Säkerhetskrav för Internetröstning

En analys av skillnader mellan konception och realisering

Heiner Schorn

One of the most difficult aspects of Internet voting is to get security right. The ongoing debate in the research community shows that the underlying problems are taken seriously. As this debate has great influence on the conception of actual voting systems, it might seem surprising that almost none of these issues have been addressed in implemented systems. This article analyses some of the differences and shows the risks that are connected with this approach. Taking the possible advantages of Internet voting as a starting point, four different approaches to define an adequate security level are presented and criticised. It is then shown in detail how some of the more important security demands that were addressed by the vendor in their initial proposition were neglected in the implementation used for the Umeå University 2001 student union election. The severity of some of these shortcomings together with the difficulty of defining an appropriate level of security shows the necessity of a more sincere application of basic security needs.

I de flesta länder med demokratisk författning finns det funderingar på om röstning via Internet kan vara ett viktigt komplement till traditionella val eller till och med ersätta dem. På lite längre sikt vilar stora förhoppningar på tekniken. I Schweiz finns det t.ex. planer på att tillåta Internetröstning fr.o.m. 2010 för alla officiella val. För att ta fram ett fungerande system vill man satsa mellan 2 och 3 miljarder svenska kronor (Schweizerische Bundeskanzlei 2002).

Det har redan gjorts försök med Internetröstning vid några officiella

Schorn, Heiner. »Säkerhetskrav för Internetröstning – En analys av skillnader mellan konception och realisering.« *HUMAN **IT*** 6.1–2(2002): 163–187

val som ansetts vara val utan större betydelse. Två av de första försöken var kårvalen i Osnabrück i Tyskland (2–3 februari 2000) och i Umeå ett år senare (27 april–11 maj 2001). Båda försöken har utvärderats. Men trots att tillverkarna av systemen anser att erfarenheterna varit genomgående positiva kan dessa försök mycket väl ha bidragit till en mera skeptisk syn på tekniken.

Även i samband med kommunernas IT-satsning får frågor kring Internetröstning en allt större betydelse. Ju mer information och ju fler diskussionsmöjligheter som erbjuds via nätet, desto mer förefaller Internetröstning eller åtminstone Internetomröstning kunna bli ett naturligt komplement. En följd härav är att kommunerna framstår som en intressant marknad för tillverkarna. Samtidigt uppmärksammar man de erfarenheter som samlas med tanke på Internetröstningens användbarhet i större sammanhang.

I denna artikel analyseras frågeställningar kring valsäkerhet i sådana fall där röstning via Internet är tillåtet. Som alltid när ny teknik betraktas ur säkerhetssynpunkt fokuserar man de aspekter där den nya tekniken antingen medför nya eller större risker än den traditionella eller tvärtom hjälper till att undvika risker som hittills funnits. Ser man på den traditionella valprocessens säkerhet så bygger den i stor omfattning på förtroendet för en fungerande demokrati, och under denna förutsättning kan den anses vara mycket säker. Internetröstningens säkerhet kräver däremot även stor tillit till den underliggande tekniken. Förväntningarna på Internetröstning inriktar sig därför inte på att förbättra säkerheten vid demokratiska val utan mot andra fördelar som jag kommer att presentera senare i samband med granskningen av Internetröstningens säkerhetsimplikationer.

Relevanta studier om röstningsteknik

Det har tidigare genomförts en del intressanta studier om röstningsteknik och Internetröstning utifrån olika perspektiv. De följande tre exemplen är ganska representativa.

Caltech/MIT Voting Technology Project poängterar problematiken

i att Internetröstning för första gången gör det möjligt för enstaka aktörer att lätt kunna förfalska kompletta valresultat (Caltech/MIT 2000, s. 49):

> *Remote Internet voting poses serious security risks. It is much too easy for one individual to disrupt an entire election and commit large-scale fraud.*

California Internet Voting Task Force ser risken, men menar att säkerheten i princip är tillräcklig för framtagning av röstningssystem som bygger på dedikerade röstningsdatorer (CIVTF 2000):

> *It is technologically possible to utilize the Internet to develop an additional method of voting that would be at least as secure from vote-tampering as the current absentee ballot process in California.*

Statskontoret har i sin utvärdering av kårvalet vid Umeå universitet tagit upp frågan ur en mer praktikorienterad synvinkel. I stället för att koncentrera sig på principiella problem eller möjligheter relaterar man dagens begränsade säkerhetsnivå till vissa typer av val (Statskontoret 2001, s. 8):

> *Internetröstning kan vara en lämplig metod för val och omröstningar där det inte ställs absoluta krav på fullständig säkerhet i alla delar av valprocessen, t.ex. kommunala folkomröstningar där Internetröstning bör kunna komplementera brevröstning och vallokalröstning.*

De tre citerade studierna utgår från olika ståndpunkter och accentuerar olika. Alla tre är dock överens om att Internetröstningens inte helt utredda risker kan påverka demokratin på ett negativt sätt. Om det finns allvarliga skäl att ifrågasätta valresultatets korrekthet kan det ha återverkningar på förtroendet för de valda representanterna.

Internetröstning – en säkerhetsfråga?

Frågan om genomförandet av Internetröstning är till att börja med ett politiskt beslut. Men för att beslutet ska kunna fattas måste de risker som är förknippade med tekniken utredas och bedömas.

Begreppet *Internetröstning* omfattar idag allt ifrån möjligheten att rösta från vilken Internetansluten dator som helst till att bara tillåta röstning via Internet från specialkonstruerade datorer i vallokaler.

Säkerhetsproblematiken är svårast att lösa för Internetval från valfria hemdatorer. Samtidigt verkar denna variant intressantast, eftersom den tillför mest jämfört med dagens valsystem. Här behandlas endast denna variant, och i det följande är termen *Internetröstning* således synonymt med röstning via en Internetansluten dator hemifrån.

IT-säkerhet har flera viktiga mål som oftast beskrivs med begreppen *korrekthet*, *autenticitet*, *sekretess* och *tillgänglighet*. Alla fyra är inte alltid lika viktiga, utan deras inbördes viktning bestäms av kontexten. När man publicerar en tidning via webben kan t.ex. sekretess sakna betydelse.

Korrekthet förutsätter att program ska ge de resultat som motsvarar deras specifikationer och att data inte ska förändras vid misstag eller som resultat av medveten förfalskning. Att ett program innehåller fel eller att en angripare förändrar innehållet i en fil är två exempel där korrektheten påverkas.

Autenticitet kräver att datakällan är den rätta och att innehållet är oförändrat. Autenticitet är inte detsamma som korrekthet. Ett datorpostbrev som t.ex. skickats av en annan avsändare än angivet kan vara korrekt enligt ovan utan att vara autentiskt. Ett program som inte är korrekt kan däremot mycket väl vara autentiskt.

Sekretess behövs när informationen inte får komma obehöriga till del. Exempel på detta är inloggningslösenord eller konfidentiella dokument.

Tillgänglighet är ett mått på i vilken omfattning tjänster och data finns till förfogande när de behövs.

Vid Internetröstning är det avgörande att alla fyra mål nås i tillräckligt stor omfattning. Även om den nödvändiga omfattningen är en politisk och inte en teknisk fråga, går det redan nu att konstatera att

säkerhetskraven är en av de största utmaningarna med Internetröstning. Detta gäller särskilt om säkerhetsnivån ska vara jämförbar med den som dagens röstningssystem erbjuder.

Förutom teoretiska resonemang har även de praktiska experimenten bidragit till en bättre förståelse för Internetröstningens effekter. Efter en säkerhetsrelaterad granskning av Internetröstningens tänkbara fördelar kommer jag först att diskutera frågan om lämplig säkerhetsnivå och därefter granska befintliga lösningar närmare.

Vilka fördelar har Internetröstning?

Frågar man sig vilka fördelar Internetröstning erbjuder så finner man egentligen bara två grundläggande förhoppningar: att valförfarandet ska bli mindre kostsamt och att valdeltagandet ska öka. Inom en representativ demokrati innebär ett högre valdeltagande större legitimitet för de valda representanterna, medan sänkta kostnader bl.a. medför bättre förutsättningar för direktdemokratiska inslag. Vid kårvalet i Umeå fanns dessutom funderingar om att hämma röstförsäljning genom att möjlighet till elektronisk ångerröstning erbjöds.

Det råder för närvarande ingen enighet om att Internetröstning verkligen har en positiv effekt i dessa avseenden. Det är t.ex. oklart i vilken mån den digitala klyftan kan påverka valresultaten på ett odemokratiskt sätt. Om Internetröstning leder till högre valdeltagande kommer fler röstberättigade att välja, men ökningen sker endast bland de befolkningsgrupper som har tillgång till Internet, vilket leder till att människor med tillgång till Internet blir överrepresenterade bland väljarna.

Även frågan om tänkbara inslag av direktdemokrati är kontroversiell i sammanhanget. Dels är det inte självklart att direktdemokrati är mer demokratisk än representativ demokrati och dels finns det farhågor om att Internetröstning kan leda till en »knapptrycksdemokrati«, där väjarna visserligen röstar enkelt och snabbt men utan större eftertanke. En bra överblick över E-röstning i allmänhet ges i IT-kommissionens observationsrapport 35/2001 (Olsson 2001). Inom ramen för denna artikel kommer jag dock endast att ta upp de aspekter som är relaterade till säkerhetsfrågor.

Kostnader

Argumentet att kostnaderna minskar går inte att belägga idag, även om det i teorin finns en stor potential för besparingar. Samtidigt innebär Internetröstning också en hel del möjliga extrakostnader, främst för att hålla en tillräckligt hög säkerhetsnivå. Det är till exempel betydligt dyrare att dela ut smarta kort till alla röstberättigade än att dela ut konventionella valsedlar. Svaret på frågan hur kostnadsräkningen kommer att se ut kan dock ges först sedan kostnaderna beräknats för elektroniska valsystem som fyller alla säkerhetskrav. Sådana system finns emellertid ej idag.

Valdeltagandet

Det finns heller inte något slutgiltigt svar på frågan om valdeltagandet kommer att öka. Än så länge bygger argumentationen huvudsakligen på olika förväntningar. Det mest spridda argumentet är att röstningen blir lättare och att fler kommer att rösta om det blir enklare att rösta.

En närmare granskning visar dock att det är ganska tveksamt om det verkligen blir enklare att rösta. Erfarenheterna från de två kårvalen tyder snarare på att tröskeln inte ligger lägre än vid brevröstning. I Umeå hoppades man t.ex. kunna höja valdeltagandet från 11,5% till 17% genom att tillåta Internetröstning, men i stället minskade deltagandet till 9,4%. Anledningen var inte att möjligheten till Internetröstning inte utnyttjades, för drygt 60% av alla avgivna röster lades elektroniskt. Det finns heller ingen anledning att anta en betydande minskning i valdeltagandet utan möjlighet till Internetröstning. Tvärtom tyder kontinuiteten i statistiken på att andra orsaker måste ligga till grund för minskningen.

Vi bör i stället ta en annan fråga på allvar, nämligen om möjligheten till Internetröstning än så länge tenderar att medföra ett minskat valdeltagande. Så länge Internetröstning på grund av den bristande säkerheten inte är tillåten i »viktiga« val som t.ex. riksdagsvalet utan bara i val som påstås vara mindre betydelsefulla, så länge kommer varje val där Internetröstning blir tillåten att få en närmast officiell stämpel av att vara mindre viktigt.

I Statskontorets enkätundersökning svarade 24% av de intervjuade studenter som hade röstat att huvudskälet till att de röstade var att de kände sig lockade att pröva Internetröstning. Tyvärr ställdes inte den motsatta frågan, huruvida förtroendebrist i Internetröstningen bidrog till att någon avstod från att välja överhuvudtaget. Nyfikenhet på Internetröstning som motivation för att delta i valet kommer att minska betydligt med tiden eftersom den bara spelar roll så länge Internetröstningen har nyhetsvärde. Brist på förtroende för valtekniken har däremot potential att öka, ju fler incidenter som blir kända.

På så sätt står vi alltså inför en paradoxal situation. Det är svårt att testa om det i praktiken överhuvudtaget finns några fördelar med att rösta elektroniskt innan vi har system till vårt förfogande som har nått en sådan mogenhet att de tillåter användning i riksdagsval.

Om möjlighet till Internetröstning verkligen skulle minska valdeltagandet kan det även utnyttjas politiskt så länge detta inte är allmänt känt. Vill man t.ex. visa att det finns en stor motvilja mot EU hos befolkningen, så kan man tillåta elektronisk röstning med den officiella förklaringen att man vill höja valdeltagandet, även om det valda röstningssystemet inte skulle vara tillräckligt säkert för användning inom viktiga val. Sedan skulle det gå lätt att i efterhand postulera att det är ointresse för Europatanken som lett till minskat valdeltagande, trots att röstningen blivit mycket enklare än förr.

Röstförsäljning

I motsats till förfarandet i Osnabrück, så var det vid kårvalet i Umeå möjligt att rösta elektroniskt flera gånger. Enligt projektledaren Markus Hällgren var detta tänkt som ett skydd mot röstförsäljning. Tanken är att ingen kan vara säker på att den man köpt rösten av inte ändå röstar vid ett senare tillfälle och på så sätt gör den köpta rösten värdelös.

Resonemanget innehåller dock minst två missuppfattningar. För dem som tillhör de 90,6% som ändå inte röstade finns det heller ingen anledning att ångerrösta ifall de skulle ha sålt sin röst. En röstköpare som köper 100 röster kan lugnt utgå ifrån att omkring 90 av dem

kommer att vara användbara för köparen. Visserligen är situationen annorlunda vid andra val, där valdeltagandet är betydligt högre, men principen är densamma. Dessutom är det just de som inte vill delta i ett val som är mest benägna att sälja sin röst, vilket avsevärt kan höja kvoten för framgångsrika röstköp.

Den andra bristen i konceptet hänger samman med systemets konkreta utformning. För att kunna ångerrösta krävdes förutom de tre sista siffrorna i personnumret en giltig »Digital Voter Certificate« (DVC) som skickades via post till väljarna. För potentiella röstköpare räckte det alltså att köpa det oöppnade kuvertet med DVC:n samt att få tillgång till personnumret. Den enda möjligheten att ångerrösta var i så fall i vallokalen efter att ha förlustanmält sin DVC.

I stället för att försvåra röstköp vid kårvalet i Umeå introducerades nya risker med ångerröstning via Internet. Eftersom det inte fanns någon möjlighet för väljaren att se om rösten ändrats i efterhand genom ångerröstning, så kunde någon annan ångerrösta i väljarens namn utan att väljaren – eller någon annan – hade möjlighet att upptäcka det. Förutsättningen var bara kännedom om personnumret och DVC:n. Personnumret är inte direkt hemligt i Sverige och DVC:n fanns på samma papper som väljarens namn och adress, ett papper som efter röstningen inte sällan hamnar i en papperskorg där andra kan hitta det. Att låta väljaren kontrollera ångerröstningar skulle inte lösa problemet, eftersom köparen då skulle få samma möjlighet som den röstberättigade.

Möjligheten till elektronisk ångerröstning har alltså försvagat säkerheten utan att kunna fungera som ett skydd mot röstförsäljning. Möjligheten till ångerröstning i vallokal kan däremot ha ett visst värde. Detta gäller även utanför Internetröstning, t.ex. vid brevröstning inom det traditionella valförfarandet, och ger således ingen säkerhetsvinst genom den nya tekniken. Förutsättningen är naturligtvis att offentlighetsprincipen inte tillåter att man i efterhand tar reda på om någon har ångerröstat i vallokalen.

Vilken säkerhetsnivå krävs för Internetröstning?

Det politiska beslutet om vilken säkerhetsnivå som kan anses vara acceptabel kommer troligtvis inte att ligga långt ifrån den traditionella valprocessens säkerhetsnivå. Hur man konkret utformar krav på säkerhetsnivån är avgörande men inte alls enkelt. Det finns olika försök att hantera frågan. Fyra av dessa ansatser analyseras i detta avsnitt.

För att kunna jämföra risken mellan olika valsystem krävs som ett första steg en definition av vad som menas med »lika hög risk«. En läsvärd introduktion i problematiken med riskbedömningar i allmänhet finns i Adams (1995). När det gäller jämförelsen av röstningssystem är det svårt att hitta en vedertagen definition. Uttrycket *lika hög risk* används vanligtvis utan att ange någon definition.

I den föreliggande artikeln utgår jag ifrån nedanstående definition. Den följer det vedertagna sättet att beräkna risker utifrån förekomsten av de händelser som anses utgöra risken.

> *Två olika röstningssystem har lika hög risk när det genomsnittliga antalet röster med bruten valhemlighet eller med påverkat innehåll är lika stort.*

Även med denna till synes enkla definition är det inte lätt att jämföra risken för olika valsystem. Vid Internetval finns det liksom vid vanliga val ingen garanti för att fusk kommer att upptäckas. I definitionen ingår emellertid inte bara antalet röster där fusk kan bevisas utan alla röster där fusk har förekommit. Som en direkt konsekvens kommer riskbedömningar i detta fall alltid att i mer eller mindre hög grad vara beroende av skattningar.

Dessa skattningar förutsätter naturligtvis att hänsyn tas till grundläggande skillnader mellan olika valtekniker. Vid traditionella val är det t.ex. betydligt svårare än vid Internetval att korrumpera hela systemet med hjälp av befintliga säkerhetsbrister. Beroende på vilka säkerhetsluckor som utnyttjas vid Internetröstning kan den som fuskar nämligen i många fall välja hur många röster som ska påverkas. Internetröstning

är alltså mycket mindre tolerant gentemot enstaka säkerhetsbrister, något som ställer särskilt höga krav vid implementationen.

Ansats 1: Det ska vara helt säkert att rösta via Internet

Att försöka nå upp till absolut säkerhet innebär naturligtvis ett mål där ambitionsnivån i alla fall inte är för låg. »Ju säkrare desto bättre« är dock inte alltid sant. Säkerhet är en avvägningsfråga. Den maximalt nåbara säkerhetsnivån begränsas alltid av andra aspekter såsom kostnader och krav kring användbarheten. Målet bör i stället vara att hitta rätt säkerhetsnivå och inte den tänkbart högsta. Bland dem som forskar kring IT-säkerhet finns det knappast någon som på allvar skulle påstå att man kan uppnå en säkerhetsnivå som kan klassificeras som »helt säker«. Erfarenheten visar också att det i praktiken är omöjligt att designa komplexa system helt utan säkerhetsbrister.

Det är emellertid inte ovanligt att absolut säkerhet utlovas när det gäller implementerade system. Så var fallet t.ex. vid kårvalet i Umeå. I den officiella valinformationen informerades de röstberättigade på följande sätt:

- »Det är omöjligt att koppla en röstare till en specifik röst.«
- »Det är omöjligt att veta vad rösten är medan den ligger i systemet.«
- »Det är omöjligt att påverka resultatet av röstningen på andra sätt än genom korrekt röstning.«
- »Den personliga integriteten är fullständig.«

Dessa fyra påståenden förutsätter att 6 av de 7 säkerhetskrav för Internetröstning som ligger till grund för Statskontorets utvärdering är tillgodosedda. Det är bara tillgänglighetskravet som inte behöver uppfyllas för att nå dessa mål. Tillsammans med Safevotes påstående att tillgänglighetsangrepp inte ställer till ett problem (Safevote 2001, s. 19) så skulle det betyda att ett helt säkert system föreligger.

> *The protection against Denial-of-Service and penetration attacks will be both preventive and interactive. However, even if there is a sudden interruption of services for any reason, even including reasons not related to or controlled by Safevote, this should not alarm Internet voters because Internet users know that the Internet is not always available and that one should try again later.*

På det viset skulle systemet klara alla i sammanhanget relevanta säkerhetskrav, hur höga de än kan vara, och vore bl.a. tillämpligt även för riksdagsval. Men tyvärr är situationen inte så gynnsam som den framställs. Statskontoret anser visserligen att bevarandet av valhemligheten liksom den säkra identifikationen av väljare har en godtagbar grad av säkerhet, men den är på inget sätt »fullständig« eller gör ett angrepp »omöjligt«. Riskerna för intrång i eller manipulation av röstningssystemet på klientnivå är enligt Statskontorets utvärdering dessutom oacceptabelt höga.

Den risk som här utpekas av Statskontoret är ett exempel på att den utlovade säkerheten inte finns. Vid intrång i en väljares dator kompromitteras väljarens personliga integritet, det blir möjligt att koppla en röstare till en specifik röst och att veta vad rösten är medan den ligger i systemet, samt att påverka resultatet av röstningen på andra sätt än genom korrekt röstning. Slutsatsen blir att inget av de fyra påståendena klarar Statskontorets utvärdering. Om de ändå är del av den officiella informationen om röstningssystemet som riktas till väljarna kan detta ha en förödande effekt på väljarnas förtroende för valets korrekthet.

Ansats 2: Säkerheten ska motsvara säkerheten vid konventionella val

Om man accepterar att det inte är möjligt att nå absolut säkerhet kan det kännas rimligt att kräva samma säkerhetsnivå som vid konventionella val. I Statskontorets (2001, s. 39) utvärdering av kårvalet vid Umeå universitet formuleras det som följande grundkrav:

> *Ett rimligt grundkrav på säkerheten vid introducerandet av Internetröstning som ett alternativ i den traditionella valprocessen – vilket var*

> *fallet i kårvalet vid Umeå universitet – är att den totala valprocessens integritet och övrig säkerhet inte ska bli lägre än vid traditionella val, dvs. val utan möjligheter för Internetröstning.*

Safevote (http://www.safevote.com) som levererat röstningssystemet till kårvalet i Umeå tolkar samma grundkrav på ett litet annorlunda sätt. Här gäller kravet på lika hög säkerhet inte för »den totala valprocessens integritet och övrig säkerhet« utan bara för Internetröstningen i sig.

> *One principle followed in the development of these Requirements is that they MUST NOT reduce the privacy, security and integrity features of paper ballot voting systems operating under best conditions even if such features are not legally required.*

När Internetröstningen fullt ut ersätter alla andra sätt att välja finns ingen skillnad gentemot Statskontorets formulering. I de fall där den endast är ett tillägg till befintliga sätt att rösta, vid sidan av poströstning och vallokalröstning, försvagas säkerhetsnivån för hela valproceduren. Så var också fallet vid kårvalet i Umeå.

Försvagningseffekten beror på att möjligheter till fusk är av olika slag vid Internetröstning och konventionella val. Om säkerhetsnivån vid två skilda sätt att rösta är lika hög, i den meningen att det i genomsnitt uppstår lika många fel, dvs. påverkade röster och bruten valhemlighet, betyder det inte att även en kombination av de olika alternativen är lika säker. Om säkerhetsbristerna är olika, innebär det nämligen också fler möjligheter att bryta säkerheten genom medvetna angrepp.

Därför skulle Internetröstning bara vara tillåten i stället för andra sätt att rösta i konventionella val och inte som tillägg, om man hårdrar Statskontorets krav angående den totala valprocessens integritet. Utan att försöka fastslå hur strikt Statskontoret ser på kravet visar citatet en del av problematiken bakom jämförelser med säkerhetsnivån vid kon-ventionella val.

Vid användning av Safevotes formulering tillåter vi i alla fall att den totala valprocessens säkerhet minskar när Internetröstning blir ett tilläggsalternativ. Beroende på omständigheterna kan det vara helt

godtagbart. En uppriktig diskussion kräver dock att vi inte gömmer undan detta faktum utan att vi enligt Statskontorets formulering ovan alltid betraktar den totala valprocessen.

Ansats 3: Säkerheten ska motsvara säkerheten inom finanssektorn

Svårigheten att jämföra säkerheten vid traditionella val med Internetval leder ibland till formuleringen att säkerheten för Internetröstning ska vara jämförbar med säkerheten inom finanssektorn, där transaktioner via Internet redan är under användning. Inom finanssektorn är säkerheten visserligen mycket viktig, men i de flesta fall ställs där helt andra krav än vid ett demokratiskt val.

Vid elektronisk överföring av pengar är det vanligtvis känt vem som betalar, vem som tar emot och hur mycket pengar det handlar om. Ifall någon lyckas påverka systemet så att minst en av dessa uppgifter ändras upptäcks det lätt vid en kontroll. Sedan kan säkerheten anpassas och skadan regleras, om inte annat via en försäkring.

Att försäkra sig mot falska valresultat är betydligt svårare, vilket inte bara beror på att det är mycket svårare att upptäcka fusk. Det är också vanskligt att bestämma en rimlig ersättning för bruten valhemlighet eller för en minskning av valdeltagandet som följd av förtroendeförlusten. Endast kostnaderna för en ny valomgång kan beräknas och således täckas. Den problematik som väger tyngst är dock svårigheten att upptäcka fusk. På grund av valhemligheten finns det inte några garantier för att fusk kan upptäckas.

Valsäkerhetens behov motsvarar alltså inte säkerhetsbehoven inom finanssektorn. Däremot kan enstaka tekniker som spelar roll i säkerhetsdiskussionen inom finanssektorn vara intressanta för frågor kring säkerheten vid Internetröstning. Ett exempel på detta är digitala pengar enligt David Chaums system för anonyma betalningar (Chaum 1985). Finanssektorns grundläggande säkerhetskrav att transaktioner via Internet inte ska kunna framkalla skador som ej går att reglera via en försäkring är däremot inte på något sätt tillräckligt när det gäller Internetval.

Ansats 4: Lokala val och omröstningar tål lägre säkerhetsnivå

På grund av svårigheterna med att definiera en lämplig säkerhetsnivå för Internetröstning har ett annat angreppssätt valts vid de försök som hittills genomförts i praktiken. Anledningen är inte att de grundläggande kraven angående valhemligheten och resultatens korrekthet principiellt var annorlunda än vid t.ex. ett riksdagsval. Det var främst funderingarna att det finns mindre att tjäna på fusk vid lokala val och omröstningar samt att konsekvenserna är mindre allvarliga.

Resonemanget är att resurserna som satsas på försök att påverka valresultaten är relaterade till valets betydelse. Samma övervägande gäller dock inte traditionella val i vallokal. De genomförs i princip på samma sätt för riksdagsval och kommunalval. Det accepteras här alltså inte att säkerhetsnivån är lägre vid lokala val.

När det gäller Internetröstning går det ännu mindre att motivera olika säkerhetsnivåer. Vid traditionella val bygger möjligheten till fusk i huvudsak på tillgång till valurnorna samt på att tillfälle för fusk föreligger, vilket förutsätter närvaro. Vid Internetval krävs däremot ingen fysisk närvaro utan bara kunskapen om hur man via nätet tar sig förbi de inbyggda skyddsmekanismerna. Alla valberättigade skulle i så fall kunna få tillgång till andras röster, bara de har tillräcklig kunskap om Internetsäkerhet.

Vid riksdagsvalet finns det visserligen fler berörda som har denna kunskap, men antalet spelar ingen avgörande roll. En person med rätt kunskap kan utgöra ett tillräckligt stort hot mot ett lokalt val. Vid Internetröstning kan det dessutom finnas andra motiv för valfusk än bara politiska. Att ha kul och att visa upp sin skicklighet för sig själv och andra är redan idag vanliga motiv för sofistikerade manipulationer på Internet, med eller utan lokal anknytning.

Det som talar mest mot tillämpningen av olika säkerhetsnivåer är dock att det går att använda ett säkert system som utvecklats för riksdagsval även i lokala sammanhang. Bortsett från eventuella licenskostnader behöver det inte medföra extrakostnader. Ett röstsystem som är godkänt för riksdagsval kommer troligtvis att bygga på specialutvecklad

hårdvara, bl.a. smarta kort. Har de en gång distribuerats till användarna finns heller inget hinder av säkerhetsskäl för att använda samma utrustning även till lokala val.

Förutom valresultatets korrekthet kräver många val också att valhemligheten säkerställs. Den ska i så fall inte bara förhindra den påverkan på valresultaten som ett öppet val kan medföra utan samtidigt också skydda väljarnas integritet. Om någon utsätts för repressalier på grund av sina politiska åsikter så spelar det ingen större roll i vilket sammanhang de politiska åsikterna avslöjades. Här finns det alltså inte heller några hållbara argument för att satsa på olika säkerhetsnivåer.

Det finns dock särskilda fall där grundkraven är helt annorlunda. I dessa fall kan Internetröstning användas även när systemet inte skulle vara tillräckligt säkert för t.ex. ett riksdagsval. Åke Grönlund (2001) tydliggör sammanhanget på följande sätt:

> *Tekniken kan alltså utformas på en rad olika sätt. Detta har betydelse för de frågor som vanligen diskuteras huvudsakligen ur ett ideologiskt perspektiv, såsom integritet, anonymitet, kontrollerbarhet och valhandlingens symbolik.*

Säkerhetskraven kan alltså skilja sig vid olika Internetval. Differenserna i säkerhetsnivå beror dock i så fall på att det är olika grundkrav på vad som behöver skyddas, inte på en bedömning att hotet är mindre. I denna artikel koncentrerar jag mig emellertid på val där grundkraven i princip är jämförbara med riksdagsval.

Finns det tillräckligt säkra lösningar redan idag?

De röstningssystem som finns idag marknadsförs som mycket säkra eller till och med som helt säkra. Det borde vara självklart att de också på vedertaget sätt är certifierade. Inget av systemen som användes vid de nämnda Internetvalen var dock certifierat. I stället var det säljarna som styrkte de utlovade säkerhetsegenskaperna. I detta avsnitt kommer säljarnas argumentation att jämföras med de praktiska resultaten enligt mina egna, Statskontorets och andras utvärderingar.

Alternativ till säkerhetscertifiering

Om ett system inte är certifierat betyder det naturligtvis inte att systemet är osäkert. Det som saknas är emellertid en oberoende undersökning som styrker säljarnas påståenden. För att testa systemets säkerhet inbjöd Safevote alla som kände sig frestade att försöka ta sig in i deras servrar och ändra röster i den (Kornblum 2000). Enligt Safevote vet man inte hur många som har deltagit i försöket (Manjoo 2000), men eftersom ingen lyckades drar Safevote slutsatsen att systemets säkerhet därmed är bevisad genom en oberoende undersökning.

Safevote är inte ensam om detta förfarande. Vid ett ungdomsval i Esslingen i Tyskland som användes som test för Internetröstning påstod organisatorerna att systemet blivit »tillräckligt säkerhetstestat« genom att man bad användare med »medelhög kunskapsnivå« att simulera angrepp mot systemet. Angrepp mot tillgängligheten testades ej, eftersom man anser att det ändå inte finns något skydd mot dem och att det dessutom inte heller behövs något skydd (Steinbeis-Transferzentrum MediaKomm 2001).

Visserligen har det funnits en del uppmärksammade tester som följer denna modell, där någon mot förmodan har lyckats bryta säkerheten, men ändå lämpar sig denna metod inte för att bevisa att ett system är säkert. Det grundläggande kruxet är att en brist som upptäcks visar på faktiska säkerhetsproblem, men om bristen inte upptäcks betyder det inte att systemet är säkert.

Med andra ord kan man inte verifiera säkerheten på detta sätt utan bara falsifiera den. Att ingen lyckas med en falsifiering betyder naturligtvis inte att motsatsen är sann, utan bara att man inte känner till svaret. Det är tänkbart att någon kommer att lyckas bättre vid ett senare tillfälle, t.ex. vid ett officiellt val. Det är helt enkelt inget bevis alls att ett okänt antal människor med okänd kompetens inte lyckats bryta sig in i ett system. Troligtvis kommer de som är intresserade av att påverka valresultat inte ens att delta i testen, eftersom de inte har något motiv till att peka ut säkerhetsluckor i förväg.

För en säkerhetsbedömning är det ointressant att överhuvudtaget

nämna tester som utförts enligt ovan nämnda metod när ingen lyckades ta sig förbi systemets inbyggda säkerhetsåtgärder. Om det däremot är någon som lyckats finns det risk för samma missuppfattning. Tillverkaren kan frestas påstå att systemets säkerhet är bevisad genom att alla befintliga säkerhetsluckor har blivit åtgärdade efter att de upptäcktes genom testen. Det enda som dessa tester kan bevisa är att ett system inte motsvarar specifikationerna, ingenting annat.

Tillverkarnas säkerhetskrav och dess omsättning i praktiken

Enligt den information som finns tillgänglig från tillverkarna har deras produkter inga fel som kan tänkas begränsa användbarheten. Om man emellertid granskar de utlovade egenskaperna närmare, så ser bilden litet annorlunda ut.

För att förtydliga ska vi se närmare på Safevotes produkt som valdes av Umeå Studentkår efter en noggrann jämförelse av flera tänkbara produkter. Resultaten är dock inte unika för just Safevote utan gäller i stor utsträckning även andra produkter.

I specifikationen av Safevotes Internet Voting System (Safevote 2001) täcks långt ifrån alla säkerhetsrelevanta frågor. Några aspekter som tas upp är:

- Realiserad som Open Source

  Som Safevote (2001, s. 49) mycket riktigt konstaterar bör hela källkoden vara offentlig. Det är ingen garanti men det ger bättre förutsättningar för att upptäcka säkerhetsproblem.

  Open review, open code. Allow all source code to be publicly known and verified (open source code, open peer review). The availability and security of the system must not rely on keeping its code or rules secret (which cannot be guaranteed), or in limiting access to only a few people (who may collude or commit a confidence breach voluntarily or involuntarily), or in preventing an attacker from observing any number of ballots and protocol messages (which cannot be guaranteed). The system SHOULD have zero-knowledge properties (i.e., observation of system messages do

not reveal any information about the system). Only keys MUST be considered secret.

En skriftlig förfrågan till Safevote om att få ta del av källkoden besvarades ej. En sökning på Internet visade att andra inte heller fick tillgång till den. I Statskontorets (2001, s. 59) utvärdering står det explicit att »systemleverantörens dokumentation av systemet inte varit offentlig i alla delar«.

- JavaScript eller ActiveX behövs ej

Både JavaScript och ActiveX är aktiva innehåll på en webbsida och kan utföra operationer på användarens dator, vilket är ett hot mot datasäkerheten.

Vid startsidan för kårvalet behövdes fungerande Cascading Style Sheets, ett hjälpmedel för webblayout. I Netscape Navigator 4.75 fungerar dessa bara när JavaScript är aktiverad. Utan aktiverad JavaScript var det alltså inte möjligt att rösta. Problemet som uppstod här beror på mångfalden av olika program och programversioner som väljarna använder, vilket är någonting som ligger helt utanför valsystemets kontroll.

- Skydd mot tillgänglighetsangrepp

Tillgänglighetsangrepp syftar till att överbelasta en dator eller en nätförbindelse så att tjänsterna som tillhandahålls av datorn inte längre går att nå. I dagsläget har tekniken vidareutvecklats till distribuerade tillgänglighetsangrepp där angriparen använder sig av upp till flera tusentals crackade datorer för att genomföra angreppet, vilket gör det mycket svårt – om inte omöjligt – att gardera sig för sådana angrepp.

Statskontorets utvärdering kommer fram till att »Röstningsservern är välskyddad mot såväl tillgänglighetsangrepp som andra cyberattacker«. Utan att gå in i en diskussion om detta påstående vill jag bara påpeka att man i stället för röstningsservern borde betrakta hela systemets säkerhet. Om inte andra delar av infrastrukturen,

såsom routrar, DNS-servrar och även startsidan till kårvalet, också är skyddade mot tillgänglighetsangrepp, så är systemet sårbart. Om startsidan t.ex. inte kan nås kan valet inte genomföras.

- Skydd mot spoofing

  Spoofing är en teknik där man förfalskar adresser för att vilseleda användarens dator så att en uppkoppling sker till angriparens dator i stället för till servern – i det här fallet röstningsservern.

  Safevote (2001) inser att skydd mot spoofing är ett viktigt krav och poängterar: »Spoofing is prevented by means of the Return Code technology« (s. 13). För en närmare förklaring av hur bl.a. skyddet mot spoofing fungerar hänvisas till en webbadress, http://www.safevote.com/tech.htm (s. 51). Men när man försöker nå den så får man meddelandet: »404 Error – File Not Found«.

  Det hade varit intressant att ta del av den utlovade förklaringen, eftersom det enligt min uppfattning inte går att förhindra spoofing med någon form of »Return Code technology« när systemet är uppbyggt så, att man kan rösta med en vanlig webbläsare från vilken Internetansluten dator som helst med bara ett DVC och ett lösenord.

  Om en angripare använder sig av en av de vanliga teknikerna för att förfalska adressinformationen så att väljaren hamnar hos angriparens dator istället för hos röstningsservern, är det en enkel uppgift att låtsas vara väljarens dator gentemot röstningsservern och att låtsas vara röstningsservern gentemot väljaren. Sedan går det att lämna returkoden som servern skickar tillbaka vidare till väljaren och samtidigt både bryta valhemligheten och ändra den avgivna rösten.

  De två spoofing-varianter som är mest användbara i samband med Internetröstning är DNS Spoofing (Bellovin 1995) och Web Spoofing (Felten 1997). För att förhindra dem krävs dock helt andra åtgärder än Safevotes »Return Code technology«.

Det finns många tänkbara risker som inte tas upp av tillverkaren. Åtgärder som är med i konceptionsfasen saknas ofta i realiseringen. De som finns med i realiseringen verkar dessutom ibland bara ha en alibifunktion.

Ett exempel är möjligheten att kunna kontrollera i systemet om rösten har registrerats, vilket framställdes som ett hjälpmedel för att upptäcka problem:

> *Här kan du via Internet verifiera att din röst är mottagen hos servrarna utan att din personliga integritet eller att din röst blivit felaktigt behandlad. Verifiering, inkluderat väljarverifiering, kan minska risken för oupptäckt bedrägeri. (Information på Safevotes röstningsserver)*

Denna åtgärd syftar till att skingra eventuella tvivel på röstningssystemets säkerhet. Den utlovade effekten att på det viset kunna minska risken för oupptäckt bedrägeri finns emellertid ej. Det gick nämligen inte att verifiera integriteten eller korrektheten så som det utlovas. Det enda som kunde verifieras var om en röst hade blivit registrerad, inte om den hållits hemlig och inte heller om den blivit registrerad på rätt sätt. Det gick inte heller att upptäcka om någon annan hade »ångerröstat« efter att väljaren hade lagt fram sin röst.

Det finns många fler exempel, men de nämnda får räcka för att påpeka att Safevote inte ens klarar av att leva upp till de egna grundkraven. De verkar endast användas som försäljningsargument. Det är inte givet att kommuner eller kårfullmäktige har möjlighet att kontrollera i vilken mån de utlovade kraven uppfylls.

Statskontorets utvärdering hittar grundläggande säkerhetsproblem, och vid de delaspekter där den kommer fram till en positiv bedömning attesteras i bästa fall bara »godtagbar säkerhet« och inte den utlovade absoluta säkerheten. Det gäller att vara medveten om att godtagbar säkerhet är relativ och bygger på en del antaganden om systemet i sin helhet som kan visa sig vara felaktiga i framtiden.

Dessutom är utvärderingen mycket noga med att poängtera att man bara har beaktat validitetsaspekter och inte alls tagit hänsyn till korrekthetsaspekter, »dvs. huruvida systemet beter sig som det förväntas enligt dess specifikation« (Statskontoret 2001, s. 41).

Motiveringen att en utvärdering av korrektheten hade krävt betydligt större resurser än de som fanns tillgängliga måste man nog acceptera,

men samtidigt visar detta på ett generellt problem med kommersiella system. Att förlita sig på tillverkarnas löften när det inte finns resurser för en korrekthetsanalys är inte tillfredsställande. Ur ett säkerhetsperspektiv borde inga system användas vid officiella val utan att systemets korrekthet har utvärderats i förväg.

Projektledarnas bedömning och andra synpunkter

Både i Osnabrück och i Umeå ansåg projektledarna att valen fungerade bra. Systemtillverkarna använder också valen som referens. De utvärderingar som gjordes kommer emellertid fram till helt andra resultat.

Naturligtvis kan man inte förvänta sig att redan de första experimenten fungerar perfekt, men det borde vara en självklarhet att inte låta marknadsavdelningen styra informationsflödet. Ett valresultat kräver också kännedom om hur det har tagits fram. När det gäller Safevotes system, så är det ingen förutom tillverkaren som vet hur resultatet har tagits fram.

Genom att det finns ett visst tryck på projektledare hos kommuner eller hos studentkåren att lyckas med valet så är faran stor att man blundar för brister som inte är helt uppenbara och tillsammans med tillverkaren försöker sälja lösningen som lyckad.

Projektledaren i Umeå uttalade i flera sammanhang att Internetvalet fungerat väl, förutom några mindre problem som dock kunde lösas. Det är möjligt att så var fallet. Det kanske var så att ingen utnyttjade säkerhetsbristerna i Safevotes system vid kårvalet. Problemet är dock att det bara är Safevote som kan bedöma det. Därför kan inte heller någon annan än Safevote veta om valresultatet är korrekt.

Situationen i Osnabrück var litet annorlunda, eftersom man där hade betydligt högre krav på säkerheten än i Umeå. Över ett år före kårvalet presenterades systemet för offentligheten. För att undvika problem med otillräcklig säkerhet i väljarens dator byggde systemet på ett eget Open Source operativsystem som skulle distribueras på CD-skiva. På så sätt går det att säkerställa att inga trojanska hästar eller bristfällig programvara kunde påverka säkerheten.

Att man dessutom ville använda sig av smarta kort för säker kryptering och autentifiering gjorde systemet mycket intressant. Vid valet användes David Chaums system, och eftersom projektledaren Dieter Otten bedömde resultaten som goda ämnar han satsa på samma teknik vid valet till Europaparlamentet 2004 (Rabanus 2000, s. 98).

I stället för det utlovade operativsystemet satsade man dock på en speciellt utvecklad programvara som skulle gå att köra ovanpå Windows, MacOs eller Linux och som skulle tillhandahållas som Open Source. Men inte heller här gick det att få tag i källkoden, så att ingen utom tillverkaren vet hur tekniken fungerar i praktiken.

Philip Hügelmeyer, informatikstudent i Osnabrück, kommer fram till en annan bedömning än projektledaren (Hügelmeyer 2001, s. 106). Han anser att de största problemen dök upp på grund av den komplicerade tekniken. Dessa problem ledde till att det i slutändan bara var 160 studenter som lyckades rösta elektroniskt. Ett annat problem var att uträkningen visade fel resultat, så att man blev tvungen att genomföra en manuell kontrollräkning.

Sammanfattningsvis kan man konstatera att båda valen har haft betydande brister och att ingen förutom tillverkaren kan yttra sig om resultatens korrekthet. Den optimism som projektledarna visade var enligt min bedömning inte berättigad och tyder på ett grundläggande problem: att det fanns ett visst tryck på att man måste lyckas, vilket försämrar möjligheterna till en neutral analys.

Slutsats

Att experimentera med Internetröstning vid officiella val och omröstningar är en känslig fråga. Följer man de argument som har framförts i denna text, så borde det vara en bättre lösning att först ta fram ett säkert system och att experimentera sedan. Att börja experimentera på lokal nivå kan bara försvaras med grund i att kostnaden för en ny valomgång är mindre och att de politiska konsekvenserna går att hantera på ett bättre sätt.

Det är vanskligt att börja experimentera innan man har system till

förfogande som i princip är tillräckligt säkra för att användas även vid riksdagsval. Faran består i att man på lång sikt minskar det allmänna förtroendet för Internetröstning som i så fall lätt kan komma att bli känd som ett opålitligt och därför oanvändbart röstningssätt. Samtidigt finns risken att man utsätter lokala val och omröstningar för en nedvärdering som »irrelevanta« val, där säkerhetsaspekter inte är särskilt viktiga, vilket i sin tur kan minska valdeltagandet och förtroendet för resultaten.

Ett säkert system måste uppfylla hårda krav. Att det är Open Source och tillgängligt för alla intresserade utan kostnad är ett av dem. Det möter inget hinder att kommersiella företag utvecklar systemet mot betalning eller bidrar med andra tjänster av olika slag.

Skillnaden mellan utlovade säkerhetskrav och deras hantering i praktiken bäddar för en diskreditering av Internetval i den allmänna opinionen, speciellt när egna kortsiktiga intressen ligger till grund för skillnaden. Debatten om Internetröstning är en rätt så ny företeelse och mångfalden aktörer med olika intressen medför att vilseledande uppfattningar lätt kan uppstå. Det främsta målet för alla inblandade borde dock vara att förstå röstningsprocessen och dess implikationer innan man förlitar sig på den, även om det både är kostsamt och kan ha en bromsande effekt i början.

Heiner Schorn är forskarstudent i informatik vid Umeå universitet med inriktning på IT-säkerhet och demokrati. Han är doktorand i forskningsprogrammet DemocrIT, ett samarbete mellan forskare inom informatik, statsvetenskap, medier och kommunikation samt historia.
E-post: Heiner.Schorn@informatik.umu.se

Referenser

ADAMS, JOHN (1995): *Risk*. London: UCL Press.

BELLOVIN, STEVEN M. (1995): »Using the Domain Name System for System Break-Ins«. I: *Proceedings of the Fifth Usenix UNIX Security Symposium*, Salt Lake City, U.T., June 1995. URL: http://www.research.att.com/~smb/papers/dnshack.ps (Även tillgänglig som PDF på URL: http://www.research.att.com/~smb/papers/dnshack.pdf)

CALTECH/MIT (2000): »Voting: What Is – What Could Be«. Caltech/MIT Voting Technology Project, July 2001. URL:
http://web.mit.edu/newsoffice/nr/2001/VTP_report_all.pdf

CHAUM, DAVID (1985): »Security Without Identification: Transaction Systems to Make Big Brother Obsolete«. *Communications of the ACM*, vol. 28, nr 10, 1030–1044.

CIVTF (2000): *A Report on the Feasibility of Internet Voting.* California Internet Voting Task Force. (January 2000). URL:
http://www.ss.ca.gov/executive/ivote/final_report.htm

FELTEN, EDWARD W. ET AL. (1997): »Web Spoofing: An Internet Con Game«. I: *20th National Information Systems Security Conference*, Baltimore, Md., October 1997. URL: http://www.cs.princeton.edu/sip/pub/spoofing.html

GRÖNLUND, ÅKE (2001): »Elektroniska omröstningar«. I: Christer Jönsson, red. *Rösträtten 80 år: forskarantologi*. Stockholm: Justitiedepartementet. 233–254.

HÜGELMEYER, PHILIP (2001): »Sind Wahlen über das Netz einfacher«. *c't: magazin für computertechnik,* nr 3, 106–107.

KORNBLUM, JANET (2000): »The News Behind the Net: Hackers Invited to Muck Up Mock Ballot«. *USA Today*, 2000-11-02. URL: http://www.usatoday.com/life/cyber/tech/jk110200.htm

MANJOO, FARHAD (2000): »Ballots Need an Upgrade«. *Wired News*, 2002-11-10. URL: http://www.wired.com/news/print/0,1294,40078,00.html

OLSSON, ANDERS R. (2001): »E-röstning: en lägesbeskrivning«. Stockholm: IT-kommissionen. (Observationsrapport, 35/2001). Tillgänglig via URL: http://www.itkommissionen.se/

RABANUS, CHRISTIAN (2000): »Online-Urnengang erfolgreich«. *c't: magazin für computertechnik*, nr 4, 98.

SAFEVOTE (2001): *Umeå University 2001 Student Union Election: Safevote Internet Voting System*. Version 1.0, March. URL: http://www.us.umu.se/arkiv/public.pdf

SCHWEIZERISCHE BUNDESKANZLEI (2002): »Bericht über den Vote Électronique: Chancen, Risiken und Machbarkeit elektronischer Ausübung politischer Rechte«. URL: http://e-gov.admin.ch/vote/e-demo-dt-09.01.02.pdf

STATSKONTORET (2001): *Internetval: en utvärdering av kårvalet vid Umeå studentkår*. Stockholm: Statskontoret. (Rapport 2001:26). URL: http://www.statskontoret.se/pdf/200126.pdf

STEINBEIS-TRANSFERZENTRUM MEDIAKOMM (2001): »Erfahrungsbericht (Online-) Jugendgemeinderatswahl in Esslingen am Neckar 09. bis 12. Juli 2001«. URL: http://www.internetwahlen.de/projekt/dokuess.pdf