O MAQUINÁRIO DA DEMOCRACIA:
PROTEGENDO AS ELEIÇÕES NUM MUNDO ELETRÔNICO

SUMÁRIO EXECUTIVO

FORÇA-TAREFA SOBRE SEGURANÇA DE SISTEMAS DE INFORMAÇÃO DO CENTRO BRENNAN

LAWRENCE NORDEN, CHEFE

SÉRIE DIREITOS ELEITORAIS E ELEIÇÕES

CENTRO BRENNAN DE JUSTIÇA DA FACULDADE DE DIREITO DA UNIVERSIDADE DE NOVA IORQUE

www.brennancenter.org

Tradução para o Português pelo Fórum do Voto Eletrônico <www.votoseguro.org>
- tradução do texto: Roger Chadel
- revisão de termos: Amilcar Brunazo Filho
- adaptação das figuras: Divino C. R. Leitão

SOBRE A FORÇA-TAREFA

Em 2005 o Centro Brennan convocou uma Força-Tarefa de cientistas renomados internacionalmente nos setores governamental, acadêmico e privado, especialistas em máquinas de votação e profissionais de segurança para efetuar a primeira análise nacional sistemática sobre as vulnerabilidades nos três sistemas eleitorais eletrônicos mais freqüentemente contratados. A Força-Tarefa levou mais de um ano efetuando esta análise e preparando este relatório. Durante este tempo a metodologia, a análise e o texto foram extensivamente revisados em paralelo pelo Instituto Nacional de Normas e Tecnologia ("NIST"). Os membros da Força-Tarefa são:

Chefe

Lawrence D. Norden, Centro Brennan de Justiça

Pesquisador principal

Eric L. Lazarus, DecisionSmith.

Especialistas do Governo

Dr. David Jefferson, Laboratório Nacional Lawrence e Chefe do Conselho de Avaliação e Opinião para Tecnologia de Sistemas de Votação da Secretaria de Estado da Califórnia

John Kelsey, PhD, NIST

Rene Peralta, PhD, NIST

Professor Ronald Rivest (MIT), Comissão de Orientações Técnicas, Comissão de Assistência Eleitoral

Especialistas Acadêmicos

Professor Matt Bishop, Universidade da Califórnia em Davis

Professor David Dill, Universidade de Stanford

Professor Douglas W. Jones, Universidade de Iowa

Joshua Tauber, PhD, ex-membro do Laboratório de Ciências da Computação e Inteligência Artificial do MIT

Professor David Wagner, Universidade da Califórnia em Berkeley

Professor Dan Wallach, Universidade de Rice

Especialistas do Setor Privado (com e sem fins comerciais)

Georgette Asherman, Consultora estatística independente, fundadora da Direct Effects

Lillie Coney, Centro de Informações da Privacidade Eletrônica

Jeremy Epstein, Cyber Defense Agency LLC

Harri Hursti, consultor independente, ex-presidente da F-Secure PLC

Howard A. Schmidt, ex-Assessor de Segurança Cibernética da Casa Branca de George W.Bush; ex-Diretor-Chefe de Segurança da Microsoft

Dr. Bruce Schneier, Counterpane Internet Security

Matthew Zimmerman, Electronic Frontier Foundation

SOBRE O EDITOR E CHEFE DA FORÇA-TAREFA

Lawrence Norden é um Conselheiro Associado do Centro Brennan, trabalhando nas áreas de tecnologia de votação, direitos de votação e responsabilidade governamental. No último ano, o Sr. Norden chefiou o projeto de avaliação de tecnologia de votação do Centro Brennan. Ele é o autor principal de *O Maquinário da Democracia: Segurança. Acessibilidade, Usabilidade e Custo de Sistemas de Votação* (Centro Brennan, a sair em 2006) e contribuinte da Enciclopédia Americana das Liberdades Civis da Routledge, no prelo. O Sr. Norden é diplomado pela Universidade de Chicago e pela Faculdade de Direito da Universidade de Nova Iorque. O Sr. Norden atua como membro adjunto da faculdade no Programa de Advocacia na Faculdade de Direito Benjamin N. Cardozo. Ele pode ser contatado pelo endereço lawrence.norden@nyu.edu.

SOBRE O CENTRO BRENNAN

O Centro Brennan de Justiça da Faculdade de Direito da Universidade de Nova Iorque une pensadores de advogados na busca de uma perspectiva de democracia participativa e eficaz. A missão da organização é desenvolver e implementar uma agenda não-partidária de estudos, educação pública e ação legal que promovam igualdade e dignidade humana, além de salvaguardar as liberdades fundamentais. O Centro trabalha nas áreas da Democracia, Pobreza, Justiça Criminal, Liberdade e Segurança Nacional. Michael Waldman é o Diretor Executivo do Centro.

SOBRE A SEÇÃO DE DIREITOS ELEITORAIS E ELEIÇÕES

O Projeto de Direitos de Votação e Eleições do Centro Brennan promove políticas que protegem os direitos de acesso eleitoral e participação política igualitária. O Projeto procura tornar o exercício do direito de voto para todos os Americanos simples e livre de armadilhas e garantir que o voto de cada eleitor é registrado e contado com precisão. Ao alinhar-se à missão do Centro, o Projeto oferece recursos de educação pública para advogados, funcionários públicos estaduais e federais, estudantes e jornalistas que estão preocupados com eleições justas e abertas. Para mais informações, por favor visite www.brennancenter.org ou ligue para ++1-212-998-6730.

Este documento é o segundo de uma série, que também inclui:

Fazendo a Lista: Processos de Controle e Verificação de Bases de Dados para Registro de Eleitores por Justin Levitt, Wendy Weiser e Ana Munoz.

Outros recursos de direitos de voto e eleições, disponíveis no site do Centro Brennan, incluem:

Resposta ao Relatório de 2005 da Comissão de Reforma Eleitoral Federal (2005) (em co-autoria com o Professor Spencer Overton).

Recomendações para Aumentar a Confiabilidade de Sistemas de Votação Eletrônica por Registro Direto (2004) (em co-autoria com a Conferência de Liderança sobre Direitos Civis).

AGRADECIMENTOS

Mais importante, o Centro Brennan agradece à NIST e seus cientistas por dedicar tantas horas para a revisão paralela extensiva e minuciosa da análise e do relatório. O relatório, na sua forma atual, não existiria sem os comentários e as contribuições importantes da NIST.

Agradecemos particularmente a John Kelsey da NIST pelo material e pelas idéias substanciais que ele trouxe, que foram incorporados no relatório e nos catálogos de ataque do relatório. Agradecemos também especialmente a René Peralta pelas suas contribuições e análise originais. Finalmente, estamos enormemente gratos a Barbara Guttman, John Wack e outros cientistas da NIST que forneceram material para os catálogos de ataque, ajudaram a desenvolver a estrutura do relatório, e editaram muitos rascunhos.

Também apreciamos extremamente os enormes esforços do Pesquisador Principal Eric Lazarus em prol deste relatório. Sua visão, tenacidade e entusiasmo contagiante se estendeu à equipe durante o longo processo de análise e redação.

Uma dívida especial de gratidão é também devida aos funcionários de eleições pelo país, que gastaram horas respondendo a pesquisas e perguntas em entrevistas relacionadas a este relatório. Além dos membros da equipe Prof. Ronald Rivest e Dr. David Jefferson, queremos agradecer particularmente a Patrick Gill, auditor da comarca de Woodbury, arquivista e ex-Presidente da Associação de Auditores de Comarcas do Estado de Iowa; Elaine Johnston, Auditor da Comarca de Asotin, Washington; Harvard L. Lomax, Arquivista de Eleitores da Comarca de Clark, Nevada; Debbie Smith, Coordenadora de Eleições, Comarca de Caleveras , Califórnia; Jocelyn Whitney, Desenvolvedor e Gerente de Projeto para atividades de Testes de Votação Paralela no Estado da Califórnia; Robert Williams, Diretor de Informática da Comarca de Monmouth, New Jersey; e Pam Woodside, ex-Diretor de Informática do Conselho de Eleições do Estado de Maryland. Queremos também agradecer à Comissão Nacional para a Integridade Eleitoral pela sua cooperação e ajuda neste esforço.

Jeremy Creelan, Advogado Associado na Jenner & Block LLP, merece crédito por conceber, lançar e supervisionar o projeto de avaliação de tecnologia de votação do Centro Brennan, incluindo o desenvolvimento deste relatório, como Diretor Adjunto do Programa de Democracia do Centro até Fevereiro de 2005. O Programa sente muito a falta dele e lhe deseja sucesso na prática privada, onde ele continua a fornecer ajuda *pro bonno* inestimável.

O Centro Brennan é grato a Lillie Coney, membro da Força-Tarefa, Diretora Associada do Centro de Informações da Privacidade Eletrônica. Entre muitas outras contribuições, ela forneceu uma ajuda inestimável ao reunir a Força-Tarefa, e ofereceu freqüentemente co Centro Brennan sábios conselhos estratégicos.

Este relatório foi grandemente beneficiado pela ajuda editorial perspicaz e minuciosa de Deborah Goldberg, Diretora do Programa de Democracia do Centro Brennan.

Estamos extremamente gratos aos professores Henry Brady da Universidade da Califórnia em Berkeley e Benjamin Highton da Universidade da Califórnia em Davis pelos seus conhecimentos sobre os possíveis efeitos dos ataques de negação de serviço em sistemas de votação. O Centro Brennan também agradece a Bonnie Blader, consultor independente, que forneceu à Força-Tarefa uma pesquisa crucial, a David M. Siegel, consultor independente de tecnologia, pelas suas contribuições originais sobre inspeções de código de software, e Tracey Lall, candidato a Ph.D. em Ciências da Computação na Universidade de Rutgers, que contribuiu com muitas horas de análise de segurança crítica. Douglas E. Dormer, CPA, CTP forneceu assistência inestimável desenvolvendo a metodologia de análise e mantendo o foco da Força-Tarefa. Joseph Lorenzo Hall

deve também ser agradecido por ajuda os membros da Força-Tarefa a entender as diferenças e as semelhanças nas arquiteturas de sistemas de votação. Muitas das pesquisas legais foram efetuadas por Gloria Garcia e Juan Martinez, candidatos a J.D. na Faculdade de Direito Benjamin N. Cardozo, e Annie Lai and S. Michael Oliver, candidatos a J.D. na Faculdade de Direito da Universidade de Nova Iorque. Lowell Bruce McCulley, CSSP, foi excepcionalmente útil ao criar os catálogos de ataque. Finalmente, agradecemos aos Associados de Pesquisa do Centro Brennan Annie Chen, Lauren Jones, Ana Munoz, e Neema Trivedi por tantas horas de assistência dedicada.

Generosas doações anônimas, a Corporação Carnegie de Nova Iorque, a Fundação Ford, a Fundação HKH, a Fundação Knight, o Instituto da Sociedade Aberta e a Fundação da Família Rockefeller ajudaram no desenvolvimento e na publicação deste relatório. As declarações e as perspectivas expressas neste relatório são de responsabilidade única do Centro Brennan.

ÍNDICE

TEXTO

FIGURAS

INTRODUÇÃO

Nestas páginas, o Centro Brennan de Justiça da Faculdade de Direito da Universidade de Nova Iorque (o "Centro Brennan") resume a primeira análise sistemática nacional das vulnerabilidades nos três sistemas eletrônicos mais freqüentemente contratados. Para desenvolver a análise, o Centro Brennan convocou uma Força-Tarefa de cientistas renomados internacionalmente nos setores governamental, acadêmico e privado, especialistas em máquinas de votação e profissionais de segurança.

A Força-Tarefa examinou ameaças de segurança às *tecnologias* usadas em sistemas de votação com Gravação Eletrônica Direta ("GED"), sistemas GEDs com Voto Impresso Conferido pelo Eleitor ("GED com VICE") e sistemas de Votação por Leitura Ótica ("VLO") na Seção Eleitoral. A análise assume que procedimentos adequados de segurança física e contabilização estejam implementados.

FIGURA 1

SISTEMAS DE VOTAÇÃO

Tipo de Sistema de Votação	Descrição do Sistema de Votação	Exemplos de Sistema de Votação
Gravação Eletrônica Direta (GED)	Uma máquina GED registra diretamente as seleções do eleitor em cada escrutínio, usando uma cédula que aparece numa tela. Máquinas GED típicas têm um painel sensível ao toque, embora outras tecnologias de telas tenham sido usadas. A característica de definição destas máquinas é que os votos são capturados e armazenados (gravados) eletronicamente.	Microvote Infinity Voting Panel Hart InterCivic eSlate Sequoia AVC Edge Sequoia AVC Advantage ES&S iVotronic ES&S iVotronic LS Diebold AccuVote-TS Diebold AccuVote-TSX Unilect Patriot
GED com Voto Impresso Conferido pelo Eleitor (GED com VICE)	Uma máquina GED com VICE guarda a escolha do eleitor em meio eletrônico interno e simultaneamente em papel. Uma GED com VICE permite ao eleitor confirmar a correção do registro em papel viabilizando a Conferência pelo Eleitor.	Sistema ES&S iVotronic com Log de Auditoria em Tempo Real Diebold AccuVote-TSX com impressora AccuView Sequoia AVC Edge com impressora VeriVote Hart InterCivic eSlate com VICE Unilect Patriot com VICE
Votação por Leitura Ótica na Seção Eleitoral (VLO)	Máquinas VLO permitem ao eleitor marcar cédulas em papel, tipicamente com lápis ou caneta, independente de máquina. O eleitor leva então sua cédula dobrada até um digitalizador. Ele desdobra a cédula e a insere no digitalizador, que registra oticamente o voto.	Diebold AccuVote-OS ES&S Model 100 Sequoia Optech Insight

O relatório completo (o "Relatório de Segurança"), que foi revisado extensivamente em paralelo pelo Instituto Nacional de Normas e Tecnologia ("NIST"), pode ser encontrado em www.brennancenter.org. Seguindo a análise detalhada aqui, o Centro Brennan e os membros da Força-Tarefa recomendam medidas que podem ser tomadas para reduzir a vulnerabilidade técnica de cada sistema de votação[1].

[1] O NIST informou ao Centro Brennan que o desenvolvimento de recomendações de políticas para sistemas de votação não está dentro da missão da agência ou sua autoridade institucional. Da mesma forma, as recomendações de políticas no relatório não devem ser atribuídas aos membros da Força-Tarefa que trabalham no NIST.

DESCOBERTAS PRINCIPAIS

Três pontos fundamentais aparecem da análise de ameaças no Relatório de Segurança:

■Todos os três sistemas têm vulnerabilidades de segurança e confiabilidade significativas, que apresentam um perigo real para a integridade das eleições nacionais, estaduais e municipais.

■As vulnerabilidades mais preocupantes de cada sistema podem ser substancialmente eliminadas se contra-medidas apropriadas forem implementadas no nível estadual e municipal.

■Poucas jurisdições eleitorais implementaram as principais contra-medidas que podem fazer com que os ataques mais simples contra os sistemas de votação tenham maior dificuldade em obter sucesso.

VULNERABILIDADES DOS SISTEMAS DE VOTAÇÃO

Depois de uma revisão de mais de 120 ameaças a sistemas de votação, a Força-Tarefa chegou às conclusões cruciais a seguir:

Para todos os três tipos de Sistema de Votação:

■Quando o objetivo é mudar o resultado de uma eleição apertada, ataques que envolvem a inserção de programas de computador maliciosos ou outros softwares corrompidos é o que há de mais fácil.

■Máquinas de votar que possuem componentes de transmissão sem fio são consideravelmente mais vulneráveis a uma grande gama de ataques. Atualmente, somente dois Estados, Nova Iorque e Minesota, proibiram o uso de componentes sem fio em todas as máquinas de votar.

Para máquinas GED sem Votos Impressos Conferidos pelo eleitor:

- Máquinas GED sem VICE não contam com uma poderosa medida para impedir ataques de software: as rotinas de auditoria automáticas pós-eleição que comparem os registros em papel com os registros eletrônicos.

Para máquinas com VICE e VLO:

- O Voto em papel Conferido pelo Eleitor, *por si só,* tem um valor de segurança relativo. O registro em papel só tem valor significativo se uma rotina automática de auditoria for desenvolvida (e se procedimentos de guarda e de segurança física bem projetados forem seguidos). Dos 26 estados que exigem Votos Impressos Conferidos pelo Eleitor, apenas 12 prevêem auditorias regulares.

- Mesmo se as jurisdições eleitorais efetuarem auditorias regulares com os votos impressos conferidos pelo eleitor, máquinas GED com VICE e VLO ainda são vulneráveis a alguns ataques e erros de software. As jurisdições eleitorais que efetuam auditorias com comprovantes impressos devem se preocupar com esses problemas potenciais.

RECOMENDAÇÕES DE SEGURANÇA

Há uma série de passos que as jurisdições eleitorais podem tomar para resolver as vulnerabilidades identificadas no Relatório de Segurança e tornar seus sistemas de votação consideravelmente mais seguros. Recomendamos a adoção das seguintes medidas de segurança:

1.Efetuar Auditorias Automáticas de rotina comparando os Votos Impressos Conferidos pelo Eleitor com os Registros Eletrônicos após cada eleição. O Voto Impresso Conferido pelo Eleitor acompanhado de uma sólida Auditoria Automática pode ser um bom caminho para tornar os ataques mais simples, bem mais difíceis.

2.Efetuar um "Teste de Votação Paralela" (seleção aleatória de máquinas de eleição e testá-las da maneira mais realista possível no dia da eleição). Para máquinas GED sem papel, especificamente, o Teste de Votação Paralela ajudará as jurisdições eleitorais a detectar ataques de software, assim como erros sutis de programação que não puderam ser percebidos durante a inspeção e outros testes.

3.Proibir o uso de máquinas de votação com componentes de transmissão sem fio. Todos os três sistemas são mais vulneráveis aos ataques se tiverem componentes de transmissão sem fio.

4.Usar um processo de amostragem transparente e aleatória para todos os procedimentos de auditoria. Para que uma auditoria seja eficaz (e para assegurar que o público tenha confiança nesses procedimentos), as jurisdições eleitorais devem desenvolver e implementar procedimentos de amostragem transparente e aleatória.

5.Assegurar a descentralização da programação e da administração dos sistemas de votação. Quando uma única entidade, como um fornecedor ou uma entidade de nível nacional ou estadual efetuar tarefas chave para várias jurisdições eleitorais, ataques em eleições majoritárias se tornam mais fáceis.

6.Instituir procedimentos claros e eficazes para tratar de evidência de fraude ou de erro. Tanto as Auditorias Automáticas quanto os Testes de Votação Paralela têm um valor de segurança questionável sem procedimentos eficazes de ações quando uma evidência de mau funcionamento e/ou fraude for descoberta. Detecção de fraude sem uma resposta apropriada não impedirão ataques de terem sucesso.

Felizmente, estes passos não são particularmente complicados ou incômodos. Em sua maioria, eles não envolvem mudanças consideráveis na arquitetura do sistema. Infelizmente, *poucas jurisdições eleitorais implementaram alguma destas recomendações de segurança.*

VULNERABILIDADES DOS SISTEMAS DE VOTAÇÃO

Boas análises de ameaças nos permitem identificar e implementar as melhores precauções de segurança.

■ O QUE É UMA ANÁLISE DE AMEAÇA E POR QUE É NECESSÁRIA?

Nos últimos anos, poucos problemas no mundo dos sistemas de votação eletrônica chamaram tanto a atenção do público quanto a segurança dos sistemas de votação. Esta atenção para a segurança dos sistemas de votação tem o potencial para ser uma força positiva. Infelizmente, muitas das discussões públicas a respeito da segurança foram relegadas a segundo plano em função de queixas e contra-queixas que estão baseadas em algo pouco além de especulação ou anedota.

Em resposta a esta discussão mal informada, e com a intenção de ajudar os funcionários de eleições e o público a fazer sua escolha sobre as máquinas de votação, a Força-Tarefa iniciou uma análise metódica das ameaças potenciais a sistemas de votação. A análise de ameaça fornece aos funcionários de eleições e cidadãos preocupados, critérios quantificáveis para medir o nível de segurança oferecido pelos sistemas de votação e as medidas potenciais de segurança. Deve ajudar as jurisdições eleitorais a decidir (a) quais sistemas de votação a certificar ou comprar, e (b) como proteger estes sistemas de ameaças de segurança depois que foram comprados. O Relatório de Segurança mostra os resultados detalhados desta análise, que está resumida aqui.

■■ ANÁLISES SISTEMÁTICAS DE AMEAÇAS DE SISTEMAS DE VOTAÇÃO JÁ DEVERIAM SER FEITAS HÁ MUITO TEMPO

A maioria dos americanos concordaria que a integridade de nossas eleições é fundamental para nossa democracia. Queremos cidadãos que tenha total confiança que seus votos serão registrados com precisão. Dado o teor atual do debate sobre a segurança dos sistemas de votação, este é um motivo suficiente para efetuar análises sistemáticas regulares de ameaças em sistemas de votação.

Tão importante, estas análises, se utilizadas para desenvolver normas e procedimentos de sistemas de votação, podem reduzir o risco de ataque em sistemas de votação. Como uma nação, não fomos sempre capazes de evitar esses ataques com sucesso — de fato, vários tipos de ataques em sistemas de votação e em eleições são uma "longa tradição" na história americana[2]. A suspeita ou descoberta destes ataques provocou geralmente indignação momentânea, seguida por períodos de amnésia histórica[3].

Toda tecnologia, não importa quanto avançada, é vulnerável a ataques em algum grau. A história de ataques em sistemas de votação no ensina como é insensato assumir que não haverá ataques a sistemas de votação no futuro. Mas podemos nos educar sobre as vulnerabilidades e tomar as devidas precauções para assegurar que os ataques mais fáceis, com o potencial de afetar a maioria dos votos, se tornam o mais difícil possível. Boas análises de ameaças nos permitem identificar e implementar as melhores precauções de segurança.

---

[2] Tracy Campbell, DELIVER THE VOTE (ATACAR O VOTO), em xvi (2005) (apontando para, entre outras coisas, uma história da compra de votos, recheio de cédulas e transposição de resultados).
[3] *Id.*

■■ ANÁLISES SÓLIDAS DE AMEAÇAS DEVEM AJUDAR A FAZER SISTEMAS MAIS CONFIÁVEIS

Há uma vantagem adicional a este tipo de análise: deve ajudar a fazer nossos sistemas de votação mais confiáveis, *independente de serem ou não atacados*. Sistemas de votação computadorizados — como todos os sistemas de votação anteriores — se mostraram vulneráveis a erros. Como detalhado no Relatório de Segurança, votos têm sido mal contados ou perdidos em resultado de *firmware* (instruções codificadas no equipamento de um sistema de computador) incorreto, software de máquina deficiente, software de servidor de totalização defeituoso, erros de programação, quebra de máquinas, dispositivos de entrada avariados e erros dos mesários.

"Um velho aforismo na área de segurança computacional se aplica claramente aqui: quase tudo que um agressor maldoso possa tentar também pode acontecer por acidente; para cada agressor maldoso, pode haver milhares de pessoas cometendo erros comuns por descuido[4]". Análises sólidas de ameaças ajudarão a expor e descobrir vulnerabilidades em sistemas de votação, incluindo não só brechas de segurança como também simples maus funcionamentos.

■ QUE METODOLOGIA FOI USADA PARA A ANÁLISE DE AMEAÇAS?

Ao desenvolver o estudo das vulnerabilidades de segurança dos sistemas de votação, o Centro Brennan trouxe alguns dos funcionários eleitorais mais destacados da nação, assim como uma Força-Tarefa de especialistas reconhecidos internacionalmente nos campos da ciência da computação, política eleitoral, sistemas de votação e estatística. Depois de considerar vários enfoques para medir a robustez da segurança de eleições, este grupo selecionou por unanimidade um modelo que: (a) identificou e classificou as ameaças potenciais aos sistemas de votação, (b) ordenou estas ameaças baseado numa métrica escolhida de comum acordo (que mede a "dificuldade" de cada ameaça ser implementada no ponto de vista do agressor), e (c) determinou (utilizando a mesma métrica empregada para ordenar as ameaças) a dificuldade acrescentada a cada ameaça catalogada depois que o conjunto de contramedidas estiver implementado.

Depois de vários meses de trabalho, incluindo uma conferência pública de análise de ameaças organizada pelo Instituto Nacional de Normas e Tecnologia (NIST), a Força-Tarefa identificou e categorizou mais de 120 ameaças aos três sistemas de votação. As ameaças recaem geralmente em uma ou mais das nove grandes categorias seguintes: (1) inserção de software corrompido dentro das máquinas antes do dia da eleição; (2) ataques remotos por transmissão sem fio ou outros no dia da eleição; (3) ataques aos servidores de totalização; (4) descalibragem de máquinas de votação; (5) desligamento de recursos de ajuda ao eleitor em máquinas de votação; (6) bloqueios na disponibilidade dos sistemas; (7) ações de corrupção de funcionários de eleições ou outros em locais de votação para afetar o registro dos votos; (8) esquemas de compra de votos; e (9) ataques a cédulas ou nos comprovantes impressos conferidos pelo eleitor.

A Força-Tarefa determinou que a melhor e mais simples métrica para determinar a "dificuldade" de cada um desses ataques é a quantidade de participantes ativos necessários para executar o ataque com sucesso. Um "participante ativo" é alguém cuja participação é necessária para fazer o ataque funcionar, e que conhece o suficiente sobre o ataque para despistá-lo ou expô-lo.

Para cada ataque, os membros da Força-Tarefa verificaram quantos participantes ativos seriam necessários para mudar o resultado de uma eleição majoritária razoavelmente apertada na qual

[4] Douglas W. Jones, *Threats to Voting Systems (Ameaças a Sistemas de Votação),* Apresentação da Oficina de Análise de Ameaças do NIST (7 de outubro de 2005), *disponível em* http://vote.nist.gov/threats/papers/threats_to_voting_systems.pdf (visitado pela última vez em 25 de maio de 2006).

todos os votos foram dados em um dos três sistemas analisados. Fizemos nossa pesquisa numa eleição fictícia para governador entre Tom Jefferson e Johnny Adams numa jurisdição fictícia, Pennasota. Pennasota foi criada agregando os resultados da eleição presidencial de 2004 em 10 estados "apertados", como foi determinado pelas pesquisas da Zogby International na primavera, no verão e no outono de 2004.

FIGURA 2

ELEIÇÃO PARA GOVERNADOR, ESTADO DE PENNASOTA, 2007

Candidato	Partido	Total de votos
Tom Jefferson	Dem-Rep	1,769,818
Johnny Adams	Federalistas	1,689,650

Para calcular quantos participantes ativos seriam necessários para alterar o resultado desta eleição e eleger Johnny Adams o próximo governador de Pennasota, os especialistas desmembraram cada ataque nas suas partes necessárias, atribuíram um valor representando a quantidade mínima de pessoas que acreditavam ser necessário para obter cada parte, e determinando então quantas vezes o ataque deveria ser repetido para inverter o resultado da eleição.

No fim deste processo, funcionários eleitorais foram entrevistados para determinar se eles concordavam com as etapas e os valores atribuídos. Quando necessário, as etapas e os valores foram modificados para refletir suas considerações.

Depois de classificar os ataques por nível de dificuldade, os membros da Força-Tarefa recalcularam como ficaria a dificuldade de cada ataque se vários conjuntos de contramedidas fossem implementados. O processo para determinar a dificuldade de superar as contra-medidas foi exatamente o mesmo que o de determinar a dificuldade do ataque: para cada etapa necessária para superar a contra-medida foi identificado e atribuído um valor igual à quantidade de pessoas necessárias para completar a etapa. Os funcionários de eleições foram outra vez consultados para confirmar que as etapas e os valores atribuídos eram razoáveis.

Para assegurar que os resultados de nossa análise eram robustos e não limitados à jurisdição eleitoral composta de Pennasota, nós confrontamos nossa análise de ameaça contra os resultados da eleição presidencial na Flórida, no Novo México e na Pensilvânia. Todos os resultados e as descobertas discutidos neste sumário foram aplicados em nossas análises nesses três estados.

O trabalho completo da Força-Tarefa, incluindo a escolha da metodologia, a análise e o relatório foram extensivamente revisados em paralelo pelo NIST.

■ QUAIS FORAM OS MAIORES RISCOS REVELADOS PELA ANÁLISE DE AMEAÇA?

Significativamente, a análise de ameaça sugere que os três sistemas de votação são igualmente vulneráveis a ataques de software

Abaixo está uma discussão das ameaças mais preocupantes identificadas pelo Relatório de Segurança.

■■ OS ATAQUES MENOS DIFÍCEIS USAM PROGRAMAS DE ATAQUE AO SOFTWARE

Os ataques "menos difíceis" contra os três sistemas (medidos pela métrica de quantidade de participantes ativos necessários para mudar o resultado de uma eleição majoritária) envolvem a inserção de software malicioso ou outros programas de ataque ao software original de modo a tomar o controle da máquina de votar. Significativamente, a análise de ameaça sugere que os três sistemas são igualmente vulneráveis a ataques de software.

O tipo mais básico de programa de ataque ao software original atingiria as máquinas de votar e passariam uma certa quantidade de votos de um candidato para outro. Esta alteração de votos pode ocorrer a qualquer momento no dia da eleição contanto que fosse terminada antes que os funcionários de eleição imprimissem o registro em papel do total de votos e extraíssem o registro eletrônico de votos das máquinas.

Inserir um programa de ataque ao software original dentro de um sistema de votação é provavelmente um desafio técnico e financeiro, principalmente se o agressor desejar evitar a detecção. Entretanto, um registro histórico substancial deste tipo de ataques contra sistemas outros que os de eleições sugere que pode ser executado com sucesso. O Relatório de Segurança detalha vários meios pelos quais um agressor pode inserir programas de ataque ao software original sem ser detectado.

Especificamente, há vários pontos no desenvolvimento e no uso do software da máquina de votar onde programas de ataque ao software original podem ser inseridos sem detecção. Entre estes pontos, programas de ataque ao software original podem ser inseridos através do "firmware[5]" que é gravado nas máquinas de votar, durante a geração do software "comercial de prateleira" ou software do fabricante usado nas máquinas de votar, através de enxertos e atualizações supostamente para melhorar o desempenho e a capacidade das máquinas de votar, durante a criação dos arquivos de configuração e de definição de eleições usados para interpretar a escolha do eleitor e os totais nas máquinas de votar, através de comunicação em rede entre máquinas de votar e fontes externas, assim como em dispositivos de "entrada/saída" como cartões de memória e impressoras.

Há muitas barreiras que um agressor deve superar para assegurar que a inserção de um programa de ataque modificou votos em quantidade suficiente para modificar o resultado de uma eleição majoritária e escapar da detecção. Depois de uma análise cuidadosa, a Força-Tarefa determinou que nenhuma dessas barreiras é intransponível. O Relatório de Segurança discute em detalhes como um agressor pode suplantar os desafios a seguir: esforços de fabricantes para prevenir ataques (pág. 32-33); obtenção de conhecimento técnico suficiente sobre como a máquina de votar e seu software trabalham (pág. 36-37); obtenção de conhecimento suficiente sobre a eleição em questão (pág. 37-38); criação de programa de ataque com a capacidade de alterar, acrescentar ou subtrair votos (pág. 39-40); esquivar-se de inspeções da Autoridade Auditora Independente ("AAI") (pág. 42-45); evitar detecção durante os testes de máquina (pág. 44-45); e evitar a detecção por meio de registros mantidos nos Arquivos de Eventos (logs) e de auditoria (pág. 45-46).

[5] Firmware são programas gravados nas memórias fixas da máquina de votar

■■ COMPONENTES DE TRANSMISSÃO SEM FIO CRIAM RISCOS DESNECESSÁRIOS

A análise de ameaças mostra que máquinas com componentes de transmissão sem fio são particularmente vulneráveis a programas de ataques ao software e outros ataques. O Relatório de Segurança conclui que este perigo se aplica aos três sistemas de votação examinados.

Fabricantes continuam a produzir e vender máquinas com componentes de transmissão sem fio. Dentre os vários tipos de ataques possíveis com componentes de transmissão sem fio estão ataques que exploram uma vulnerabilidade não planejada no software e no hardware para colocar um Cavalo de Tróia[6] dentro da máquina. Para este tipo de ataque, um Cavalo de Tróia não precisa ter sido inserido previamente. Pelo contrário, um agressor ciente da vulnerabilidade do software ou do firmware do sistema de votação pode simplesmente dirigir-se à seção eleitoral e transferir seu Cavalo de Tróia para a máquina usando um PDA (palmtop) com transmissão sem fio.

Portanto, virtualmente qualquer pessoa com algum conhecimento de software e um PDA[7] pode efetuar este ataque. Isto é particularmente preocupante quando se sabe que a maioria das máquinas roda com software e/ou sistema operacional de prateleira; as vulnerabilidades destes softwares e sistemas são freqüentemente bem conhecidas[8]. Contra todos os três sistemas, os agressores podem usar componentes de transmissão sem fio para subverter *todos* os testes. Especificamente, um programa de ataque pode ser escrito para manter-se dormente até receber um comando particular através de uma comunicação sem fio. Isto pode permitir aos agressores esperar até uma máquina ser usada para gravar os votos no dia da eleição antes de ativar o ataque de software.

Os agressores podem também usar comunicação sem fio para obter o controle sobre um programa de ataque previamente inserido num conjunto particular de máquinas (p. ex. trocar três votos no segundo cargo na terceira máquina), ou obter informações sobre como os eleitores estão votando comunicando-se com a máquina enquanto está sendo usada.

Finalmente, redes sem fio apresentam vulnerabilidades de segurança adicionais em jurisdições eleitorais que usam máquinas GED com VICE e VLO. Um problema logístico importante para um agressor que quer mudar tanto os registros eletrônicos quanto impressos é como fazer os novos registros impressos substituírem os velhos. Com rede sem fio, a máquina GED ou VLO pode transmitir informações específicas ao agressor sobre o que deve aparecer nesses registros impressos. Em resumo, permitir componentes de transmissão sem fio em máquinas GED com VICE ou máquinas VLO torna o trabalho do agressor muito mais simples na prática.

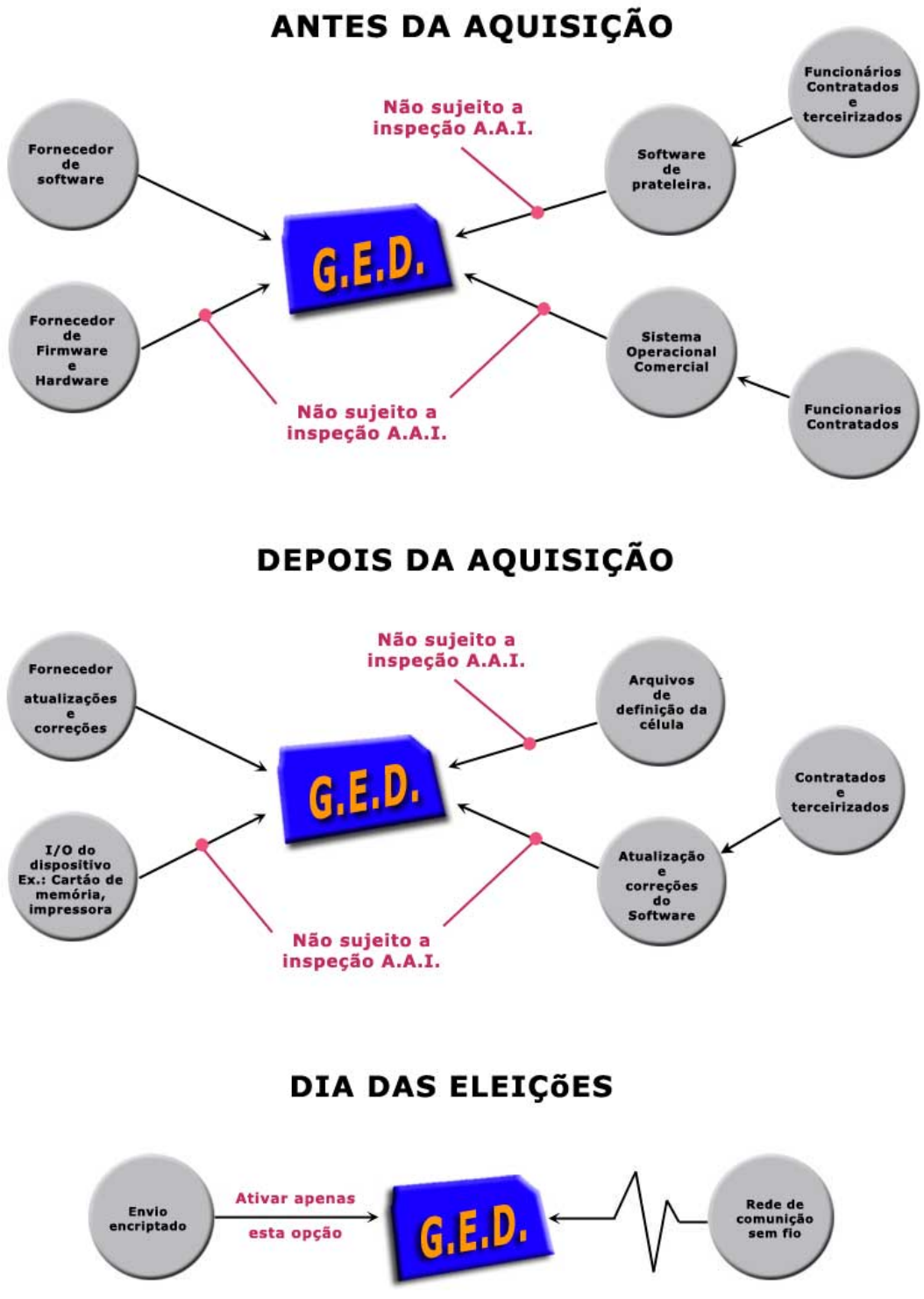
---

[6] Um "Cavalo de Tróia" é um tipo de programa de ataque ao software que simula um programa benigno.

[7] Assistentes Digitais Pessoais ("PDA" ou "palmtop") são aparelhos de mão projetados originalmente para serem agendas pessoais. Os PDA podem sincronizar seus dados com um computador.

[8] *Ver, p. ex.,* Brian Krebs, *Windows Security Flaw is 'Severe,' (Falhas de Seguranças do Windows são 'severas')* Washington Post, 30 de dezembro de 2005, em D1 (tornando pública uma falha no Microsoft Windows previamente desconhecida).

Figura 3 – PROGRAMA DE ATAQUE DE SOFTWARE: PONTOS DE ENTRADA



■■ SISTEMAS COM REGISTROS EM PAPEL AINDA ESTÃO SUJEITOS A ATAQUES.

Sistemas com Voto Impresso Conferido pelo Eleitor propiciam poucas vantagens, se alguma, sobre sistemas sem tais registros a menos que haja recontagens ou auditorias regulares com os votos impressos

Sistemas de votação com algum tipo de registro em papel verificado pelo eleitor (p. ex. máquinas GED com VICE ou VLO) oferecem uma vantagem de segurança importante contra programas de ataque ao software original não oferecida pelos sistemas de votação sem registros em papel verificados pelo eleitor (isto é, GED *sem* VICE): as jurisdições eleitorais podem efetuar uma auditoria dos registros em papel verificados pelo eleitor e compara-los com os totais de votos eletrônicos.

Infelizmente, a maioria dos Estados que exigem Votos Impressos Conferidos pelo Eleitor não exigem auditorias automáticas dos comprovantes em papel depois de cada eleição. *Nossa análise mostra que sistemas com comprovantes impressos verificáveis pelo eleitor garantem pouco ou nenhuma segurança em relação a sistemas sem esses registros, a menos que sejam feitas regularmente auditorias e/ou recontagens dos registros em papel.*

Mesmo assumindo que estas auditorias e/ou recontagens regulares sejam efetuadas, juridições que usam, ou estejam pensando em comprar máquinas GED com VICE ou VLO devem prevenir-se de ataques específicos a estes sistemas.

■■■ ATAQUES A MÁQUINAS GED COM VICE

Pelo menos um estudo sugeriu que um percentual extremamente baixo de eleitores que usam máquinas GED com VICE revisa o comprovante em papel[9].

Se esta descoberta estiver correta, um agressor poderia subverter uma recontagem ou auditoria criando um programa de ataque que faça a máquina registrar o voto errado tanto no registro eletrônico quanto no papel. Se ambos os registros forem similarmente imprecisos, conferir um contra o outro numa auditoria ou numa recontagem não evidenciará o ataque.

Na prática, é desta forma que funcionaria na eleição para governador em Pennasota:

- Quando um eleitor específico escolher Tom Jefferson, a tela mostraria que ele votou em Tom Jefferson.

- Depois de ter completado a votação em todos os cargos, a máquina GED imprimiria um papel listando as escolhas para cada cargo, exceto para governador. No cargo de governador, ela registraria que o eleitor selecionou Johnny Adams.

- Quando a máquina GED pedir ao eleitor para confirmar que o papel registrou seu voto corretamente, uma de duas coisas pode acontecer:

    - O eleitor não percebe que o papel não registrou corretamente o voto e aceita o registro em papel; ou

    - o eleitor rejeita o registro em papel e vota novamente.

[9] Ted Selker e Sharon Cohen, *An Active Approach to Voting Verification (Um Enfoque Ativo para a Verificação da Votação),* Projeto Tecnológico de Votação do CalTech/MIT, Documento de Trabalho nº28 (Maio de 2005), disponível em http://vote.caltech.edu/media/documents/wps/vtp_wp28.pdf (visitado última vez em 25 de maio de 2006).

- Se o eleitor rejeitar o registro em papel, a segunda vez ele mostrará que o eleitor votou em Tom Jefferson. Isso pode levá-lo a crer que ele selecionou inadvertidamente o candidato errado da primeira vez. De qualquer jeito, é pouco provável que ele diga a alguém que a máquina fez um erro.

Podemos imaginar o ataque visualmente desta forma:

Figura 4

Este ataque não exige nenhum participante adicional para a conspiração. Nem, como foi demonstrado no Relatório de Segurança, está claro que muito poucos eleitores perceberão os votos mal registrados para evitar que o ataque funcione.

O Relatório de Segurança detalha as contramedidas que permitem à jurisdição interceptar este ataque. Especificamente, mesmo se um pequeno percentual de eleitores perceber que a máquina registrou "erroneamente" seu voto, haverá um número grande número incomum de "cancelamentos" nos registros em papel. Uma jurisdição eleitoral que registrou e então revisou a quantidade de cancelamentos durante uma auditoria de 2% terá evidência suficiente para identificar um problema e perceber que uma investigação mais aprofundada é necessária.

Claro, incentivar os eleitores a revisar os registros em papel pode também ajudar substancialmente a reduzir o risco de um ataque bem sucedido nos registros de papel.

■ATAQUES A VLO

Uma das vantagens das máquinas VLO em relação à Apuração por Leitura Ótica Centralizada (que são freqüentemente usadas para contagem de votos de ausentes) é que elas têm uma proteção de "excesso/falta de votos". A proteção de excesso/falta em maquinas VLO funciona assim: quando

um eleitor preenche sua cédula, mas acidentalmente marca dois candidatos para o mesmo cargo (excesso) ou acidentalmente pula um cargo (falta), a máquina recusa o registro de voto e o devolve ao eleitor para verificação. O eleitor tem então a oportunidade de revisar sua cédula e corrigi-la antes de submetê-la novamente.

Já foi demonstrado que Máquinas de Apuração por Leitura Ótica Centralizada perdem muito mais votos do que máquinas VLO. Em seções com mais de 30% de eleitores afro-americanos, por exemplo, a taxa "residual" ou de votos perdidos em Máquinas de Apuração por Leitura Ótica Centralizada chegou a 4,1% comparado com 0,9% em máquinas VLO[10].

A falta de proteção por excesso/falta em Máquinas de Apuração por Leitura Ótica Centralizada pode ser o motivo para essa diferença.

Nosso agressor em Pennasota provavelmente *não* teria possibilidade de alterar os votos para governador de Jefferson para Adams apenas inserindo um programa de ataque que possa desligar a proteção de excesso/falta em máquinas VLO. Mesmo se assumirmos que o resultado de desligar a proteção seria uma perda de 4% dos votos em cada máquina, e que todos os votos iriam para Tom Jefferson, isso resultaria numa perda de apenas 20 mil votos. Isso ainda deixaria Jefferson (que ganhou por 80 mil votos) com uma margem confortável (embora mais estreita) de vitória.

Não obstante, este ataque poderia causar a perda de milhares de votos. Há pelo menos três meios possíveis de interceptar este ataque:

■Teste de Votação Paralela (assumindo que o programa de ataque não tenha descoberto um meio de se desligar quando ele estiver sendo testado);

■Testes periódicos da proteção de excesso/falta no dia da eleição;

■Contagem de excesso/falta durante uma auditoria dos comprovantes impressos verificados pelo eleitor para determinar se há uma quantidade desproporcional de votos perdidos.

[10] Lawrence Norden *et al.*, *Voting System Usability (Usabilidade dos Sistemas de Votação), em* THE MACHINERY OF DEMOCRACY (a ser publicado em julho de 2006) (pesquisa original pelo Prof. David Kimball).

RECOMENDAÇÕES DE SEGURANÇA

Existe uma possibilidade substancial de que os procedimentos e contramedidas atualmente em vigor na maioria dos Estados não detectem um programa de ataque ao software original projetado com inteligência. Os procedimentos para Rotina Automática de Auditoria para Teste de Votação Paralela propostos no Relatório de Segurança são ferramentas importantes para defender os sistemas de votação de muitos tipos de ataques, incluindo programas de ataque ao software original.

Muitas jurisdições eleitorais não implementaram medidas de segurança deste tipo. Dos 26 estados que exigem Votos Impressos Conferidos pelo Eleitor, somente 12 exigem Auditorias Automáticas destes votos, e somente dois – Califórnia e Washington – efetuam Testes de Votação Paralela[11].

Além disso, mesmo aqueles estados que implementaram estas contramedidas não desenvolveram as melhores práticas e protocolos necessários para assegurar sua eficácia em prevenir ou revelar ataques ou falhas nos sistemas de votação.

RECOMENDAÇÃO Nº 1:

■ EFETUAR AUDITORIAS AUTOMÁTICAS DE ROTINA DOS VOTOS EM PAPEL

Os defensores do Voto Impresso Conferido pelo Eleitor têm tido muito sucesso nas assembléias legislativas por todo o país. Atualmente, 26 estados exigem que seus sistemas de votação produzam um comprovante verificável pelo eleitor, mas 14 destes estados não exigem auditorias automáticas de rotina[12]. A Força-Tarefa concluiu que o comprovante em papel independente conferido pelo eleitor sem uma Rotina Automática de Auditoria, tem um valor de segurança questionável[13].

Em contrapartida, um Voto Impresso Conferido pelo Eleitor acompanhado de uma sólida Rotina Automática de Auditoria pode ser um bom caminho para tornar os ataques mais simples, bem mais difíceis. Especificamente, as medidas recomendadas abaixo forçariam um agressor a envolver centenas de participantes mais ativos em seu ataque.

■Um pequeno percentual de todas as máquinas de votação e seus Votos Impressos Conferidos pelo Eleitor deve ser auditado.

■As máquinas a serem auditadas devem ser selecionadas de modo aleatório e transparente.

■A indicação dos auditores das máquinas de votar deve ocorrer imediatamente antes da auditoria. A auditoria deve ser feita às 9 hs da manhã do dia seguinte ao encerramento da eleição.

■A auditoria deve incluir uma contagem de votos descartados (no caso de Votos Impressos cancelados pelo eleitor), votos excedentes e faltando.

---

[11] O Estado de Maryland, que não exige Voto Impresso Conferido pelo Eleitor, também efetua Testes de Votação Paralela em nível estadual. Os 12 Estados que devem efetuar auditorias automáticas dos votos em papel são: Alasca, Califórnia, Carolina do Norte, Colorado, Connecticut, Havaí, Illinois, Minnesota, Novo México, Nova Iorque, Virgínia do Oeste e Washington.

[12] Os 26 Estados são: Alasca, Califórnia, Colorado, Connecticut, Havaí, Idaho, Illinois, Maine, Michigan, Minnesota, Missouri, Montana, Carolina do Norte, New Hampshire, Nova Jérsei, Novo México, Nevada, Nova Iorque, Ohio, Oregon, Dakota do Sul, Utah, Vermont, Washington, Wisconsin e Virgínia do Oeste.

[13] As leis que prevêem recontagens baratas por iniciativa do candidato podem, também, acrescentar segurança para o Voto Impresso Conferido pelo Eleitor. A Força-Tarefa não examinou estas recontagens como uma contramedida potencial.

■Deve ser efetuado um exame estatístico de anomalias, tais como cancelamentos e votos excedentes e faltando acima do esperado.

Sólidas práticas com relação à guarda e segurança física dos votos em papel antes da Rotina Automática de Auditoria devem ser seguidas.

RECOMENDAÇÃO Nº 2:

■ EFETUAR TESTES DE VOTAÇÃO PARALELA

Não é possível efetuar uma auditoria dos comprovantes em papel em máquinas GED sem VICE, porque os Votos Impressos Conferidos pelo Eleitor não existem nessas máquinas. Isto significa que jurisdições eleitorais que usam máquinas GED sem VICE não têm acesso a uma contramedida importante e poderosa.

Para máquinas GED sem papel, o Teste de Votação Paralela é provavelmente o melhor meio de detectar ataques ao software original, assim como erros sutis de programação que não puderam ser percebidos durante a inspeção e outros testes. Para máquinas GED com VICE e dispositivos marcadores de cédulas, o Teste de Votação Paralela dá a oportunidade de descobrir um tipo específico de ataque (por exemplo, a impressão da escolha errada no voto impresso a ser conferido pelo eleitor) que não pode ser detectado simplesmente revisando os registros em papel depois de terminada a eleição. Entretanto, mesmo nas melhores circunstâncias, o Teste de Votação Paralela é uma medida de segurança imperfeita. O teste cria uma "corrida armada" entre os testadores e o agressor, mas os testadores nunca podem ter a certeza de que eles ganharam.

Concluímos que os passos a seguir tornarão o Teste de Votação Paralela mais eficaz:

■As técnicas precisas usadas para Teste de Votação Paralela (p. ex. exatamente como e quando a máquina é ativada, como códigos de ativação/flash cards/*etc*. são produzidos para permitir a votação, *etc*.) não devem ser totalmente determinadas ou reveladas até imediatamente antes da eleição. Detalhes de como o Teste de Votação Paralela é feito devem mudar a cada eleição.

■Pelo menos duas de cada tipo de máquina GED (significando tanto fabricante quanto modelo) devem ser selecionadas para Testes de Votação Paralela.

■Pelo menos duas máquinas GED das três maiores comarcas de cada Estado devem passar por Testes de Votação Paralela.

■As localidades devem ser notificadas o mais tarde possível que máquinas de suas seções foram selecionadas para Teste de Votação Paralela.

- Canais de comunicação sem fio de máquinas de votar devem estar desligados para assegurar que não possam receber comandos. Máquinas com componente de comunicação sem fio são particularmente vulneráveis ao ataque.

■Máquinas de votar nunca devem ser conectadas a outras durante a votação. Algumas máquinas GED com ou sem VICE podem ser projetadas para não funcionar se não estiverem conectadas a outras. Os funcionários eleitorais devem discutir esta questão com os fornecedores de sistemas de votação.

■Máquinas de votar devem estar completamente isoladas durante a eleição, e devem imprimir ou mostrar seus totais antes de serem conectadas a algum servidor central para enviar seus totais.

■Os roteiros de Teste de Votação Paralela devem incluir detalhes, tais como a rapidez ou lentidão da votação, quando "cometer erros" e talvez até quando depositar cada voto.

■O Teste de Votação Paralela deve ser filmado para assegurar que a contradição entre registros eletrônicos e em papel quando o Teste de Votação Paralela estiver terminado não é o resultado de um erro do testador.

Embora poucas jurisdições eleitorais tenham tomado o cuidado de efetuar Testes de Votação Paralela limitados, sabemos de três Estados, Califórnia, Maryland e Washington, que efetuam Testes de Votação Paralela regularmente numa base estadual. Vale notar que dois destes Estados, Califórnia e Washington, empregam Auditorias Automáticas de Rotina *e* Testes de Votação Paralela como contramedidas estaduais contra possíveis ataques.

RECOMENDAÇÃO Nº 3:

■ PROIBIR COMPONENTES DE TRANSMISSÃO SEM FIO EM TODAS AS MÁQUINAS DE VOTAÇÃO.

Nossa análise mostra que máquinas com componentes de transmissão sem fio são particularmente vulneráveis a ataques. Concluímos que esta vulnerabilidade se aplica aos três sistemas de votação. Somente dois Estados, Nova Iorque e Minnesota, proibiram componentes de transmissão sem fio em todas as máquinas[14]. A Califórnia também proibiu componentes de transmissão sem fio, mas somente em máquinas GED. Componentes de transmissão sem fio não devem ser permitidos em nenhuma máquina.

RECOMENDAÇÃO Nº 4:

■ EXIGIR PROCEDIMENTOS DE AMOSTRAGEM TRANSPARENTES E ALEATÓRIOS.

O desenvolvimento de procedimentos de amostragem transparentes e aleatórios para todas as auditorias é primordial para a eficácia da auditoria. Isto inclui a escolha das máquinas para serem auditadas ou testadas em votação paralela, assim como a indicação dos próprios auditores. O uso de procedimentos de amostragem transparentes e aleatórios permite ao público saber que o método de auditoria foi justo e substancialmente passível de descobrir fraudes ou erros nos totais de votação. Em nossas entrevistas com funcionários eleitorais nós descobrimos que muito freqüentemente o processo para selecionar máquinas e auditores não era nem transparente nem aleatório.

Num processo de amostragem transparente e aleatório:

■O processo todo é publicamente observável e gravado em fita.

■A amostragem aleatória é publicamente verificável, isto é, qualquer um que a observe é capaz de verificar que a amostra foi escolhida aleatoriamente (ou pelo menos que o número escolhido não está sob o controle de um pequeno número de pessoas).

- O processo é simples e prático dentro do contexto da prática de eleição atual de modo a evitar encargos desnecessários aos funcionários das eleições.

[14] Dois outros Estados, Virgínia do Oeste e Maine, proíbem o uso de máquinas em rede sem proibir especificamente os componentes de transmissão sem fio. Proibir o *uso* de componentes de transmissão sem fio (mesmo quando isso envolve seu desligamento), em vez de exigir a *remoção* destes componentes, continua deixando os sistemas de votação desnecessariamente inseguros. Entre outros motivos, um programa de ataque ao software pode ser projetado para reativar qualquer componente de transmissão sem fio desligado.

RECOMENDAÇÃO Nº 5:

■ ASSEGURAR A DESCENTALIZAÇÃO DA PROGRAMAÇÃO E DA ADMINISTRAÇÃO DOS SISTEMAS DE VOTAÇÃO.

Quando uma única entidade, como um fornecedor ou uma autarquia de nível nacional ou estadual efetuar tarefas chave (como produzir arquivos de definição de candidatos) para várias jurisdições eleitorais, ataques em nível global se tornam mais fáceis. O controle centralizado desnecessário oferece muitas oportunidades para implementar ataques em múltiplas localidades.

RECOMENDAÇÃO Nº 6:

■ IMPLEMENTAR PROCEDIMENTOS EFICAZES PARA TRATAR EVIDÊNCIAS DE FRAUDE OU ERRO

Tanto Auditorias Automáticas de Rotina quanto Teste de Votação Paralela têm um valor de segurança questionável sem procedimentos eficazes de ações quando uma evidência de mau funcionamento de máquina e/ou fraude for descoberta. Detecção de fraude sem uma resposta apropriada não impedirão ataques de terem sucesso. Na revisão minuciosa das leis e práticas eleitorais estaduais no Centro Brennan, e durante as entrevistas com funcionários eleitorais para a análise de ameaças, não encontramos nenhuma jurisdição eleitoral com procedimentos detalhados publicamente, adequados e práticos para tratar das evidências de fraude ou erro descobertas durante uma auditoria, recontagem ou Teste de Votação Paralela.

Abaixo estão exemplos de procedimentos que permitiriam às jurisdições eleitorais responder eficazmente à detecção de erros ou a programas de ataque ao software em Testes de Votação Paralela:

■Impor e efetuar uma perícia técnica transparente em todas as máquinas que mostrarem discrepâncias inexplicáveis durante o Teste de Votação Paralela.

■Quando a evidência de um erro ou ataque for descoberta (ou nenhuma explicação plausível para a discrepância for dada), efetuar uma perícia técnica em todas as máquinas GED usadas no estado durante a eleição[15].

■Identificar as máquinas que mostram evidência de adulteração ou falha de software que possa ter afetado a contagem eletrônica dos votos.

■Revisar a margem de vitória reportada em cada cargo potencialmente afetado. Baseado em (a) margem de vitória, (b) quantidade de máquinas afetadas e (c) natureza e escopo da adulteração ou da falha, determinar se existe a possibilidade substancial que a adulteração ou a falha possa ter mudado o resultado da eleição a um cargo específico.

■Quando houver uma probabilidade substancial que a adulteração possa ter mudado o resultado da eleição a um cargo específico, marcar uma nova eleição para esse cargo.

---

[15] *Ver* RECOMMENDATIONS OF THE BRENNAN CENTER FOR JUSTICE AND THE LEADERSHIP CONFERENCE ON CIVIL RIGHTS FOR IMPROVING RELIABILITY OF DIRECT RECORDING ELECTRONIC VOTING SYSTEMS (2004), *disponível em* http://www.brennancenter.org/programs/downloads/voting_systems_final_recommendations.pdf (última vez visitado em 25 de maio de 2006) (recomendando que as zonas eleitorais contratem especialistas em segurança independentes e criem painéis de fiscalização de segurança independentes para implementar e vigiar medidas de segurança). Especialistas em segurança independentes e membros do painel de fiscalização devem estar presentes durante qualquer investigação judicial para aumentar a transparência.

Abaixo está um conjunto ilustrativo de procedimentos que permitiriam às jurisdições eleitorais responder eficazmente às discrepâncias entre os registros eletrônicos e em papel durante uma Rotina Automática de Auditoria:

■Efetuar uma perícia transparente de todas as máquinas onde os registros eletrônicos e em papel não batem para determinar se há alguma evidência que ocorreu uma adulteração dos registros em papel.

- Na certeza de não haver evidência de que os votos em papel tenham sido adulterados, acatar os resultados dos votos em papel.

■Se houver evidência de que os votos em papel tenham sido adulterados, conceder a presunção de legitimidade aos registros eletrônicos.

■Depois de ter concedido a presunção de legitimidade aos registros eletrônicos, efetuar uma perícia judicial em todas as máquinas onde os registros eletrônicos e em papel não bateram para determinar se há alguma evidência que ocorreu uma adulteração dos registros eletrônicos.

■Se a adulteração dos registros eletrônicos puder ser descartada, acatar os resultados os registros eletrônicos[16].

■Quando houver evidência de que tanto os registros eletrônicos quanto os de papel tiverem sido adulterados, efetuar uma recontagem total para determinar se, e em que medida, os registros eletrônicos e em papel não podem ser reconciliados.

■Na conclusão da recontagem total, determinar a quantidade total de máquinas que reportam registros eletrônicos e em papel diferentes.

■Depois de quantificar a quantidade de máquinas que foram adulteradas, determinar a margem de vitória para cada cargo potencialmente afetado.

- Baseado em (a) margem de vitória, (b) quantidade de máquinas afetadas e (c) natureza e escopo da adulteração ou da falha, determinar se existe a possibilidade substancial que a adulteração ou a falha possa ter mudado o resultado da eleição a um cargo específico.

- Quando houver uma probabilidade substancial que a adulteração possa ter mudado o resultado da eleição a um cargo específico, marcar uma nova eleição para esse cargo.

[16] Quando a legislação de um Estado determinar que deve ser dada presunção de legitimidade aos registros eletrônicos, o processo reverso deve ser seguido: primeiro investigar os registros eletrônicos para adulteração e, se necessário, examinar os registros em papel.

CONCLUSÃO

A Força-Tarefa descobriu que os três sistemas de votação mais comumente adquiridos hoje em dia são vulneráveis a ataques e erros que podem mudar o resultado de eleições majoritárias. Esta descoberta não deve surpreender ninguém. Uma revisão da história na literatura das fraudes eleitorais e dos sistemas de votação nos Estados Unidos mostra que os sistemas de votação sempre foram vulneráveis a ataques. Na verdade, é impossível imaginar um sistema de votação que seja imune a ataques.

Mas existem contramedidas objetivas que podem reduzir substancialmente os riscos de segurança mais sérios apresentados pelos três sistemas.

As recomendações da Força-Tarefa apontam o caminho para as jurisdições eleitorais com desejo político de proteger de ataques os seus sistemas de votação. Nenhuma das medidas aqui identificadas – Auditoria dos Votos Impressos Conferidos pelo Eleitor, proibição de componentes de transmissão sem fio, uso de procedimentos de auditoria transparentes e de amostragem aleatórias, adoção de políticas eficazes para tratar de evidências de fraude ou erro nos totais de votos, execução de Testes de Votação Paralela – é particularmente difícil ou cara para implementar[17]. O Centro Brennan incentiva os funcionários de eleições e os legisladores a adotar as medidas de segurança recomendadas o mais rápido possível.

[17] Mesmo rotineiros Testes de Votação Paralela e Auditorias com os Votos Impressos Conferidos pelo Eleitor – talvez as mais caras e demoradas contramedidas vistas na análise conjunta de ameaças – mostraram ser bastante econômicas. Jocelyn Whitney, Desenvolvedor e Gerente de Projeto para atividades de Teste de Votação Paralela no Estado da Califórnia, forneceu ao Centro Brennan os dados mostrando que o custo total do teste paralelo na Califórnia foi de aproximadamente *12 centavos de dólar por voto* dado em máquinas GED. E-mail de Jocelyn Whitney a Lawrence Norden, Conselheiro Associado, Centro Brennan de Justiça (25 de fevereiro de 2006) (arquivado no Centro Brennan). Harvard L. Lomax, do Cartório Eleitoral da Comarca de Clark, Nevada, estima que uma equipe de auditores pode revisar 60 votos impressos numa seção de quatro horas. Assumindo que os auditores são pagos a 12 dólares por hora e que cada equipe tem dois auditores, o custo destas auditorias deve ser pouco mais de *3 centavos de dólar por voto*, se 2% dos votos forem auditados. Harvard L. Lomax entrevistado por telefone por Eric L. Lazarus e Lawrence Norden (23 de março de 2006). Cada um destes custos representa uma fração minúscula do que a zona eleitoral já gasta anualmente com as eleições. O estudo de custos de sistemas de votação do Centro Brennan de Justiça mostra que, por exemplo, a maioria das zonas eleitorais gasta bem mais do que isso imprimindo cédulas (cerca de 92 centavos de dólar por cédula), programando máquinas (freqüentemente mais de 30 centavos de dólar por voto por eleição), ou armazenando e transportando sistemas de votação. Lawrence Norden, *Voting System Cost (Custos de Sistemas de Votação), em* THE MACHINERY OF DEMOCRACY (a ser lançado em julho de 2006).

CONSELHO DE DIRETORES E FUNCIONÁRIOS DO CENTRO BRENNAN DE JUSTIÇA

CENTRO BRENNAN DE JUSTIÇA

DA FACULDADE DE DIREITO DA UNIVERSIDADE DE NOVA IORQUE

161 Avenue of the Americas

12th Floor

New York, NY 10013

212-998-6730

www.brennancenter.org