressão, claramente não há quase nenhuma auditabilidade, e mostrar que a urna é segura se torna muito mais complicado, como veremos nas próximas seções.

A comprovação do voto não é um luxo, mas é uma peça chave para realizar um sistema eleitoral auditável, o que, pode-se argumentar, é um direito fundamental do povo numa democracia. Se o TSE abolir a impressão do voto, deve-se estudar outras tecnologias para conseguir a comprovação do voto e a auditabilidade.

No resto deste capítulo estamos supondo que não há impressão dos votos, nem outra tecnologia provendo uma comprovação da vontade do eleitor.

3.5 O software da Urna

Podemos abordar a questão de segurança da seguinte maneira:

1. O conjunto de programas produzido pelo TSE deve ser correto;
2. Os programas encontrados na urna no dia de eleição devem ser iguais àqueles produzidos pelo TSE;
3. O resultado de uma urna não pode ser modificado entre o momento que sai da seção eleitoral e chega no TRE;
4. A totalização nos TREs e TSE deve ser correta.

3.5.1 A corretude dos programas na urna

Apesar de termos ido três vezes ao TSE, num total de 13 dias, e apesar de *acreditarmos* que a urna seja segura, *não* podemos atestar isto com 100% de segurança. As razões incluem:

O tamanho dos programas-fonte não permite uma auditoria rigorosa por terceiros. Um subsistema tem tipicamente um tamanho de 10.000 linhas de código em linguagem C. Não temos uma estimativa do tamanho total, mas ele deve ter pelo menos 100.000 linhas de código em linguagem C, falando-se apenas dos programas de aplicação da urna. Ou seja, há ainda o BIOS[1], e o sistema operacional a considerar.

Não foi possível verificar todos os programas. Especificamente, o sistema operacional usado nos modelos 1996, 1998 e 2000 da urna, o VirtuOS, não era auditável pelos partidos políticos. Veja seção 3.6.

O processo de compilação é muito complexo e mal-documentado, impossibilitando a verificação por terceiros das opções empregadas ou arquivos adicionais. Por exemplo, duvidamos que seja possível reproduzir o executável apenas usando a documentação existente, sem a ajuda de vários técnicos do TSE.

Em essência, não foi possível verificar a corretude dos programas-fonte e a versão compilada produzida pelo TSE, apesar de termos acompanhado o trabalho dos técnicos do TSE, solicitado explicações, visto os códigos-fonte, etc.

Queremos deixar muito claro que não encontramos nenhum vestígio de fraude. Todas as dúvidas foram esclarecidas com profissionalismo, cortesia e paciência. Muitas vezes o pessoal estava muito motivado a falar conosco. Porém, na hipótese de que alguém tivesse colocado algo suspeito, a probabilidade de um terceiro descobrir isto durante nossas sessões no TSE é quase zero. A segurança e corretude dos programas usados na urna baseia-se em confiar na boa fé dos técnicos do TSE. Repetimos: não há nenhuma razão para duvidar da boa fé destas pessoas. Mas isto fere as boas práticas de segurança.

Uma aplicação mais rigorosa de padrões na área de segurança (como o *Common Criteria* [11], hoje adaptado como padrão da ISO no. 15408) e no desenvolvimento de software (como o *Software Capability Maturity Model* [13]) poderia ajudar. Mesmo assim, não é provável que uma equipe de dois ou três profissionais sem conhecimento prévio consiga absorver todos os detalhes de forma a opinar definitivamente sobre a corretude e segurança dos programas da urna.

Se houvesse uma forma de comprovação do voto, esta preocupação diminuiria em muito, porque a auditabilidade garante a possibilidade de verificação posterior. Sem uma comprovação do voto esta questão merece mais estudo.

3.5.2 A preparação da urna

Como foi mencionado, um segundo ponto é que os programas empregados na urna no dia de eleição devem ser iguais àqueles produzidos no TSE.

[1] Basic Input Output System

Uma vez compilados, os programas do TSE são disponibilizados para os TREs. Existe um programa especial que copia os programas e os dados (candidatos e eleitores) de várias seções eleitorais, e que grava este conjunto de informações em um cartão de memória Flash, chamado *Flash de Carga* (FC).

Não acompanhamos o processo de geração do FC, e desconhecemos os detalhes deste procedimento. Porém, a comunicação entre o TSE e os TREs é através de um sistema fechado e bastante seguro – podemos excluir a possibilidade de alguém modificar os programas sem a conivência de um funcionário do TRE/TSE.

O Flash de Carga é usado para configurar as urnas das seções correspondentes, um processo chamado *inseminação*. Isto é feito da seguinte maneira: insere-se o Flash de Carga na urna, e liga-se a urna. Automaticamente, o software começa a copiar os programas e dados no cartão de memória *flash* interno (FI) da urna, gerando um número aleatório que corresponderá a uma identificação desta carga. O FC guarda esta informação, com o número série da urna e da identificação da seção eleitoral, chamada de *correspondência*, para mandá-los depois ao TRE.

Depois deste passo, substitui-se o FC por um Flash de Votação (FV), que não contém dados. Depois liga-se a urna, que executa um programa de teste. Uma parte consiste em conferir o estado interno da urna, integridade dos dados e arquivos, etc. Outra parte testa a interface e requer uma resposta do operador: Teclado funcionando? Luz piscando? Tela funcionando? Emitindo som? Etc. Também verifica-se e, se necessário, corrige-se o relógio interno, que pode ter acumulado uma diferença de dezenas de minutos durante o longo intervalo de inatividade. Terminado o teste com êxito, lacra-se e embala-se a urna, que será religada somente no dia de eleição após as 07 horas, na presença de todos os mesários e dos fiscais dos partidos.

O processo da inseminação da urna é simples. O que complica o acompanhamento pelos partidos políticos é a quantidade de urnas para serem inseminadas, muitas vezes num prazo muito curto. Fala-se de 350.000 urnas que devem ser inseminadas num prazo de aproximadamente uma semana. Para economizar tempo, constrói-se uma ”linha de montagem”: alguém desembala a urna, outro faz a preparação, outro faz o teste e a lacração, e outro embala a urna pronta. O trabalho é executado por funcionários, sob supervisão de um juiz eleitoral.

A logística da inseminação é diferente em cada estado: em alguns, insemina-se em poucos lugares centralizados, e distribui-se a urna depois. Em outros estados, existem dezenas de lugares onde a inseminação acontece. Mesmo um partido bem organizado teria dificuldades para acompanhar e fiscalizar a inseminação de todas as urnas.

Observe que o teste da urna não inclui uma verificação efetiva da eleição: não se verifica, por exemplo, se todos os candidatos com suas fotos estão realmente presentes na urna. Tal verificação seria completamente inviável por causa do trabalho enorme que isto implicaria. Em outras palavras, a responsabilidade de inseminar toda urna com os dados certos fica completamente nas mãos dos funcionários eleitorais.

Teoricamente, os partidos políticos têm o direito de testar até 3% das urnas inseminadas. Existe uma aplicação, chamada VERIFICAÇÃO PRÉ-ELEIÇÃO, que possibilita verificar a presença de nome e fotos dos candidatos[2]. Ela possibilita também a impressão de uma lista de todos arquivos no Flash Interno e Flash de Votação, junto com seus resumos criptográficos.[3]

Constatamos que, na prática, o acompanhamento do processo de inseminação pelos partidos políticos não acontece. Não vimos na época das visitas nenhuma documentação explicando os mecanismos descritos acima[4], o que faz com que os partidos fiquem completamente perdidos, sem orientação. Portanto, no fundo a integridade dos programas e dados usados na urna baseia-se na boa fé dos funcionários eleitorais. Mas mesmo com uma boa orientação, esta verificação não seria muito viável, por causa de quantidade de trabalho.

A preparação da urna não é efetivamente fiscalizada pelos partidos políticos, em parte por falta de documentação, em parte por falta de interesse do lado dos partidos. Recomendamos a criação de

[2]No primeiro turno do 2002, esta aplicação não funcionou direito porque ela não era dimensionada para urnas com um grande número de candidatos.

[3]No segundo turno das Eleições 2002, a lista com os resumos criptográficos mudou durante o período da inseminação, dificultando gravemente o trabalho dos fiscais.

[4]Apenas em 2003 ficamos sabendo da existência do manual *Procedimento de conferência e verificação da UE (V-pré / V-pós)* do TSE, datado setembro 2002.

uma página web contendo informações sobre os procedimentos e sobre os direitos dos partidos. Porém, se os partidos tomassem seus direitos ao pé da letra, a preparação ficaria inviável. Por isso é necessário repensar este processo para chegar a uma solução para que os funcionários eleitorais possam realizar seu trabalho eficientemente, ao mesmo tempo permitindo que haja um acompanhamento efetivo e sério pelos partidos.

3.5.3 A integridade da urna no início da eleição

O eleitor que vai votar deve ter certeza de que o equipamento a sua frente é realmente a urna preparada pela Justiça Eleitoral, sem mudanças. Quem quer fraudar pode pensar em romper os lacres para mudar os programas, ou até em trocar a urna legítima por uma urna falsa.

Romper um lacre pode ser difícil, mas não impossível. Será que os lacres de todas as urnas são verificados posteriormente, para ver se há lacre rompido? E esta verificação é feita por uma pessoa diferente daquela que foi responsável pela urna antes da eleição?

No ataque contemplado aqui, é primeiro necessário copiar o conteúdo de um Flash de Carga. Para isto é necessário colocá-lo num notebook com um slot para cartões de memória *flash*, um procedimento relativamente fácil e rápido. Usando estes dados, é possível criar um Flash de Carga falso, com programas modificados. Depois, usa-se a FC para re-inseminar uma urna autêntica, agora com software alterado. Observe que a grande vantagem de cartões de memória *flash*, sua flexibilidade, se torna uma desvantagem na área de segurança: quem tiver acesso a ele, modifica o seu conteúdo com facilidade, sem deixar traços.

Claramente, este ataque pressupõe a conivência de várias pessoas, o que pode inviabilizá-lo. Na realidade, nunca tivemos condições para ver o conteúdo do Flash de Carga e do Flash de Votação para inspeção, impossibilitando uma avaliação mais detalhada de sua segurança.

Os cartões de memória flash passam pelas mãos de milhares de pessoas, e são uma tecnologia que não fornece nenhuma proteção física contra modificações. Desconhecemos as proteções lógicas que poderiam ter sido incorporadas, mas estamos céticos em relação a qualquer tipo de proteção feita em software, por acreditarmos que esta sempre pode ser comprometida. Não estamos cientes de qualquer proteção contra engenharia reversa, o que deixa os programas executáveis e dados armazenados nos cartões de memória *flash* vulneráveis.

Sugerimos que seja simulado um ataque contra os cartões de memória *flash*, como os usado na urna, por uma equipe de especialistas independentes, que se comportarão como um hacker tentando modificar os programas da urna.

Usando-se técnicas mais avançadas de criptografia, é possível desenvolver uma urna mais segura (como foi mostrado em [16]). A utilização de HSM no hardware da urna poderia agregar uma maior confiança à mesma. Esta questão merece mais estudo.

Se houvesse uma comprovação do voto, estas preocupações diminuiriam muito, porque a auditabilidade garante a possibilidade de verificação posterior. Sem uma comprovação do voto, estas questões merecem mais estudo.

3.5.4 A integridade da urna durante a eleição

Embora possível teoricamente, nos parece que, na maioria dos casos, um ataque feito durante a eleição pode também ser feito antes ou depois da eleição com menos risco de seus perpetradores serem flagrados. Como explicado na seção 3.5.2, existem mecanismos para impedir a troca de uma urna por uma falsa.

3.5.5 A integridade dos resultados de uma urna

Supondo que não haja fraude nos programas, é necessário garantir que os resultados de cada urna cheguem sem modificações no TRE.

A urna não conta votos ao encerrar a sessão (normalmente às 17 horas). Esta contagem é feita durante o dia: cada vez que um eleitor aperta `confirma`, o contador associado ao candidato escolhido pelo eleitor é incrementado[5]. Em outras palavras, a urna mantém a contagem por candidato armazenada num estado interno, que é atualizado sempre que o eleitor aperta `confirma`.

Portanto, obter os resultados da urna corresponde simplesmente a extrair o estado interno e fazer um relatório. Este relatório, contendo o nome e número de todos os candidatos e a quantidade de votos que cada um ganhou, é chamado o *boletim de urna*, ou *BU*. Para finalizar uma sessão de votação, o presidente da mesa inicia o seguinte procedimento:

- o programa extrai os dados, gera uma imagem do Boletim de Urna e guarda-a num arquivo temporário no Flash de Votação;
- Imprime 5 vias do Boletim de Urna;
- Grava no disquete 5 arquivos: o Boletim de Urna em texto claro, o Boletim de Urna cifrado, o arquivo de log, as justificativas (eleitores em trânsito), e os faltosos (lista de títulos de eleitor de quem não compareceu)
- Muda o nome do arquivo no Flash de Votação para um nome definitivo.

Qual é a dificuldade de forjar um Boletim de Urna? O que dificulta qualquer tipo de fraude depois do encerramento é o fato de que o resultado já é público: as 5 vias impressas ao final da votação devem ser assinadas pelos fiscais dos partidos, e uma via do Boletim de Urna deve ser afixada no local de votação. Além disso, os partidos têm direito a uma via adicional do Boletim de Urna, que pode ser comparado posteriormente com aqueles divulgados pelo TRE.

Este processo de comparar o Boletim de Urna emitido na Seção Eleitoral com o boletim publicado pelo TRE já funciona razoavelmente bem, mas pode ser aperfeiçoado, aumentando a transparência e facilitando muito o trabalho dos partidos.

A idéia de melhoria, descrita em extenso em [16], tem dois aspectos chave:

- O programa que gera o Boletim de Urna também deve calcular um resumo criptográfico do boletim. O formato exato é sujeito a discussão, mas é importante que ele permita que o resumo seja anotado e comunicado por pessoas (e não por computadores). Pode-se pensar por exemplo num número de 10 algarismos, incluindo um dígito verificador.
- Assim que possível, o Boletim de Urna deve ser publicado na Internet.

Se esta idéia for adotada, um fiscal do partido precisa apenas anotar 10 algarismos por urna, e comunicá-os (por exemplo por telefone ou por email) a um lugar central. Assim que for publicado o Boletim de Urna daquela urna, o partido recalcula o resumo criptográfico, e compara-o com o valor comunicado pelo fiscal.

Aliás, o procedimento proposto em [16] é ainda mais rigoroso. Lá propõe-se que *o presidente da mesa* comunique o resumo ao TRE, que o publica imediatamente na Internet. Podemos até imaginar que isto aconteça automaticamente: o presidente telefona para um certo número, digita um número que identifica sua Seção Eleitoral, digita uma senha para autenticar-se, e digita o resumo, tudo sem interação humana. O propósito é impossibilitar qualquer tipo de fraude que possa ser contemplada entre o encerramento e a transmissão do Boletim de Urna ao TRE, por mais improvável que seja.

A publicação dos Boletins da Urna na Internet tem uma outra grande vantagem: qualquer organização com recursos computacionais razoáveis (como os partidos políticos, universidades, a SBC) pode fazer um programa ou um conjunto de scripts para ler todos os Boletins da Urna e fazer sua própria totalização, assim verificando os resultados publicados pelos TREs. Alternativamente, podemos imaginar que a SBC, em cooperação com o TSE/TRE, desenvolva tal programa, que será completamente aberto. Se os TREs

[5] Em urnas com impressão, a incrementação acontece no momento que o eleitor confirma que o voto impresso realmente corresponde à sua vontade.

também publicarem os resultados parciais (por zona eleitoral, por município, por região) o trabalho de verificação pode ser distribuído facilmente.

Usar um resumo criptográfico num formato "humano" e publicar os Boletins da Urna na Internet daria uma grande transparência à totalização.

3.5.6 A integridade dos arquivos de log

Cada urna guarda um arquivo de log, em que são armazenados os eventos principais, por exemplo, quando a urna foi ligada, emissão da zerésima, ações do presidente da mesa, quando um eleitor começa e termina a votação, encerramento da eleição, emissão do Boletim da Urna, etc. Além de ser a fonte principal de informação caso haja suspeita de manipulação da urna, eles fornecem também informações sobre falhas de hardware, e até indicações sobre o comportamento de eleitores (duração por eleitor; em qual parte do dia há mais eleitores).

Para motivos de auditoria posterior é importante que a integridade deste arquivo seja protegida, no sentido de que qualquer mudança no arquivo seja detectada. Uma técnica comum para conseguir esta propriedade é usar uma função de resumo criptográfico para criar dependências entre sucessivas linhas do arquivo. Veja [12] para exemplos e técnicas mais sofisticadas.

Em princípio, não vemos nenhum impedimento para publicar o arquivo de logs de cada urna na Internet. Além de inspeção visual por pessoas, é possível escrever programas que analisam um arquivo log e verificam se houve irregularidades.

3.5.7 Criptografia na urna e o papel da ABIN

Para projetar e desenvolver as técnicas de criptografia empregadas na urna, o TSE contratou o CEPESC, um órgão subsidiário da ABIN. Seguindo a filosofia de compartimentalizar, a comunicação entre os funcionários do CEPESC e do TSE foi mínima. Os dois grupos definiram um pequeno conjunto de interfaces de função, especificado em linguagem C. Ou seja, o CEPESC fornece um conjunto de funções criptográficas sem saber o que acontece na urna. Os funcionários do TSE podem invocar estas funções a qualquer hora, sem saber como funciona a criptografia.

Entrevistamos os funcionários do CEPESC e vimos os programas-fonte das funções de criptografia. A criptografia assimétrica é baseada em curvas elípticas, uma tecnologia conhecida. O algoritmo simétrico é proprietário e parece robusto o suficiente. Apesar do TSE ser tecnicamente o dono deste algoritmo, o CEPESC prefere não divulgá-lo, já que técnicas semelhantes são usadas em outros sistemas, e a política de não-divulgar é considerada uma boa prática.

Aliás, mesmo se o TSE não tivesse querido contratar o CEPESC, isto teria sido difícil porque não há uma alternativa: existem no Brasil poucas pessoas ou organizações capazes de dar uma boa assessoria na área de criptografia.

Até onde sabemos, são infundadas as suspeitas de que tivesse havido interferência ou manipulação eleitoral do lado da ABIN através das funções de criptografia. O algoritmo proprietário para criptografia simétrica poderia ser substituído por um algoritmo público, como o AES, assim eliminando qualquer suspeita sobre o papel da ABIN.

O número de pessoas no Brasil com uma competência e conhecimento profundo na área de criptografia é muito pequeno. Sendo uma área estrategicamente importante, não somente do ponto de vista militar, como também cada vez mais dando apoio às tecnologias de informação, é importante que o governo brasileiro, através do MEC ou do CNPq, estimule o ensino e a pesquisa nesta área.

3.6 O sistema operacional na urna

Atualmente, um dos pontos mais controversos da urna é seu sistema operacional.

É óbvio que o sistema operacional é uma parte crucial para ser considerada na avaliação da segurança de um sistema computadorizado como a urna. O sistema operacional é responsável por capturar os sinais do teclado, detectando quando uma tecla foi pressionada, capturando o código da mesma e enviando este para o programa de aplicação.

Para um programador habilidoso que conheça o sistema operacional é relativamente fácil escrever um programa que captura cada tecla pressionada e copia seu valor para um arquivo secreto no computador (tais programas são conhecidos como *keyloggers* ou *keyboard sniffers*). Se for registrada a ordem em que cada eleitor votou (o que cada observador na seção eleitoral pode observar e registrar), poder-se-á deduzir o voto de cada eleitor, quebrando a confidencialidade do voto. Podemos inclusive pensar em ataques mais avançados: um programa que troca o código da tecla pressionada por um outro código poderia ocasionar que a urna mostrasse a foto de um candidato diferente daquele escolhido pelo eleitor. Assim, um possível ataque poderia ser mostrar a foto do candidato escolhido pelo eleitor, mas ter o voto contabilizado para um candidato diferente.

3.6.1 VirtuOS

Em 1996, o TSE especificou um sistema operacional multi-threaded, para poder executar tarefas simultaneamente: votar, monitorar hardware, digitar título do próximo eleitor. A escolha caiu sobre o sistema operacional VirtuOS produzido pela empresa brasileira Microbase. Este sistema operacional está sendo usado nos modelos 1996, 1998 e 2000 da urna, ainda em uso atualmente.

Durante uma das sessões de apresentação do código-fonte realizadas no TSE em agosto de 2002, nós tivemos a oportunidade de conversar com o diretor da Microbase, responsável técnico por este produto. Segundo o diretor, o contrato (de 1996) não prevê a possibilidade de terceiros inspecionar os códigos-fonte do VirtuOS. No entanto, o diretor entregou estes códigos como cortesia ao TSE. Ele se mostrou disposto a mostrar os códigos-fonte para nós; porém, por falta de tempo e dado o tamanho do código, isto não aconteceu.

3.6.2 WindowsCE

O modelo 2002 da urna usa o WindowsCE como sistema operacional. Até onde sabemos, esta não foi uma decisão do TSE, mas da UNISYS, a empresa que venceu o processo licitatório. A Microsoft proveu os códigos-fonte do WindowsCE, uma vez que este é montado para cada diferente plataforma de hardware.

O sistema operacional é uma das camadas mais internas de uma plataforma computacional e a falta de conhecimento e auditoria da mesma pode prejudicar a verificação dos programas da urna eletrônica. Acreditamos que este problema deve ser levado em consideração em futuras verificações do software da urna eletrônica.

Por outro lado, será que ter acesso a mais um programa de, digamos, 10000 linhas, aumenta a segurança da urna, visto a dificuldade de auditar a quantidade enorme de todos os programas da urna?

3.7 Conclusão

Como pode ser constatado, é muito difícil, senão impossível, dadas as condições atuais do sistema da urna eletrônica brasileira, concluir-se se a mesma é confiável ou não. Isso leva à necessidade de considerar a urna uma “caixa preta” e que desta forma, deve ser realizada a auditoria externa e paralela de suas operações. A impressão do voto é uma maneira simples de se conseguir este intento.

Capítulo 4

Considerações Finais

Este capítulo apresenta, na forma de itens, algumas das principais conclusões de nosso trabalho.

(1) A urna eletrônica é melhor do que um sistema com cédulas em papel. Estamos convencidos de que o sistema informatizado é muito melhor do que o sistema antigo com cédulas em papel. O projeto da urna é muito bem feito, merecendo admiração. O novo sistema apresenta o resultado das eleições em dias ou até em horas, em vez de semanas, dependendo da eleição. Os resultados do novo sistema automatizado são mais confiáveis do que os resultados obtidos manualmente. A interface da urna faz com que a opção de voto do eleitor não seja subjetiva, sujeita a uma interpretação de um funcionário. Isto eliminou uma grande classe de fraudes e dificultou fraudes mais simples, porém abriu portas para outros tipos de fraude.

(2) Até onde sabemos, a urna eletrônica é segura. Acompanhamos de perto as eleições do ano 2002 e estudamos detalhadamente o hardware e o software da urna. Não encontramos nada estranho, nenhum vestígio de fraude, nada suspeito.

Por outro lado, não podemos declarar que a urna é 100% segura. Embora tenhamos dedicado bastante tempo estudando o sistema eleitoral, não foi possível ver tudo. Mesmo se tivéssemos visto tudo, não seria possível declarar a urna segura, pelas razões explicadas no item (4).

(3) O projeto da urna não elimina a possibilidade de que a identidade do eleitor seja vinculada a seu voto.

Como foi explicado em 3.3, para registrar quem votou, o título do eleitor é digitado num equipamento que está eletronicamente ligado à urna. Já que o eleitor usa a urna para votar, uma mudança simples de software permitiria vincular a identidade do eleitor a seu voto, o que fere o sigilo do voto. Não foi encontrado qualquer vestígio desta vinculação ter sido implementada. No entanto, acreditamos que o registro de quem votou deva ser implementado de uma forma diferente.

(4) A transparência e a auditabilidade da urna deixam a desejar.

No inicio, a segurança da urna se baseou em técnicas clássicas, principalmente separando as funcionalidades dos subsistemas, e as responsabilidades dos funcionários envolvidos.

Para nós é obvio que ultimamente o TSE está mais aberto, que ele realmente quer convencer terceiros de que o sistema eleitoral brasileiro é seguro. Observe-se que o TSE tem esta obrigação para com os partidos políticos e a sociedade em geral. Infelizmente, achamos que os mecanismos oferecidos não são suficientemente convincentes.

Os principais mecanismos de auditoria à disposição dos partidos políticos são:

(a) sessões abertas, em que o TSE mostra seus programas, tanto os da urna, quanto os da totalização;

(b) um sistema de resumos criptográficos e assinaturas digitais, para demonstrar que os arquivos mostrados na sessão correspondem aos usados no dia de eleição;

(c) a impressão da zerésima (um relatório que mostra que todos os candidatos têm zero votos) da urna e do sistema de totalização no início da votação;

(d) a impressão do boletim da urna, quando esta for encerrada;

(e) a divulgação por CD de todos os dados (votos por candidato, etc.) de todas as urnas pelos TREs;

(f) a votação paralela[1];

(g) a impressão do voto.

Com exceção do último item (a impressão do voto), nenhum destes mecanismos vão convencer um cético uma vez que:

(a) (sessões abertas): Primeiro, a quantidade de software da urna é enorme–tão grande que é impossível estudar tudo durante uma semana. Segundo, o sistema operacional não foi mostrado. Infelizmente, como foi explicado em 3.6, ataques no nível de sistema operacional apresentam uma ameaça real. Terceiro, mesmo se tudo fosse mostrado, seria muito difícil excluir com certeza a possibilidade de que houvesse um programa malicioso escondido em algum lugar. Um pequeno arquivo de alguns kilobytes seria suficiente para quebrar a integridade da urna;

(b) (resumos criptográficos dos arquivos) Primeiro, como ter certeza de que o programa que calcula os resumos faz realmente o que foi especificado, em particular durante a verificação dos resumos na urna? Segundo, como foi mencionado em 3.5.2, o trabalho de verificação é lento e trabalhoso, e a amostragem é apenas uma fração mínima do total. Aliás, durante o segundo turno, os resumos publicados na página do TSE foram mudados, dificultando o trabalho dos partidos. Terceiro, mesmo que todos os arquivos fonte do ambiente de desenvolvimento sejam iguais aos mesmos da urna, como ter certeza que eles serão realmente executados no dia de eleição?

Ressaltamos que o que estamos colocando aqui são ataques hipotéticos que, ainda por cima, muitas vezes implicam a conivência de um ou vários funcionários da Justiça Eleitoral. Não estamos dizendo que estes ataques existem de verdade, ou que já foram realizados alguma vez. O que queremos dizer é que não existem mecanismos efetivos que permitam aos partidos políticos verificarem que a eleição ocorreu de uma maneira honesta. Existe uma zona cinza em que, no final das contas, todo partido político (e todo cidadão) precisa ter fé na Justiça Eleitoral e em seus funcionários. Apesar de termos toda confiança neles, temos a opinião de que a existência desta zona, em princípio, é errada.

(c), (d), (e) (zerésima e boletim da urna) A combinação de (c), (d) e (e) dá uma grande confiabilidade ao processo de totalização: os partidos políticos podem obter um grande número de boletins da urna. Além disso, os partidos podem verificar que os dados, tal como divulgados pelo TRE, correspondem aos dados em todos os boletins obtidos, e que os totais foram calculados de forma certa. Obviamente, cada diferença seria uma indicação de um problema grave. Na prática, esta parte já funciona razoavelmente bem. Contudo, propusemos em 3.5.5 uma mudança simples que facilitará muito o trabalho de fiscalização pelos partidos;

(f) (votação paralela): A votação paralela perde um pouco em credibilidade, porque o sorteio acontece no dia anterior ao da eleição. Teoricamente, pessoas maliciosas podem esperar até sábado de manhã antes de começar a adulterar a urna. Porém, confiscar uma urna e executar uma votação paralela no dia de eleição é logisticamente muito difícil em estados muito grandes. Os ataques em que a urna sabe distinguir entre uma votação de verdade e uma simulação, como explicado em [14], não são nossa primeira preocupação.

(5) A impressão do voto aumenta muito a transparência e auditabilidade.

Em princípio, a impressão do voto é um mecanismo que dá muita confiabilidade e transparência ao sistema eleitoral, por ser um mecanismo que registra a vontade do eleitor, usando uma tecnologia simples, diferente e independente da tecnologia usada na urna. Com a impressão do voto, a urna ganha uma nova propriedade: ela torna-se auditável, porque há possibilidade de recontagem. Acreditamos que a possibilidade de

[1] Um dia antes da eleição, em todos os Estados, duas urnas são sorteadas, lacradas e transportadas ao TRE. No dia da eleição, numa sessão aberta e gravada por vídeo, simula-se uma votação nelas em que todos os votos são escolhidos pelos fiscais e testemunhas e são abertos. Depois, confere-se o resultado emitido pela urna, que deve corresponder à contagem manual.

recontagem seja uma propriedade de suma importância, porque elimina completamente os problemas mencionados em (a) e (b): com a impressão dos votos não é mais necessário verificar a corretude dos programas fonte, e verificar se os programas fonte mostrados na sessão do TSE são iguais aos na urna.

De todas as técnicas conhecidas por nós, a impressão do voto é a forma mais fácil de implementar a propriedade de recontagem. Se a impressão for abolida, outros mecanismos devem ser estudados.

O futuro da urna brasileira

É importante que a sociedade brasileira inicie uma discussão sobre o futuro do sistema informatizado de eleições. Algumas preocupações e requisitos que serão desejáveis no futuro são: separação do sistema de criação da cédula do sistema de apuração; cédula impressa mais legível; contagem usando equipamentos leitores capazes de fazer reconhecimento ótico de caracteres; padronização do formato da impressão; utilização de equipamentos com código e tecnologia abertos.

Recomenda-se à SBC a organização de um workshop sobre tecnologia eleitoral e a urna. Isso permitirá uma total isenção e transparência para abordar o problema sob uma ótica adequada.

Referências Bibliográficas

[1] Rosa Maria Oliveira Pedro Antunes Américo Monteiro, Natércia Soares. Sistemas Electônicos de Votação. Technical Report TR-01-9, Departamento de Informática, Universidade de Lisboa, Outubro 2001. http://www.di.fc.ul.pt/biblioteca/tech-reports/01-9.pdf.

[2] Brunazo. Comunicação pessoal, 2002.

[3] CALTECH-MIT. Voting – What is, What could be, the CALTECH-MIT Voting Technology Project, 2001. http://www.vote.caltech.edu.

[4] Paulo César Bhering Camarão. *O Voto Informatizado: Legitimidade Democrática*. Empresa das Artes, 1997.

[5] David Chaum. Secret-Ballot Receipts and Transparent Integrity, 2001. http://www.vreceipt.com/article.pdf.

[6] David Chaum. A survey of current ballot systems, 2001. http://www.vote.caltech.edu/wote01/pdfs/survey.pdf.

[7] Augusto Jun Devegili. Farnel: Uma proposta de protocolo criptográfico para votação digital. Master's thesis, Curso de Pós-Graduação em Ciência da Computação da Universidade Federal de Santa Catarina, 2001.

[8] C. L. Tozzi et al. Avaliação do Sistema Informatizado de Eleições (Urna Eletrônica). Technical report, Unicamp, 2002.

[9] Rebecca Mercuri. *Electronic Vote Tabulation – Checks & Balances*. PhD thesis, School of Engineering and Applied Science of the University of Pennsylvania, Philadelphia, PA, October 2000.

[10] Débora Cabral Nazareno. Uma Análise da Segurança da Urna eletrônica e do Sistema Eleitoral Brasileiro. Master's thesis, Curso de Pós-Graduação em Ciência da Computação da Universidade Federal de Santa Catarina, 2003.

[11] NIST. The Common Criteria, 2003. http://csrc.nist.gov/cc.

[12] Schneier and Kelsey. Secure Audit Logs to Support Computer Forensics. *ACMTISS: ACM Transactions on Information and System Security*, 2, 1999.

[13] SEI. *The Capability Maturity Model: Guidelines for Improving the Software Process*. Addison Wesley, 1995.

[14] Jorge Stolfi. [sbc-l] (no subject). Email à lista da SBC. 21/10/2002.

[15] P. P. Swire. What should be hidden and Open in Computer Securty: Lessons from deception, the Art of War, Law and Economic Theory. Draft version, 2001.

[16] Jeroen van de Graaf and W. S. Caldas. Melhorando a segurança e a transparência da urna eletrônica. In *Terceiro simpósio sobre segurança em informática*, pages 221–230, São José dos Campos (SP), 24 a 26 de outubro 2001.

Apêndice A

São Gabriel de Cachoeira

A estória de São Gabriel de Cachoeira começou numa conversa informal e inocente entre Custódio e eu. "Gostaria de saber quantas urnas são transportadas num barco para chegar no local de eleição." Era quinta-feira a noite num quarto de hotel em Brasília, e um pouco cansando de quatro dias de trabalhos no TSE, surgiu a interesse para outros aspectos do fascinante processo eleitoral do Brasil, neste caso o aspecto de logística e transporte. "No máximo 50," respondeu o Custódio. "Tá louco? O norte de Brasil é só água!" eu rebati.

Na tarde do dia seguinte, relatei (Custódio já tinha saído) a nossa conversa ao Osvaldo Catsumi Imamura, dizendo que tinha "apostado um almoço" com Custódio sobre o assunto. Catsumi estava mais do que disposto para me ajudar, e me mostrou o relatório *Seções rurais do Estado do Amazonas (2000)* do TRE-AM, contendo uma descrição por município de como a urna chega na sua destinação. Pode-se ler que a urna é transportada por qualquer meio de transporte imaginável, inclusive voadeira, carro, barco, trator, pick-up, helicóptero, moto, avião, lancha, expresso, caminhada, motor e rabeta. Também lê-se que, segundo este relatório, somente no Amazonas mais do que 600 urnas são transportadas num barco (há 699 seções, das quais 86 não mencionam um tipo de barco). Ou seja, ganhei a minha "aposta".

O município de São Gabriel de Cachoeira chamou minha atenção porque o relatório disse o seguinte sobre o transporte: "bandeirantes: 1h; helicóptero: 2h45; voadeira: 36h." Mostrei isso aos outros presentes e, sempre dispostos a combinar o trabalho com lazer, já começamos a imaginar um comitê multi-partidário para acompanhar as eleições lá (despesas pagas, claro). No início achei que Bandeirantes era um carro 4x4 (Toyota), só depois minha mulher me contou que é um avião.

A cidade virou um destaque, um exemplo. Contra as minhas expectativas, ela constava no mapa do Brasil na minha sala. Sem saber, escolhi um dos maiores e mais remotos municípios do Brasil: fica no canto norte-oeste do Brasil, beirando a Colômbia e Venezuela. Com 109669 quilômetros quadrados[1] é aproximadamente duas vezes e meio o tamanho do Estado de Rio de Janeiro (ou da Holanda ...), tem 30 mil habitantes, e há lugares com menos de dez eleitores[2]. E por acaso encontrei uma noticia no site da Folha de São Paulo sobre São Gabriel de Cachoeira[3]:

> **Satélite será usado para apurar votos em regiões isoladas**
> *da AGÊNCIA FOLHA, em Manaus, 26/09/2002*
> *Eleitores de comunidades ribeirinhas e aldeias indígenas da Amazônia terão os votos apurados este ano por um sistema de telefonia móvel digital via satélite.*
> *A tecnologia será utilizada em regiões rurais de difícil acesso dos Estados do Amazonas, Amapá, Acre, Maranhão, Rondônia, Roraima, Mato Grosso e Mato Grosso do Sul depois que o TSE (Tribunal Superior Eleitoral) fez um contrato com a empresa Globalstar do Brasil, responsável pelo sistema.*
> *No Amazonas 7% dos votos dos 1,5 milhão de eleitores serão apurados com a nova tecnologia, que vai agilizar a apuração de localidades como Cucuí, onde a população é formada por índios, ribeirinhos e militares, no município de São Gabriel da Cachoeira 858 km a oeste de Manaus.*
> *Os eleitores de Cucuí já votam na urna eletrônica desde 2000, mas os votos só foram apurados pelo TRE (Tribunal Regional Eleitoral) do Amazonas depois que os técnicos viajaram de helicóptero para levar o disquete ao local de apuração, em Manaus. A operação durou cerca de dois dias.*
> *Agora os eleitores de Cucuí irão as seções eleitorais localizadas em barcos para votar na urna eletrônica. Ao fim da votação, o disquete contendo a totalização dos votos será inserido num computador portátil.*
> *Técnicos da Universidade do Amazonas operarão o sistema. O computador é conectado ao telefone móvel digital, que envia os dados em até 5 minutos para o TRE. "Somos um país de terceiro mundo utilizando em*

[1] http://servidor.ipaam.br/amazonas/municipios.htm
[2] http://www.tre-am.gov.br/munic/municip1.htm
[3] http://www.uol.com.br/folha/brasil/ult96u38538.shtml

uma eleição desse porte uma tecnologia disponível de maneira racional, econômica e com uma apuração quase imediata", disse Danna Valente, assessora do TRE.

Contei e escrevi este texto para ilustrar as dificuldades logísticas do processo eleitoral do Brasil.

Somente uma semana depois do primeiro turno, quando visitei o TSE para a sessão de software, fiquei sabendo do desastre: no dia 4 de outubro o avião com três alunos da Universidade de Manaus contratados pelo TRE para operar os equipamentos, tinha caído logo depois da decolagem do aeroporto de São Gabriel de Cachoeira. Ninguém sobreviveu ao acidente. Os nomes dos estagiários são: José Gorgonha de Miranda, Túlio Yuchi Sakamoto e Fagner Oliveira da Costa. O piloto, Comandante Celso Reinaldo Salmozzo, morreu também.

O que tinha começado com uma conversa engraçada, acabou em tristeza.

[JvdG]

Apêndice B

Pedido de Auditoria da Subcomissão do Voto Eletrônico do Senado

Seminário do Voto Eletrônico
Subcomissão do Voto Eletrônico - SVE
CCJ do Senado Federal
- maio de 2001 -
Pedido de Auditoria EXTERNA sobre o Sistema Eleitoral Informatizado (SEI) do TSE

Objetivo: Analisar e avaliar a Segurança e a Confiabilidade o Sistema Eleitoral Informatizado do TSE (SEI) com o objetivo de DETECTAR E APONTAR EVENTUAIS FALHAS DE SEGURANÇA que possam por em risco a certeza de INTEGRIDADE e INVIOLABILIDADE do voto.

As falhas de segurança apontadas nesta auditoria servirão para orientar a elaboração de um posterior relatório de sugestões de melhorias e correções do SEI ser enviado do Senado para o TSE e também para a elaboração de projetos de lei a serem apresentados.

Comunicação ao TSE: Os ministros do TSE deverão ser comunicados deste pedido de auditoria pois seu apoio e colaboração é essencial para permitir o acesso irrestrito dos auditores os dados necessários e para levar a auditoria a bom termo.

Auditores: A Universidade de Campinas, UNICAMP, deverá ser chamada a efetuar esta auditoria.

Obs.: *Em contato preliminar de sondagem com o Prof. Dr. Hermano Tavares, Reitor da UNICAMP, e com o Prof. Dr. Álvaro Crósta, Chefe de Gabinete Adjunto da Reitoria da UNICAMP e coordenador da equipe da UNICAMP que fez a auditoria no Painel do Senado, houve a aceitação prévia desta incumbência, devendo, no entanto, as condições específicas desta auditoria serem acertadas em contatos formais.*

Assistentes Técnicos: A SVE poderá nomear Assistentes Técnicos para acompanharem o levantamento de dados em campo, durante a auditoria, e para elaborarem novos quesitos específicos aos dados levantados.

Prazo: O prazo para a apresentação do relatório final desta auditoria proposta deverá ser definido pela SVE e ser informado à equipe da UNICAMP durante o acordo inicial. Não está prevista a apresentação de relatórios preliminares.

Escopo:

A avaliação da Segurança do SEI deve abranger o Subsistema de Votação e Apuração (urna eletrônica) bem como o Subsistema de Totalização dos Votos na rede do TSE.

Devem ser analisados OS PROCEDIMENTOS DE PRODUÇÃO de todos programas (software) utilizados no SEI, mais a GUARDA, IMPLANTAÇÃO E OPERAÇÃO dos mesmos até a divulgação de resultados oficiais.

A existência de equipamentos e *chips* padronizados ou proprietários que tenham programas gravados em *firmware* também deve ser apontada e analisada.

A avaliação deve abranger também os procedimentos de FISCALIZAÇÃO EXTERNA, que foram realizados NA PRÁTICA pelos partidos políticos, para se determinar a EFETIVIDADE desta fiscalização.

Não é necessário que se aprofunde a auditoria até a análise e interpretação de códigos-fonte ou compilados dos programas do SEI, a não ser que os próprios auditores concluam que tal análise seja importante para embasar suas conclusões.

Se, durante a análise da segurança do SEI, se detectar a necessidade, o escopo desta auditoria poderá ser estendido para cobrir também o projeto e construção de equipamentos (hardware).

Ponto de vista:

Toda a análise de segurança do SEI deve ser feita a partir do ponto de vista do eleitor, por ser este o real detentor do direito de inviolabilidade e a justa apuração (integridade) do seu voto.

Assim, todos os quesitos se referem a segurança do eleitor em primeiro lugar. A segurança do ponto de vista da Justiça Eleitoral, dos Partidos Políticos e dos candidatos são desejáveis, mas são acessórias.

Foco:

Toda a análise deve ter seu foco principal voltado para DETECÇÃO DE FALHAS DE SEGURANÇA contra ataques externos e principalmente INTERNOS, que possam permitir violação ou desvio de votos, e para a DETERMINAÇÃO DA EFICÁCIA DA FISCALIZAÇÃO EXTERNA.

Obs.: por ataque interno, se entende aquele efetuado por ou com a ajuda de pessoas diretamente ligados à Justiça Eleitoral ou a seus fornecedores de serviços ou mão-de-obra.

Todos pontos do SEI cuja segurança depender da confiabilidade, disciplina e integridade de pessoas envolvidas, como projetistas, operadores e técnicos de manutenção, devem ser apontados e avaliados quanto ao RISCO DE VIOLAÇÃO POR DESONESTIDADE das pessoas responsáveis.

Todos os procedimentos relativos a criptografia e assinatura digital devem ser avaliados na sua adequabilidade ao processo e aplicação correta.

Ainda que o foco da auditoria esteja centrado na detecção de falhas de segurança e avaliação da fiscalização, se forem encontradas fraudes ou indícios de fraudes, estas também deverão ser apontadas e descritas.

Norma Técnica:

Os princípios propostos na Norma Técnica Internacional ISO/IEC 15.408 de Dez/99, que estabelece Critérios de Avaliação da Segurança no âmbito da Tecnologia de Informação, também chamada de *Common Criteria*, devem ser utilizados como modelos orientativos para a auditoria do SEI, inclusive deve ser apontado que cuidados foram tomados dentro do SEI que atendam aos requisitos desta norma.

Quesitos Principais:

1) Qual o nível de segurança e as falhas de segurança que tem o Sistema Eleitoral Informatizado do TSE contra ataques por agentes externos que visem violar ou desviar votos tanto na apuração dos votos (na urna eletrônica) quanto na rede de totalização?

2) Qual o nível de segurança e as falhas de segurança que tem o Sistema Eleitoral Informatizado do TSE contra ataques por agentes internos desonestos que visem violar ou desviar votos tanto na apuração dos votos quanto na rede de totalização?

3) O controle e a fiscalização externa permitida e efetivamente praticada pelos fiscais dos partidos políticos, durante o processo de produção, guarda, implantação e operação do SEI, é suficiente para detectar ou garantir a inexistência de fraudes de violação ou desvio de votos?

Quesitos Complementares:

4) O controle e a fiscalização externa permitida e efetivamente praticada pelos fiscais dos partidos políticos durante o processo de produção (escrita e compilação) e implantação (inseminação) dos programas da urna eletrônica, é suficiente para garantir a inexistência de eventuais vícios implantados por agentes internos desonestos agindo em conluio?

5) O prazo de cinco dias concedido aos partidos para conhecerem e avaliarem o sistema, sem ferramentas profissionais de análise e "debug", é suficiente para uma avaliação completa e eficaz? Os testes permitidos aos fiscais, nas urnas carregadas, são eficazes para detecção de eventuais programas fraudulentos?

6) De que forma podem os candidatos ou partidos políticos efetuarem a recontagem dos votos ou conferência da apuração no caso de suspeita de fraude ou falhas nos programas da urna eletrônica?

7) No ano de 2000, os programas usados nas urnas eletrônicas foram modificados depois de mostrados aos fiscais dos partidos? Se sim, qual a natureza e motivo destas modificações e que procedimentos foram adotados para apresentar as alterações aos fiscais?

8) A existência de programas de criptografia FECHADA, feitos por um órgão ligado ao poder executivo, tanto nas máquinas de apuração (urnas eletrônicas) quanto na rede totalização é imprescindível para garantir a INTEGRIDADE dos dados transmitidos das urnas para a rede ou poderiam ser substituídos por outros métodos transparentes e PROGRAMAS ABERTOS que, cumprindo a mesma função de garantir a integridade dos dados, pudessem ser apresentados para a fiscalização dos partidos?

9) O ambiente de compilação dos programas do SEI é seguro contra invasão e ataques internos? É possível adulterar o ambiente de compilação de forma a introduzir vícios mesmo nos programas-fontes corretos? Que procedimentos foram tomados para dar garantia da integridade às bibliotecas padrão dos compiladores?

10) O Art. 66 da Lei Eleitoral 9.504/97 aborda a questão da apresentação dos programas do SEI aos fiscais dos partidos políticos concedendo-lhes amplo direito a fiscalização. A Portaria 142/00 e a Resolução 20.714/00, ambas do TSE, abordam a mesma questão limitando, porém, o direito prescrito em lei. O Art. 66 da Lei 9.504/97 foi integralmente respeitado pelo TSE?,

11) A Portaria 142/00 e a Resolução 20.714/00 do TSE foram contestadas em processo jurídico por desrespeitarem o Art. 66 da Lei Eleitoral 9.504/97. Qual a solução jurídica dada pelo TSE no julgamento do mérito desta questão?

12) A segurança física dos equipamentos eleitorais é efetiva? É feito um controle sistemático para detectar e avaliar os casos de acesso indevido ao equipamento eleitoral? Podem ter ocorrido casos de acesso indevido ao equipamento eleitoral que não foram detectados pelo TSE? Quantos casos foram detectados analisados pelo TSE? Houve roubo ou desvio temporário de urnas, flash-cards, etc.? Quantos foram detectados?

13) Foi feito algum Teste de Penetração, como recomenda a norma ISO 15.408, por especialistas externos contratados para este fim, para se avaliar a resistência do SEI (Urnas Eletrônicas e Rede de Totalização) a ataques externos?

Quesitos Complementares Adicionais:

Os Assistentes Técnicos do Senado, nomeados para acompanharem o levantamento de dados pela equipe de auditores, poderão elaborar novos quesitos específicos aos dados levantados.

Apêndice C

Termos de compromisso de sigilo

TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO (Público)

Eu, — , portador do documento de identidade no. —, expedido em —, comprometo-me a guardar sigilo acerca de tudo a que tiver acesso ou de que tiver conhecimento, por ocasião da "Análise e Lacre dos Programas a serem utilizados no 2o turno das Eleições de 2002", no Tribunal Superior Eleitoral, facultada pelo art. 66 da Lei no 9.504, de 30.9.97, com a redação dada pelo art. 3o da Lei 10.408, de 10.1.02, submetendo-me ás penalidade e demais conseqüências previstas na legislação, em especial o disposto nos arts 153, 154, 325 e 327 do Dec. -Lei no 2.848, de 7.12.40 (Código Penal Brasileiro), no art. 207 do Dec. -Lei no 3.689, de 3.10.41 (Código de Processo Penal), nos arts. 13 e 14 da Lei no 7.170, de 14.12.83 (Lei de Segurança Nacional), nos arts. 1o, 2o, 3o, 4o, e 5o da Lei no 8.027, de 12.4.90 (Normas de Conduta dos Servidores Públicos Civis), nos arts. 116, 117 e 132 da Lei no 8.112, de 11.12.90 (Regime Jurídico Único); no Decreto no 1.171, de 22.6.94 (Código de Ética Profissional do Servidor Público Civil do Poder Executivo); nos arts. 4o, 6o, 23 e 25 de Lei no 8.159, de 8.1.91 (Lei dos Arquivos), no Decreto no 2.134, de 27.1.97 (Documentos Públicos Sigilosos) e no Decreto no 2.910, de 29.12.98 (Normas para Salvaguarda de Documentos, Materiais, Comunicações e Sistemas).

E como assim me comprometo, sob as penas da lei, assino o presente Termo de Compromisso, em presença das testemunhas abaixo nomeadas.

Brasília - DF, 11 de Outubro de 2002

Assinatura

Testemunhas:

Nome: RG: