UM DISPOSITIVO SEGURO

Engenheiro que criou as camadas de proteção da urna eletrônica explica por que o equipamento é confiável

Yuri Vasconcelos e Neldson Marcolin

Um ano antes de cada eleição, reúne-se na sede do Tribunal Superior Eleitoral (TSE), em Brasília, um grupo de pessoas previamente inscritas com o objetivo de tentar invadir a urna eletrônica. Trata-se do Teste Público de Segurança (TPS), um evento que ocorre desde 2009 com especialistas em computação independentes ou ligados a instituições de pesquisa que realizam planos de ataque contra o equipamento. Em 2021, foram tentadas 29 invasões feitas por 26 investigadores, como são chamados os que tentam burlar o sistema eleitoral. Cinco deles descobriram algum tipo de fragilidade, que foi corrigida pelo corpo técnico do TSE. Os ataques foram repetidos em uma segunda etapa, já em maio de 2022 – e, dessa vez, sem nenhum sucesso.

Um dos idealizadores da urna, o engenheiro eletrônico Osvaldo Catsumi Imamura, ainda acompanha os TPS, a cada eleição. Formado pelo Instituto Tecnológico de Aeronáutica (ITA) e pesquisador do Departamento de Ciência e Tecnologia Aeroespacial (DCTA), centro de pesquisa ligado à Aeronáutica localizado em São José dos Campos (SP), ele esteve desde o primeiro momento, em 1995, na equipe que projetou e desenvolveu a arquitetura da urna eletrônica. O engenheiro foi o principal responsável por garantir a segurança do equipamento. Até hoje, nunca houve nenhum tipo de comprovação de que o sistema tivesse sido violado e algum voto fraudado, algo relativamente comum quando a votação era feita com cédulas de papel. Catsumi, de 66 anos, saiu da equipe técnica do TSE em 2005, continuando como consultor e colaborador eventual, e aposentou-se do DCTA no ano passado. Na entrevista abaixo, contou a *Pesquisa FAPESP* por que a urna segue sendo segura 26 anos depois de sua criação.

O senhor participou das duas etapas do TPS para a eleição deste ano. O que foi testado ali e quais os resultados?
Os testes são decorrentes de vários pedidos internos e externos ao TSE para ampliar a verificação da urna eletrônica. Sempre discutimos como poderiam ocorrer essas avaliações de modo a tornar o sistema mais transparente possível. Em 2009 surgiu a ideia de fazer um teste público, algo que já ocorria em outros lugares, no exterior. Isso garantiria que as pessoas que queriam formar opinião sobre uma determinada situação relacionada à urna pudessem elas mesmo realizar o teste para, aí sim, ratificar ou retificar as suas próprias observações. E assim começaram os testes.

De lá para cá, o que mudou?
De uma forma geral, a avaliação da urna não mudou quase nada, em termos de escopo. Os investigadores interessados podem requerer acesso a qualquer parte do sistema, como o hardware da urna e seus softwares. Só é necessário apresentar uma proposta do que se deseja avaliar. Desde o início foram feitos alguns ajustes em todo o processo e chegou-se

Catsumi no Museu Aeroespacial Brasileiro, em São José dos Campos, ao lado de um dos primeiros modelos de urna projetados para o TSE

LÉO RAMOS CHAVES / REVISTA PESQUISA FAPESP

à versão atual em que os testes são realizados em duas etapas. A primeira, normalmente no final do ano anterior das eleições na data mais próxima à lacração final dos códigos. Isso dá tempo para os investigadores analisarem o sistema que será usado nas eleições no ano seguinte. Alguns meses depois do primeiro teste os investigadores podem conferir os ajustes que o TSE realizou.

Investigadores são pesquisadores da área?

Uma parte, sim, mas já participaram pessoas da sociedade que entendem de computação e queriam avaliar pessoalmente como funciona a urna. Há entidades acadêmicas que se inscrevem para que os professores deem uma oportunidade aos alunos de computação exercitar os seus conhecimentos. Houve até um estudante do curso de computação da Universidade Federal de Mato Grosso do Sul que sugeriu fazer um TCC [trabalho de conclusão do curso de graduação] em segurança das eleições. O aluno convenceu o docente a participar junto com ele.

Durante o TPS tudo pode ser testado?

Isso mesmo. No TPS de novembro de 2021 verificamos que vários ataques tinham como objetivo ver a parte de criptografia, o manuseio do registro dos votos, a totalização. Acabamos agrupando os investigadores para que eles pudessem colaborar entre si, já que havia equipes que iriam olhar a mesma parte do sistema eleitoral.

O que diferencia a primeira fase de testes, no ano anterior, da segunda, já no ano das eleições?

Na primeira, a pessoa faz as verificações que deseja no sistema e, quando finaliza, nós, da comissão de avaliação, conferimos se ela conseguiu avançar no que pretendia, se atacou uma determinada situação e se trilhou por caminhos que não deveria ter conseguido trilhar. Nesse caso, mesmo que não tenha alcançado o objetivo final, eles são avaliados como um primeiro sucesso. Fazemos um relatório para o TSE e sua equipe técnica tem três a quatro meses para explicar por que isso aconteceu e dar sugestões de como corrigir ou aprimorar. Na segunda etapa de testes, vemos se o trabalho interno da equipe técnica atingiu os objetivos desejados. Por isso chamamos novamente os investigadores para eles analisarem se a urna ainda tem vulnerabilidades. Mesmo que não tenha acontecido nada e nenhum investigador tenha conseguiu avançar em alguma parte do sistema, o TSE faz uma revisão geral em todos os processos. Como sempre surgem novas tecnologias, pode ser que algo que foi tentado hoje tenha algum impacto lá na frente. Esses cuidados servem como parâmetro para avaliar mudanças futuras no sistema eleitoral.

Existe a possibilidade de a urna ser violada?

Teoricamente, sim. Os processos e as tecnologias são sempre dependentes do tempo. As tecnologias que são empregadas para proteger a urna e seus periféricos passam por uma rigorosa análise para serem selecionadas e permitir que todos os componentes do sistema eleitoral estejam prontos até um ano antes das eleições. Hoje, talvez os invasores não tenham o tempo hábil de atingir seus objetivos, como fazer a adulteração do voto. Existe muita discussão na imprensa sobre possíveis violações. Também na academia seguimos debatendo. Alguns

pesquisadores são mais puristas, mais teóricos, e produzem argumentos de que, na teoria, nos modelos matemáticos, é possível demonstrar que dá para burlar os códigos. Vem daí a afirmação de que a urna é violável. Não está errado. A questão toda é fazer essa teoria funcionar. Até agora, não há evidências reais.

Uma das críticas ao TSE é a de que o eleitor precisa confiar cegamente no sistema eleitoral. Isso porque ele se baseia no conceito de segurança por obscuridade, algo que, conforme os críticos, não combina com a sociedade democrática.
Segurança por obscuridade significa não tornar evidentes algumas informações. É como dizer: está seguro porque guardou segredo. A maioria dos códigos dos produtos criptográficos de segurança do mundo é controlado para evitar invasões aos sistemas. O código usado nas urnas não é aberto nem público, mas é verificável. Só um público mais seleto, de especialistas, tem condições de fazer essa verificação. É verdade que tem um ponto obscuro no código, que é a chave. Ela não é nem tem de ser pública da mesma forma que não passamos a chave do acesso da nossa conta bancária para ninguém. Quando tomamos essa decisão, é porque acreditamos que a obscuridade nos protege. Essa crítica contra a urna não se sustenta. No TPS, alguns ataques foram para tentar achar a chave na forma digital e invadir o sistema. Ninguém conseguiu obter todas as chaves necessárias.

Para entrar no sistema da urna, seria preciso romper as diversas camadas de segurança. Já foi dito que isso talvez não seja verdade porque bastaria penetrar em uma delas para estar dentro do sistema. Isso é real?
Toda segurança está em camadas. Não há uma proteção única, exclusiva da Justiça Eleitoral, porque a urna tem de ser colocada tanto em uma escola comum como em lugares distantes de difícil acesso. Hoje, 80% das urnas são transportadas por pessoas comuns. Não existe comboio de polícia militar ou das Forças Armadas fazendo escolta. Existem níveis ou camadas de segurança que precisaram ser criados pensando nessas circunstâncias e condições até que a urna entre na fase de oficialização da seção eleitoral no dia da eleição. A partir do momento que se oficializa, as camadas que continuam existindo são exclusivas da Justiça Eleitoral. As camadas anteriores, não. Se um ladrão roubar uma urna, significa que invadiu uma primeira camada. A eleição está comprometida? Não. Só estaria comprometida se fosse roubada uma quantidade absurda de urnas, inviabilizando a eleição por falta do dispositivo.

Mas não seria possível adulterar a urna durante o transporte, por exemplo, para que seja instalado um programa malicioso de forma a direcionar os votos a um candidato?
Vamos supor que alguém consiga romper uma camada específica e inserir um programa em algumas urnas. Quando o equipamento é inicializado, além da verificação de autenticidade, o tal programa malicioso vai encontrar outras camadas de proteção. Para conseguir avançar, é preciso que a urna funcione sem as validações necessárias quando se liga a chave. A urna é um computador, um hardware, e dá para mexer no sistema operacional. Mas não dá para seguir em frente com os resultados adulterados nem é possível assinar o boletim de urna, que é o resultado final daquela máquina, para ser validado pela Justiça Eleitoral. Essa é só uma etapa. Há várias outras camadas de proteção. Alguns investigadores tentaram, sem sucesso, atacar esse ponto no TPS, de tentar fazer a urna inicializar sem precisar ficar fazendo essas conferências de modo a conseguir executar o código invasor.

> **“Na teoria, dá para burlar os códigos da urna. A questão é fazer essa teoria funcionar. Até agora, não há evidências de que se tenha conseguido**

Quantas camadas há no total?
Depende da etapa do processo: ligar a urna, iniciar uma votação, terminar uma votação. Cada ação dessas tem de duas a três camadas de proteção. Somando tudo isso tem pouco mais de meia dúzia de camadas do processo como um todo. O envio dos resultados da votação é outro processo, que também tem as suas camadas. A urna, desde a sua preparação até o encerramento com a geração dos resultados, não se conecta com nada. A conexão com a rede ocorre somente com os sistemas de transmissão dos resultados de cada seção eleitoral para o sistema de totalização final. Além dos mecanismos de segurança lógica, existem outros componentes de segurança para garantir o funcionamento físico do conjunto, tornando-o tolerante a falhas e garantindo a integridade da eleição.

No momento em que as informações são enviadas ao TSE não há risco de um ataque hacker? Como ter certeza de que o resultado daquela urna é o mesmo que chegou ao tribunal?
Por conta das camadas que existem tanto na inicialização da urna como na finalização do trabalho da urna. Nesses processos existe uma chave única, dentro de cada equipamento. Se ela for tirada ou trocada, o hardware se torna inválido. Essa chave assina o resultado e permite que a Justiça Eleitoral verifique as informações de cada urna. Se a máquina for substituída por algum problema físico ou falha, o TSE usa urnas de reserva.

Como vê a reivindicação de a urna poder ser auditada com o voto impresso?
Vou dar um exemplo. A barragem de Brumadinho, que rompeu, foi auditada. Não obstante, a falha de projeto não foi verificada na auditoria. A auditoria é um evento importante para verificar as conformidades da execução com o planejamento operacional, com base nos registros e documentos técnicos e administrativos. Auditoria não é sinônimo ou garantia de segurança. Todos os sistemas lógicos que são empregados nas eleições passam por um ritual de assinaturas digitais para assegurar que o que foi lacrado seja exatamente o que será usado, permitindo uma auditoria antes e depois das eleições. Todavia, a auditoria não é suficiente para atestar a segurança dos sistemas envolvidos. A

Urnas fabricadas pela empresa Procomp, em 2004, durante a fase final de teste

OSVALDO CATSUMI IMAMURA

única forma de verificar a correção de um sistema lógico são os testes e uma análise técnica dos códigos. O TPS foi elaborado para atender essa demanda.

E o voto impresso?

Ele representa uma pseudoconfiança. O eleitor pode receber um papel, mas qual a segurança de que a informação impressa naquele papel foi contabilizada? A fraude no voto em papel nunca aconteceu na mão do eleitor, quando ele o inseria na urna; ocorria na apuração, quando a urna era aberta e os votos impressos eram dispostos na mesa. Por isso, um dos focos do projeto da urna eletrônica foi aprimorar essa parte do processo. A Justiça Eleitoral busca garantir que o voto realizado na urna é o mesmo que seja apurado.

O voto eletrônico se sobrepõe, então, ao impresso?

Existe um tipo de medição chamado tempo médio entre falhas, o MTBF, que indica mais ou menos quando qualquer produto deve começar a apresentar problemas. O MTBF de componentes eletrônicos, como a urna, é acima de 100 mil horas; de uma impressora, que é um dispositivo mecânico, está entre 10 e 20 mil horas. Não há como realizar uma validação cruzada usando elementos que têm probabilidade de falhas diferentes. Em outras palavras, não dá para validar o que a urna imprimiu com o que foi registrado eletronicamente, a menos que essa diferença esteja equalizada. Na concepção da urna eletrônica em 1995, um dos ministros do TSE pediu à nossa equipe: "Vocês precisam apresentar garantias técnicas para que, caso haja contestação, a corte possa julgar de forma bem fundamentada". Por enquanto, o que vale é o eletrônico porque é possível provar tecnicamente que a ocorrência de inconsistências da parte eletrônica é muito menor do que da mecânica.

Como foi que o senhor entrou para o grupo de criadores da urna?

No final de 1994 e no início do ano seguinte o ministro Carlos Veloso, então presidente do TSE, recomendou que algo teria de ser feito que fosse melhor do que a contabilização manual de cédulas de papel. A Justiça Eleitoral abriu um concurso para contratar os primeiros técnicos na área de tecnologia da informação [TI]. Paralelamente, foi feito um convite para o Executivo, que contava com engenheiros e técnicos nas instituições dos ministérios da Ciência e Tecnologia, da Educação, da Indústria e Comércio, da Comunicação, e militares. Um dos convites foi para o antigo Ministério da Aeronáutica. O DCTA [Departamento de Ciência e Tecnologia Aeroespacial], que é o centro de pesquisa da Força Aérea em São José dos Campos, foi consultado. O convite chegou até o IEAv [Instituto de Estudos Avançados], onde eu trabalhava. Assim, fui indicado como representante do Ministério da Aeronáutica para compor a equipe técnica.

O senhor integrou um grupo que ficou no TSE por vários anos. Quem mais fazia parte dele?

A equipe foi formada inicialmente com 14 pessoas. Passados três meses de trabalho, quando a arquitetura da urna e o edital foram concluídos, a maioria dos integrantes voltou para suas instituições de origem, exceto eu e outros três que vieram do Inpe – Paulo Seiji Nakaya, Antônio Ezio Marcondes Salgado e Mauro Hissao Hashioka. Assumi no TSE a coordenação de desenvolvimento de hardware e software; Nakaya liderou a área de logística; Salgado responsabilizou-se pelas redes de comunicação e produção fabril; e Hashioka assumiu a gerência-geral. O Giuseppe Dutra Janino, dentre os técnicos concursados, foi uma das pessoas do TSE que formamos para dar continuidade ao processo, assumindo o cargo de secretário de TI do tribunal em 2005.

A sua função já era zelar pela segurança do sistema?

No início a equipe deveria gerar requisitos de todo o sistema, o que incluía a segurança. Como eu já tinha trabalhado em outros processos do gênero e conhecia especialistas da academia nessa área, tornei-me o responsável pela segurança do sistema de 1998 a 2005. Sugeri o envolvimento da Agência Brasileira de Inteligência [Abin], que tem uma instituição, o Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações [Cepesc], voltada a cuidar de módulos criptográficos do governo. Fizemos um convênio para que desenvolvessem módulos exclusivos para o TSE.

Como vê hoje o Brasil no panorama internacional de urnas eletrônicas?

Existem vários modelos no mundo, alguns mais sofisticados, outros menos. Alguns países fazem todo o processo de forma eletrônica – e não mais no papel –, como é o nosso caso, enquanto outros usam inclusive a internet como parte do sistema eleitoral. É o caso da Estônia, que tornou virtual todos os processos possíveis, não só as eleições, mas também os administrativos do governo. Eles votam pela internet há mais de 10 anos, mas já sofreram um forte ataque hacker. No mundo dos sistemas cibernéticos, o elo mais fraco hoje é a conexão em rede, isto é, a internet. ■

A entrevista mais extensa está na versão on-line.