Auditoria Especial no Sistema Eleitoral 2014

Amílcar B. Filho[1], Marco A. M. Carvalho[1], Márcio C. Teixeira[1], Marcos A. Simplicio Jr.[2], Clovis T. Fernandes[1,3],

[1] CMIND - Comitê Multidisciplinar Independente
[2] EPUSP - Escola Politécnica da Universidade de São Paulo
[3] ITA - Instituto Tecnológico de Aeronáutica;

amilcar@brunazo.eng.br, marcocarvalho@sosdados.com.br,
marcio@teixeira.in, mjunior@larc.usp.br, clovistf@uol.com.br

Abstract. *This work is an extract of the technical report for the Brazilian Election System Special Auditing 2014, authorized by the election authority (TSE) in November/2014 after request by a political party. The conclusions were: a) the Brazilian Electronic Election System does not allow an effective auditing of the results it produces; b) the vote collection and counting processes done with the electronic voting machine could not have its reliability ascertained due to severe restrictions imposed by the election authority; c) regarding the transmission and totalization processes, we found no critical issue indicating that its reliability was compromised.*

Resumo. *Este trabalho é um extrato do relatório técnico resultante da Auditoria Especial no Sistema Eleitoral de 2014, autorizado pelo TSE em novembro/2014 atendendo solicitação de um partido político. As conclusões foram: a) o Sistema Eleitoral Informatizado Brasileiro não permite auditoria independente efetiva do resultado produzido; b) a etapa de votação e apuração dos votos feitos nas urnas eletrônicas não pode ter sua confiabilidade determinada devido às severas restrições impostas pela autoridade eleitoral; c) na etapa de transmissão e totalização dos votos, não foram encontrados problemas graves que indicassem comprometimento da sua confiabilidade.*

1. Introdução

Devido a um elevado número de dúvidas e de denúncias de fraude ao final do 2° turno da eleição presidencial de 2014 no Brasil, o partido político derrotado solicitou permissão ao Tribunal Superior Eleitoral (TSE) para auditar o sistema de votação eletrônico utilizado. O pedido foi submetido à Procuradoria Geral Eleitoral (PGE), que se manifestou pelo indeferimento, e também à Secretaria de Tecnologia de Informação (STI) do TSE, que emitiu parecer no sentido de atender o pedido dentro de limitações e restrições contidas nas Resoluções TSE 23.397/2013 e 23.399/2013. Em novembro de 2014, o TSE aprovou o pedido, impondo as limitações inscritas da Res. 23.397/13, como sugerido pela STI, sendo que desdobramentos de natureza burocrática (e.g., assinatura de acordos de não-divulgação) adiaram o início efetivo dos trabalhos da auditoria para janeiro de 2015.

O presente trabalho apresenta a coleção das dúvidas que levaram o Partido à iniciativa de solicitar a auditoria e o plano de trabalho idealizado para o início e andamento da auditoria. Em seguida, são descritas as condições fortemente restritivas que os auditores enfrentaram no desenvolvimento de seus trabalhos, a análise conjunta de todas as informações coletadas, e as conclusões resultantes.

2. Dúvidas iniciais que auditoria visava esclarecer

Após as eleições, houve duas denúncias de caráter geral com alguma consistência ou evidência aparente (antes de uma auditoria específica), que chegaram à coordenação do partido. A primeira referia-se ao *desvio de votos nas urnas*: o modelo das urnas brasileiras (DRE - dependente do software) permitiria inserir software malicioso para desviar votos durante seu registro ou apuração; esta denúncia era agravada por testes de penetração bem sucedidos [Hursti 2006, Feldman et al. 2007], no exterior, em modelos do mesmo fabricante das urnas brasileiras. Já a segunda era o *desvio de votos na transmissão e na totalização dos votos*: a percepção de fraude foi agravada por ter se tornado público que um grupo pequeno de pessoas sob coordenação da STI/TSE teve acesso em ambiente fechado aos dados parciais da totalização antes da divulgação oficial, às 20h.

Houve também diversas denúncias mais específicas, cuja procedência a auditoria visava avaliar, as quais abordavam o seguinte: (a) Geração de Mídias: computadores que geravam as mídias de carga das urnas tinham conexão ativa com a Internet; (b) Smartmatic: funcionários da empresa, estrangeira, tiveram acesso à transmissão dos resultados e teriam fraudado a totalização; (c) Eleitor "já votou": eleitor não pôde votar porque alguém já tinha votado em seu nome (inclusive em seções com urnas biométricas); (d) Eleitor "justificado": eleitor que justificou sua ausência constatou que alguém votou em seu lugar; (e) Fraude do Mesário: mesários inseriam votos nas urnas no final do dia; (f) Urna votava "sozinha" (com vídeo ilustrando); (g) Documentos da seção eleitoral jogados no lixo (com vídeo ilustrando); (h) Uma zerésima tinha 400 votos para a candidata Dilma Roussef; (i) Urna registrava 44 quando se tentava digitar 45 (com video ilustrando).

3. O plano de trabalho

Por ser um sistema eminentemente dependente do software [Rivest and Wack 2006] a auditoria dos votos registrados nas urnas eletrônicas teria que ser feita indiretamente, por meio da validação dos códigos fonte e compilados, e pela certificação da carga do software nas mais de 420 mil urnas utilizadas no dia da eleição. Por outro lado, a existência do Boletim de Urna (BU) impresso nas urnas, que poderia ser coletado pelos Partidos no dia da eleição, permite uma auditoria contábil direta (por amostragem) da segunda etapa do processo eleitoral, que é a transmissão e a totalização dos resultados.

O plano de trabalho inicial (PTI) consistia nas seguintes etapas gerais: (1) Coleta Inicial de Dados: coleta de dados digitais e físicos gerados pelo sistema (como arquivos de log, BUs, tabelas de correspondências e Registros Digitais do Voto – RDVs), para verificação da coerência interna entre eles; (2) Auditoria da Apuração nas Urnas: em qualquer sistema dependente do software, tal atividade consiste na validação e na certificação do software usado; (3) Auditoria da Transmissão e da Totalização: proceder uma auditoria contábil dos Boletins de Urna produzidos pelas urnas e totalizados; (4) Demais denúncias específicas e localizadas: procurar evidências das demais denúncias nos TRE e nos Cartórios, bem como analisar os procedimentos de segurança do sistema. Este plano inicial poderia ser detalhado ou complementado conforme o desenvolvimento das atividades previstas indicasse a eventual necessidade.

4. Restrições encontradas durante o processo de auditoria

Os auditores enfrentaram obstáculos de natureza administrativa que dificultaram seus trabalhos a ponto de comprometer o resultado obtido. Muitas atividades do plano de trabalho

inicial, em especial a validação e certificação do software das urnas, não puderam ser desenvolvidas regularmente por impedimentos impostos pelos administradores do processo sob auditoria, como se resume a seguir.

4.1. As resoluções do TSE impostas ao processo de auditoria

O TSE decidiu impor suas Resoluções TSE 23.397 e 23.399, de 2013 como normas regulamentadores da auditoria. Entretanto, tais resoluções abordam basicamente procedimentos de avaliação que ocorrem *antes e durante* a eleição. Logo, não preveem qualquer atividade condizente com as técnicas comuns de uma auditoria forense sobre o desempenho das urnas eletrônicas, como, por exemplo, recontagem dos votos realmente vistos pelo eleitor, verificação direta e sem restrições do conteúdo da memória dos equipamentos, testes de funcionamento em condições controladas, etc.

Com isso, criaram-se fortes obstáculos: afinal, vários procedimentos de auditoria não foram permitidos pela autoridade eleitoral com o argumento simples de que não estavam previstos na normatização que eles próprios, os auditados, haviam criado.

4.2. A organização administrativa e o controle do processo pelo auditado

A auditoria foi tratada e desenvolvida nos mesmos moldes de um processo jurídico, que leva a um forte formalismo burocrático. Isto provocou lentidão, em especial pela exigência de trâmites complexos (e.g., submissão formal, por escrito, de qualquer pergunta sobre o sistema) no lugar de soluções expeditas de entraves. Por outro lado, na prática, os procedimentos da auditoria eram decididos e comandados unilateralmente pelo auditados, o que é incongruente com qualquer dos três dos tipos de auditoria de sistemas de informação reconhecidos e padronizados [Beveridge 2015]: (a) avaliação simples (*review*); (b) auditoria profunda (*examination*); e (c) auditoria de procedimentos acordados (*agreed-upon procedures engagement*).

5. Análise dos dados disponibilizados

5.1. Coleta de dados — item (1) do PTI

O TSE demorou dois meses para entregar os dados digitais solicitados inicialmente. O volume dos dados entregues, referentes a todas as urnas do Brasil, era de 360 GB, incluindo mais de 2,1 milhões de arquivos de dados (BU, RDV, logs, etc.) e mais de 2 bilhões de registros de log a serem processados e analisados. A coleta de dados das urnas não foi permitida por cópia direta do conteúdo das suas mídias, mas sim indiretamente, usando os programas RED (recuperador de dados) e VPP (verificador pré e pós eleição) das próprias urnas, que geraram novas mídias com os arquivos de log, BU e RDV. O impedimento de se obter os dados pela leitura direta das mídias de memória das urnas criou uma grave lacuna na auditoria, afastando-a em termos de qualidade e de confiabilidade de uma auditoria forense: afinal, como os dados fornecidos são gerados pelo próprio software que se deseja auditar, sua confiabilidade para tal fim fica totalmente comprometida.

In loco, foram coletados dados de 684 urnas de 18 Estados, a saber: Acre, Alagoas, Amazonas, Bahia, Ceará, Distrito Federal, Goias, Maranhão, Minas Gerais, Paraíba, Pará, Paraná, Pernambuco, Piauí, Rio de Janeiro, Rio Grande do Norte, São Paulo. A quantidade de equipamentos passíveis de auditoria (mais de 420 mil) e sua dispersão geográfica criaram obstáculos de natureza econômica e logística à auditoria. Porém,

entende-se que o impedimento de acesso direto às mídias de memória foi um grave obstáculo adicional, artificialmente introduzido pela autoridade eleitoral.

5.2. Auditoria da apuração, via software — item (2) do PTI

A autoridade eleitoral determinou que o software eleitoral seria analisado durante 10 dias úteis, nas dependências do TSE, usando os arquivos extraídos do DVD oficial lacrado antes da eleição. Foi rejeitada pelo TSE a participação de duas pessoas na equipe de auditores, alegando que sua presença atentaria contra a soberania nacional: o analista de segurança Rodrigo Branco (engenheiro pelo ITA, *Principal Security Researcher* na Intel Corporation) e o prof. Alex Halderman (Professor Associado em Ciência da Computação na University of Michigan e diretor do *Center for Computer Security and Society*). Sendo ambos especialistas em segurança com experiência em hardware de sistemas de votação, esta recusa acabou por prejudicar eventuais trabalhos da auditoria nessa frente.

Para auditar a apuração por validação do software, o PTI previa doze tarefas. Porém, os resultados foram fortemente prejudicados por restrições impostas aos trabalhos: dez das tarefas previstas no PTI não puderam ser concluídas a contento e as restantes (avaliação dos lacres e da Votação Paralela) revelaram impropriedades, conforme segue.

5.2.1. Quantidade de votos gravados

Foram solicitados os arquivos de BU, RDV, log e de eleitores aptos e faltosos para se verificar a consistência dos totais de votos válidos em cada arquivo. No entanto, a autoridade eleitoral recusou-se a fornecer os arquivos de eleitores faltosos.

A comparação dos totais de votos computados registrados nos demais arquivos não constatou incoerências significativas, mas considera-se incompleta essa etapa da auditoria do software das urnas, por não ter sido permitido comparar os dados de todos os arquivos disponíveis, mas apenas dos arquivos escolhidos pelos auditados.

5.2.2. Requisitos de segurança, salvaguardas e normas técnicas

Para a surpresa dos auditores, a autoridade eleitoral alegou "questões de sigilo" e recusou-se a fornecer uma descrição formal e completa dos requisitos de segurança e as normas técnicas adotadas no projeto do sistema eleitoral. Considera-se que o argumento usado para tal recusa é infundado e até absurdo, contrariando princípios básicos de segurança [Kerckhoffs 1883] e a alegação do TSE de total transparência no processo eleitoral.

Consequentemente, não foi possível afastar as hipóteses de que, de fato: (1) a autoridade eleitoral não possui uma relação formal de requisitos de segurança no projeto das urnas eletrônicas; e (2) o sistema eleitoral eletrônico brasileiro não está em conformidade com qualquer norma técnica reconhecida de projeto voltado a segurança.

5.2.3. Certificação digital

O TSE optou por criar sua própria autoridade certificadora, que não passa por qualquer auditoria externa ou pela certificação oficial da ICP-Brasil. Sendo assim, o certificado raiz,

bem como todos os demais certificados utilizados no processo eleitoral, são gerados pelo próprio TSE, de modo que: (1) não existe qualquer certificado de um terceiro confiável que possa ser utilizado para validar todos os certificados da certificadora do TSE; (2) ninguém externo ao grupo dos executores das eleições é capaz de certificar se houve alguma fraude ou problema com algum certificado utilizado nas eleições; (3) o certificado raiz não é público para ser conferido ou usado na conferência das demais assinaturas digitais; (4) o carimbo de tempo de uma assinatura (e.g., do software oficial) não pode ser verificado de forma confiável por agentes externos. Também seria de vital importância que as assinaturas digitais pudessem ser verificadas em equipamentos de confiança dos auditores, pois a princípio não se pode aceitar como confiável um equipamento sobre o qual não tenha controle. Porém, a autoridade eleitoral só permite que verificações de assinaturas sejam feitas com o uso dos seus próprios computadores e urnas eletrônicas previamente configurados.

Conclui-se que a certificação digital, no processo eleitoral informatizado, não se apresenta em conformidade com o padrão oficial ICP-Brasil, tendo sido utilizado como uma caixa preta pelos fiscais e auditores, comprometendo fortemente a confiabilidade do processo de verificação das assinaturas digitais utilizadas.

5.2.4. Metodologia e documentação do software

O software do sistema eleitoral é de grande porte (mais de 50 mil arquivos e 17 milhões de linhas de código fonte) e deve ser considerado de missão crítica. Esperava-se, portanto, que o mesmo possuísse uma documentação completa e de qualidade. Entretanto, não foi o que se observou durante a auditoria: a documentação do software disponibilizada para análise mostrou-se bastante incompleta, muitas vezes inconsistente com a correspondente parte do código-fonte, o que dificultou sua validação. A análise realizada mostra a ausência (ou, ao menos, uma adoção insuficiente) de boas práticas em Engenharia de Software voltadas a projetos de grande porte e de missão crítica.

Para justificar tal lacuna, o TSE alegou a adoção de uma metodologia ágil no desenvolvimento do sistema, o que teria resultado em reduzida documentação. Entretanto, como métodos ágeis não são os mais apropriados para criar software ao mesmo tempo de missão crítica e de grande porte [Sommerville 2011, Stober and Hansmann 2010, SAPM 2014], pode-se afirmar que a própria abordagem de desenvolvimento constitui um ponto falho do sistema eleitoral brasileiro. Cabe notar que fragilidade semelhante na metodologia e na documentação do software eleitoral foi descrita no Relatório COPPE-UFRJ [Rocha et al. 2002], sugerindo que o problema persiste desde então.

5.2.5. Análise do código fonte

O DVD oficial lacrado com códigos fonte e compilados do sistema eleitoral não continha a biblioteca de segurança desenvolvida pela ABIN, nem o firmware do BIOS e do circuito de segurança MSD (*Master Secure Device*) desenvolvidos pela fabricante das urnas (Diebold). Embora esses componentes de software sejam críticos para a segurança da urna eletrônica, evidenciou-se que a autoridade eleitoral não tem posse nem domínio dos mesmos, recusando-se a apresentar os códigos fonte e compilado do firmware sob a alegação

de que tais itens não constavam do pedido inicial. Com tal restrição, os auditores não puderam determinar se o sistema de fato resiste a ataques de adulteração da BIOS como, e.g., o "ataque de Princeton" [Feldman et al. 2007].

A análise do restante do código disponibilizado ocorreu durante 10 dias em ambiente controlado pelo TSE, no qual os analistas foram impedidos de realizar atividades como cópia, análise dinâmica, compilação do código fonte, etc. Mesmo limitados a uma análise estática do código fonte, o uso de ferramenta para este fim, o CppCheck, apontou mais de 1000 trechos identificados como erros e mais de 2000 alertas, incluindo vulnerabilidades graves como "*buffer overflow*", que figura como o terceiro erro de software mais perigoso na lista CWE/SANS de 2011 (`http://cwe.mitre.org/top25/`). Também foi verificado que a porção do código utilizado para gerar números aleatórios usados no embaralhamento do BU foi modificado para evitar as vulnerabilidades descritas em [Aranha et al. 2014], embora o mesmo problema conceitual (combinação das funções `srand()` e `time()`) apareça em outros pontos do código.

Com relação ao sistema operacional (SO) utilizado pelas urnas, o TSE optou pelo Linux com *kernel* congelado na versão 2.6.16.62 de 2009, no qual foram feitas alterações em *drivers* de dispositivos e em utilitários do SO, pelo TSE e por seus fornecedores. Foram observados dezenas de pontos críticos nas alterações introduzidas, mas, sob as condições restritas de trabalho (pouco tempo e somente análise estática), não foi possível elaborar uma análise conclusiva sobre as potenciais vulnerabilidades encontradas.

Em resumo, com a impossibilidade de se verificar o registro e a contagem dos votos em cada urna eletrônica devido à inexistência do voto impresso conferível pelo eleitor, aliada às restrições encontradas para validação segura do software usado nas urnas, considera-se impossível determinar a integridade do software usado e, portanto, se foram justos o registro e a apuração dos votos no 2° turno da eleição de 2014.

5.2.6. Análise dos compiladores

A possibilidade de inserção de código malicioso via programas compiladores é bem documentada na literatura acadêmica há décadas [Thompson 1984] e a verificação da integridade do compilador é uma tarefa dada como necessária em normas internacionais de desenvolvimento de software seguro, como a ISO/IEC 15408 – "Common Criteria". Porém, a STI/TSE informou que "não há políticas estabelecidas pela instituição de auditoria sobre esses compiladores" e não permitiu acesso aos programas compiladores usados para se verificar a sua integridade, sob a alegação de que esta seria uma atividade que extrapolaria o concedido pela autoridade eleitoral.

Assim, reforça-se a conclusão da Seção 5.2.5 de que é impossível determinar se estava íntegro o software usado nas urnas durante o 2° turno de 2014.

5.2.7. Auditoria da compilação

Além dos compiladores, o processo de compilação (scripts, configurações, redes, etc.) também é um momento vulnerável à inserção de código malicioso no software eleitoral. Porém, o TSE não permitiu que fosse feita uma recompilação dos códigos fonte para

confirmar a integridade do compilado correspondente. Como agravante, alegou ainda que as variáveis de ambiente e meta-comandos usados não permitiriam a reprodução de um binário idêntico ao disponível no DVD oficial lacrado. Constatou-se, portanto, que os procedimentos de compilação desenvolvidos pela STI/TSE não foram planejados para ser este um processo determinístico e que permita auditoria posterior.

Portanto, com os procedimentos de compilação adotados e sob as restrições impostas, tornou-se impossível verificar se os executáveis lacrados no DVD oficial de 2014 derivaram de fato dos fontes apresentados para análise.

5.2.8. Certificação do software nas urnas

A autoridade eleitoral não permite a verificação direta das memórias das urnas para confirmar se o software nelas gravado contém a assinatura correta, mas apenas usar a própria urna eletrônica para, indiretamente, recalcular os hashes dos aplicativos nela gravados, como regulamenta a Res. TSE 23.397. Tal procedimento, porém, não tem utilidade para auditoria: afinal, se um código malicioso fosse inserido com sucesso na urna eletrônica, ele também fraudaria o cálculo do hash para prover sempre os resultados esperados. Esse problema já havia sido apontado na seção 4.3 do Relatório Unicamp [Unicamp 2002], que apontava a ausência de mecanismos simples e eficazes para confirmar que os programas na urna de fato correspondiam aos lacrados e guardados pelo TSE.

Como o procedimento de auditoria permitido é de baixa confiabilidade, ficou totalmente prejudicado aos auditores procederem, com razoável nível de confiança, a certificação do software embarcado nas urnas usadas no 2° turno das eleições de 2014.

5.2.9. Auditorias internas

Essa tarefa prevista no PTI ficou impossibilitada, uma vez que a autoridade eleitoral informou que não efetua qualquer auditoria posterior para avaliar o comportamento real dos equipamentos eleitorais, visando identificar potenciais tentativas de fraude ou mesmo para refutar eventuais denúncias de ocorrências indevidas.

5.2.10. Lacres das urnas eletrônicas

Foi avaliado o estado dos lacres de 684 urnas eletrônicas de 18 Estados. Foram encontradas irregularidades em aproximadamente 21% das urnas examinadas, tais como lacres fixados com sinal de rompimento, lacres descolados sem sinais de rompimento e lacres com numeração incorreta. Constatou-se que, nesses casos, nenhuma observação constava nas respectivas atas da seção eleitoral e que nenhuma providência administrativa foi gerada por motivo de lacres danificados ou soltos durante a eleição.

Testes revelaram ainda que se um lacre for retirado com cuidado, colado sobre um papel adesivo branco e depois reaplicado no seu lugar, facilmente passará despercebido por uma inspeção não profissional como a que normalmente é feita pelos eleitores e fiscais de partidos nas seções eleitorais.

Sob essas circunstâncias, a conclusão é que, embora importantes, os lacres colocados nas urnas são apenas parcialmente efetivos em sua função de revelar eventuais ataques ao software. Isto ocorre porque elas podem ser burladas inspeções amadoras e desatentas que parecem ocorrer durante a eleição, constatação reforçada pelo fato de que não se encontrou qualquer caso de lacres rompidos ou descolados que tivesse levado a alguma atividade de segurança para sua avaliação e correção.

5.2.11. Teste de votação paralela

O Teste de Votação Paralela (TVP) é anunciado como uma das salvaguardas de segurança mais importantes do sistema eleitoral. É procedimento obrigatório por lei, com o objetivo de submeter uma amostra de urnas eletrônicas a um teste de votação controlada e desenvolvido sob condições normais de uso no mesmo dia das eleições.

Em 2014, 68 urnas foram submetidas ao TVP nos TRE de todo o Brasil, 45 delas tendo seus logs analisados na presente auditoria. Nessa análise, constatou-se sinais evidentes de uso fora das "condições normais de votação". Nas urnas com biometria avaliadas, a liberação de votos por senha do mesário foi superior a 98%, enquanto em eleições normais este número fica abaixo de 7%. Já nas urnas sem biometria, a taxa de abstenção simulada nos testes foi abaixo da metade do usual, e a porcentagem de votos nulos e brancos simulada foi maior que o dobro do usual. Sob essas condições, não seria difícil para um eventual programa malicioso detectar, com elevada confiança, que está sob o TVP: bastaria analisar o log da urna e abortar a fraude quando sob teste.

Conclui-se que o TVP de 2014 não atingiu um nível de efetividade na tarefa de detectar eventuais adulterações maliciosas no software embarcado nas urnas eletrônicas testadas, caso tais adulterações tenham sido produzidas para intencionalmente abortar a fraude quando sob teste. O caso das urnas com biometria é ainda mais grave, porque elas são incompatíveis com esse tipo de teste legal ao exigirem liberação repetida do eleitor pelo mesário, sempre sendo possível para um software malicioso facilmente burlar o teste. Na prática, o uso de urnas com biometria do eleitor torna ineficaz o $\S 6^{\circ}$ do Art. 66 da Lei 9.504, que, por razões de segurança, institui o TVP.

5.3. Auditoria da transmissão e da totalização

De forma diferente do que ocorre com a auditoria da apuração nas urnas, a etapa de transmissão dos dados e a totalização dos votos no Brasil têm como ser auditadas por via externa e independente do software usado.

Em uma análise inicial, a tabulação dos dados digitais por seção eleitoral recebidos (BU digital) revelou coerência com o resultado oficial da totalização (BUweb). Após esta verificação, foi feita a conferência, por amostragem, entre os Boletins de Urna impressos, emitidos por urnas usadas nas seções eleitorais, e os BU digitais recebidos. Para isso foram verificados 503 BU impressos, recolhidos pelo Partido e pelos auditores no dia da eleição, e mais 7.020 BU fotografados e conferidos pelo projeto Você Fiscal (`www.vocefiscal.org`). As seções cobertas nesse caso foram recolhidas ao acaso, sem uma distribuição planejada. Outros 684 BU impressos foram recolhidos diretamente de urnas auditadas nos TRE e, nesse caso, foram escolhidas urnas que atendiam alguns critérios de risco. Destaca-se que essa análise não abrange a apuração dos votos nas urnas, i.e., não

avalia a correção do resultado registrado em cada BU em si, mas apenas se o BU impresso equivale ao respectivo BU recepcionado pelo sistema totalizador.

Durante a análise, não foi possível reconstruir o gráfico da totalização no tempo dos votos, dado que o TSE não mantém documentos de auditoria que permitam saber em que momento cada BU foi totalizado. Ainda assim, considera-se que, por sua aleatoriedade e volume, a amosta usada foi suficiente para indicar, com boa margem de confiança, que a transmissão dos dados produzidos pelas urnas e a totalização desses dados no 2° turno de 2014 ocorreram sem sofrer adulteração capaz de inverter o seu resultado final.

5.4. Denúncias específicas

5.4.1. Geração de mídias

Verificou-se que os computadores dos Cartórios Eleitorais que executam o sistema de geração das mídias usadas na carga e preparação das urnas eletrônicas não têm qualquer restrição quanto a sua conexão à Internet, viabilizando o acesso remoto às mídias quando geradas. Essa constatação contraria o que é costumeiramente divulgado como "salvaguarda" do sistema eleitoral, de ausência de conexão com a Internet nos pontos críticos do processo, pois aparentemente essa preocupação só se aplica à urna eletrônica em si.

5.4.2. Smartmatic

A empresa Smartmatic foi alvo de várias denúncias que alegavam sua participação em fraudes eleitorais em outros países, bem como de um esquema de fraude na totalização dos votos no Brasil. Desde 2012, a Smartmatic vem sendo contratada pelo TSE e por alguns TRE para fornecimento, entre outros, dos seguintes serviços [Rezende 2015]: "*(e) procedimentos de atualização de software embarcado e certificação digital nas urnas de modelos a partir de 2009, inclusive;(f) preparação, instalação, carga de software de eleição (até 1/3 podendo ser executado em outro local que não o de armazenamento), testes e operacionalização das urnas eletrônicas, suporte à geração do B.U.; (g) recepção de mídias e transmissão dos boletins de urna (BU), via sistema de apuração*."

Esses são, claramente, serviços críticos: pelo item (e) se tem oportunidade de inserção de porta-dos-fundos dentro do circuito de segurança MSD das urnas de modelo 2009 em diante; o item (f) dá acesso às urnas no momento de carga do software de eleição; e o item (g) dá acesso às mídias de resultado transmitidas para a totalização.

Durante a auditoria, a conferência da transmissão e da totalização dos votos que foi possível ser desenvolvida (Seção 5.3, acima) não detectou sinais de ataques sistemáticos ou abrangentes, por funcionários da Smartmatic, que tenham ocorrido no 2° turno de 2014, valendo-se do item (g) acima. Já a auditoria da apuração, que não pôde ser realizada de forma satisfatória (Seção 5.2, acima), não teve como eliminar a possibilidade de ter ocorrido ataque via software das urnas por tais agentes valendo-se dos itens (e) e (f).

5.4.3. Eleitor já votou

Foram muitas as reclamações de eleitores que não puderam votar porque, alegadamente, já teriam votado antes, algo que poderia ser causado por erros de digitação pelo mesário.

Já em urnas com biometria esse tipo de erro não deveria ocorrer pois, em condições normais, ao se verificar a digital do eleitor um eventual erro de digitação do mesário seria descoberto e corrigido.

A análise de eventos do tipo "eleitor já votou" nos logs das urnas não indicou a ocorrência de números que pudessem inverter o resultado da eleição. Todavia, os logs das urnas usadas no TVP revelaram um problema inesperado: diversos casos de falso-positivo (FP), i.e., aceitação de votação de eleitores ilegítimos, em urnas com biometria. Nesses casos, as impressões digitais dos operadores do TRE foram identificadas como sendo dos eleitores verdadeiros. A média observada de FP nessas urnas do TVP foi de 1,41%, sendo o máximo de 5,85% na urna que seria usada na SE 0473 da ZE 0003 de Recife. Este fato potencialmente explica a ocorrência inesperada desse tipo de denúncia em Seções Eleitorais que usaram urnas biométricas em 2014. Porém, a taxa de falso-negativo (FN), i.e., quando um eleitor legítimo não é reconhecido, foi de 6,7% no 2° turno de 2014. Combinados, esses são números bastante surpreendentes, pois ficam bem acima da taxa esperada considerando avaliações similares com o mesmo sistema de software biométrico [NIST 2014]: uma taxa de FP de 0.1% seria esperada para uma taxa de FN próxima a 2.2%, e uma taxa de FP inferior a 0.05% deveria ser obtida para taxas de FN superiores a 2.5%. Verifica-se, portanto, que o sistema utilizado pelo TSE está se comportando consideravelmente fora da faixa de operação observada no documento do NIST.

5.4.4. Eleitor justificado

Documentos enviados por um eleitor comprovam que ele estava no exterior no dia da eleição e que o TSE certificou que ele votou na sua seção eleitoral. Nesses casos de duplicidade, pode-se entender que a justificativa é o dado correto e o voto é o dado incorreto (falso), e a fraude poderia ser detectada com a simples análise dos arquivos de eleitores aptos/faltosos e arquivos de justificativa.

Contudo, não foi possível se verificar a incidência desse problema porque a autoridade eleitoral negou o fornecimento desses arquivos sob o argumento redundante de que não estava previsto na própria regulamentação. Soube-se, ainda, que a autoridade eleitoral não desenvolve qualquer cruzamento de dados de votantes e justificativas para orientar medidas preventivas futuras. Assim, em casos de duplicidade, a autoridade eleitoral acaba desprezando a justificativa (dado com maior probabilidade de estar correto) e considera válido o voto (dado mais provavelmente falso), sem tomar ações para coibir tais atos.

5.4.5. Fraude do mesário

Denúncias de fraude de mesários costumam referir-se ao final do período de votação, quando os fiscais abandonam a seção eleitoral e abrem a oportunidade para mesários inescrupulosos inserirem votos em nome de eleitores que ainda não compareceram. A inserção desses votos ilegais costuma ser feita de forma rápida e sequencial depois das 16h ou das 16h30 e, por isso, também são chamados de "votos rápidos e tardios".

Os arquivos de log das urnas podem revelar se houve uma alteração no ritmo de inserção de votos no final do período da votação e, para urnas biométricas, se houve

crescimento na taxa de liberações do voto pelo mesário (simulando um FN). A análise minuciosa desses dados chegou a encontrar seções eleitorais com tal comportamento, mas não mostrou incidência de votos rápidos e tardios em quantidade e regularidade que pudessem inverter o resultado eleitoral.

5.4.6. Problemas Localizados

Houveram denúncias de fraudes como: urna votava "sozinha", documentos da seção eleitoral jogados no lixo, em uma zerésima havia 400 votos para a candidata Dilma Rousseff e urna registrava 44 quando se tentava digitar 45. Essas denúncias eram individuais e localizadas, não evidenciando um problema sistêmico, e foram esclarecidas pelo TSE logo no voto inicial que aprovou a auditoria. Em especial, o caso da zerésima com 400 votos era grosseira falsificação. A conclusão é que todas essas denúncias de fraude foram infundadas e sem potencial de alterar a verdade eleitoral.

6. Conclusões sobre as eleições do 2° turno de 2014

Sobre a coleta de dados para auditoria, sua confiabilidade foi prejudicada porque o processo enfrentou restrições administrativas, tendo sido negada a entrega de parte dos dados solicitados. Em especial, foi negada permissão para coletar os dados diretamente das mídias de memória das urnas eletrônicas.

Similarmente, a auditoria da apuração dos votos das urnas eletrônicas não permitiu determinar a confiabilidade dos resultados produzidos pelas urnas eletrônicas. A primeira razão para isto é que não é possível se fazer uma auditoria contábil da apuração dos votos, já que o sistema que é essencialmente dependente de software e não produz um registro material (e.g., impresso) do voto que tenha sido visto e conferido pelo eleitor, podendo então ser usado como trilha de auditoria. Adicionalmente, devido a restrições impostas pela autoridade eleitoral, não foi possível verificar a integridade do software embarcado nas urnas eletrônicas ou sua correspondência com o código fonte apresentado aos auditores, devido a restrições impostas pela autoridade eleitoral. De qualquer forma, mesmo sem tais restrições, o processo de validação e certificação do software das urnas é uma tarefa que, para ser bem executada, requer tempo e recursos muito elevados; na prática, isto tem o potencial de inviabilizar tal procedimento como forma de garantir a confiabilidade do sistema. Finalmente, o Teste de Votação Paralela, conforme executado nas eleições brasileiras, não é eficiente para detectar um software de votação caso este verifique a existência de condições de uso fora do comum. Em especial, tais testes são pouco efetivos quando utilizados em urnas biométricas

Já com relação ao processo de transmissão e totalização dos votos, não foram encontrados indícios de fraudes ou de erros sistemáticos que pudessem alterar os resultados depois que estes saem das urnas eletrônicas.

Com estas considerações, pode-se concluir que a auditabilidade do sistema eletrônico de votação do TSE em seus moldes atuais é prejudicada por diversos fatores. O sistema não está projetado e implementado para permitir uma auditoria externa independente e efetiva dos resultados que produz, nem para obter certificação do software de votação, em especial da urna eletrônica, de acordo com padrões internacionais de segurança. Ainda, a forma de auditoria imposta pela autoridade eleitoral ("*auditoria*

comandada pelo auditado") não se enquadra em qualquer modelo reconhecido e padronizado por entidades internacionais que normatizam auditorias de sistemas de informação.

Agradecimentos. O trabalho de auditoria que deu origem ao presente artigo contou com a participação adicional dos seguintes auditores: Prof. Edson S. Gomi, Felipe R. Campos, Giuliano Giova, Gustavo Batistuzzo, Ney C. Dória Jr e Wanderley J. Abreu Jr. O autor Marcos A. Simplicio Jr é bolsista de produtividade CNPq (processo 305350/2013-7).

Referências

[Aranha et al. 2014] Aranha, D., Karam, M., Miranda, A., and Scarel, F. (2014). (in)segurança do voto eletrônico no Brasil. *Cadernos Adenauer 1/2014: Justiça Eleitoral*, pages 117–133. Disponível: www.kas.de/wf/doc/13775-1442-5-30.pdf.

[Beveridge 2015] Beveridge, J. (2015). Information systems auditing: Tools and techniques. Technical report, ISACA. Disponível: www.isaca.org/.

[Feldman et al. 2007] Feldman, A., Halderman, J., and Felten, E. (2007). Security analysis of the diebold accuvote-ts voting machine. In *Proc. of the USENIX Workshop on Accurate Electronic Voting Technology (EVT'07)*, pages 2–2. USENIX Association.

[Hursti 2006] Hursti, H. (2006). Diebold TSx evaluation. Technical report, Black Box Voting, Inc. Disponível: www.blackboxvoting.org/BBVtsxstudy.pdf.

[Kerckhoffs 1883] Kerckhoffs, A. (1883). La cryptographie militaire. *Journal des sciences militaires*, IX:5–83 (Jan), 161–191 (Feb).

[NIST 2014] NIST (2014). NISTIR 8034 - fingerprint vendor technology evaluation. Technical report, National Institute of Standards and Technology. Os dados citados foram extraídos das Tabelas 7 e 8 (pág. 26) e do gráfico da Fig. 90 (pág. 104).

[Rezende 2015] Rezende, P. (2015). Levantamento de atuações da empresa Smartmatic no processo de votação do TSE. http://www.cic.unb.br/˜rezende/trabs/eleicoes2014/#smart (última visita: 03/10/2015).

[Rivest and Wack 2006] Rivest, R. and Wack, J. (2006). On the notion of "software independence" in voting systems. Disponível: people.csail.mit.edu/rivest/pubs/RW06.pdf.

[Rocha et al. 2002] Rocha, A., Travassos, G., Souza, G., and Mafra, S. (2002). Relatório de avaliação do software TSE realizada pela Fundação COPPETEC. Technical report, COPPE/UFRJ. Disponível: www.angelfire.com/journal2/tatawilson/coppe-tse.pdf.

[SAPM 2014] SAPM (2014). Agile and critical systems. SAPM: Course Blog (blog.inf.ed.ac.uk/sapm/2014/03/06/agile-and-critical-systems).

[Sommerville 2011] Sommerville, I. (2011). *Engenharia de Software – 9 ed.* Pearson Education BR.

[Stober and Hansmann 2010] Stober, T. and Hansmann, U. (2010). *Agile Software Development: Best Practices for Large Software Development Projects*. Springer-Verlag.

[Thompson 1984] Thompson, K. (1984). Reflections on trusting trust. *Commun. ACM*, 27(8):761–763.

[Unicamp 2002] Unicamp (2002). Avaliação do sistema informatizado de eleições (urna eletrônica). Technical report, Universidade de Campinas. www.tse.jus.br/arquivos/relatorio-final-de-avaliacao-do-sistema-informatizado-das-eleicoes.