Une analyse de sécurité du système d'information “expérience électronique sécurisée d'inscription électorale et de vote", ou SERVE (Secure Electronic Registration and Voting Experiment).

21 janvier 2004

[traduction en français non officielle, les [] sont des ajouts du traducteur]

[l'original modifié est en http://www.servesecurityreport.org/paper.pdf]

Dr. David Jefferson, d_jefferson@yahoo.com
Dr. Ariel D. Rubin, rubin@jhu.edu
Dr. Barbara Simons, simons@acm.org
Dr. David Wagner, daw@cs.berkeley.edu

Sommaire pour responsables (Executive Summary)

Ce rapport est une revue et une analyse critique des problèmes de sécurité informatique et réseaux [SSI] de l'expérience d'inscription et de vote électronique sécurisés (SERVE: Secure Electronic Registration and Voting Experiment), un système de vote à travers internet en cours de construction dans le cadre du programme fédéral d'aide au vote (FVAP Federal Voting Assistance Program) pour le département de la Défense des États-Unis. Le site Web du programme est http://www.serveusa.gov/. Bien que ce système soit appelé une expérience, il va être employé pour décompter de vraies voix dans les prochaines élections générales. Les auteurs [de ce rapport] sont les membres du groupe d'examen par les experts de sécurité ("SPRG Security Peer Review Group"), une réunion d'experts en matière de sécurité d'élections électroniques qui a été choisie par le FVAP pour l'assister dans l'évaluation de la sécurité du système SERVE. Notre tâche a été d'identifier des vulnérabilités potentielles que le système pourrait avoir face à des agressions SSI variées ("cyber-attaques"), d'évaluer les niveaux des risques qu'ils représentent pour l'intégrité d'une élection, et de faire des recommandations au sujet des moyens d'atténuer ou supprimer ces risques.

Le système SERVE est prévu pour un déploiement dans les élections primaires de 2004 et dans les élections générales, et il permettra aux électeurs qui y auront accès d'abord de s'enregistrer pour voter dans la circonscription de leur domicile, et ensuite pour voter, de façon entièrement électronique à travers l'internet depuis n'importe où dans le monde. À côté de sa limitation aux électeurs d'outre-mer et au personnel militaire, le système SERVE est pour l'instant limité aux personnes qui votent dans l'un des de cinquante comtés choisis dans les sept États suivants qui participent [à l'expérience]: Arkansas, Floride, Hawaï, Caroline du Nord, Caroline du Sud, Utah et Washington. On s'attend à ce que le programme traite jusqu'à 100.000 voix cette année, y compris les primaires et l'élection générale. (Pour comparer, approximativement 100 millions de voix ont été exprimées dans les élections générales de l'année 2000.) Le but final du système SERVE est de traiter la totalité de la population des citoyens d'outre-mer concernés plus des militaires et des personnes à charge. On estime que cette population s'élève environ à 6 millions, ainsi la mise en œuvre en 2004 du système SERVE doit être considéré comme un prototype pour un futur système possible très important en taille.

Nos conclusions sont résumées comme suit :

a) Les systèmes de vote électroniques dits DRE (enregistrement direct électronique) ont été largement critiqués ailleurs pour différentes insuffisances et vulnérabilités de sécurité : leur logiciel est totalement fermé et propriété [d'une entreprise] ; ce logiciel ne subit qu'un examen minutieux insuffisant pendant la qualification et la certification ; ils sont particulièrement vulnérables à diverses formes d'attaques d'initiés (de programmeur) ; et ces DREs n'ont aucun journal de contrôle a posteriori vérifiable par les électeurs (sur papier ou autrement) qui pourrait en grande partie éviter ces problèmes et améliorer la confiance des électeurs. Toutes ces critiques, que nous approuvons, s'appliquent tout autant directement au système SERVE.

b) Mais de plus, comme le système SERVE est à la fois un système sur internet et un système à base de micro-ordinateurs personnel de type PC, il a de nombreux autres problèmes fondamentaux de sécurité qui le laissent vulnérable à une variété d'attaques bien connues sur les réseaux ("cyber attacks") (attaques d'initié, refus/déni de service, mascarade ("spoofing"), achats automatisés de voix, attaques virales sur des PC des électeurs, etc.), chacune d'entre elles pourrait être catastrophique.

c) De telles attaques pourraient se produire à une grande échelle, et pourraient être lancées par n'importe qui, depuis un mécontent isolé jusqu'à à une agence ennemie bien financée et hors d'atteinte des lois des États-Unis. Ces attaques pourraient avoir comme conséquence des privations de droits civiques sélectives et à grande échelle pour des électeurs, et/ou la violation du secret électoral, et/ou les achats et ventes de voix, et/ou le changement de la valeur de la voix allant jusqu'au point de renverser les résultats de beaucoup d'élections en une fois, y compris l'élection présidentielle. Si elles sont soigneusement conçues, certaines des attaques pourraient réussir et pourtant rester complètement non détectées. Même si elles sont détectées et neutralisées, de telles attaques pourraient avoir un effet dévastateur sur la confiance publique en matière d'élections.

d) Il est impossible d'estimer la probabilité d'une attaque réseau réussie ("cyber attacks") ou d'attaques réussies multiples sur une élection donnée. Mais nous montrons que les attaques qui nous causent le plus de soucis sont tout à fait faciles à commettre. Dans certains cas il y a des ensembles d'outils ("kits") faciles à accéder sur l'internet qui pourraient être modifiés ou employés tels quels pour attaquer une élection. Et nous devons considérer le fait évident qu'une élection générale aux États-Unis offre l'une des cibles les plus tentantes pour une attaque réseau ("cyber attack") dans l'histoire de l'internet, que le motif de l'attaquant soit manifestement politique ou simplement sa propre gloriole.

e) Les vulnérabilités que nous décrivons ne peuvent pas être réparées par des changements dans l'architecture du système SERVE ou des corrections d'erreurs du système SERVE. Ces vulnérabilités sont fondamentales dans l'architecture de l'internet ainsi que dans le matériel et le logiciel des micro-ordinateurs personnels de type PC qui

est omniprésent aujourd'hui. Elles ne peuvent pas toutes être éliminées dans un avenir prévisible sans un saut qualitatif radical imprévu. Il est tout à fait possible qu'elles ne seront pas éliminées sans une nouvelle architecture et un remplacement d'une grande partie des matériels et des logiciels de sécurité qui font partie ou qui sont reliées à l'internet d'aujourd'hui.

f) Nous avons examiné de nombreuses variantes pour le système SERVE afin d'essayer de recommander un système de vote sur internet solution de remplacement qui serait légèrement moins confortable pour l'électeur en échange d'une diminution du nombre et de la gravité des vulnérabilités de sécurité. Cependant, toutes ces variantes souffrent des mêmes natures de vulnérabilités fondamentales que le système SERVE ; nous regrettons, mais nous ne pouvons recommander aucune de ces variantes. Nous suggérons une architecture de kiosque comme point de départ pour concevoir [reconstruire] un système alternatif de vote avec des objectifs semblables à ceux de SERVE, mais qui ne s'appuie ni sur l'internet ou ni sur les logiciels non sûrs des PC (annexe C).

g) Le système SERVE pourrait sembler fonctionner sans incidents en 2004, sans attaques réussies détectées. Il est aussi malheureux qu'inévitable qu'une expérience de vote apparemment réussie dans une élection présidentielle des États-Unis impliquant sept états serait considérée par la plupart des personnes comme une preuve forte que le système SERVE est un système de vote fiable, robuste, et sûr. Des tels résultats encourageraient l'extension du programme par FVAP dans des élections futures, ou la commercialisation du même système de vote par des fournisseurs aux juridictions électorales dans tous les États-Unis, et aussi bien dans d'autres pays.

   Cependant, le fait qu'aucune attaque réussie n'est détectée ne signifie pas qu'aucune ne s'est produite. De nombreuses attaques seraient extrêmement difficiles à détecter, en particulier, si elles sont habilement dissimulées, même dans les cas où elles modifient les résultats d'une élection importante. En outre, l'absence d'une attaque réussie en 2004 ne signifie pas que les attaques réussies seraient moins potentielles à l'avenir; tout au contraire, les attaques futures seraient potentiellement plus réelles, à la fois parce qu'il y a plus de temps pour préparer l'attaque, et parce que l'augmentation de l'utilisation du système SERVE ou de systèmes semblables rendrait le gain plus intéressant. En d'autres termes, un essai "réussi" du système SERVE en 2004 est le haut d'une pente glissante vers des systèmes encore plus vulnérables à l'avenir. (L'existence du système SERVE a été déjà citée comme une justification du vote à travers l'internet dans les primaires du parti démocrate au Michigan [février 2004].)

h) Tout comme les partisans du système SERVE, nous croyons qu'il devrait y avoir un meilleur soutien pour le vote de nos soldats outre-mer. Cependant, nous regrettons de devoir être contraints de conclure que la meilleure voie est de ne pas employer du tout le système SERVE. Puisque le danger des attaques réussies et à grande échelle est si important, nous recommandons à contre-cœur d'arrêter immédiatement le développement du système SERVE et de n'essayer dans le futur aucune solution semblable tant que les deux infrastructures mondiales, celle l'internet et celle de l'ordinateur personnel, n'ont pas été fondamentalement remodelées, ou que quelques autres avancées imprévues de sécurité ne soient apparues.

Nous voulons rendre clair qu'en recommandant que le système SERVE soit fermé, nous n'adressons aucune critique au FVAP, ou à Accenture, ou à qui que ce soit de leurs personnels ou de leurs sous-traitants. Ils ont été complètement conscients tout au long [du projet] des problèmes de sécurité que nous décrivons ici, et nous avons été impressionnés par la sophistication de l'ingénierie et les compétences techniques qu'ils ont consacrées aux tentatives d'amélioration [de la sécurité] et d'élimination des vulnérabilités. Nous ne croyons pas qu'un projet organisé différemment puisse faire un meilleur travail que l'équipe actuelle. La vraie barrière pour le succès n'est pas un manque de vision, de compétences, de ressources, ou de niveau d'engagement ; c'est le fait que, étant donné [d'une part] le niveau technique actuel de la sécurité de l'internet et des micro-ordinateurs de type PC, et [d'autre part] les objectifs [de sécurité] d'un système de vote à distance sécurisé et tout-électronique, le FVAP a entrepris une tâche par nature impossible. Il n'y a vraiment aucune bonne manière de construire un tel système de vote sans un changement radical de l'architecture globale de l'internet et du PC, ou une certaine avancée imprévue de sécurité. Le projet du système SERVE est ainsi beaucoup trop en avance sur son temps, et devrait attendre tant qu'il n'y a pas une infrastructure solide sur laquelle construire.

1. Introduction

Ce rapport est une revue critique des problèmes de sécurité des systèmes d'information (informatique et réseaux) du système de vote dit SERVE (expérience électronique sécurisée d'enregistrement et de vote), un système de vote s'appuyant sur internet construit par Accenture et ses sous-traitants pour le FVAP (programme fédéral d'aide au vote) du département de la Défense des États-Unis. La mission du FVAP est de réduire les obstacles au vote pour tous les citoyens couverts par la loi UOCAVA (Uniformed and Overseas Citizens Absentee Voting Act) les citoyens outre-mer ou sous l'uniforme. UOCAVA couvre les services sous l'uniforme : les citoyens des États-Unis qui sont des membres des services en tenue ainsi que les membres de leurs familles, et les citoyens d'outre-mer: les citoyens des États-Unis qui résident hors des États-Unis. Les services en tenue comprennent les forces armées par États-Unis (armée de terre, marine, troupe de marine, armée de l'air et garde côtier), agent de la marine marchande, corps du service de santé publique (PHS) et de la météorologie nationale (NOAA).

Un groupe d'experts en matière de sécurité des systèmes d'information pour les élections, appelé le groupe d'examen par les pairs de sécurité (SPRG: Security Peer Review Group) a été rassemblé par le FVAP pour aider à évaluer le système SERVE. La tâche était d'identifier des vulnérabilités potentielles que le système pourrait présenter face à diverses types d'agressions (''cyber-attacks''), afin d'évaluer les risques que ces attaques représentent pour l'intégrité d'une élection, et afin de faire des recommandations au sujet de la façon d'atténuer ou d'éliminer ces risques.

L'analyse et les conclusions décrites ici s'appuient sur deux réunions de trois jours du groupe SPRG avec les commanditaires de FVAP et les architectes techniques primaires du système SERVE ; celles-ci ont eu lieu en juillet 2003 au Caltech à Pasadena en Californie, et en novembre 2003 chez Accenture à Reston en Virginie. Les auteurs de ce rapport sont le sous-ensemble [des personnes] du groupe SPRG qui ont assisté aux deux réunions. Beaucoup de problèmes et d'améliorations d'architectures ont été proposées et acceptées lors de ces réunions; ce rapport se focalise sur les problèmes restants qui n'ont pas été résolus.

1.1 Qu'est-ce que le système SERVE?

Une partie de la mission du programme FVAP est de réduire les obstacles à l'inscription sur les listes électorales et au vote pour deux groupes d'électeurs concernés: (1) les citoyens américains vivant hors des États-Unis, et (2) les personnels militaires et les personnes à leur charge, indépendamment du fait qu'ils résident aux États-Unis ou outre-mer. Pour des Américains qui vivent outre-mer, voter peut être une tâche décourageante; elle peut prendre cinq allers-retours ou plus à travers les services des postes des États-Unis et de l'étranger pour demander les fiches d'inscriptions électorales et les votes par correspondance du comté d'origine, de les recevoir et puis de leur renvoyer -un processus qui prend du temps et est incertain au mieux, et doit être accompli en temps utile pour éviter de manquer des dates-limites légales. Le processus est si malcommode pour les soldats qui sont mobiles, ou qui sont localisés à un endroit où le service des postes est mauvais, qu'on pense que leurs taux participation sont très faibles.

Le système SERVE est prévu pour une mise en œuvre dans les élections primaires et générales de 2004, et il est conçu pour permettre à des électeurs concernés par la loi UOCAVA à la fois de s'inscrire sur les listes électorales dans leurs districts d'origines, et également pour voter, de façon entièrement électronique par le canal de l'internet, depuis n'importe où dans le monde. Bien qu'il soit désigné par le programme FVAP sous le nom d'une expérience, et soit considéré de cette façon par ses développeurs/producteurs, il est important de se rendre compte que ce n'est pas simplement un essai ou une simulation d'un système de vote. Le système SERVE sera un système de vote complet, d'échelle moyenne, qualifié au niveau fédéral et certifié par l'État, et il traitera de vraies voix.

Pour participer, un électeur concerné doit d'abord s'inscrire dans le programme du système SERVE, ce qui peut être fait complètement par voie électronique si l'électeur a l'identification appropriée des militaires (une carte commune d'accès), ou en présentant les documents appropriés de citoyenneté et d'identification face à face avec un agent de confiance, par exemple un officier militaire ou tout autre fonctionnaire désigné qui joue un rôle semblable à celui d'un notaire public. Après l'enregistrement [dans le système], l'électeur pourra s'inscrire pour voter, et puis voter, en une ou deux sessions courtes depuis n'importe quel micro-ordinateur de type PC relié à internet. Le micro-ordinateur de type PC doit utiliser un système d'exploitation de Microsoft Windows et le butineur internet Explorer ou Netscape. Le butineur doit être configuré pour permettre l'utilisation de Javascript et Java ou de scripts ActiveX, et il doit également autoriser l'échange de "cookies" (biscuits de session) ; cependant, aucun matériel ou logiciel additionnel n'est exigé.

Le système SERVE est architecturé comme un service de la Toile (''Web-based Service)''. Les électeurs se connectent à un serveur central en utilisant un butineur habituel, comme décrit ci-dessus. L'enregistrement et le vote sont accomplis à travers l'interface de la Toile (''Web''). Le système SERVE exige une interaction directe entre le service de vote et le responsable local des élections (LEO: Local Election Officer) dans les circonscriptions électorales d'origine. Ainsi, quand

les personnes s'enregistrent pour voter, leurs données sont conservées sur le serveur central sur la Toile pour un télédéchargement ultérieur par le responsable local des élections, qui à ce moment-là met à jour sa base de données. Quand quelqu'un vote pour l'élection, le bulletin de vote complet est stocké sur le serveur central, et plus tard téléchargé par le reponsable local des élections qui le conserve pour la scrutation [des votes] à venir.

La communication entre le butineur de l'utilisateur et l'application de vote sur le serveur central est protégée en utilisant le chiffrement et l'authentification construits dans le protocole sécurisé de la couche SSL (Secure Socket Layer). Une fois que ce raccordement est établi, un contrôle ActiveX (décrit plus loin) est téléchargé sur le micro-ordinateur de type PC de l'électeur, parce que l'application de vote exige des fonctions qui ne sont pas disponibles dans les butineurs courants. Pour les utilisateurs de Netscape, une appliquette Java interprète le contrôle ActiveX. Pour des utilisateurs d'internet Explorer, le contrôle ActiveX s'exécute directement sur la machine de l'électeur.

Au- delà de la limitation aux électeurs d'outre-mer et au personnel militaire, le système SERVE 2004 sera limité pour les électeurs de 50 comtés dans les sept états (Arkansas, la Floride, Hawaï, la Caroline du Nord, la Caroline du Sud, Utah, et Washington) qui ont accepté de participer. On s'attend à ce que l'essai de 2004 traite jusqu'à 100.000 voix cette année, y compris les primaires et l'élection générale. (Par comparaison, approximativement 100 millions de voix ont été exprimées dans les élections générales de l'année 2000.)

Cependant, l'un des buts du système SERVE est de déterminer si un système semblable pourrait convenir, et être étendu à l'avenir à tous les électeurs d'outre-mer. La totalité des citoyens d'outre-mer concernés plus les militaires et les personnes à charge est estimé à environ 6 millions d'électeurs. En outre, des systèmes semblables au système SERVE pourraient par la suite être proposés par Accenture ou d'autres fournisseurs à la certification dans beaucoup plus d'États, et avec cette fois un emploi généralisé à tous les électeurs, au lieu simplement d'une population limitée. Pour ces raisons, nous analysons le système SERVE non pas comme une expérience, mais comme un système de vote réel dont l'emploi pourrait être sensiblement étendu dans les années futures.

1.2 Une brève histoire du vote sur l'internet.

Le système SERVE est le successeur d'un système de vote FVAP antérieur appelé VOI (voter par internet; “VOI: Voting Over the internet”). VOI a été construit par un autre titulaire de marché (Booz-Allen & Hamilton) et a utilisé une autre architecture et une base de programmes différents, de sorte que VOI et SERVE ne peuvent être comparés que d'une manière générale. VOI a été utilisé uniquement dans les élections générales de l'an 2000, traitant un total de 84 voix dans quatre états (la Floride, la Caroline du Sud, le Texas, et Utah). Toutes étaient de vraies voix, pas des votes de test.

Le bureau de FVAP a publié un rapport sur le système VOI en juin, 2001 (Voting Over the internet Pilot Project Assessment Report). Seule une petite partie du rapport est consacrée à la sécurité, mais la plupart des soucis que nous mentionnons ci-dessous comme s'appliquant au système SERVE ont été mentionnés dans le rapport sur VOI. Une conclusion du rapport est que l'expérience de VOI était si petite que ce n'était pas une cible vraisemblable d'une attaque, et que même une attaque réussie n'aurait presque certainement fait aucune différence dans les résultats de n'importe quelle élection. (Le fait que 50 voix ont été exprimées en Floride en utilisant VOI, et qu'un changement de 269 voix dans le décompte officiel de cet État aurait eu comme conséquence que Al Gore soit le président, montre combien de telles hypothèses peuvent être dangereuses. Nous notons que la Floride participe en 2004 au programme SERVE.)

Le système VOI a également ignoré des éléments critiques du problème de la sécurité du vote sur internet en prenant la position que, pour le système pilote VOI, le poste de travail de l'électeur était en dehors du périmètre de sécurité du système. En d'autres mots, le système VOI n'a fait aucune tentative pour se défendre contre certaines des attaques les plus sérieuses auxquelles il était vulnérable.

Cependant, le rapport sur VOI a exprimé des inquiétudes concernant des problèmes de sécurité concernant le vote "à distance" à travers internet (c'est à dire le vote à partir de tout ordinateur relié à internet, depuis n'importe où dans le monde, comme cela est autorisé sous le système SERVE), et le rapport a explicitement refusé de recommander le vote à distance jusqu'au moment où dans l'avenir les menaces les plus sérieuses auront été résolues :

> "[Le vote "à distance" à travers internet] est sujet aux mêmes préoccupations de sécurité que le système actuel VOI. Pour cette raison, nous ne pouvons pas [le] recommander comme un développement succédant immédiatement au système pilote VOI. ... Par conséquent, nous recommandons que la recherche continue sur ces problèmes de sécurité de façon que cette solution de remplacement puisse être mise en réalisation ["implementation"] à l'avenir quand des mesures de sécurité adaptées seront disponibles pour contrecarrer les logiciels malveillants (par exemple, les virus et les chevaux de Troie) et les tentatives [de production] de refus de service (section 6.2.4)".

En dépit de cette recommandation, le programme du système SERVE déploie un système de vote à distance à travers

l'internet comme le successeur de VOI, bien que [les problèmes de] logiciels malveillants, de refus de service, et d'autres menaces n'aient pas été résolus.

En l'année 2000 il y avait plusieurs autres expériences de vote à travers l'internet dans des élections publiques aux États-Unis. Dans certains cas, les voix ont compté officiellement; dans d'autres cas, non. La plus importante et la plus connue était les primaires présidentielles démocrates de l'Arizona, pilotées par election.com (dont les actifs ont été acquis en 2003 par Accenture) en mars de cette année [2003], où approximativement 85.000 votes ont été exprimés et scrutés. L'élection primaire nationale du “parti de la réforme” a été également conduite à travers internet cet été, de même que les diverses expériences de vote non officiel sur internet dans quelques comtés de Washington, de Californie, d'Arizona et ailleurs.

Plusieurs études sur le vote à travers internet, y compris les problèmes de sécurité, ont été entreprises en 1999-2000. La première fut celle du groupe de travail sur le vote à travers l'internet du Secrétaire d'État de Californie, dont le rapport a été publié en janvier 2000 et est accessible en ligne à http://www.ss.ca.gov/executive/ivote. Ce rapport était le premier à articuler clairement la plupart des problèmes de sécurité technique qui concernent en général le vote à travers l'internet, et il a manifestement refuser de recommander que l'État pousse vers le vote à distance à travers internet (par exemple, des micro-ordinateur de type PC à la maison, au bureau, dans les écoles, dans les bibliothèques, et dans les cybercafés), en raison des nombreux problèmes de sécurité qu'il a détaillé. Ces problèmes de sécurité ne trouvaient alors aucune bonne solution, et maintenant, quatre ans plus tard, ces problèmes demeurent [toujours] sans solutions.

Une autre étude a été entreprise par l'institut de la politique d'internet (internet Politic Institute) avec un financement de la NSF, National Science Foundation. Leur rapport (rapport de l'atelier national sur le vote à travers internet : problèmes et planification des recherches, désigné sous le nom de rapport NWI -*Report of the National Workshop on internet Voting: Issues and Research Agenda)* s'appuyait sur une conférence tenue en octobre 2000, et a été éditée en mars 2001. Ce qui suit est un paragraphe clé du sommaire de ce rapport:

> *"les systèmes de vote à travers internet posent un risque significatif pour l'intégrité du processus de vote, et ne devraient pas être utilisés pour un emploi dans des élections publiques jusqu'à ce que les problèmes substantiels tant techniques que sociaux soient traités* [en italique dans l'original]. Les risques de sécurité liés à ces types de systèmes sont nombreux et diffus, et, dans beaucoup de cas, ne peuvent même pas être résolus en utilisant la technologie actuelle la plus sophistiquée. En outre, plusieurs des problèmes sociaux concernant les effets du vote distance sur le processus électoral devraient être traités avant qu'un tel système puisse être déployé de façon responsable. Pour cette raison, il est impératif que des fonctionnaires publics se forment au sujet des dangers posés par le vote à distance à travers l'internet, et les ramifications d'un échec [éventuel] sur la légitimité du processus électoral."[1]

Les risques de sécurité "nombreux et diffus" visés dans le rapport NWI sont semblables à ceux décrits dans le rapport du groupe de travail de Californie.

Le projet technologie et vote [Voting technology project] commun au Caltech et au MIT a édité son rapport (*Voter : ce qui existe, ce qui pourrait avoir lieu;* [Voting: What Is, What Could Be]) en juillet 2001. Il est accessible en ligne à l'adresse réticulaire http://www.vote.caltech.edu/Reports/2001report.html. Ce rapport était pessimiste de même façon au sujet de la sécurité du vote à travers l'internet, affirmant que "le vote à distance à travers internet présente des risques sérieux de sécurité. Il est beaucoup trop facile pour un [seul] individu de perturber une élection entière et de commettre une fraude électorale à grande échelle."

Dans les sections 2, 3 et 4 de ce document nous argumentons du fait que toutes les vulnérabilités de sécurité qui ont été exprimées clairement dans ces études de 1999-2001 restent présentes dans l'architecture du système SERVE, avec au moins un risque supplémentaire qui n'avait pas été souligné alors, à savoir la possibilité de fraude interne [administrateur?]. Nous proclamons que, étant donné la technologie actuelle, ces vulnérabilités sont inhérentes à n'importe quelle architecture de vote [à distance] à travers internet qui autorise des personnes à voter à partir d'ordinateurs privés, et qu'aucune innovation technologique ne changera ce fait dans un futur prévisible.

1.3 Pourquoi la sécurité pour le vote à travers internet est bien plus difficile que pour le commerce électronique.

[1] Le rapport NWI a ajouté une note de bas de page affirmant "Cependant, le vote à distance à travers Internet peut être approprié à court terme pour des populations particulières, telles que les militaires et les employès du gouvernement et leurs personnes à charge qui sont basés outre-mer. De telles exceptions devraient être examinées au cas-par-cas." Cependant, les virus, les vers, les chevaux de Troie et les espiogiciels ["spyware"] de Trojan que nous avons vu ces dernières années sont beaucoup plus malveillants que ceux qui existaient au moment de la publication de ce rapport, et beaucoup des questions de la fraude interne et le besoin de traces vérifiables par l'électeur n'ont été seulement comprises et clairement exposées que depuis.

Beaucoup de personnes supposent de façon fausse que, puisqu'elles peuvent sans risques conduire des transactions commerciales à travers internet, elles peuvent aussi voter à travers internet sans risques D'abord, elles sous-estiment habituellement les aléas des transactions financières en ligne, et ne sont pas au courant de plusieurs des risques qu'elles prennent même si elles prennent la précaution de ne traiter qu'avec des sites "sûrs" sur la Toile au moyen du protocole SSL. Mais elles font aussi l'hypothèse que le vote est comparable d'une façon ou d'une autre à une transaction financière en ligne, alors qu'en fait la sécurité du vote à travers internet est bien plus difficile que la sécurité du commerce électronique. Il y a trois raisons à cela: les enjeux plus élevés, l'incapacité à corriger les effets des échecs, et les différences de structures importantes entre les exigences pour les élections et le commerce électronique.

En premier lieu, un haut niveau de sécurité est essentiel pour les élections. La démocratie se fonde sur la large confiance dans le caractère intègre de nos élections, ainsi les enjeux sont énormes. Simplement, nous ne pouvons pas nous permettre d'incident dans ce domaine. En conséquence, le vote exige un niveau plus élevé de sécurité que le commerce électronique. Bien que nous sachions établir des systèmes de commerce électronique avec une sécurité acceptable, *la sécurité de type commerce électronique n'est pas assez bonne pour des élections publiques.*

En second lieu, la sécurisation du vote à travers internet est structurellement différente -et fondamentalement plus exigeante - que la sécurisation du commerce électronique. Par exemple, ce n'est pas une faute de sécurité si votre conjoint emploie votre carte de crédit avec votre consentement; il est courant de déléguer son autorité pour accomplir des transactions financières. Mais c'est une faute de sécurité que votre conjoint puisse voter en votre nom, même avec votre consentement; le droit de vote n'est pas transmissible, et ne doit être ni délégué, ni vendu, ni commercialisé ou ni donné au loin. Une autre distinction entre le vote et le commerce électronique est qu'alors qu'une attaque en refus de service sur des transactions de commerce électronique peut signifier que des affaires sont perdues ou remises à plus tard, elle ne détruit pas la légitimité des autres transactions qui étaient inchangées. Cependant, dans le cas des élections, une attaque en refus de service peut avoir comme conséquence la privation de droits civiques irréversible pour des électeurs et, en fonction de la sévérité de l'attaque, le caractère légitime de l'élection tout entière pourrait être compromise.

En troisième lieu, les exigences spécifiques d'anonymat dans les élections publiques rendent très difficile de détecter, encore moins de corriger les effets des incidents de sécurité d'un système de vote à travers internet, alors que dans le commerce électronique la détection et la correction des effets sont beaucoup plus faciles parce que le commerce électronique n'est pas anonyme. Dans un accord commercial, les gens peuvent détecter la plupart des erreurs et des fraudes en vérifiant de façon croisée des factures, des rapports, et des reçus ; et quand un problème est détecté, il est possible de corriger (au moins partiellement) au moyen de remboursements, d'assurances, des déductions d'impôts, ou des actions judiciaires. Au contraire, les systèmes de vote ne doivent pas fournir de reçus, parce qu'ils violeraient l'anonymat et rendrait possible des achats de voix et des pressions ou des intimidations sur l’expression du vote. Cependant, même si un système de vote ne peut publier des reçus qui indiqueraient comment les personnes ont voté, il est toujours essentiel que le système soit suffisamment transparent que chaque électeur ait confiance que sa voix personnelle est correctement prise en considération et décomptée, et plus généralement, que tous les autres le sont également. Il n'y a aucune exigence de ce type pour des systèmes de commerce électronique. En général, [architecturer et] concevoir un système de vote à travers internet qui peut détecter et corriger tout type de fraude électorale, sans publier des reçus par électeur pour la façon dont ils ont voté, et sans risquer le caractère privé du vote en liant les électeurs à l'expression de leurs votes, est un problème profond et complexe de sécurité qui n'a aucun analogue dans le monde du commerce électronique. Pour ces raisons, l'existence d'une technologie pour fournir une sécurité adéquate pour le commerce sur internet n'implique pas que le vote à travers internet peut être rendu sûr.

1.4 Critères pour évaluer la sécurité du système SERVE : quel est le niveau suffisant de sécurité ?

En évaluant la sécurité du système SERVE, nous avons besoin d'une norme à laquelle la comparer, c'est à dire une réponse à la question: "quel est le niveau suffisant de sécurité?" Nous reconnaissons qu'aucun système de sécurité n'est parfait, et il serait irresponsable et naïf d'exiger la perfection. Cependant, puisque nous ne devons pas permettre des risques inacceptables de fraude électorale qui corrompraient nos élections nationales, nous devons avoir un certain ensemble de critères pour décider quels sont les risques acceptables.

D'une part, la sécurité des élections doit être regardée comme une composante de la sécurité nationale, puisque la légitimité même du gouvernement démocratique repose sur des élections qui sont justes, ouvertes, dignes de confiance, et considérées ainsi. Ceci argumenterait en fait pour les normes les plus élevées de sécurité - de façon idéale de sorte que pas un seul suffrage exprimé ne doit être perdu, falsifié, corrompu, mal compté, acheté, ou vendu, et que l'électeur ne puisse être contraint ou ne perde l'anonymat de son suffrage dans n'importe quel scénario crédible de menace, même si l'attaquant dispose de ressources importantes, de la connaissance complète de l'architecture du système SERVE, et d'une complicité

interne.

D'autre part, le système SERVE est conçu pour être une forme de vote à distance pour des citoyens concerné par la loi UOCAVA. Les électeurs distants votent de quelque part ailleurs que dans les bureaux de vote de leur circonscription électorale , traditionnellement en cochant ou en poinçonnant un bulletin de papier et en le renvoyant par courrier aux fonctionnaires du comté, bien qu'il soit parfois autorisé de l'envoyer par télécopie. Dans quelques États de l'ouest, 30% ou plus de toutes les voix sont des votes à distance; l'Orégon, en particulier, a éliminé ses bureaux de votes de circonscriptions électorales, de sorte que tous les votes s’expriment à distance. Puisque le but du système SERVE est de faciliter le vote à distance, il peut être argumenté que le niveau de sécurité du vote à distance devrait être la mesure minimale face à laquelle le système SERVE est comparé.

Notre analyse a donc posé comme prémisse le principe suivant : *Pour le moins, n'importe quelle nouvelle forme de vote à distance devrait être aussi sûre que les systèmes de vote à distance actuels.*

Tandis que les procédures [actuelles] de vote à distance offrent un degré équilibré de sécurité et d'anonymat ("privacy") [du vote], il y reste quelques vulnérabilités intrinsèques dont chacun est averti et que nous, la société, avons accepté de tolérer. Il y a beaucoup de façons pour un attaquant de compromettre un nombre *restreint* de votes à distance sans être détecté, par exemple en espionnant ou en contraignant les électeurs, en particulier dans des situations institutionnelles comme des maisons de repos; ou en payant des électeurs ; ou en intervenant dans le transport des votes par le courrier, etc... Cependant, le point clé qui rend le vote à distance tolérable malgré ses nombreuses vulnérabilités est qu'il reste très difficile de monter une attaque quelconque sur le processus qui soit automatisée ou à grande échelle sans se faire prendre. Il n'y a aucun point de vulnérabilité unique par lequel beaucoup de voix exprimées à distance passent excepté aux bureaux des fonctionnaires des élections du comté et de leurs bureaux de poste locaux. Dans les deux cas, il y a de nombreuses procédures de contrôle prévues par la loi dont l'application augmente les risques d'être pris pour les fraudeurs. Même si une complicité organisée de fraude électorale était commise dans l'un de ces endroits et échappait d'une façon ou d'une autre à la détection, sa portée serait limitée à un simple comté, et, dans la plupart des États, uniquement au pourcentage relativement faible des votes à distance exprimés dans ce comté, de sorte que le risque de se faire prendre et les sanctions sont supérieurs à la valeur du petit nombre de voix qui pourraient être compromises.

Ce niveau de sécurité -des vulnérabilités à des attaques à petite échelle non détectées, mais peu ou aucune vulnérabilité aux attaques à grande échelle- semble un objectif raisonnable pour un nouveau système de vote tel que le système SERVE, de sorte que cela assurerait que son ajout à la variété des autres systèmes d'expressions des votes déjà en service ne réduirait pas la sécurité globale que les élections montrent actuellement, et n'ajouteraient pas de nouvelles vulnérabilités d'un caractère différent ou d'une échelle différente. Ce que nous devons éviter à tout prix est tout système dans lequel il serait possible à une attaque réussie à grande échelle ou automatisée de compromettre beaucoup de voix. Il doit être essentiellement impossible que des telles attaques à grande échelle se produisent sans être détectées; ou qu'une telle attaque puisse être si facile et si peu coûteuse qu'une personne agissant seule pourrait la mener à bien; ou que la personne menant une telle attaque puisse ne jamais être identifiée; ou qu'une telle attaque puisse être effectuée à distance, depuis un territoire étranger, éventuellement par une agence étrangère en dehors de la portée des lois des États-Unis, de sorte que les attaquants ne font face qu'à peu ou pas de risques. Tout système de vote avec l'une des formes quelconque de ces vulnérabilités est, nous le croyons, totalement inadapté pour l'emploi dans des élections publiques des États-Unis. Malheureusement, le système SERVE montre toutes ces vulnérabilités, comme nous le décrivons dans le reste de ce rapport.

1.5 Les menaces sur les systèmes de votes.

Tout système de vote véritablement démocratique doit disposer des moyens de traiter cinq menaces importantes. Une première menace sérieuse est la privations de droit civique de citoyens ou de groupes d'électeurs. Un souci important est que des groupes des électeurs pourraient être privés des droits civiques, en tenant compte de la probabilité de l'expression particulière de leur vote. Le vote à travers internet présente des opportunités de privations sélectives de droits civiques qu'il peut être difficile à détecter et encore plus difficile à corriger.

Une deuxième menace est qu'un bulletin de vote pourrait être modifié par un tiers. Avec les bulletins papier conventionnels, ceci pourrait être fait par exemple en ajoutant une voix pour un bureau pour lequel l'électeur n'avait pas voté ou en infirmant les bulletins exprimés en ajoutant trop de voix additionnelles. Comme nous le verrons, cependant, le vote électronique crée de nouvelles occasions pour miner le caractère secret du vote, et pour automatiser la modification systématique de votes exprimés, [occasions] qui n'existaient pas auparavant.

Une troisième menace est la perte de l'anonymat ("privacy") -ce qui sape le bulletin secret. Le vote à un bureau de vote correctement géré de la circonscription électorale au moyen de bulletins papiers qui sont mélangés à d'autres dans une urne physique est la meilleure protection pour l'anonymat du vote, et son caractère privé. Le caractère privé dans un bureau de

vote est protégé en ne permettant pas à deux personnes d'entrer ensemble dans un isoloir, même si elles le désirent. (Une exception peut être faite pour des personnes handicapées qui ne peuvent pas voter sans aide). Puisque le vote est immédiatement mélangé à d'autres votes dans l'urne, il est pratiquement impossible de reconstruire qui a exprimé quel choix dans la circonscription. Il est beaucoup plus difficile de protéger l'anonymat de l'électeur à distance quand le vote est exprimé en utilisant les votes à distance sous forme papier complétés à la maison ou au travail et envoyés par courrier, et encore plus difficile quand un vote à distance électronique est traité par une grande quantité de logiciels sur plusieurs ordinateurs différents.

Une quatrième menace, un type bien connu de fraude électorale, est qu'un électeur puisse voter plus d'une fois. Citons les services répressifs de Floride: "Ceux qui penchent pour ce type de fraude peuvent profiter de l'accès d'autres [électeurs] à un vote à distance en exprimant leur vote à leur place, le plus souvent sans que l'électeur réel ne sache ce qui s'est produit. Ceci fournit une occasion terrible de fraude électorale, en particulier pour ceux qui ont accès aux malades ou aux infirmes ou à ceux qui n'ont pas la capacité de résister à l'influence des autres quand elles sont forcées à voter de la façon demandée. Ceci encourage également ces fraudeurs à commettre la fraude électorale en recherchant à utiliser les votes à distance de ceux dont l'intérêt pour le vote est marginal ou inexistant[2].

Comme dans le cas de la modification des bulletins, le vote à travers internet présente de nouveaux moyens de votes multiples en permettant à ceux qui sont prêts à investir du temps dans l'analyse sociale pour déterminer ceux des électeurs enregistrés qui sont le moins susceptibles de participer à une élection. Une fois obtenue cette information, le vol d'identité permettrait que le vote à travers internet soit automatisé afin de réaliser une quantité significative de participations falsifiées à toute élection donnée.

Une cinquième menace, intrinsèque au vote à distance, est l'achat, la vente et le commerce de voix. Comme nous le montrons, cette menace est également amplifiée par le vote à travers internet.

En conclusion, un thème que toutes ces menaces partagent est la question de l'échelle. Les ordinateurs sont extrêmement efficaces pour automatiser des tâches répétitives, mais ceci diminue [les coûts] de deux façons : il est également facile d'utiliser des ordinateurs pour automatiser des attaques. Quand la sécurité des systèmes d'information fait défaut, les incidents sont à grande échelle. Un risque important dans toute organisation centralisée de vote à travers internet comme le système SERVE est qu'une simple faute pourrait affecter des centaines de milliers d'électeurs.

1.6 Vulnérabilités du système SERVE

Manque de journaux vérifiables par l'électeur et attaques d'initiés. Des systèmes de vote dits DRE (enregistrement direct électronique) ont été largement critiqués parce qu'ils sont essentiellement impossibles à contrôler ("unauditable"). D'abord, il n'y a aucune manière qu'un électeur puisse vérifier que la voix enregistrée à l'intérieur de la machine est identique à la voix qu'il a saisie et vue affichée sur l'écran sensitif de la machine. Et plus tard, si les problèmes sérieux se produisent dans le dépouillement des bulletins (ce qui arrive somme toutes fréquemment avec les DREs), il n'y a aucun moyen de vérification rétrospective indépendante des voix pour aider à résoudre le problème.

Ces problèmes ont été discutés largement dans la nation ces dernières années, et la communauté des spécialistes en SSI, y compris tous les auteurs de ce rapport, soutient de façon presque unanime la position qu'on ne devrait autoriser aucun système de vote de DRE qui n'a pas une espèce de journal de vérification rétrospective vérifiable par l'électeur. La vérification par l'électeur est la seule défense efficace facilement disponible contre des attaques planifiées d'initiés. Puisque beaucoup a été écrit sur ce sujet nous ne répéterons pas les arguments ici. Pour de plus amples informations voir, par exemple, le site sur la Toile http://www.verifiedvoting.org du professeur David Dill, ou le site http://www.notablesoftare.com/evote.html du professeur Rebecca Mercuri, ou le rapport du secrétaire d'État de Californie et ses directives concernant les systèmes de vote à écran sensitif en http://www.ss.ca.gov/elections/touchscreen.htm. Ce que nous souhaitons noter ici est que chacun des arguments au sujet du besoin de vérification et de contrôle par l'électeur qui ont été exprimés à propos des systèmes DRE, s'appliquent également, essentiellement sans changement, au système SERVE. En effet, du point de vue de l'électeur, on peut dire que le système SERVE n'agit que comme une gigantesque machine de saisie et d'enregistrement (DRE).

Anonymat [et caractère privé [du vote]. Le système SERVE vise à fournir au moins les mêmes niveaux d''anonymat et de sécurité que le vote conventionnel à distance. Comme les États traitent différemment les votes à distance par la poste, nous analyserons comment la Californie essaye de protéger l'anonymat [de l'électeur] dans un vote à distance par la poste. L'électeur insère le vote dans une enveloppe intérieure, qui ensuite est insérée dans une enveloppe extérieure. Les informations qui identifient l'électeur, telles que le nom de l'électeur et sa signature, sont écrites sur l'enveloppe externe.

[2] http://www.fdle.state.fl.us/publications/voter_fraud.asp

Quand un vote exprimé par courrier est reçu, le nom et la signature sur l'enveloppe externe sont vérifiés par rapport à la liste électorale. En supposant qu'ils correspondent à ceux d'un électeur inscrit qui n'a pas encore voté, l'enveloppe externe est ouverte en présence d'au moins deux personnes. La date de l'ouverture de l'enveloppe intérieure est déterminée par des règlements de l'État et du comté. Tandis que les soucis d'anonymat exigeraient que l'enveloppe intérieure soit ouverte de façon qu'elle ne puisse être liée à l'enveloppe externe, ceci peut se produire quelquefois. Et même si les meilleures précautions sont prises, l'électeur qui oublie de mettre son bulletin dans l'enveloppe intérieure aura son vote rendu visible dès que l'enveloppe externe sera ouverte.

Le système SERVE essaye de séparer le nom de l'électeur de l'expression de son vote par l'utilisation de cryptographie à clés publiques. Dans les systèmes à clés publiques, chaque participant a une paire de clés se composant d'une clé privée et d'une clé publique. La partie privée est connue seulement du participant, et, comme son nom l'indique, la clé publique est disponible à tous. Dans chaque district électoral qui participe au système SERVE, un fonctionnaire local responsable des élections (LEO Local Elections Official pour SERVE) génère une paire de clés de ce type. La clef publique de LEOs est employée pour chiffrer (brouiller) les votes des électeurs sur le système SERVE de cette zone. Une fois qu'un vote a été chiffré, il ne peut être lu que s'il est déchiffré par l'utilisation de la clef privée unique connue seulement du LEO.

Quand un électeur utilise le système SERVE pour exprimer un vote, son navigateur/butineur sur la Toile envoie le vote exprimé, accompagné d'un identificateur, comme le nom de l'électeur, à un serveur sur la Toile du système SERVE. Cette information est transmise au système SERVE sous forme chiffrée, de sorte que seul le serveur sur la Toile du système SERVE peut la déchiffrer. Puisque le vote est chiffré avant la transmission, si quelqu'un interceptait le vote chiffré en route, il lui serait impossible de déchiffrer le bulletin exprimé réel. Notez que, à ce moment, la paire de clés du LEO n'a pas encore été employée.

Quand le vote est reçu, le système SERVE vérifie que l'électeur est bien inscrit et n'a pas encore voté. SERVE déchiffre le bulletin de vote en utilisant la clef privée du système SERVE, sépare le bulletin de vote du nom de l'électeur, et puis chiffre le vote (sans le nom de l'électeur) en employant la clé publique du LEOs. Par conséquent, seul le LEO correspondant pourra déchiffrer le vote chiffré. Le vote chiffré est conservé pour la transmission postérieure vers le responsable LEO. Le système SERVE garde une copie du vote chiffré, même après qu'une copie a été envoyée au LEO. Le système SERVE place également le nom de l'électeur sur une liste de personnes qui ont déjà exprimé leur vote, de sorte qu'elles ne puissent pas voter une deuxième fois.

Cette architecture présente plusieurs risques d'atteinte à l'anonymat de l'électeur. D'abord, le LEO pourrait déduire la nature des votes des électeurs de sa circonscription en déchargeant les voix du système SERVE à une telle fréquence qu'il obtienne au plus un nouveau nom de d'électeur et une valeur de voix à chaque fois. Rappelez-vous que le LEO peut demander au système SERVE une liste de noms des électeurs de la zone du LEO qui ont déjà voté par l'intermédiaire de l'internet et la liste (réordonnée aléatoirement) des votes chiffrés pour ces électeurs. Si un LEO curieux fait la demande suffisamment souvent, il pourrait en déduire comment chaque électeur individuel a voté, un risque évident de perte d'anonymat.

En second lieu, le fait que les votes exprimés (bulletins) subsistent non chiffrés sur le serveur pendant une brève période avant d'être rechiffrés avec la clé du LEO présente d'autres risques de perte d'anonymat. Par exemple, les administrateurs gestionnaires du système SERVE pourraient regarder comment les électeurs ont voté. En outre, si les machines du système SERVE étaient compromises, les bulletins non chiffrés pourraient être divulgués à des tiers {non autorisés}. Voir dans l'annexe A un complément de discussion sur ce risque.

Troisièmement, le fait que les votes chiffrés ainsi que les noms des électeurs soient conservés dans une base de données du système SERVE signifie que toute personne disposant de la clé privée de LEO et d'un accès à la base de données du système SERVE pourrait déterminer le contenu des bulletins de tous les électeurs du système SERVE pour cette circonscription électorale cette zone de vote, un autre risque significatif de parte d'anonymat.

Quatrièmement, les votes chiffrés sont conservés pendant une longue période sur des ordinateurs de SERVE, ce qui augmente la fenêtre du risque. Nous avons compris que, au minimum, des votes chiffrés seront conservés jusqu'à 18 mois après la fin des élections. Nous croyons qu'il est possible que les votes chiffrés puissent demeurer accessibles pendant une période encore plus longue, et peut-être indéfiniment, par exemple sur les bandes de sauvegarde ou d'autres ordinateurs, indépendamment de l'intention des réalisateurs du système. En effet, les informations demeurent souvent plus longtemps accessibles que les réalisateurs ne le prévoient; dans les systèmes modernes, les informations sont typiquement copiées à tant d'endroits qu'il peut être un défi [impossible] de les trouver et de les effacer toutes. En conséquence, il est imaginable que l'anonymat de l'électeur puisse être compromis à une date future si l'information devait échouer dans de mauvaises mains et que de vieilles clés soient exposées. Des progrès mathématiques futurs, par exemple, pourraient exposer des clés anciennes.

Dans les sections 2 et 3, nous décrivons en détail plusieurs autres risques pour l'anonymat du vote. Tandis que les systèmes

de vote à distance d'aujourd'hui ont leurs propres risques en ce qui concerne l'anonymat du vote ("privacy"), en considérant tous ces risques comme un tout nous croyons que le système SERVE augmente le risque de compromission à grande échelle de cet anonymat.

Achat et vente de voix. La vente de voix est un problème dans toutes les élections, mais c'est un souci spécial pour le vote à travers internet, puisque l'internet peut faciliter à grande échelle des achats et des ventes de voix en permettant à des acheteurs de voix d'automatiser le processus. Pendant les élections présidentielles de 2000 nous avons vu la première tentative de permutation de voix à travers internet dans une élection présidentielle avec la création d'un site Web pour faciliter les permutations de voix entre les électeurs de Al Gore et ceux de Ralph Nader. Alors que la permutation Gore/Nader reposait sur l'honneur et qu'aucun argent ne changeait de main, ce qui est nouveau au sujet du système SERVE est qu'une approche analogue pourrait être employée pour fournir des services *forcés* de permutation de voix ou de troc de voix, ou pour acheter des voix des électeurs utilisant le système SERVE. En raison de la facilité à automatiser de telles attaques, le déploiement du système SERVE pourrait mener aux achats ou aux échanges de voix à une plus grande échelle que ce qui a été vu auparavant.

Le schéma d'achat de voix le plus direct comporterait la vente des moyens du vote ("credentials"), à savoir les informations personnelles d'identification et le mot de passe de l'électeur ou sa clé privée. Une défense possible que nous avons envisagée serait que le système SERVE interdise la soumission des voix multiples depuis la même adresse internet. La restriction du nombre de soumissions depuis une adresse particulière de la Toile [*NdT sic!*] n'est pas une défense forte, car il est possible, cependant, qu'un acheteur des voix trompe le système SERVE en lui faisant croire que les voix viennent de différentes adresses. En outre, en raison des serveurs de procuration ("proxy servers"), les utilisateurs légitimes semblent souvent venir de la même adresse IP, ainsi cette défense supposée ne peut pas être mise en oeuvre dans la pratique. Un exemple extrême de ceci est AOL, qui emploie la même adresse IP pour tous les utilisateurs venant de son domaine. Enfin, il est possible que beaucoup d'utilisateurs du système partagent le même ordinateur, donc évidemment, ces voix viendraient légitimement de la même adresse.

Une autre approche pour l'achat de voix serait que l'acheteur fournisse au vendeur une version modifiée du composant script ActiveX employé par le système SERVE. Une version convenablement modifiée pourrait s'assurer que le vote est fait selon les souhaits de l'acheteur de la voix. Il ne semble y avoir aucune manière pour que le système SERVE se défende contre ce modèle d'achats de voix. En bref, les possibilités pour les achats, les ventes, et les permutations de voix à grande échelle et par voie automatique dans le système SERVE dépassent n'importe quelle possibilité du système actuel du vote à distance.

Intimidation. L'intimidation est un problème potentiel pour toutes les formes de vote à distance, puisque l'électeur n'a pas la garantie d'anonymat offerte par l'isoloir. Mais elle peut être encore un problème plus important avec le vote à travers l'internet si l'électeur n'utilise pas sa machine personnelle, puisque le propriétaire de la machine a pu avoir installé un logiciel qui enregistrerait ce que l'électeur fait.

Conséquences à grande échelle. Puisque le système SERVE est vulnérable à beaucoup de types différents d'attaques, un pourcentage significatif des voix exprimées à travers d'nternet est également vulnérable, et une simple attaque réussie pourrait être capable d'affecter une grande fraction de toutes les voix exprimées à travers le système SERVE. En revanche, quand le vote est conduit dans des locaux précis avec des dispositifs mécaniques ou avec les votes sur bulletins de papier, les manipulations de voix, au degré où elles se produisent, se limitent à une échelle bien plus petite: aucune attaque n'est susceptible d'affecter un grand nombre de voix. Pour rendre la comparaison plus explicite, un simple adolescent, un passionné d'informatique, ou toute autre acteur malveillant pourraient éventuellement affecter des dizaines, ou des centaines de milliers de voix exprimées à travers le système SERVE, alors qu'il est extrêmement peu probable que n'importe quelle personne isolée puisse conduire une fraude électorale à une si grande échelle dans des élections actuelles non électroniques. En conséquence, les vulnérabilités touchant le système SERVE pourraient avoir des conséquences bien plus significatives que cela n'était possible avant l'introduction des ordinateurs et de l'internet dans le processus des élections.

Trop d'attaques possibles. Puisqu'il y a beaucoup de sortes différentes d'attaques qui pourraient être conduites contre le système SERVE, comme nous le discutons ci-dessous, il est par essence impossible de se protéger contre elles toutes. Tandis que n'importe quelle attaque particulière prise isolément pourrait disposer d'une méthode pour y parer, le coût de la défense pourrait être élevé et serait ajouté au coût de la défense contre toutes les autres attaques qui ont été prévues. Pire encore, les défenses créées pour empêcher un type d'attaque peuvent amplifier les risques face aux autres attaques. Et naturellement, une attaque qui n'a pas été prévue demeure un risque sérieux.

Beaucoup de sources d'attaques. L'internet ne connaît aucune frontière nationale. En conséquence, une élection tenue à travers l'internet est vulnérable aux attaques menées à partir n'importe où dans le monde. Non seulement, un parti politique pourrait essayer de manipuler une élection en attaquant le système SERVE, mais de la même façon les différents intrus, les criminels, les terroristes, les organismes tels que la Mafia, et même d'autres pays pourraient le faire. Il n'y a aucune

nécessité de faire l'hypothèse d'une grande conspiration ou d'adversaires hautement sophistiqués; plusieurs des attaques que nous décrivons pourraient être montées par des individus isolés avec la formation universitaire de premier niveau en informatique et programmation.

Des attaques indétectables. La fraude électorale s'est produite dans beaucoup d'élections de différents types. Un exemple récent a impliqué des urnes qui ont été trouvées flottant dans la baie de San Francisco en novembre, 2001. Il y a également eu des élections dans lesquelles des personnes décédées ont voté. Sans aucun doute, beaucoup d'exemples de fraude électorale n'ont pas été détectés. Mais, quand il y a un vote physique, il y a une chance que la fraude, ou même les erreurs involontaires, puissent être corrigées ou tout au moins découvertes.

Avec le vote à travers internet, cependant, il n'y a plus aucun moyen ni de vérifier que la voix qui a été reçue par le système SERVE représente exactement l'intention de l'électeur, ni, pour l'électeur, de vérifier que sa voix a bien été reçue par le système SERVE et exactement enregistrée par le représentant local (LEO). La seule présence d'un écran de confirmation ne prouve pas que la voix a été enregistrée correctement. Ces soucis sont analogues à ceux qui ont été exprimés au sujet des boîtiers de vote électronique sans journaux vérifiables par l'électeur.

La fraude détectée pourrait être presque causer autant de problèmes que la fraude non détectée. Si la fraude qui touche les voix exprimées dans le système SERVE venait à être être détectée, ce qui se produirait ne parait pas évident. Un juge peut demander une nouvelle élection dans une circonscription, et les États peuvent décider comment traiter les questions liées aux élections. Mais, il n'y a aucune disposition pour reprendre une élection fédérale. Si l'élection de 2004 est aussi serrée que l'élection de 2000 l'était, il est possible que les voix exprimées dans le système SERVE puissent pousser l'élection en faveur d'un des candidats. S'il y avait des raisons de croire que ces voix étaient non fiables ou probablement trafiquées, ceci pourrait avoir un impact défavorable sur un public déjà cynique.

Campagne électorale par écran interposé. Beaucoup d'États ont des lois qui encadrent les campagnes électorales en interdisant toute forme de campagne à une certaine distance d'un bureau de vote. En Californie, par exemple, la distance est de 100 pieds. Cependant, il n'y a encore aucune loi pour empêcher les genres les pires de campagnes électorales à l'intérieur d'une fenêtre d'un butineur de la Toile ("web browser") pendant que quelqu'un vote. Par exemple, un fournisseur d'accès internet (ou une entreprise fournissant un butineur, etc...) peut tirer un revenu de la publicité, comme le fait AOL, et aurait ainsi la capacité de cibler la publicité en fonction de l'adresse IP à laquelle un utilisateur est relié à un moment donné. Celle-ci pourrait prendre la forme de publicité instantanée ou même de publicité dans la fenêtre du butineur. Le problème est que, au moment même où un électeur se connecte à l'adresse du serveur de vote du système SERVE (ou à un emplacement pour informer les électeurs) il pourrait être bombardé avec toutes les sortes de publicités politiques. Il est même possible qu'au moins quelques formes de publicités finiront par être protégées par le premier amendement, et alors là, il n'y aura plus aucun moyen de leur échapper.

1.7 L'organisation de ce rapport

Le reste de ce rapport est organisé comme suit. Le noyau technique du rapport analyse trois menaces significatives pour la sécurité du système SERVE :

- les attaques rendues possibles par le manque de contrôle de l'environnement de vote (section 2),
- la substitution de serveurs sur la Toile, et les attaques en tiers interposé ("man in the middle") (section 3), et
- les attaques en refus/déni de service (“denial of service) (section 4).

Enfin, nous présentons nos conclusions et recommandations (section 5). En outre, plusieurs annexes détaillent d'autres problèmes comprenant d'autres risques de sécurité pour le système SERVE (annexe A), une expérience antérieure concernant un vote à travers internet (annexe B), une alternative possible au système SERVE (annexe C), et des problèmes fondamentaux pour écrire du logiciel sûr et exempt d'erreurs (annexe D).

Les menaces sur la sécurité du système SERVE sont récapitulées dans le tableau 1, où nous caractérisons ces menaces en termes de niveaux de compétences exigés pour monter des attaques, en termes de conséquences des attaques réussies, en termes de réalisme de ces attaques et finalement en fonction des contre-mesures qui pourraient être employées pour les contrecarrer.

2. Le manque de contrôle de l'environnement du vote.

C'est peut-être le plus grand défi pour le vote à travers internet; il résulte du fait que, contrairement aux élections conventionnelles, les autorités électorales n'ont plus le contrôle de tout l'équipement employé par des électeurs. Avec le système de vote à travers l'internet du système SERVE, les électeurs peuvent voter de chez eux ou d'ailleurs sur leurs propres ordinateurs ou voter à partir d'autres endroits au moyen d'ordinateurs contrôlés par les tiers. En conséquence, les "hackers" et d'autres tiers pourraient pouvoir obtenir le contrôle d'un grand nombre d'ordinateurs utilisés pour voter, et les fonctionnaires responsible des élections seraient impuissants à protéger l'intégrité de l'élection. Cet aspect de l'architecture du système SERVE de vote à travers l'internet crée des risques significatifs pour la sécurité des élections. Le manque de contrôle des machines utilisées pour le vote ouvre trois classes d'attaques: la compromission de l'anonymat du vote, le refus de l'exercice des droits civiques [électoraux], et les modifications des voix. Les deux prochaines sections décrivent comment un attaquant pourrait obtenir le contrôle de l'environnement de vote, et ce qu'il pourrait faire une fois que ce contrôle est obtenu.

2.1 Comment un attaquant pourrait contrôler l'environnement de vote.

Il y a deux scénarios de base suivant lesquels un attaquant pourrait contrôler l'environnement de vote: quand un électeur emploie l'ordinateur de quelqu'un d'autre et quand les électeurs possèdent un ordinateur qui contient un logiciel malveillant. Le dernier cas pourrait se produire en raison des applications préinstallées conçues pour attaquer l'élection, ou en raison d'un code à distance malveillant, tel qu'un ver ou un virus conçu pour exploiter des failles dans le logiciel d'exploitation de Windows ou d'autres applications.

Si le vote a lieu dans un cybercafé, les propriétaires ou les administrateurs gestionnaire du cybercafé contrôlent l'ordinateur. En outre, un visiteur précédent du cybercafé pourrait avoir pris le contrôle de l'ordinateur et avoir installé un logiciel d'espionnage ou de contrôle à distance. Il y a les risques semblables à voter à partir de n'importe quel ordinateur partagé de ce type tel que ceux des bibliothèques publiques.

Si le vote a lieu au travail, l'employeur contrôle l'ordinateur. Une étude a trouvé que 62% des principales entreprises des États-Unis surveillent les connexions internet de leurs employés, plus d'un tiers conservent et examinent les fichiers sur les ordinateurs de leurs employés[3]. Alors qu'une surveillance des raccordements à internet en écoutant de façon passive n'affecterait pas la sécurité du système SERVE, puisque le système emploie le protocole sécurisé SSL (“Security Socket layer”) qui chiffre le trafic, toute surveillance qui s'appuie sur un logiciel fonctionnant sur l'ordinateur des employés pourrait être utilisée pour des buts malveillants. Un employeur est également en mesure de contraindre les employés qui votent depuis leur travail de voter d'une certaine manière.

Menaces	Compétences nécessaires	Conséquences	Réaliste ?	Contre-mesures
refus (déni) de service (types variés)	faibles	refus de droits civiques (potentiellement ciblé)	courant aujourd'hui sur internet	pas d'outils simples; exige des heures de travail d'ingénieurs réseaux; lançable depuis n'importe où dans le monde
cheval de Troie sur le micro-ordinateur personnel PC pour empêcher le vote	faibles	refus de droits civiques	des millions de transactions complexes pour que le vote se bloque	limiter le risque en contrôlant soigneusement le logiciel du PC; la raison de l'échec peut ne jamais être diagnostiquée.
propagande sur écran	faibles	gêne de l'électeur, frustration, distraction, influence incorrecte	trivial avec la Toile dans son état actuel	l'électeur ne peut rien faire pour l'empêcher; cela demande une nouvelle loi.
faux serveur SERVE (différents types)	faibles	vol de vote, compromission du secret du vote	substitution de serveurs attaque courante et relativement facile.	aucune contremesure n'existe; reste vraisemblablement non détecté, lançable de partout dans le monde
falsification du client	faibles	Refus de droits civiques	un exemple: modifications des droits sur le fichier “cookie”. Beaucoup d'autres exemples simples	rien n'existe pour couvrir tous les mécanismes. trop difficile d'anticiper toutes les attaques; vraisemblablement non diagnostiqué

[3] http://www.amanet.org/research/pdfs/ems_short2001.pdf

Menaces	Compétences nécessaires	Conséquences	Réaliste ?	Contre-mesures
attaque d'initiés sur les serveurs systèmes	moyennes	Compromission totale d'une élection	les attaques d'initiés sont les plus courantes, dangereuses et difficiles à détecter des violations de sécurité.	Aucune mesure prévue dans l'architecture de SERVE; un moyen de vérifier les votes est nécessaire voir Annexe C; vraisemblablement non détecté.
Achat/vente automatisés de voix	moyennes	effondrement de la démocracie	très réaliste; car des électeurs sont volontaires	aucune mesure; les acheteurs peuvent ne pas être sous la loi des USA.
intimidation	moyennes	effondrement de la démocracie	plus difficile à faire que l'achat/vente, mais l'interposition en tiers permet de le faire sans grandes compétences	aucune mesure; vraisemblablement non détecté.
Virus spécifique au système SERVE	moyennes ou élevées	vol de votes, violation du secret du vote, refus de droits civiques	certaines attaques exigent seulement un test sur SERVE; d'autres requièrent des fuites de spécifications ou de code de SERVE et un attaquant compétent	les logiciels anti-virus ne peuvent détecter que les virus connus, mais pas les nouveaux; vraisemblablement non détecté
Cheval de Troie sur PC pour modifier ou espionner les votes	élevées	vol de votes, violation du secret du vote	les espiogiciels largement disponibles sont un bon point de départ	limiter le risque pa un contrôle soigneux du logiciel PC; plus difficile à contrôler en cybercafé ou dans des réseaux d'institutions; vraisemblablement non détecté

Tableau 1 Ce tableau décrit, pour chaque menace potentielle sur le système SERVE, quelles compétences sont nécessaires pour l'attaquant, les conséquences d'une attaque réussie, le caractère réaliste de l'attaque, et quelles sont les parades pour la contrer.

Le logiciel qui fonctionne sur l'ordinateur d'un électeur crée également des risques. Des portes dérobées, placées dans le logiciel et activées quand un utilisateur essaye de voter, peuvent surveiller de façon invisible ou subvertir le processus du vote. La présence de prétendus *Œufs de Pâques* (Easter Eggs) dans beaucoup de produits logiciels populaires montre qu'il s'agit d'une vraie possibilité. (Les *œufs de pâques* sont des extra séduisants qu'un réalisateur de logiciel ajoute à l'application sans autorisation, pour s'amuser. Un exemple est bien connu: la feuille de calcul [le tableur] Microsoft Excel97 contient un véritable simulateur de vol qui peut être lancé en utilisant une séquence cachée de caractères).

Les ordinateurs d'aujourd'hui sont fournis équipés de logiciels développés par beaucoup d'entités différentes; n'importe quel employé de toutes ces entreprises pourrait peut-être laisser une porte dérobée pour attaquer le système SERVE. Les systèmes d'exploitation, les jeux, les applications de production, les modules de gestion de périphériques, les applications multimédia, les appliquettes de butineur ("browser plug-ins"), les économiseurs d'écran, et les macros de Microsoft Office sont tous des vecteurs possibles. Chaque fois que quelqu'un télécharge un nouveau logiciel, le risque est augmenté.

En plus de la menace de la part des applications préinstallées, il y a une menace par des attaquants à distance. Un tel attaquant pourrait obtenir le contrôle d'un ordinateur sans être détecté. Par exemple, un attaquant pourrait exploiter une vulnérabilité de sécurité dans le logiciel d'un ordinateur d'un électeur. L'attaquant pourrait alors prendre à distance le contrôle de la machine en utilisant nombre de produits. Des exemples de logiciels de contrôle à distance sont PCAnywhere et BackOrifice. C'est un fait incontournable que les ordinateurs d'aujourd'hui sont inadéquats pour se protéger contre cette menace. L'intrusion réussie même dans des ordinateurs bien défendus est un fait courant et commun.

Les ordinateurs personnels des électeurs ont peu de chance d'être aussi soigneusement défendus que ceux des entreprises, et par suite les ordinateurs des électeurs sont particulièrement susceptibles aux attaques. Des attaques peuvent être facilement automatisées ; les passionés en informatique ("hacker") balayent systématiquement des milliers ou même des millions d'ordinateurs à la recherche de ceux qui sont les plus faciles à compromettre. Nous pouvons envisager des scénarios dans lesquels les ordinateurs des électeurs qui utilisent le système SERVE ont été compromis à une grande échelle, mettant en cause toutes les voix exprimées à travers l'internet. C'est regrettable, mais un tel scénario est tout à fait possible.

Des attaques à distance pourraient être lancées en utilisant l'un des nombreux vecteurs d'attaque. Peut-être le plus effrayant est un virus ou un ver qui se répand et contient une charge utile malveillante conçue pour prendre le contrôle des machines et causer la ruine d'une future élection. Comme les programmes qui vérifient les logiciels contre les virus ne défendent que contre les virus déjà connus, ces programmes anti-virus ne peuvent souvent pas suivre la diffusion de nouveaux virus et vers. En conséquence, les vers malveillants sont diffusés sur les ordinateurs reliés à internet aujourd'hui. Par exemple, en 2001, le ver CodeRed a infecté 360.000 ordinateurs en 14 heures, et en 2003 le ver Slammer a bloqué beaucoup

d'automates bancaires et a compromis beaucoup de machines sur l'internet[4]. Les vers modernes sont bien plus virulents, sont souvent diffusés par des méthodes multiples, sont capables de passer les gardes-barrières ("firewall") et d'autres défenses, et peuvent être difficiles à analyser. Par exemple, cela a pris un certain temps pour se rendre compte que SoBig.F était un cheval de Troie à grande échelle conçu pour installer [chez les utilisateurs et à leur insu] des moteurs d'envoi de pourriel[5] ("Spam").

La menace de virus spécifiques au système SERVE ne devrait pas être négligée. La première question qui vient à l'esprit est: "Les vérificateurs anti-virus peuvent-ils détecter empêcher cette menace?” La réponse, nous le croyons, est "non". De nouveaux virus ne seront presque certainement pas détectés par la plupart des vérificateurs anti-virus. Par ailleurs, il n'est pas trop difficile pour les attaquants de construire de nouveaux virus, ou de modifier suffisamment les virus existants pour qu'ils évitent la détection. On peut même trouver des kits de construction de virus sur internet. En outre, l'attaquant a l'avantage de pouvoir essayer de nouvelles versions des virus en utilisant les vérificateurs anti-virus publiquement disponibles employés par les victimes potentielles afin de s'assurer que le virus ne sera pas détecté avant son lancement. Selon notre expérience, les nouveaux virus diffusent habituellement rapidement jusqu'à ce que leur signature soit connue et que les fournisseurs d'anti-virus mettent à jour leurs fichiers de définition, mais ceci peut arriver trop tard: les dommages à l'élection pourraient déjà avoir eu lieu.

La menace des vers est également tout à fait réelle. Il est facile pour n'importe quel programmeur compétent d'écrire un simple ver brut; le code source des vers précédents peut être obtenu et modifié pour créer de nouveaux vers. L'écriture d'un ver sophistiqué est sensiblement plus difficile. Un ensemble d'experts estime qu'une petite équipe de programmeurs expérimentés pourrait, après des mois de travail, développer un ver qui pourrait compromettre la majorité de tous les ordinateurs reliés à internet en quelques heures [SPW02]. Nous ignorons si un projet aussi ambitieux réussirait dès sa première tentative, et il semble qu'il n'y a aucun consensus clair au sein de la communauté des spécialistes de sécurité des SI pour dire combien de temps, dans le pire des cas, un ver pourrait rester non détecté. Certains avancent qu'ils seraient détectés en quelques heures ou jours, alors que d'autres avancent qu'il peut être possible de cacher leur existence pendant des semaines voire même plus longtemps. De toute façon, les vers restent un risque significatif. Un ver à une échelle plus petite et visant plus sélectivement une population moindre serait beaucoup plus difficile à détecter, et probablement pourrait échapper indéfiniment à la détection. Même une attaque à grande échelle lancée et non réussie pourrait causer un dommage à la confiance des électeurs.

Il y a d'autres voies par lesquelles les attaques pourraient se répandre. Une attaque possible implique de balayer un grand nombre d'ordinateurs et de les attaquer directement. Cette technique est [aujourd'hui] largement répandue par les "hackers". Nous pourrions également voir les attaques diffusées par l'insertion de vers malveillants dans des courriers électroniques afin d'influencer une élection utilisant le système SERVE. Des élections pourraient également être minées par l'utilisation de serveurs sur la Toile ("web sites") qui auraient été changés pour contenir des logiciels malveillants. Tout utilisateur qui visite un tel serveur se ferait détourner son ordinateur à son insu. Puisque le système de vote du système SERVE exige que les électeurs permettent certains dispositifs dangereux sur leurs ordinateurs, le risque d'attaques par des serveurs de la Toile est augmenté. Par exemple, le système SERVE ne fonctionne que sur Microsoft Windows, une plateforme qui a souffert de beaucoup de problèmes de sécurité: de plus, le système SERVE exige que les électeurs permettent les scripts ActiveX, les "cookies", les appliquettes Java, et les scripts JavaScript -des instruments techniques de la Toile qui créent des risques significatifs pour la sécurité des ordinateurs des électeurs.

Les scripts ActiveX constituent une technologie de Microsoft qui permet à du code en provenance de l'internet de fonctionner directement sur les machines clientes. Il y a une architecture de sécurité pour ActiveX qui est hors de la portée de ce rapport. Comme indiqué plus haut, le système SERVE exige ActiveX parce qu'une partie de la fonctionnalité requise dans le système ne peut pas être réalisée à l'intérieur d'un butineur ("browser"). Cependant, l'utilisation d'ActiveX introduit des vulnérabilités additionnelles dans le système, comme cela est montré ci-dessous.

Une dangereuse attaque hybride consiste à placer un contenu malveillant sur des serveurs de la Toile ("Web sites") particulièrement choisis. Par exemple, un attaquant qui veut du mal à un candidat pourrait piéger le site Web de ce candidat, de sorte que ceux qui visitent le site du candidat sur la Toile (“web”) ne puissent pas voter en utilisant le système SERVE. Un tel refus sélectif de droits civiques pourrait éliminer plusieurs centaines de voix pour un candidat, donnant de ce fait l'élection à son adversaire.

Il y a plusieurs manières de piéger un serveur de la Toile ou un courriel qui ne posent aucune difficulté technique majeure à l'attaquant. Une méthode simple est de placer sur le serveur de la Toile ou dans le courriel un script ActiveX malveillant qui, une fois lancé, modifie la machine de l'électeur de sorte qu'elle ne fonctionne plus avec le système de vote du système SERVE. (Nous donnons quelques exemples dans la section suivante). Pour qu'un script d'ActiveX malveillant s'exécute

[4] http://securityresponse.symantec.com/avcenter/venc/data/w32.sqlexp.worm.html.

[5] http://securityresponse.symantec.com/avcenter/venc/data/w32.sobig.f@mm.html

effectivement, il doit être marqué comme une commande de confiance[6]. Tout programmeur qui devient un éditeur valide, c'est-à-dire, dont la clé publique est signée par Microsoft, Verisign, GTE, Thawte ou une autorité de certification de signatures d'entreprises, peut produire du code auquel est implicitement fait confiance par le système d'exploitation Windows. Il y a eu des cas documentés de personnes ayant trompé Microsoft quant à la signature d'un script ActiveX malveillant.

Des attaques ciblées pourrait être effectuées à grande échelle ou à petite échelle. Cela pourrait être des attaques utilisant des courriels ou des attaques utilisant des serveurs de la Toile qui toucheraient des centaines de milliers ou même des millions d'utilisateurs: la fréquence extraordinaire du pourriel ("Spam") est un témoin de l'effet de levier des attaques utilisant des courriels. Par exemple, ces techniques pourraient permettre aux adhérents d'un parti d'empêcher de voter une grande fraction des partisans de l'autre bord, tout en laissant indemnes la plupart ou tous leurs propres partisans. Bien qu'il puisse être possible de construire des attaques sophistiquées à base de courriels ou de serveurs de la Toile qui échappent à toute détection, il semble vraisemblable que de tels stratagèmes seraient remarqués s'ils sont employés à grande échelle. Néanmoins, même si une telle attaque devait être détectée, il serait possible que des petites [attaques] pourraient aller plus loin que d'invalider la totalité de l'élection, une conséquence vraiment indésirable.

2.2 Que peut faire l'attaquant s'il contrôle l'environnement du vote?

Un attaquant qui contrôle l'ordinateur de l'électeur est en position pour observer comment quelqu'un vote, et compromettre le secret du bulletin.

Par exemple, un tel attaquant pourrait placer un logiciel espion sur l'ordinateur pour enregistrer silencieusement tous les actes de l'électeur. Aujourd'hui, des logiciels espions sont aisément accessibles sur le marché pour enregistrer toutes les frappes dactylographiées, les serveurs de la Toile ("Web sites") visités, et les actions effectuées par l'utilisateur. Ce qui est surprenant n'est pas qu'un tel logiciel existe, mais qu'il soit aisément accessible à tous ; on peut trouver un tel logiciel pour moins de 50 dollars des États-Unis, comme des douzaines de versions gratuites. D'ailleurs, si un attaquant veut surveiller beaucoup d'électeurs en même temps, le logiciel pourrait être, sans trop de difficultés, adapté aux besoins pour cibler spécifiquement les élections à travers le système SERVE. Pire [encore], l'utilisateur ordinaire d'un ordinateur n'aurait aucun moyen de détecter si des tiers ont observé son vote.

Un attaquant qui contrôle l'environnement du vote pourrait neutraliser ActiveX ou les "cookies" du serveur de la Toile ("Web"), par exemple, en changeant les permissions sur le dossier des "cookies" pour en interdire l'accès en écriture, de sorte que l'utilisateur ne puisse plus voter par le système SERVE. Il est facile de monter une telle attaque. Une attaque intelligente pourrait être conçue de sorte que l'utilisateur ne puisse plus remettre les permissions nécessaires. Dans ce cas, l'électeur se rendrait compte qu'il a été privé de ses droits civiques. Des attaques plus sophistiquées pourraient causer la privation de droits civiques d'une manière que l'électeur moyen ne détecterait pas.

La privation de droits civiques ciblée sur des électeurs constitue une menace sérieuse pour l'intégrité de l'élection. Il est possible d'imaginer les attaques largement diffusées qui viseraient tous les électeurs d'un parti particulier pour supprimer leurs droits, laissant tranquille [les partisans de] l'autre parti. Une telle attaque aurait des conséquences graves.

Tandis que la facilité avec laquelle il est possible de refuser sélectivement le vote de certains reste une préoccupation profonde, un autre risque est qu'un tiers malveillant qui contrôle l'ordinateur d'un électeur enregistré pourrait employer ce contrôle pour fabriquer un bulletin non autorisé, violant de ce fait l'intégrité de l'élection. Le vote frauduleux pourrait sembler venir de l'électeur autorisé mais en réalité il aurait été rempli par l'attaquant. Ou bien, un attaquant pourrait attendre pour voir comment l'électeur vote et puis changer l'expression du vote par l'électeur avant qu'il ne soit traité par le script ActiveX du système SERVE. Une telle attaque exigerait une certaine sophistication, mais elle n'est pas impossible. Il y a plusieurs protections dans la conception du système SERVE qui gêneraient cette attaque. Mais, une fois que l'attaquant a le contrôle du client [sur l'ordinateur de l'électeur], ces protections pourraient être contournées. La technique la plus facile pourrait être de modifier le script ActiveX qui fonctionne sur la machine [utilisée par l'électeur] de sorte que les protections du système SERVE soient arrêtées au vol et non vues par l'utilisateur. La commande ActiveX *ainsi corrigée* agirait comme un tiers dans la chaîne ("man in the middle") (voir ci-dessous), en donnant à l'électeur l'impression prévue quand il vote de façon correcte, tout en modifiant son bulletin. Dans l'un des scénarios possibles, l'attaquant pourrait permettre à l'expression du vote de rester sans modification quand il convient à l'agresseur, qui, dans le cas contraire, le modifierait ou l'écarterait.

La compromission de l'anonymat du vote, le refus des droits de vote, et la fraude électorale pourraient être commises sans que personne ne s'en rende compte. L'électeur pourrait ne pas se rendre compte que sa voix a été surveillée ou modifiée par

[6]. Le code est marqué comme [digne] de confiance en y appliquant une signature numérique avec une clé privée dont les contre-parties publiques sont des éléments du système de Windows, ou dont les composantes publiques ont été certifiées par Microsoft.

un tiers malveillant. De même, les agents chargés des élections n'auraient probablement aucun moyen de détecter le comportement de tels tiers malveillants.

3. Substitutions [frauduleuses] et attaques par interposition d'un tiers dans la chaîne (“man in the middle”).

En dépit de toutes les protections mises en place dans le système SERVE, il existe certaines attaques qui ne peuvent pas être empêchées. Dans cette section, nous décrivons la vulnérabilité du système SERVE en ce qui concerne la compromission de l'anonymat du vote et la subversion des élections. Nous décrivons les attaques dans l'ordre croissant de gravité.

La première attaque que nous décrivons est l'intervention d'un tiers dans la chaîne qui protège l'anonymat de l'électeur. Le mécanisme de l'intervention du tiers est celui dans lequel l'adversaire s'interpose entre les parties communicantes légitimes et simule chaque partie à l'autre partie. Pour simplifier la discussion, nous nous concentrons sur l'anonymat du vote, où un attaquant cherche à apprendre comment les diverses personnes ont voté. La capacité d'un étranger arbitraire à apprendre sur une large échelle comment les électeurs ont voté est une menace contre la démocratie suffisante pour que nous pensions que cela seul justifie l'annulation du projet de système SERVE. Le fait que cette attaque est relativement facile à monter rend seulement notre demande plus forte.

Il y a plusieurs façons pour qu'un adversaire devienne un tiers qui opère dans la chaîne:

Contrôler la machine du client: comme cela est décrit dans la section précédente, si un adversaire peut contrôler la machine à partir de laquelle on vote, alors l'adversaire peut agir comme un tiers dans la chaîne et contrôler l'expression du bulletin, même sur une session chiffrée.

Contrôler le réseau local: si l'attaquant a le contrôle de l'environnement local de réseau, tel qu'un employeur sur un lieu de travail ou n'importe qui qui partage un réseau sans fil, alors l'attaquant peut s'interposer comme un tiers dans la chaîne de n'importe quelle communication.

Contrôler un réseau montant: un fournisseur d'accès internet (FAI/ISP) ou un gouvernement étranger qui contrôle l'accès du réseau de l'électeur vers le serveur de vote pourrait se masquer en interposition (en tiers dans la chaîne).

Se substituer au serveur de vote: même sans un accès physique aux voies du réseau entre un électeur et le serveur de vote et sans aucun accès à la machine, il existe des attaques par manipulation des personnes où un électeur peut être trompé en lui faisant croire qu'il communique avec le serveur de vote. Cette attaque pourrait être mise en application, par exemple, en signalant ou en envoyant par message électronique un lien qui semble désigner le serveur de vote, mais qui ne le désigne pas.

Attaquer le service de noms de domaine (DNS: Domain Name Service): Les attaques contre le DNS pourraient envoyer le trafic à un attaquant au lieu de l'envoyer au service légitime des élections.

Clairement, il y a beaucoup de moyens pour un attaquant de s'interposer en tiers dans la transaction. L'utilisation du protocole de couche sécurité (SSL Secure Socket Layer) fait peu pour atténuer ce risque d'interposition si le seul but [de l'agresseur] est de compromettre l'anonymat du vote. N'importe quel agresseur qui s'est interposé pourrait agir comme un intermédiaire du protocole SSL ("SSL gateway"), faisant passer les données entre l'électeur et le serveur des élections, sans les changer. L'attaquant serait capable de lire tout le trafic en le déchiffrant et le rechiffrant au passage entre les deux. En effet, l'attaquant communiquerait en utilisant deux sessions SSL, l'une entre lui-même et l'électeur, et l'autre entre lui-même et le serveur de voix, et ni l'un ni l'autre ne sauraient qu'il y avait un problème.

Une tentative pour empêcher l'interposition d'un attaquant dans les transactions serait, pour le script ActiveX en provenance du serveur de vote, de signer l'adresse IP de la destination finale de SSL en même temps que le bulletin exprimé. Cependant, ce n'est pas une bonne défense: il serait facile pour un agresseur qui s'interpose de battre ces contre-mesures en appliquant une modification simple au script ActiveX au cours de son transport depuis le serveur vers l'électeur. La modification inscrirait définitivement l'adresse IP correcte au bon endroit pour la signature. Naturellement, l'attaquant aurait également à signer à nouveau le script ActiveX ainsi modifié; devenir capable de signer des scripts ActiveX exige de tromper une des autorités de certification, ou tout simplement de leur acheter une clé. Les butineurs sont fournis avec plus de cent clés par défaut auquel on fait déjà complètement confiance, que les utilisateurs finaux le sachent ou pas.

Nous avons soigneusement analysé le système SERVE par rapport à cette attaque et nous en tirons la conclusion que l'attaque serait relativement simple à monter, et qu'elle pourrait réussir.

Au cours de l'analyse de l'anonymat du vote, nous avons découvert une autre vulnérabilité du système SERVE, dans

laquelle le système pourrait être employé pour la vente de voix de la façon suivante. Le vendeur de voix a installé un serveur relais mandataire ("proxy server"), comme décrit ci-dessus, et attire des électeurs sur son serveur. Dans ce cas, les électeurs vont délibérément sur le serveur de l'attaquant, avec le résultat que l'anonymat du vote pourrait être compromis. Puisque l'attaquant pourrait voir comment les personnes ont voté, l'accord de vente de voix pourrait être vérifié. De même, des attaquants désireux d'exercer une contrainte sur des électeurs pourraient employer les mêmes techniques pour savoir comment les victimes auraient voté, augmentant ainsi les possibilités de contraindre des électeurs.

Des attaques d'interposition en tiers dans les transactions pourraient également être employées pour priver de droits civiques des électeurs, augmentant encore le niveau de gravité de cette vulnérabilité. Une fois qu'un attaquant peut agir en tiers interposé dans la transaction, l'attaquant peut complètement exclure le serveur légitime des élections et simuler l'interaction complète du vote avec l'électeur. Bien que le système SERVE ait installé quelques mesures de sauvegardes, celles-ci supposent que l'électeur sait parfaitement à quoi s'attendre lors de la transaction de vote; il est probablement sûr de supposer qu'un attaquant pourrait créer une transaction [fictive] de vote telle que l'électeur la croie correcte. Une fois que l'attaquant peut se substituer au serveur du service des élections, les électeurs sont complètement privés de leurs droits civiques. L'attaquant pourrait les inciter à penser qu'ils ont voté, et les électeurs ne sauront pas que leurs communications n'ont jamais atteint le serveur des élections. Une mesure de sauvegarde dans le système SERVE est que les électeurs puissent vérifier pour constater que leurs voix ont été enregistrées. Ce qui se passerait n'est pas clair si, après l'élection, un pourcentage important des électeurs à distance affirme qu'ils avaient voté mais n'ont pas vu leurs noms. Il est plus vraisemblable que peu d'électeurs prendraient la peine de vérifier. Dans l'un ou l'autre cas, l'élection serait considérablement perturbée.

Des attaques analogues pourraient fonctionner contre le procédé d'inscription sur les listes électorales [électroniques]. Des électeurs pourraient être conduits à croire qu'ils se sont inscrits avec succès, alors qu'en fait ils communiquaient directement avec l'adversaire et ne traitaient pas avec le serveur légitime d'inscription [sur les listes électorales électroniques]. Les électeurs le découvriraient quand, en essayant de voter, ils constateraient qu'ils n'ont pas été enregistrés, ce qui pourrait être une perturbation très grave.

Peut-être la conséquence la plus grave des attaques en interposition en tiers dans les transactions est que les attaquants pourraient s'engager dans la fraude électorale en se substituant au serveur des élections et en observant comment l'électeur vote. Si une voix plaît aux attaquants, un message d'erreur est donné et l'électeur est simplement réorienté vers le service SERVE, serveur légitime des élections, et, dans ce le cas, la voix sera décomptée. Si l'attaquant n'est pas satisfait du bulletin de vote, alors toute la session de vote entière est simulée; dans ce cas, l'utilisateur pense qu'il a voté, mais en fait la voix n'a été jamais reçue par le système SERVE et elle ne sera pas décomptée. Par exemple, un attaquant pourrait faire que des voix pour un candidat soient reçues et décomptées par le système SERVE, alors que des voix pour d'autres candidats ne soient jamais décomptées voire vues par le système SERVE. Ainsi, l'attaquant a pu employer la violation de l'anonymat du vote décrite ci-dessus pour subvertir réellement les résultats de l'élection.

Bien que que les concepteurs du système SERVE soient très doués et bien qu'ils aient essayé d'atténuer plusieurs des menaces liées au vote à distance à travers l'internet, les attaques du riers se plaçant en interposition dans les transactions et les attaques en substitution demeurent des menaces qui ne sont pas maîtrisées dans ce système. Il n'est pas clair pour nous [de voir] comment on saurait éviter de telles menaces dans l'environnement actuel du réseau internet. Ceci est l'une des bases de notre conclusion que le vote à travers internet ne peut pas être rendu sûr pour un usage dans des élections réelles dans un avenir prévisible.

4. Les attaques en refus (déni) de service

Si un intrus pouvait surcharger le serveur des élections sur la Toile ("election web server”) et empêcher ainsi des citoyens de voter, l'intégrité et la signification de l'élection seraient compromises. De telles attaques, où des utilisateurs légitimes sont empêchés d'utiliser le système à cause d'une action malveillante, sont connues sous le nom d'*attaques en refus de service* (DoS Denial of Service). Nous croyons que les attaques en refus de service constituent un risque sérieux pour le système SERVE.

Les attaques en refus de service sont possibles dans la vie quotidienne. Par exemple, la submersion du numéro du téléphone d'une victime sous un déluge d'appels téléphoniques non désirés peut causer suffisamment d'ennuis pour que la victime débranche son téléphone, devant ainsi inaccessible aux appels légitimes. Sur le réseau internet, les attaques en refus de service sont souvent beaucoup plus dévastatrices, parce que les attaques en refus de service sur internet peuvent être automatisées au moyen d'un [micro-]ordinateur, et parce que de telles attaques peuvent souvent être effectuées sur le réseau internet sans y laisser de traces.

Une variante particulièrement nuisible d'attaques en refus de service est l'*attaque distribuée en refus de service* (DDoS Distributed Denial of Service). Dans une attaque de type DDoS, beaucoup de machines attaquantes collaborent pour monter une attaque commune sur la cible. Dans ce scénario, un attaquant pourrait prendre d'abord le contrôle de beaucoup de [micro-]ordinateurs à l'avance en diffusant un virus ou un ver fait pour cela. Dans le jargon des experts de la sécurité des systèmes d'information, les machines compromises sont souvent décrites comme des "zombies" ou des esclaves, parce que l'attaquant y laisse un logiciel caché qui fait obéir aveuglément ces machines infectées aux commandes suivantes de l'attaquant. Les réseaux de "zombies" sont largement répandus aujourd'hui par des intrus pour monter des attaques en refus de service (et pour envoyer du pourriel -"spam"-).

Le refus de service n'est pas une menace théorique; ce risque est bien trop réel. Les attaques en refus de service sont devenues une source constamment croissante d'ennuis depuis plusieurs années. Des outils automatisés pour monter des attaques en DDoS ont circulé dans la communauté des intrus depuis au moins l'année 1999 [HW01], et les intrus constituent couramment de grands réseaux "zombies" de machines compromises. En février 2000, des attaques importantes en DDoS ont été montées contre plusieurs des serveurs sur la Toile de grande visibilité, y compris CNN, Yahoo et eBay[7]. On a découvert plus tard que ces attaques qui ont causé des dégâts avaient été commises par un seul adolescent et depuis l'extérieur des États-Unis[8].

Depuis, les attaques de DDoS sont devenues courantes. Une étude a répertorié plus de 10.000 attaques de refus de service pendant une période de trois semaines en 2001 [MVS01]. En 2001, le ver CodeRed a infecté 360.000 ordinateurs en 14 heures; il a contenait du code pour monter une attaque en DDoS sur le serveur [institutionnel] sur la Toile de la Maison Blanche. (Heureusement, l'attaque de DDoS a été détournée à la dernière minute[9]). En 2003, une élection à travers internet au Canada a été perturbée par une attaque en refus de service le jour de l'élection[10]. Ces exemples ne sont pas isolés; il est beaucoup trop facile de monter des attaques en DDoS, et les coupables sont rarement pris.

4.1 Comment un attaquant pourrait monter une attaque en refus de service

En gros, il y a deux formes principales que peuvent prendre les attaques en refus de service sur internet. Dans la première catégorie, il y a les attaques par lesquelles un adversaire pourrait inonder le raccordement au réseau d'un serveur sur la Toile visé avec des données pourries qui obstrueraient le réseau et empêchent par ailleurs le trafic légitime de passer à travers. La seconde catégorie comprend les attaques dans lesquelles l'adversaire peut surcharger les ressources de calcul du serveur sur la Toile de tâches inutiles qui le maintiennent occupé ; si le serveur est trop occupé, il peut ne pas pouvoir répondre aux demandes d'accès des utilisateurs légitimes. Nous analyserons les deux catégories.

Dans une attaque par submersion du réseau, l'adversaire envoie d'énormes volumes de données en direction de la victime, afin de saturer le raccordement au réseau de la victime et de rendre impossible l'accès des utilisateurs légitimes à la victime. Les serveurs sur la toile du service SERVE sont exposés aux risques de ce type d'attaque ; si leur raccordement de réseau est débordé par une attaque en refus de service, alors les électeurs concernés ne pourront pas voter en utilisant le système SERVE.

7 http://www.nipc.gov/investigations/mafiaboy.htm

8 http://www.cnn.com/2000/TECH/computing/04/18/hacker.arrest.01/

9 http://www.symantec.com/avcenter/venc/data/codered.worm.html

10 http://cbc.ca/stories/2003/01/25/ndp_delay030125

En général, la robustesse d'un serveur de la Toile face à des attaques de submersion du réseau est déterminée en grande partie par le débit du réseau affecté et disponible pour ce serveur. Par exemple, un site Web avec un lien de un Giga bps à l'internet serait aux abois pour pouvoir résister à une attaque distribuée de un Giga bps . Les grands serveurs de commerce électronique ont typiquement un lien de 10 Gbps au plus. À titre de comparaison, les chercheurs ont observé des attaques de DDoS avec des taux de trafic maximum au-dessus de 150 Gbps [MVS01, MPSSSW03]. Il nous semble peu probable que le système SERVE puisse résister à une attaque avec un aussi fort débit en DDoS.

Dans la deuxième catégorie d'attaque en refus de service, l'adversaire envoie beaucoup de demandes apparemment valides à la victime afin d'essayer de surcharger l'ordinateur de la victime et de le maintenir occupé avec du travail inutile. Il y a beaucoup d'opportunités pour de telles attaques, et il serait difficile de les prévoir toutes. À la place, nous décrirons un exemple d'une attaque de cette catégorie, pour en donner l'idée générale. Des principes analogues peuvent s'appliquer à beaucoup d'autres aspects de l'architecture du système SERVE.

Le système SERVE emploie un serveur de la toile protégé par le protocole SSL. Cependant, le SSL est susceptible à une attaque en refus de service. Un adversaire pourrait envoyer beaucoup de demandes de démarrage de nouveaux raccordements en SSL, et le protocole de SSL exige que le destinataire effectue une opération cryptographique lente (typiquement un calcul de clef privée RSA) en répondant à chacune de ces demandes. Le coût exact d'exécution dépend du niveau de sécurité fourni, mais avec les tailles de clés les plus rapides et de sécurité la plus basse qui sont aujourd'hui considérées comme acceptables (c'est à dire, 1024 bits RSA), les ordinateurs modernes peuvent manipuler environ 100 nouvelles demandes de raccordements par seconde; les accélérateurs en matériel élèvent ce chiffre aux milliers de nouveaux raccordements par seconde. Les plus grands serveurs actuels de commerce électroniques peuvent manipuler jusqu'à 15.000 nouveaux raccordements SSL par seconde. Comme point de comparaison, un attaquant pourrait pouvoir lancer environ 500.000 nouveaux raccordements de SSL par seconde, en s'appuyant sur l'hypothèse suivante : Il est plausible qu'un attaquant puisse constituer un réseau "zombie" de 10.000 ordinateurs esclaves, et que chaque ordinateur puisse lancer environ 50 nouveaux raccordements SSL par seconde. En conséquence, un attaquant pourrait produire de 10 à 100 fois plus de trafic SSL que le serveur sur la toile du système SERVE n'est susceptible de pouvoir manipuler. Ainsi, une attaque de type DDoS contre les serveurs de la Toile [protégés par] SSL du service SERVE pourrait rendre le système SERVE inaccessible aux électeurs et perturber une élection en cours.

Malheureusement, atténuer [ces risques] ou répondre aux attaques en refus de service est très difficile. La technologie d'aujourd'hui n'est pas suffisante pour cette tâche. Par exemple, aucune bonne défense contre des attaques de submersion de réseau sur l'internet n'est connue aujourd'hui. Il peut être possible de se défendre contre l'attaque particulière SSL que nous décrivons; cependant, défendre contre toutes les variantes de ce scénario est difficile. Comme un attaquant attaquera le maillon le plus faible dans n'importe quel système, le système SERVE doit se protéger contre toute les attaques possibles en refus de service -une tâche très difficile-.

En résumé, nous sommes inquiets que, quelque soit la quantité d'énergie investie dans des contre-mesures défensives, une protection adéquate contre des attaques en refus de service reste inaccessible avec la technologie dont nous disposons aujourd'hui. Quelque soit le soin apporté par les concepteurs, le système SERVE reste inévitablement en danger.

4.2 Les implications des attaques de refus de service sur SERVE

Un attaquant pourrait monter une attaque en refus de service à grande échelle sur le système SERVE qui rend le serveur de vote du service indisponible le jour d'une élection. Ceux qui votent le jour de l'élection ne pourraient pas voter, mettant en question la validité de l'élection.

Une autre possibilité est que des services de réseau pourraient être neutralisés ou dégradés pour des secteurs où la population particulière est connue pour voter pour un des partis. Les résultats de l'élection pourraient [alors] être déterminés par une telle attaque. La détection d'une attaque aussi sélective de privation de droit civique serait possible, mais savoir comment y répondre n'est pas clair; une fois les scrutins terminés, il peut ne plus y avoir de bon choix.

Bien que le processus de vote à distance d'aujourd'hui prive déjà de droits civiques quelques électeurs, nous craignons que le système SERVE puisse encore aggraver le problème et non améliorer la situation. Nous identifions que les électeurs concernés par UOCAVA ont plus de difficultés pour voter qu'ils ne devraient, et il y a des raisons de croire qu'un nombre significatif (peut-être 20% à 30%, selon certaines évaluations) des électeurs militaires échouent dans leur tentative de voter à distance [par correspondance]. Néanmoins, le système SERVE court le risque d'aggraver ces problèmes. Avec le système SERVE, il y a la possibilité que le taux de refus des droits civiques s'élève à près de 100%, si une attaque en refus de service est montée avec succès contre le système SERVE. En outre, le système SERVE crée le risque de refus sélectif à grande échelle des droits civiques, qui n'existe pas aujourd'hui dans le système de vote à distance. Le refus sélectif des droits civiques à grande échelle est particulièrement problématique parce qu'il pourrait être employé pour influencer les résultats d'une élection.

Une différence importante entre le système SERVE et le vote en personne dans un bureau local est que les électeurs choisis peuvent voter à tout moment pendant une fenêtre de trente jours commençant trente jours avant le jour de l'élection et se prolongeant jusqu'à la fin des scrutins le jour de l'élection. Si des électeurs pouvaient être persuadés de voter tôt dans cette fenêtre de temps, l'impact des attaques en refus de service pourrait être réduit: dans le passé, la plupart des attaques en refus de service n'ont duré que quelques jours, et quand l'attaque se calme, les électeurs touchés pourraient alors voter, si les scrutins n'étaient pas encore clos.

Cependant, on ne peut pas compter sur la fenêtre de trente jours du système SERVE pour défendre contre des attaques en refus de service. Il y a des raisons de croire qu'une grande proportion de la population des électeurs voudra voter le jour [même] de l'élection. (voir l'annexe B pour un exemple). Ceci introduit à la menace des *attaques du “dernier jour” en refus de service* dans lesquelles l'attaquant monte une attaque en refus de service commençant le matin du jour de l'élection et durant jusqu'à la clôture des scrutins. Puisque la réponse aux attaques en refus de service prend du temps, il est probable qu'un attaquant puisse faire toute la journée une attaque du dernier jour en refus de service, de sorte que les services du système SERVE demeurent inaccessibles pour toute la journée de l'élection. Dans un tel scénario, n'importe quel citoyen d'outre-mer qui avait eu l'intention de voter le jour même de l'élection ne pourrait pas voter en utilisant le système SERVE, et il ne pourrait probablement pas trouver un autre moyen de voter avant la fin des scrutins, et il serait ainsi privé de ses droits civiques.

Nous nous attendons à ce que les attaques [potentielles] en refus de service du dernier-jour sachent priver de droits civiques une fraction substantielle de la population qui utilise le système SERVE. Il semble y avoir peu de chances que le système SERVE puisse faire face à de telles attaques. Pour ces raisons, nous considérons les attaques du dernier-jour en refus de service comme une menace significative à la sécurité des élections à travers le système SERVE.

5. Des conclusions

Nos conclusions, qui s'appuient sur les arguments développés dans ce rapport sont récapitulées comme suit :

a) Les systèmes de vote électroniques dits DRE (enregistrement direct électronique) ont été largement critiqués ailleurs pour différentes insuffisances et vulnérabilités de sécurité : leur logiciel est totalement fermé et propriété [d'une entreprise] ; ce logiciel ne subit qu'un examen minutieux insuffisant pendant la qualification et la certification ; ils sont particulièrement vulnérables à diverses formes d'attaques d'initiés (de programmeur ["insider"]) ; et ces DREs n'ont aucun moyen de vérification a posteriori par les électeurs (papier ou autre) qui pourrait en grande partie éviter ces problèmes et améliorer la confiance des électeurs. Toutes ces critiques, que nous approuvons, s'appliquent tout aussi bien directement au système SERVE.

b) Mais en outre, comme le système SERVE est sur le [réseau] internet et utilise des micro-ordinateurs de type PC, il a beaucoup d'autres problèmes fondamentaux de sécurité qui le laissent vulnérables à une variété d'attaques bien connues en SSI ["cyberattack"], (attaques d'initié, attaques en refus de service, attaques par substitution, automatisation d'achats de voix, attaques par virus [informatiques] sur les [micro-ordinateurs] de type PC des électeurs, etc.), dont n'importe laquelle pourrait être catastrophique.

c) De telles attaques pourraient se produire à une grande échelle, et pourraient être lancées par n'importe qui depuis un individu isolé mécontent jusqu'à une agence ennemie bien financée en dehors de la portée des lois des États-Unis. Ces attaques pourraient avoir comme conséquences le refus des droits civiques aux électeurs de façon sélective et à grande échelle, et/ou la violation de l'anonymat du vote, et/ou les achats et ventes de voix, et/ou les échanges de voix au point même même jusqu'au degré de renverser les résultats de beaucoup d'élections en une fois, y compris l'élection présidentielle. Conçues avec soin, certaines de ces attaques pourraient réussir, et cependant rester totalement non détectées. Même si elles sont détectées et neutralisées, de telles attaques pourraient avoir un effet dévastateur sur la confiance publique en élections.

d) Il est impossible d'estimer la probabilité d'une attaque SSI réussie ("cyberattack") (ou d'attaques multiples réussies successivement) sur une élection quelconque. Mais nous montrons qu'il est relativement facile de commettre les attaques dont nous sommes les plus soucieux. Dans certains cas il y a des boites à outils ("kits") facilement accessibles sur le réseau internet qui pourraient être modifiés ou employés tels quels pour attaquer une élection. Et nous devons considérer le fait évident que l'élection générale aux États-Unis offre une des cibles pour attaquant SSI les plus attractives dans l'histoire de l'internet, que les motivations de l'attaquant soient manifestement politiques ou simplement auto-glorificatrices.

e) Les vulnérabilités que nous décrivons ne peuvent pas être corrigées par des changements d'architectures ou des corrections de bogue au système SERVE. Ces vulnérabilités sont au cœur de l'architecture du réseau internet et ainsi

que l'architecture du matériel et du logiciel de micro-ordinateurs de type PC , toutes deux omniprésentes aujourd'hui. Elles ne peuvent pas être toutes éliminées dans l'avenir sans une avancée [technique encore] imprévue. Il est tout à fait possible qu'elles ne seront pas éliminées sans une reprise complète de l'architecture et le remplacement d'une grande partie des systèmes de sécurité en matériel et en logiciel qui font partie ou sont reliés au réseau internet d'aujourd'hui.

f) Nous avons examiné de nombreuses variantes du système SERVE afin d'essayer de recommander un autre système qui puisse fournir légèrement moins de confort pour les électeurs en échange d'une diminution du nombre ou de l'importance des vulnérabilités de sécurité. Cependant, toutes ces variantes souffrent des mêmes types de vulnérabilités fondamentales que le système SERVE; de façon regrettable, nous ne pouvons recommander aucune d'entre elles.

   Nous suggérons une architecture de kiosque comme point de départ pour architecturer un autre système de vote avec des objectifs semblables à ceux du système SERVE, mais cela ne s'appuie ni sur l'internet, ni sur le logiciel sans garantie des [micro-ordinateurs de type] PC (annexe C).

g) Le système de SERVE pourrait sembler fonctionner sans parfaitement en 2004, sans détection d'attaques réussies. Il est aussi malheureux qu'il est inévitable qu'une expérience de vote apparemment réussie dans une élection présidentielle des États-Unis impliquant sept états serait considérée par la plupart des personnes comme une preuve forte que le système SERVE est un système de vote fiable, robuste, et sûr. De tels résultats encourageraient l'extension du programme par le FVAP dans de futures élections, ou la commercialisation du même système de vote par les fournisseurs aux juridictions dans tous les États-Unis, et aussi bien dan d'autres pays. (L'existence du système SERVE a été déjà citée comme une justification du vote à travers internet dans les primaires du parti démocrate au Michigan.)

   Cependant, le fait qu'aucune attaque réussie n'est détectée ne signifie pas qu'aucune ne s'est produite. Il serait extrêmement difficile détecter de nombreuses attaques, en particulier, si elles sont habilement dissimulées, même dans les cas où elles modifient les résultats d'une élection importante. En outre, l'absence d'une attaque réussie en 2004 ne signifie pas que les attaques réussies seraient moins possibles dans l'avenir; tout au contraire, les attaques futures seraient plus possibles, à la fois parce qu'il y a plus de temps pour préparer l'attaque, et parce que l'augmentation de l'utilisation du système SERVE ou de systèmes semblables rendrait le gain [d'une attaque] plus intéressant. En d'autres termes, un essai "réussi" du système SERVE en 2004 est le haut d'une pente glissante vers des systèmes encore plus vulnérables à l'avenir.

h) Tout comme ceux qui proposent le système SERVE, nous croyons qu'il devrait y avoir un meilleur soutien pour le vote de nos soldats outre-mer. Tout de même, nous regrettons de devoir être contraints de conclure que la meilleure voie est de ne pas employer du tout le système SERVE. Puisque le danger des attaques réussies et à grande échelle est si important, nous recommandons à contrecœur d'arrêter immédiatement le développement du système SERVE et de n'essayer dans le futur aucune solution semblable analogue tant que l'infrastructure du réseau internet et celle des micro-ordinateurs personnels au niveau du monde n'ont pas vu leur architectures refondue, ou que quelques autres avancées imprévues en sécurité ne soient apparues.

Nous voulons rendre clair qu'en recommandant que le système SERVE soit arrêté, nous n'adressons aucune critique ni au FVAP, ni à Accenture, ou ni à qui que ce soit de leurs personnels ou de leurs sous-traitants. Ils ont été complètement conscients tout au long [du projet] des problèmes de sécurité que nous décrivons ici, et nous avons été impressionnés par la sophistication de l'ingénierie et les compétences techniques qu'ils ont consacrées aux tentatives d'amélioration [de la sécurité] et d'élimination des vulnérabilités. Nous ne croyons pas qu'un projet organisé différemment puisse faire un meilleur travail que l'équipe actuelle. La vraie barrière pour le succès n'est pas un manque de vision, de compétences, de ressources, ou de niveau d'engagement ; c'est le fait que, compte-tenu du niveau technique actuel de la sécurité du réseau internet et des [micro-ordinateurs de type] PC, et des objectifs d'un système de vote à distance sécurisé et tout électronique, le FVAP a entrepris une tâche par nature impossible. Il n'y a vraiment aucune bonne façon de construire un tel système de vote sans un changement radical de l'architecture globale du réseau internet et du [micro-ordinateur de type] PC, ou sans une certaine avancée imprévue dan le domaine de la sécurité. Le projet du système SERVE est ainsi beaucoup trop en avance sur son temps, et devrait attendre jusqu'à ce qu'il y ait une infrastructure de sécurité significativement améliorée pour pouvoir se construire dessus.

Remerciements

Nous remercions Kim Alexander, le docteur Steve Bellovin, Lillie Coney, le professeur David Dill, le professeur Doug Jones, Yoshi Kohno, le professeur Deirdre Mulligan, le professeur Ron Rivest, le professeur Gene Spafford and Adam Stubblefield pour leurs commentaires utiles.

Références:

[AK96] Ross Anderson and Markus Kuhn, “**Tamper Resistance - a Cautionary Note,**” Proceedings of the Second Usenix Workshop on Electronic Commerce, pages 1-11, November, 1996.

[Garman81] John R. Gamran, “**The “bug” heard round the world,**” ACM Software Engineering notes, 6(5):3, October, 1981.

[HW01] Kevin J. Houle, George M. Weaver, “**Trends in Denial of Service Attack Technology**”, October 2001.

[Kohno03] Tadayoshi Kohno, Adam Stubblefield, Aviel D. Rubin, and Dan S. Wallach, “**Analysis of an Electronic Voting Machine**”, Johns Hopkins Information Security Institute Technical Report TR-2003-19, July 23, 2003.

[MVS01] David Moore, Geoffrey M. Voelker, Stefan Savage, “**Inferring internet Denial-of-Service Activity**”, Usenix Security 2001.

[MPSSSW03] David Moore, Vern Paxson, Stefan Savage, Colleen Shannon, Stuart Staniford, Nicholas Weaver, “**Inside the Slammer Worm**”, IEEE Security & Privacy 2003.

[Pfleeger03] Charles P. Pfleeger and Shari Lawrence Pfleeger, **Security in Computing** third edition, Prentice Hall, 2003.

[SPW02] Stuart Staniford, Vern Paxson, Nicholas Weaver, “**How to Own the Internet in Your Spare Time**”, Usenix Security 2002.

Annexe A

Le corps principal du rapport couvre certains des risques de sécurité les plus sérieux en grand détail, mais nous n'avons pas essayé d'en donner une liste approfondie. Cette annexe est prévue pour compléter cette liste. Dans cette annexe, nous discutons brièvement plusieurs autres questions de sécurité qui créent également des risques sérieux pour le système SERVE.

Des vulnérabilités dans des serveurs pourraient ouvrir une brèche dans la sécurité des élections

Le système SERVE utilise des ordinateurs centralisés (serveurs) pour enregistrer et expédier des voix. Si ces serveurs sont compromis, chaque bulletin exprimé [passant] par le système SERVE pourrait être modifié ou remplacé, et l'intégrité de l'élection toute entière serait atteinte de façon irréparable. Puisque les serveurs sont un point central unique de risque, il est absolument essentiel qu'ils résistent aux attaques.

Le risque d'intrusion dans les ordinateurs centralisés du système SERVE est, malheureusement, significatif. Le système SERVE a déployé une architecture de gardes-barrières ("firewall") soigneuse et bien faite conçue pour bloquer beaucoup de types d'attaques directes; cependant, il reste des vulnérabilités potentielles dans le logiciel exposé au monde extérieur qui pourraient permettre à des attaquants, depuis n'importe où sur le réseau internet, de pénétrer les défenses du système SERVE et d'obtenir ainsi le contrôle des serveurs. Quelques exemples de types de vulnérabilités sont des débordements de tampons ("buffer overflows"), des vulnérabilités de chaînes de formatage ("format string"), des bogues de traversée de répertoire ("directory traversal"), des conditions de courses ("race conditions"), des bogues d'écritures croisées ("cross scripting"), des bogues d'injection de commandes SQL ("SQL injection"), des erreurs cryptographiques, et des faiblesses dans les authentifications de sessions. Il est important de comprendre qu'il n'y a aucune méthode exhaustive pour éviter, ou déterminer par des essais ces vulnérabilités et bogues. En conséquence, même le logiciel le plus largement utilisé du monde, après un ensemble d'essais exhaustifs, présente généralement beaucoup de vulnérabilités de ce type. Le système SERVE a déployé plusieurs stratégies de réduction [des risques] que nous n'énumérerons pas ici, mais ces stratégies ne sont pas suffisantes, de notre point de vue, pour ramener les risques à des niveaux acceptables.

Du logiciel digne d'une haute confiance peut être trouvé dans les systèmes critiques pour leur fiabilité tels que des sous-ensembles de contrôles de réacteurs nucléaires, des commandes de vol électroniques des avions commerciaux, le système de contrôle de trafic aérien de la FAA (Federal Aviation Authority), la navette spatiale, et certaines applications militaires. Les architectes de systèmes critiques pour leur fiabilité évitent typiquement l'emploi de logiciels du commerce, parce qu'il est largement reconnu que les pratiques de programmation commerciales "standards" créent un risque inacceptable pour de telles applications. Les architectes des logiciels critiques pour leur fiabilité emploient des techniques connues pour construire des logiciels hautement fiables. Ces techniques raffinées et coûteuses n'ont pas été employées dans le développement du système SERVE. Par conséquent, nous devons reconnaître que les pratiques commerciales "standards" utilisées dans le système SERVE, et dans les logiciels du commerce disponible sur étagères (COTS Commercial Off The Shelf) sur lequel il est construit actuellement conduisent à un risque inévitable d'échec.

Les processus existants restent insatisfaisants pour certifier les logiciels de vote.

La loi électorale dans la plupart des États [de l'Union] exige que tous les systèmes de vote -électronique ou non- soient qualifiés par un laboratoire accrédité au niveau fédéral connu sous le nom d'autorité d'essai indépendante (ITA Independant Test Authority), et puis soumis à l'État pour la certification. Le but manifeste de ces procédures est de s'assurer que le système de vote répond aux normes de vote fédérales volontaires promulguées par le comité fédéral pour les élections FEC -"Federal Election Committee"- (et à l'avenir, par le NIST), et qu'elles se conforment aux lois électorales des États. Il est tentant de placer beaucoup de confiance dans des procédures de certification comme moyens d'empêcher des accidents de sécurité. Nous croyons qu'une telle confiance est sans garantie. Nous donnons comme argument que même un programme prolongé et consciencieux d'essais et d'examen par les personnes les plus qualifiées ne peut pas nous fournir les garanties de sécurité nécessaires. En fait, en général, aucun processus ne le peut, puisque dans la plupart des cas le problème d'établir qu'un programme répond à toutes les exigences particulières de sécurité est connu pour être fondamentalement non résoluble [Pfleeger03].

Avec les systèmes de vote électronique et les systèmes de vote à travers le réseau internet la partie la plus importante du

processus de qualification d'ITA est la revue et les essais du logiciel. Nous donnons comme argument cependant, que cette revue et ces essais ne garantissent pas et ne peuvent pas garantir que le logiciel dans les systèmes de vote fait réellement le travail qu'il est censé faire. Dans le monde idéal, on désirerait construire les essais pour vérifier que le logiciel est au moins *correct*, c'est à dire qu'il saisit et compte les voix correctement dans toutes les conditions normales, dans n'importe quelle élection possible, et avec n'importe quel comportement légal d'électeurs. Il devrait également vérifier que le logiciel est *robuste* et *fiable*, c'est à dire qu'il fonctionne raisonnablement même en présence de divers scénarios de bogue et d'incidents, y compris les comportement aberrants de la part des utilisateurs (tels que les employés et les électeurs, etc...) ; et que le logiciel est *sûr ou sécurisé* ,c'est à dire qu'il ne contient aucune logique malveillante interne (code de cheval de Troie) et n'est vulnérable à aucun des scénarios externes d'attaques potentielles dans une vaste gamme .

Malheureusement, cependant, ni les ITAs, ni n'importe qui d'autre ne pourrait, même à distance, réaliser la revue et les essais de façon suffisamment complète pour établir n'importe laquelle de ces propriétés parce que le temps et la main d'œuvre nécessaires seraient vraiment astronomiques. Il y a des limites fondamentales à ce que les essais peuvent obtenir ; c'est un truisme du monde du logiciel de dire que "*les essais peuvent être employés pour vérifier que des bogues et des vulnérabilités de sécurité sont présentes, il peuvent ne jamais prouver qu'ils sont absents*".

Ce que font réellement les ITAs pour qualifier les logiciels des systèmes de vote est bien moins que l'idéal. Ils simulent des élections avec des bulletins de tests pour vérifier que le logiciel apparaît fonctionner comme cela est exigé dans des conditions normales. Cette quantité d'essais est probablement suffisante pour détecter des erreurs simples de programmation et des défauts évidents, bien que ceux-ci aient été déjà probablement trouvés par les développeurs. (Nous ne le savons pas vraiment parce que, comme nous le noterons plus tard, les résultats de ces essais dans le système SERVE sont secrets.) Mais d'une manière générale, un processus d'essais ne peut pas être prévu pour faire plus que filtrer et expurger les bogues les plus évidentes, laissant intactes des bogues plus subtiles qui sont déclenchées moins fréquemment. Et on peut dire assurément que les ITAs font très peu d'essais pour examiner la fiabilité des logiciels, la sécurité, ou les problèmes de codes malveillants, car les essais sont généralement inefficaces pour ces objectifs.

À côté des essais, les ITAs examinent également le code source du logiciel. La majeure partie de l'examen du code est sous forme de programmes ("scripts") automatisés qui parcourent le texte source et y recherchent les propriétés simples exigées par les normes du FEC, par exemple s'il y a des commentaires suffisants dans le code, si les modules dans les programmes ne sont pas trop longs, et si chacun a bien une seule entrée et une seule sortie. Ce sont des conditions de syntaxe et de style qui sont seulement des indicateurs bruts de bonnes pratiques en matière d'ingénierie du logiciel; elles n'indiquent rien du tout quant à la correction, la fiabilité, ou à la sécurité du code.

On nous a dit que les ingénieurs des ITA inspectent également le code source à la main, recherchant des fragments de code apparemment suspects qui pourraient indiquer la présence d'un bogue, d'une vulnérabilité de sécurité, ou de logique malveillante. Si cela est vrai, cela peut donner aux ingénieurs des ITAs une meilleure idée de la compétence en ingénierie du logiciel de ceux qui ont contribué à l'élaboration du programme. Mais il est peu probable qu'une personne hors de l'équipe de développement ne repère beaucoup de bogues subtiles dans une grande quantité de code, parce qu'il ne peut jamais prendre le temps de comprendre entièrement la structure globale du code au niveau de détail nécessaire. Et, contrairement à l'intuition de beaucoup de gens, il est peu probable, à l'extrême, que quiconcque, que ce soit dans l'équipe de développement ou en dehors, ne détecte une logique malveillante qui a été délibérément cachée par un programmeur intelligent, et ce, quels que soient les efforts entrepris pour cette recherche[11]. Il est beaucoup plus facile de cacher une aiguille dans une botte de foin que de l'y trouver [NdT sans outils spéciaux].

Cependant, même si les ITAs devaient faire un excellent travail d'examen du logiciel utilisé dans des systèmes de vote, nous aurions toujours des soucis importants. Il est regrettable que les ITAs fonctionnent sous la même couverture de secret que les fournisseurs de machines à voter. Les essais effectués par les ITAs et les résultats de ces essais sont tous deux secrets. Quand même, il y a quelques éléments que nous connaissons sur la façon dont ITAs ont évalué les machines automatiques à écran tactile (DREs), et il y a d'autres éléments que nous pouvons déduire de quelques incidents flagrants dans les DREs qui n'avaient pas été détectés par les ITAs. Il est raisonnable de supposer que les limitations des ITAs en ce qui concerne les DREs se reproduiront pour la certification du vote à travers le réseau internet.

Par exemple, il y a des différences fondamentales entre les systèmes logiciels modernes et les systèmes de vote précédents. En particulier, les systèmes d'aujourd'hui qui s'appuient sur des logiciels sont plus complexes de plusieurs ordres de grandeur que les machines à voter mécaniques et à papier, et les défis énormes pour la vérification sont créés par cette complexité. Dans une machine à voter mécanique, il y a seulement un certain nombre de pièces mobiles et seulement un certain nombre de manières que le système puisse fonctionner de travers. En revanche, les systèmes logiciels modernes sont exceptionnellement complexes, avec l'équivalent électronique des centaines de milliers ou millions de pièces mobiles; de telles machines peuvent échouer de manières compliquées et imprévisibles. Le fait même que Microsoft et d'autres fournisseurs de logiciel sont contraints de publier des corrections ("patches") fréquentes de logiciel (voir ci-dessous)

[11] Pour un exemple de problèmes qui n'ont pas été détectés par les tests ITA voir [Kohno03]

démontre que la complexité des systèmes logiciels modernes rend impossible de détecter toutes les erreurs de logiciel, encore moins le code malveillant, au moyen de [simples] revues du code et d'essais. Puisque les méthodes courantes sont bonnes pour explorer uniquement les incidents simples, ces méthodes ne sont pas des moyens fiables de certifier le logiciel.

Même si les pratiques en vigueur étaient efficaces pour vérifier que le système de vote se comporte comme il le doit pendant les opérations normales, la sécurité est par définition [l'assurance du bon] comportement du système quand il est soumis à des attaques par une entité malveillante, une situation qui est anormale (espérons le).

Puisqu'il est difficile de prévoir comment des attaquants pourraient se comporter, il est difficile de déterminer des failles de sécurité. Les pratiques existantes peuvent presque certainement être améliorées, mais il y a des limitations sur ce qui peut être réalisé étant donné nos connaissances actuelles.

Il est encore plus difficile de détecter les failles de sécurité intentionnelles qui auraient été installées délibérément par des initiés. Après une analyse soigneuse, nous avons conclu que si un initié malveillant avec un accès au logiciel du système SERVE voulait insérer une porte dérobée dans les systèmes logiciels du système SERVE, il est vraisemblable que l'attaquant pourrait camoufler suffisamment l'attaque pour éviter la détection par les ITAs au cours du processus de certification, particulièrement en l'absence d'une revue de code significative.

Comme si ces problèmes dans le processus de certification n'étaient pas suffisants, il y a une lacune géante dans les exigences du FEC : le logiciel commercial, accessible sur étagères (COTS) n'a pas à être examiné du tout par les ITAs. Il est simplement supposé exempt d'erreurs, de chevaux de Troie, et invulnérable aux attaques externes.

Et, en conclusion, nous notons que pour des systèmes où la sécurité est critique, les essais devraient être faits dans un environnement véritablement hostile. Comme Anderson et Kuhn le précisent dans [AK96], "bien qu'il soit nécessaire de concevoir les systèmes commerciaux de sécurité avec beaucoup plus de soin, ce n'est pas suffisant. Ils doivent également subir des essais hostiles." Le système SERVE a subi des essais en ITA mais ils n'ont pas eu lieu dans un environnement véritablement hostile. Il y a des exemples bien connus de code qui ont subi des essais extrêmes et qui ont échoué une fois déployés dans la réalité. Un exemple qui illustre cela est que la première tentative de lancer une navette spatiale a échoué en raison d'une erreur de synchronisation de logiciel [Garman81]. Très peu de systèmes logiciels sont examinés aussi rigoureusement que celui qui fonctionne sur la navette spatiale, mais un bogue sérieux n'a pas été trouvé avant l'incident [lors du lancement].

Étant donné ces difficultés, ce n'est pas une surprise que les expériences récentes avec la certification des systèmes de vote de logiciel n'ont pas été encourageantes. De façon regrettable, il n'y a aucune bonne solution en vue. La communauté des experts en sécurité des systèmes d'information a lutté à bras le corps avec ces problèmes pendant des décennies, et il est peu vraisemblable qu'ils soient résolus dans un futur proche.

Le logiciel commercial disponible sur étagère (COTS) crée un risque important pour la sécurité des élections.

Le système SERVE s'appuie lourdement sur du logiciel commercial disponible sur étagère (COTS). Les électeurs voteront à partir de [micro-]ordinateurs utilisant un système d'exploitation de Microsoft, et l'infrastructure du système SERVE est construite sur les logiciels d'exploitation et les applications usuels. Nous sommes inquiets car la grande confiance accordée aux logiciels COTS introduit des risques significatifs.

Un des problèmes fondamentaux liés à l'emploi de logiciel COTS dans un système de vote est qu'il est exempté, suivant les instructions du FEC, d'une évaluation par l'ITA pendant la qualification fédérale. Il n'a pas à se conformer aux normes de codage du FEC et son code source n'a pas besoin d'être inspecté du tout. Il n'a pas du tout à faire l'objet d'essais sauf dans le cadre du système de vote complet dont il fait partie. La plus grande partie du logiciel compris dans le système SERVE -des millions des lignes, y compris le cœur cryptographique (c'est à dire le logiciel qui fait les opérations cryptographiques)- est du logiciel commercial disponible sur étagère (COTS) et est ainsi dispensé d'un examen attentif et minutieux.

Quelques avocats de la dispense pour le COTS présentent l'argument que le logiciel COTS est universel -que c'est le logiciel le plus largement répandu au le monde, et donc le plus complètement testé et fiable-. Nous croyons que cet argument est fondamentalement erroné. Alors que nous convenons que le logiciel COTS est largement diffusé, nous sommes en désaccord sur le fait que l'emploi très répandu est une raison de confiance en sa sécurité. En effet, une expérience très étendue de son utilisation a seulement souligné le fait que les logiciels d'exploitation et les applications les plus largement répandues de type COTS soient livrés avec des bogues et infestés de défauts de sécurité. De nouvelles vulnérabilités de sécurité dans les logiciels de type COTS sont découvertes tous les jours. Par exemple, plus de 4.000 nouvelles vulnérabilités sur des logiciels de type COTS ont été signalées dans la seule année 2002. De telles statistiques

rendent vraisemblable que le logiciel COTS sur lequel le système SERVE s'appuie aura beaucoup de vulnérabilités inconnues, dont certaines pourraient compromettre la sécurité des élections si elles sont découvertes et exploitées.

Ceci soulève la question: "Que faisons-nous si une nouvelle vulnérabilité de sécurité est découverte dans le logiciel de type COTS sur lequel le système SERVE s'appuie ?". Actuellement, quand un trou de sécurité est découvert, le fournisseur de logiciel publie une correction ("patch") de sécurité, ce qui se produit assez fréquemment. Puisque les corrections de sécurité modifient le système de vote, le système SERVE doit être soumis à nouveau à un ITA et aux États pour la certification. Cette procédure prend normalement environ deux semaines de la publication de la correction jusqu'à l'installation. Aujourd'hui, il est courant de voir des intrus exploiter des vulnérabilités de sécurité quelques jours seulement après qu'elles aient été annoncées ou après que la correction soit rendue accessible.

Ainsi, d'un côté, un délai de deux semaines peut être trop long pour empêcher l'exploitation des vulnérabilités. D'un autre côté, deux semaines peuvent être insuffisantes pour installer, examiner de façon adaptée, et certifier une nouvelle correction [de sécurité]. Par conséquent, nous croyons que l'utilisation importante de logiciel de type COTS dans le système SERVE, les risques associés [bien] connus en sécurité, et la dispense d'examen pour la qualification représentent des risques significatifs pour le système SERVE.

Annexe B

L'expérience de [vote électronique à distance pour] l'ICANN (Internet Corporation for Assigned Names and Numbers)

Le vote à travers le réseau internet a été utilisé depuis plusieurs années, dans les cas les plus habituels pour des élections privées, comme pour des élections d'actionnaires, ou des élections de responsables d'organismes privés.

Les élections à travers le réseau internet pourraient peut-être être acceptables si les enjeux ne sont pas importants. Par exemple, si les questions sur lesquelles des actionnaires votent ne sont pas controversées, alors il y a peu d'intérêts à subvertir un vote d'actionnaires. En revanche, il y a beaucoup d'intérêts à subvertir des élections présidentielles et ou parlementaires nationales.

En l'an 2000, l'Internet Corporation for Assigned Names and Numbers ((ICANN)[12] [12] a tenu une élection à travers le réseau internet. Toute personne de seize ans ou plus avec une adresse sur le réseau internet avait le droit de voter. Le monde avait été divisé en cinq régions, et des candidats ont été nommés dans chaque région par un comité de nomination. Il y avait aussi une procédure de nomination des membres qui comprenait l'approbation d'un candidat potentiel à travers l'internet.

Des problèmes d'accès au serveur sur la Toile ("web site") officiel se sont produits dans chacune des phases de l'élection à l'ICANN, y compris celle de l'enregistrement des électeurs, celle de l'approbation, et celle du vote. L'ICANN a sous-estimé de manière significative les ressources informatiques qui auraient été nécessaires, d'autant plus que les gens ont eu tendance à attendre jusqu'à la date limite des diverses étapes pour essayer d'accéder au au serveur de l'ICANN sur la Toile. En outre, certains des processus que l'ICANN avait mis en place pour essayer de réduire au minimum la fraude, tel qu'exiger une activation de l'adhésion après qu'un membre se soit enregistré, ont semé la confusion chez les électeurs. Beaucoup d'électeurs ne purent pas voter parce qu'ils n'avaient pas activé leur adhésion à la date limite.

Bien que des mots de passe individuels aient été expédiés à des adresses physiques, certains ont prétendu avoir voté plusieurs fois. Il y a eu également des rapports nombreux de personnes ayant été privées du droit de vote. La privation du droit de vote s'est produite parce que le site Web d'ICANN a croulé sous la demande, parce que quelques électeurs n'ont jamais reçu leurs mots de passe ou les ont perdus après les avoir reçus, et parce que des électeurs ne se sont pas rendus compte que l'enregistrement n'était pas suffisant pour voter. Malgré les difficultés d'enregistrement, environ 158.000 personnes se sont enregistrées. Alors que 76.183 des électeurs enregistrés ont activé leur adhésion, le nombre qui est parvenu à voter pour l'élection n'était que de 34.035[13]. Ces chiffres suggèrent un refus de droit de vote à grande échelle pour les électeurs à chaque étape du processus, avec moins d'un quart des électeurs enregistrés au commencement qui ont voté réellement. Selon le rapport de la Fondation Markle, "les faiblesses techniques du le système d'enregistrement ont rendu pratiquement impossible d'estimer l'intégrité de la liste électorale, la sécurité du code porteur personnel, et l'anonymat du vote.”

Il y avait également des rumeurs au sujet de pays ou d'entreprises concurrents de mettre la main su la liste des électeurs pendant les phases postérieures à la période d'enregistrement. Les problèmes techniques ressentis pendant le premier jour du vote, qui eut lieu durant une période de dix jours, créèrent, selon le rapport Markle "un problème de crédibilité ... avec des électeurs et des ayant droits intéressés qui observaient le processus".

[12] L'un des auteurs de cet article, Barbara Simons, avait été choisie par le processus de nomination des candidats; elle était le second en Amérique du Nord, laissant la place à Karl Auerbach.

[13] **Report on the Global, On-Line, Direct Elections for Five Seats Representing At-Large Members on the Board of Directors**, a report by the Markle Foundation, http://www.markle.org/News/Icann2_Report.pdf

Annexe C

Une [solution] alternative au système SERVE

Bien que nous soyons inquiets parce que l'architecture du système SERVE a trop de vulnérabilités sérieuses pour une utilisation dans des élections publiques, nous convenons néanmoins qu'il y a un besoin d'abaisser des obstacles à un accès au vote pour les Américains d'outre-mer et les militaires. Ici nous proposons une autre architecture alternative qui, selon nous, dispose de la plupart des avantages qu'offre le système SERVE, mais avec beaucoup moins de vulnérabilités. Nous ne proposons pas que ce schéma soit adopté, mais nous proposons que ce soit un meilleur point de départ pour un système de vote destiné à cette population.

Les difficultés rencontrées avec le système SERVE dérivent de trois choix fondamentaux d'architectures: il emploie lourdement le réseau internet, avec toutes les vulnérabilités que cela implique (par exemple, le refus de service, la substitution [frauduleuse], et les attaques d'interposition en tiers dans les transactions). Il s'appuie sur des électeurs qui utilisent des [micro-ordinateurs de type] PC privés, sans sécurité et munis du logiciel privé et commercial configuré pour accepter du code mobile, avec toutes les vulnérabilités que cela implique (par exemple, des attaques de virus, divers types de violations des données personnelles). Et le système SERVE lui-même est un logiciel [appartenant à une firme] privée, avec toutes les vulnérabilités que cela implique (par exemple, des trous de sécurité, des bogues, des fraudes d'initiés).

Nous suggérons de construire un système qui évite les dangers de ces choix d'architecturaux. Voici comment il pourrait être fait :

a) Le système s'appuierait sur des kiosques, à placer dans les consulats et les bases militaires à des emplacements importants autour du monde. Les électeurs viendraient au kiosque pour voter, plutôt que de voter depuis leurs propres PCs.

b) Le logiciel sur le kiosque serait amorcé à partir d'une copie propre, maintenue et configurée par des fonctionnaires qualifiés pour les élections de sorte que l'environnement de logiciel sur la machine de vote soit connu et contrôlé.

c) Le kiosque n'est jamais connecté au réseau internet; par conséquent, aucune attaque relative au réseau internet n'est possible. Il reçoit le logiciel et les bases de données par l'intermédiaire de disques (tels que DVD à écriture unique mais relecture multiple "WORM Write Once Read Many") livrés par courrier recommandé avant l'élection. Il ne transmet pas les bulletins en retour aux comtés par internet; bien plutôt, il les imprime, et ils sont expédiés en retour aux comtés, juste comme pour n'importe quel autre vote à distance.

d) Le kiosque a trois bases de données qui lui permettent d'exécuter les fonctions du vote. Les trois ensembles tiennent sur un disque de DVD-WORM.

   i) Une base de données d'identification pour authentifier tous les électeurs qui se sont enregistrés pour voter par l'intermédiaire du système de système SERVE. Ceci aurait tout au plus 6 millions d'articles, puisque c'est la taille de la population concernée,

   ii) Une base de données d'enregistrement d'électeurs pour indiquer quelle type de bulletin (modèle) chaque électeur est censé recevoir. Ces données sont compilées de l'information fournie par toutes les juridictions des comtés aux États-Unis qui souhaitent participer (3000+). Il y a approximativement 200 millions d'électeurs enregistrés aux États-Unis, mais seulement au plus 6 millions d'enregistrement correspondent à ceux qui sont concernés pour voter par l'intermédiaire du système SERVE.

   iii) Une base de données nécessaire d'image de bulletins, contenant une représentation en PDF ou en XML de chaque modèle de bulletin de vote utilisé dans chacun des comtés aux États-Unis qui participent au système SERVE. Il y a de l'ordre de 100.000 tels modèles de bulletin de vote. Ceux-ci également seraient fournis par l'autorité électorale (LEO) dans les comtés qui participent au système SERVE.

e) L'électeur présent au kiosque s'identifie en utilisant l'identification militaire ou toute autre information d'authentification fournie par le système SERVE. Le kiosque vérifie que l'électeur est enregistré pour voter, et recherche quel est le bulletin à afficher. Alors l'électeur indique ses choix sur un écran tactile et imprime un vote exprimé sur un bulletin de vote. L'électeur examine le vote imprimé pour s'assurer qu'il indique correctement ses choix. (si ce n'est pas le cas, l'électeur voit le fonctionnaire local responsable de l'élection pour l'aider à annuler le vote et effectuer un nouveau vote.) Cette dernière étape prévoit un bulletin vérifiable par l'électeur, et s'assure ainsi qu'aucun bogue potentiel ou cheval de Troie logique dans le code du système ne peut enregistrer de façon inexacte

les intentions de vote.

Enfin, l'électeur dépose le vote exprimé sous enveloppe adressée à son comté d'origine pour un renvoi par la poste, tout comme un vote à distance traditionnel.

Le système que nous avons décrit est essentiellement une imprimante à distance de bulletins située près de la plupart des Américains dans le monde entier. Sa conception devrait être un peu plus détaillée avec des fonctions et des procédures additionnelles de sécurité. Ces procédures seraient chargées d'empêcher le vote multiple, de contrôler des clefs de chiffrement pour les bases de données, et déterminer quels genres d'enregistrements électroniques des transactions de vote les machines gardent et ce qu'elles font de ces enregistrements.

Nous insistons sur le fait que cette architecture n'est pas un système complet; c'est seulement un point de départ. Les détails devraient être établis, et ce processus pourrait toujours présenter des questions imprévues. Pour cette raison, nous croyons qu'il est crucial qu'un tel système subisse une revue hostile, et que toutes les communautés appropriées soient impliquées dans la conception et l'évaluation du système. Cependant, si on y met le soin approprié, nous croyons qu'un tel système pourrait fournir les avantages significatifs. Un tel système réduirait la transaction de vote de trois à un seul échange par le courrier, et avec un développement approprié nous prévoyons qu'il pourrait être rendu bien moins vulnérable que le système SERVE à n'importe quel genre d'attaque à distance ou programmée.

Annexe D

Dans cette annexe, nous travaillons sur certaines des questions qui sont souvent mal comprises au sujet du logiciel, quant à la difficulté de trouver du code ou des failles cachées dans les programmes. Nous analysons également pourquoi le réseau internet et les [micro-]ordinateurs personnels courants ne sont pas des plates-formes appropriées pour des applications de vote.

La détermination que du logiciel est exempt de bogues et de vulnérabilités de sécurité est généralement impossible

En mathématiques, il y a une longue histoire de résultats profonds en matière d'impossibilité, c'est à dire des théorèmes déclarant que certains problèmes sont fondamentalement impossibles à résoudre quels que soient les efforts ou les réflexions qu'on y applique. Par exemple, la trisection d'un angle est impossible (le diviser en trois parts égales) par des moyens classiques de la règle et angle droit; il est impossible de résoudre un polynôme du cinquième degré (équation polynomiale en X5) en utilisant seulement l'addition, la soustraction, la multiplication, la division et l'extraction des racines [carrées] ; il est impossible de construire une axiomatique cohérente et complète (ensemble de règles) pour l'arithmétique.

La théorie de la calculabilité a obtenu beaucoup de tels résultats, désignés sous le nom des problèmes non résolubles ou non calculables. Ils sont typiquement de la forme suivante: "il n'existe aucun programme d'ordinateur qui peut faire X". Le premier et le plus célèbre de tels résultats, dû à Alan Turing, est connu comme le problème de l'arrêt : il n'existe aucun programme H qui peut déterminer (en un nombre fini d'étapes) si un autre programme P arbitraire s'arrête ou pas. Ni langage de programmation employé ni l'ordinateur utilisé n'ont d'importance, ni sa vitesse, ni sa mémoire disponible, ni la longueur du programme etc.; il n'y a simplement aucun programme H qui peut résoudre le problème de l'arrêt.

Si un problème est non résoluble dans ce sens, alors des personnes ne peuvent pas le résoudre non plus. Ceci peut sembler contraire à l'observation commune qu'il y a des choses que les humains peuvent faire facilement et qu'aucun programme machine ne peut faire, par exemple comprendre l'anglais; mais ce sont là des exemples de choses qu'aucun programme déjà écrit ne peut faire, plutôt que des exemples des choses qu'aucun programme ne pourrait faire. En général, si des personnes peuvent accomplir une tâche de traitement de l'information, alors elles le font en utilisant une certaine méthode dans le cerveau. Nous pouvons ne pas connaître la méthode; mais si nous la connaissons, nous pourrions écrire le programme (complexe) qui simule la même méthode et accomplit la tâche aussi bien. Il existe bien un programme qui comprend l'anglais, même si personne ne sait à l'heure actuelle comment l'écrire, ainsi la compréhension de l'anglais n'est pas un problème non résoluble.

Malheureusement plusieurs des questions importantes que l'on pourrait poser sur le comportement du logiciel -- son caractère correct ("correctness"), sa fiabilité ("reliability"), ou sa sécurité -- se révèlent être des problèmes non résolubles. Voici une liste partielle de tels problèmes qui sont relatifs au caractère correct des programmes (absence de bogues), à la sécurité des programmes, et à la protection des données privées nécessaires pour les logiciels utilisés dans des élections. Elles sont énoncées de manière non formelle parce que l'appareil mathématique pour les énoncer avec précision est au delà de la cible visée par ce rapport ; mais chacun d'entre eux a pu être formalisé et prouvé mathématiquement.

Il est impossible de déterminer en un nombre fini d'étapes, pour un programme donné:

- s'il s'arrête (une formulation simplifiée du problème d'arrêt) ;
- s'il a un type particulier de bogue (par exemple une erreur de limites de tableau, erreur de dépassement de barrière -"fencepost"-, pointeur dans le vide) ;
- s'il est correct (c'est à dire s'il correspond aux caractéristiques décrites "spécifications") ;
- s'il a une fonctionnalité cachée (c'est à dire s'il fait des choses supplémentaires non mentionnées dans ses caractéristiques, en particulier des actions malveillantes) ;
- s'il préserve les données privées (s'il ne conserve pas et ne divulgue pas l'information qui ne devrait pas l'être) ;
- s'il est fiable (c'est à dire fait quelque chose de raisonnable malgré divers genres de défauts, par exemple sur la mémoire, les communications, ou défauts de logiciels) ;
- s'il est sécurisé (c'est à dire exécute son travail en dépit de divers genres d'aggressions).

La lecture de cette liste devrait vous fournir l'impression qu'au sujet de tout ce que vous voulez vraiment connaître du comportement d'un logiciel important, y compris des logiciels pour les élections, reste justement impossible à déterminer

de façon certaine. Et c'est en effet le cas. S'il y avait une manière sûre de détecter des bogues dans les programmes, alors les logiciels commercialisés seraient exempts d'erreurs. Et s'il y avait une manière infaillible de trouver ou d'éviter des vulnérabilités de sécurité, alors les compagnies productrices de logiciels de systèmes d'exploitation emploieraient ces méthodes, et n'auraient pas à publier des corrections de sécurité de façon régulière.

Si tous ces problèmes logiciels importants sont non résolubles, comment donc fait-on, pour arriver à construire du logiciel sécurisé. C'est le sujet de l'ingénierie du logiciel. La réponse générale est que, avec suffisamment d'analyse soignée mathématique et algorithmique en avance de phase, avec suffisamment de soin et de discipline méthodique de la part des programmeurs, avec un contrôle féroce pour obtenir une architecture simple, avec suffisamment d'essais systématiques et aléatoires du logiciel, avec des preuves formelles que les parties critiques du programme ont bien les propriétés critiques, et avec assez d'ouverture pour que le logiciel puisse être contrôlé par beaucoup d'experts, alors la fréquence des défauts tels que des bogues, ou des vulnérabilités de sécurité peut souvent (mais pas toujours) être diminuée à un niveau tolérable. Mais il n'existe aucune méthode pour écrire du logiciel totalement indemne de bogues, ou de logiciel totalement sécurisé ; et si par un miracle un tel logiciel devait être créé, il n'y a aucun moyen général de prouver qu'il est exempt d'erreurs ou sécurisé. C'est la réalité mathématique. Quiconque annonce qu'un programme donné non trivial est exempt d'erreurs ou sécurisé simplement parce qu'il a été largement répandu ou complètement testé est mal informé. Les utilisations ou les essais, quel que soient leur nombre, sont insuffisants pour le prouver.

Bien qu'il y ait eu des recherches substantielles sur de nouvelles méthodes pour l'ingénierie du logiciel, par exemple, le code source contenant des preuves et l'analyse statique de programme, parmi d'autres, ces technologies ne sont actuellement pas encore mûres, et elles sont loin d'être applicables au type complexe de logiciels nécessaires pour les élections.

Du code malveillant.

Le logiciel est généralement conçu pour servir à un objectif clair, bien documenté, et les personnes comptent bien qu'il fasse ce que ses caractéristiques et sa documentation indiquent. Mais du logiciel peut être écrit pour faire d'autres choses en plus de, ou au lieu de, ce qu'il est censé faire, c'est à dire il peut avoir une fonctionnalité secrète ou cachée qui n'est pas documentée. Parfois c'est légitime, mais parfois la fonctionnalité cachée est malveillante, c'est à dire qu'elle fait quelque chose que le programmeur ou le fournisseur veut, mais que l'utilisateur ne veut pas, et elle le fait donc à l'insu de l'utilisateur. Un tel code malveillant pourrait espionner l'utilisateur en envoyant subrepticement des informations confidentielles à un serveur de la Toile sur le réseau internet; il pourrait lancer des publicités à la figure de l'utilisateur ; il pourrait neutraliser des protections de sécurité [présentes] sur l'ordinateur pour permettre des effractions ultérieures par des personnes non autorisées; il pourrait installer d'autres programmes non désirés; il pourrait faire des dégâts au hasard en supprimant des données ou des dossiers ; ou il pourrait faire n'importe laquelle de mille autres choses malveillantes.

Les termes de *cheval de Troie*, de *virus*, et de *ver* désignent tous des types de code malveillant, qui ne diffèrent que par les moyens par lesquels ils réussissent à atteindre l'ordinateur et y sont activés. La plupart des personnes sont informées de l'existence des virus de courrier électronique, qui sont du code malveillant sous forme de pièces jointes de courrier, mais il y a beaucoup d'autres voies d'infections, y compris, par exemple, les codes malveillants en langages interprétés -"scripts"- (Control ActiveX, programmes en Javascript, ou des "appliquettes" en Java) qui peuvent entrer dans votre ordinateur comme un effet secondaire invisible de la visite d'une page sur la Toile ["web page"]. Le code malveillant est l'une des menaces de sécurité les plus sérieuses pour toute application, parce qu'il est si facile à installer, et si difficile à détecter.

Dans le contexte du système de vote du système SERVE, le code malveillant est une menace de deux façons distinctes. D'abord, il est possible qu'un initié (un des programmeurs qui construit le système SERVE) puisse insérer le code malveillant dans le logiciel de système SERVE lui-même, peut-être pour espionner les voix exprimées ou pour en éliminer de façon sélective. (Nous ne suggérons pas du tout que ce soit probable ; mais le fait est que [c'est possible et] ce ne peut être exclu.) L'autre menace est du code malveillant qui infecte les ordinateurs des électeurs, de sorte qu'il espionne le processus de vote, ou empêche de voter, ou même change des voix sans être détecté.

Il est important de comprendre, comme cela a été discuté plus haut, qu'il n'y a aucun essai incontestable pour savoir si du code non malveillant est installé. Les détecteurs de virus, par exemple, peuvent détecter la présence des virus qui ont été vus auparavant, étudiés par des experts, et pour lesquels une empreinte a été extraite ; mais ils ne peuvent pas détecter de nouveaux virus à coup sûr. Même des experts avec un accès au code source d'un programme peuvent ne pas pouvoir dire s'il contient du code malveillant, puisqu'il est relativement facile de déguiser le code malveillant de sorte qu'il soit extraordinairement difficile de le trouver.

La défense la plus puissante contre de la logique malveillante est, en ce qui concerne la sécurité des élections, de ne pas dépendre du tout de sa détection, et de structurer le système de vote pour pouvoir garantir que cela fonctionne correctement

même si de la logique malveillante est présente. Les journaux vérifiables rétrospectivement par les électeurs sont parmi les dispositifs les plus simples et les plus forts qui puissent fournir de telles garanties (bien qu'il puisse y en avoir d'autres). Mais à notre avis une certaine forme de protection contre la logique malveillante est impérative pour n'importe quel système de vote s'appuyant sur du logiciel.

Les faiblesses de sécurité de l'internet

L'internet révolutionne la communication, le commerce, et le divertissement, mais suivant des voies qui n'ont été jamais envisagées par ses concepteurs. Les protocoles de base de transmission de données, d’attribution de nom, et de choix de route [cheminement des paquets], toujours en service sur l'internet d'aujourd'hui, appelés collectivement TCP/IP, ont été conçus vers la fin des années 1970 et le début des années 1980, à une époque où tous les utilisateurs du réseau formaient une communauté unique, quand les ingénieurs du réseau se connaissaient tous personnellement, et qu'il y avait une confiance universelle entre les utilisateurs. Il y avait peu de besoins de sécurité parce que la communauté des utilisateurs était petite et chacun coopérait. Les buts principaux des protocoles originaux de l'internet étaient l'adaptabilité à grande échelle, la facilité d'utilisation, les performances en communication, et la fiabilité ; la sécurité n'était pas une priorité, et les questions n'étaient pas, à cette époque, bien comprises de toutes façons.

Mais aujourd'hui, alors que la taille de l'internet s'est multipliée par plusieurs millions, l'internet reste une fédération mondiale volontaire de réseaux de grande diversité, sans autorité centrale et ni culture ou ni buts communs. Il relie des centaines de millions de personnes et d'organismes qui sont la plupart du temps des étrangers les uns pour les autres, mais parfois concurrents ou même ennemis. Dans un tel environnement, la sécurité est d'une profonde importance, et beaucoup de protocoles de sécurité ont été placés au-dessus des protocoles de base avec pour objectifs de sécuriser certains types d'applications, comme par exemple le courrier électronique ou les transactions financières, contre certaines menaces spécifiques.

Cependant, quelle que soit l'importance de la sécurité aujourd'hui, l'internet n'a aucune architecture générale de sécurité; en fait, il est bien connu pour être riche de vulnérabilités très générales. Il se fonde sur la coopération volontaire de milliers d'entreprises autour du monde pour maintenir cohérente son infrastructure d’attribution des noms [des objets] et de choix des routes [cheminement des paquets], et il emploie des adresses publiques et falsifiables pour l'origine de chaque paquet qu'il transmet. En conséquence, il n'est pas possible de garantir exactement où un paquet de données émis sera envoyé, ou bien d'où un paquet reçu est venu. Ces limitations sont la raison de fond pour laquelle il est si facile commettre des attaques en substitution d'identité ("spoofing") et en interposition en tiers ("man in the middle") et qu'il est si difficile de se défendre contre elles dans toutes les applications sur internet, pas seulement dans le cas des élections. De même les commutateurs de paquets ("routers") et les serveurs, distribués partout dans le monde, qui forment l'infrastructure de plus haut niveau du réseau internet ne sont eux-mêmes que des ordinateurs avec leur propre tableau de vulnérabilités de sécurité, connues et inconnues ; ils sont souvent facilement falsifiés, par des initiés [au courant de leur nature] ou des agresseurs extérieurs.

Il est extrêmement difficile de construire une application entièrement électronique sécurisée [et sûre] entièrement appuyée sur internet, par exemple un système bancaire, un système judiciaire [ou de contrôle de légalité], ou un système pour les élections, en s'appuyant sur une telle fondation fondamentalement faible pour la sécurité. À notre avis, personne ne devrait essayer une telle chose sans des moyens de vérifications à posteriori par les électeurs [bulletins papiers imprimés] et en utilisant des canaux hors bande (c'est à dire hors internet) de communication entre l'autorité chargée des élections et l'électeur, ou bien sans un saut qualitatif en sécurité encore inconnu.

Faiblesses de sécurité du micro-ordinateur personnel (PC)

La plate-forme de micro-ordinateur personnel (PC) qui est employée comme la machine pour exprimer le vote dans le système SERVE est un autre élément dangereusement faible de l'architecture de sécurité. Un micro-ordinateur utilisant le logiciel Windows est très facilement compromis, et jamais autant que quand il est connecté à l'internet.

Le micro-ordinateur personnel (PC) a été à l'origine conçu comme un système possédé et maintenu individuellement par une seule personne (c'est pourquoi il est appelé un micro-ordinateur personnel -PC-). Ce fait a semblé réduire au minimum les besoins de sécurité sophistiqués puisque l'unique détenteur et utilisateur pourrait toujours se faire confiance à lui-même. L'internet n'avait pas à l'origine une préoccupation de sécurité [pour ces machines] parce que la famille des architectures de PC a été conçue au début des années 1980, longtemps avant qu'il y ait eu une idée que les PCs seraient directement reliés à l'internet [*NdT ???*]. De toute façon, on a généralement fait l'hypothèse que quelle que soit la sécurité légère qui puisse être utile, comme la protection par mot de passe, elle pourrait être mise en application entièrement dans le logiciel de façon

satisfaisante.

En conséquence, le matériel des PCs a évolué jusqu'à ce jour essentiellement sans aucun souci pour la sécurité. La plupart des cartes mères de PC, par exemple, ne contiennent aucune clé cryptographique qui résiste à la falsification et puisse être employée comme élément de base pour l'identification, et ni aucune source de véritables nombres aléatoires pour la génération de clés cryptographiques. En outre, les dispositifs principaux d'interface homme machine pour des PCs (clavier, pointeur [souris, ...] , écran, ou haut-parleurs) ne sont pas conçus pour savoir effectuer des opérations cryptographiques. Ceci a l'effet de contraindre à manipuler des données critiques en clair (non chiffré) sur l'espace principal du PC, là où il est vulnérable aux logiciels malveillants.

L'ensemble des logiciels de Microsoft pour le PC a également été à l'origine conçu sans penser à la sécurité. Les buts primaires de l'architecture de Windows et d'internet Explorer ont été le maximum de fonctionnalités et de facilités d'utilisation, mais pas la sécurité. Ce n'est que tout récemment que Microsoft fait de la sécurité une priorité importante, mais leurs systèmes d'exploitations sont encore bien connus pour être complètement truffés de vulnérabilités de sécurité. En vérité, pendant des années, pas une seule semaine n'a passé sans publication de plusieurs corrections de sécurité par Microsoft. En vérité, pour mieux contrôler le problème, Microsoft a commencé à traiter en lots [mensuels] les corrections de sorte que des paquets de corrections sont livrés mensuellement.

Windows est particulièrement vulnérable aux attaques malveillantes en logiciel. Il y a tant de formes de logiciel, et tant de vecteurs de transmission, qu'il est impossible de les contrôler toutes. Des utilisateurs sont constamment encouragés à télécharger et installer des logiciels, parfois [même] sans le savoir, y compris les mises à jour et les corrections du système d'exploitation et du butineur, des modules de gestion de périphériques, des extensions pour des butineurs et d'autres applications, des instructions interprétables ("scripts") liés aux pages Web et aux documents de bureau, des programmes en partagiciel ("shareware"), et naturellement, des applications complètes. N'importe lequel de ces types de programmes peut contenir de la logique malveillante qui pourrait complètement miner le degré de sécurité du PC, et donc de tous les bulletins de vote exprimés par ce moyen, sans jamais que l'utilisateur/électeur ne s'en rende compte.

Ces limitations de la sécurité du matériel et du logiciel de PC sont largement reconnues. Un consortium à l'échelle industrielle connu sous le nom d'alliance pour un ordinateur de confiance (“Trusted Computing Platform Alliance”) (http://www.trustedcomputing.org) qui a décrit des additions de matériel à l'architecture des PCs prévues pour remédier à certaines de ses insuffisances de sécurité. Jusqu'ici [janvier 2004], il n'y a aucune réalisation de matériel des descriptions [spécifications] de TCPA et aucune utilisation par un système d'exploitation. Il est possible que, dans quelques années des PCs équipés de TCPA commenceront à être vendus, et que, quelques années plus tard qu'ils remplaceront en grande [NdT?] partie toute la génération courante des PCs. Mais il n'y a aujourd'hui [janvier 2004] aucune description publique des dispositifs et outils de sécurité que Microsoft mettra en application à l'aide du matériel TCPA, ou même s'ils suffiront pour permettre un vote sûr depuis un PC sur l'internet.

Annexe E

Biographies des auteurs

David Jefferson est un informaticien du laboratoire national de Laurence Livermore (LLNL) où il fait de la recherche en calcul parallèle à dimension variable ("scalable supercomputing"). Il a également travaillé pendant plusieurs années dans le domaine de la technologie et de la sécurité pour les élections, comme Président du Comité technique du Secrétaire d'État de la Californie pour un groupe de travail sur le vote à travers internet en 1999-2000; comme membre du comité de direction du groupe [d'experts] de la NSF sur le vote à travers l'internet en 2000-2001 ; et comme membre du groupe de travail du Secrétaire d'État de la Californie sur l'urne électronique à écran tactile en 2003. Il a été en activité au plan national comme orateur et conseiller sur les systèmes de vote électroniques publics, et est après l'avoir présidé, actuellement membre du conseil d'administration de la fondation des électeurs de Californie. Avant de joindre le LLNL, il était informaticien spécialiste aux laboratoires de DEC/Compaq à Palo Alto, et auparavant il avait été professeur associé d'informatique à UCLA, où il était plus connu comme l'inventeur de la méthode de chaîne temporelle de simulation discrète parallèle d'événement ("Time Warp method of parallel discrete event simulation").

Aviel D. Rubin est professeur associé d'informatique et directeur technique de l'institut de la sécurité de l'information à l'université de Johns Hopkins. Avant de joindre l'université Johns Hopkins, Rubin était chercheur aux laboratoires de AT&T. Rubin est auteur de plusieurs livres comprenant "Firewall et sécurité d'internet", deuxième édition (avec Bill Cheswick et Steve Bellovin, Addison Wesley, 2003), "White Hat Security Arsenal" (Addison Wesley, 2001), et "Web Security Sourcebook" (avec Dan Geer et Marcus Ranum, John Wiley et Sons, 1997). Il est rédacteur associé des Transactions de l'ACM sur la technologie d'internet ("ACM Transaction on internet Technology"), rédacteur associé de Sécurité et données privées de l'IEEE (IEEE Security and Privacy"), et membre du comité consultatif pour les collections de livres de la sécurité de l'information et de cryptologie chez Springer. Rubin est membre du conseil d'administration de l'association USENIX et du groupe d'étude technologique en Science de l'information à la DARPA.

Barbara Simons est une consultante en matière de politique technologique. Elle a obtenu un Ph.D. de l'U.C. Berkeley, et était chercheuse en informatique chez IBM, où elle a travaillé sur l'optimisation de compilateurs, l'analyse d'algorithmes, et la théorie de l'ordonnancement des programmes. Simons a été présidente de l'association pour l'informatique ("ACM Association of Computing Machinery"), elle préside Comité de la politique publique américaine de l'ACM (USACM ACM’s US Public Policy Committee). Elle a été membre du conseil du groupe de la NSF (National Science Fondation) sur le vote à travers internet, membre du sous-comité de conseil du Président à l'exportation concernant la cryptologie, et du conseil du Président sur le passage à l'an 2000. Elle est membre de plusieurs conseils d'administration, y compris des fonds d'U.C. Berkeley Engineering ("U.C. Berkeley Engineering Fund") et de l'EPIC centre d'information sur les données privées ("EPIC Electronic Privacy Information Center"), comme du comité consultatif de l'institut internet d'Oxford et du comité consultatif du registre d'intérêt public [des adresses internet en] .ORG. Elle a témoigné devant les représentants des États-Unis et de Californie. Elle est une notabilité ("Fellow") l'ACM et de l'association américaine pour l'avancement de la Science (AAAS). Elle a reçu le prix de la meilleure ancienne élève du département d'informatique de Berkeley, le prix Norbert Wiener du CPSR, le prix pour contribution exceptionnelle à l'ACM, et le prix du pionnier de l'EFF (Electronic Frontier Foundation).

David Wagner est professeur assistant au département d'informatique de l'université de Californie à Berkeley. Il a une expérience étendue en sécurité des systèmes d'information et en cryptologie; et [il a à son actif] plus de 50 publications techniques. Avec ses collègues de Berkeley, il est connu pour avoir découvert une grande variété de vulnérabilités de sécurité dans diverses normes de téléphonie cellulaire, dans les normes 802.11 de réseaux sans fil et d'autres systèmes largement déployés. En outre, il était un concepteur qualifié aux finales pour la norme de chiffrement avancé (AES), et il reste actif dans les secteurs de la sécurité, de la cryptologie, et de la protection des données personnelles et patrimoniales dans les systèmes. Wagner est un titulaire d'un "Alfred P. Sloan Research fellow" et d'une bourse CRA pour le gouvernement électronique CRA (CRA Digital Government).