Linnéuniversitetet
Kalmar Växjö

Datavetenskap, självständigt arbete

# Webbaserad Röstning

Säkerhetsrisker med en webbaserad röstning

*Författare:* Marco Villegas
*Handledare:* Johan Leitet
*Examinator:* Johan Leitet
*Termin:* VT 2016
*Ämne:* Datavetenskap
*Nivå:* Högskoleexamen
*Kurskod:* 1DV42E

# Abstrakt
Uppfinningen av telegrafen, telefon, radio och dator la grunden för kommunikation över långa sträckor. Internet som den är idag har revolutionerat datorn och kommunikationen mellan mänskor som ingenting innan. Dagens samhälle är mer och mer beroende av snabba elektroniska kommunikationsformer för enkelhet, snabbhet och tillgänglighet. En stor majoritet av medborgarna i de utvecklade länderna har enkel tillgång till Internet, och tillgång till internet i utvecklingsländerna blir vanligare.

Internet är en plattform för informationsspridning och ett medium för samarbete och samverkan mellan individer och deras datorer utan hänsyn till geografiskt läge. Internet tillkomst lett till att många individer både inom och utanför vall myndigheter började spekulera om möjligheten att använda den nya tekniken till att effektivisera och legitimera demokratiska val på ett set som tisdagar inte varit möjligt. Men för att hoppa från pappers val till att rösta genom Internet kräver en hel del mellanliggande steg.

Flera studier och experiment har gjort i olika länder och med blandade resultat. En sak som alla studier är eniga om är att Internetröstning innebär många risker som måste hanteras på rätt sätt innan omfattande utbyggnad kan ske. Denna uppsats undersöker de utmaningar och risker som finns i ett webbaserat röstningssystem.

# Nyckelord
Webbaserad röstning, Webb säkerhet, webbaserat röstningssystem risker,

# Innehåll

**1 Inledning** 1

**2 Bakrund** 2
2.1 Frågeställning 2
2.2 Tidigare Forskning 2

**3 Metod** 3
3.1 Data 3
3.2 Sökord 4
3.3 Metoddiskussion 4

**4 Rapporter** 4
4.1 2013, E-röstning och andra valfrågor 4
*4.1.1 Säkerhet* *4-5*
4.2 2013, Internet voting in Australian election systems 5
*4.2.1 Säkerhet* *5*
4.3 2012, International Experience with E-Voting 5
*4.3.1 Säkerhet* *5-6*
4.4 2011, E-public, e-participation and e-voting in Europe 6
*4.4.1 Säkerhet* *6*
4.5 2011, Discussion Paper: Internet Voting 6
*4.5.1 Säkerhet* *6-7*

**5 Resultat** 7
5.1 Internetröstning 7
5.2 Klienten 7-8
5.3 Server 8-9
5.4 Kommunikationsvägen 9

**6 Diskussion** 10-11

**7 Slutsats** 11-12

**Referenser** 13-14

# 1 Inledning

Webben har visat sig vara ett av de mest dynamiska fenomenen i vår tid. Från ett nätverk som ursprungligen utvecklades för en relativt liten grupp av institutionella användare, har det vuxit till en viktig del av människors liv över hela världen. Med tiden har de typiska formerna av tillgång till webben ändrats från stationära datorer på kontor och hem, till smartphones och tabletts. Facebook och YouTube är två nya applikationer som har skapat nya former av Internetanvändning som har blivit sociala och kulturella företeelser[7].

Under de senaste decennierna har en ny typ av samhälle växt fram, ett samhälle där människor kan påverka sin omgivning genom webben och information inte längre bara finns i fysisk form utan också i digitalt form. I dagens samhälle är det vanligt att vara online. I en studie som gjorts i Sverige visar det sig att 88% av befolkningen använder webben på jobbet och privat[2], samt 80% är online dagligen i hemmet[6,S. 5-10]. Vi har nu möjlighet att interagera med tusentals människor över hela världen på ett sätt som tidigare inte var möjligt. På väldigt kort tid har internet bidragit till att stärka informations- och yttrandefriheten runt om i världen.

Som ett resultat av webben framväxt så har nya virtuella tjänster skapats. Dessa tjänster har automatiserat uppgifter som tidigare kunde ta flera dagar att utföra, samt skapat interaktiva platser där medborgarna och politiker kan mötas[1]. Webbaserade tjänster blir viktigare i det moderna samhället. I takt med webbens tillväxt och inflytande, ökar den demokratiska betydelsen av att information ska vara tillgängligt för alla[3].

Exempel på några webbaserade tjänster är e-deklaration, ansökning till utbildning och bankärenden[4]. I dag både deklareras och utförs bankärenden på internet. Människor är vana vid webbaserade tjänster som innebär att man kan utföra det mesta vid en dator. Mot den bakgrunden så är syftet med uppsatsen att ta reda på vad det finns för säkerhetsrisker med en webbaserad röstningstjänst.

# 2 Bakgrund

Huruvida webbaserad röstning ska införas i Sverige är en fråga som befolkningen har väldigt delade åsikter om. Förespråkare för en sådan användning av webben ser det som ett potentiellt kraftfullt och kanske oundvikligt sätt att göra det möjligt för väljarna eller vissa kategorier av väljare att rösta bekvämt och effektivt. Motståndarna till webbaserad röstning, på pekar osäkerheten med webbaserade system och anser att ett sådant system kan påverka integriteteten negativt i valprocesser[5].

Fokus i denna uppsats kommer inte vara på etiska frågor, utan på tekniska säkerhetsrisker med en webbaserad röstningstjänst. De tekniska säkerhetsrisker som kommer att studeras är de riktade mot väljare och inte sabotage mot vall lokaler, Dator anläggningar, ström försörjning eller likande attacker som kan göras på platser och utrustning som används i ett val.

## 2.1 Frågeställning

Vad finns det för tekniska säkerhetsrisker med en webbaserad röstningstjänst?

### 2.2 Tidigare forskning

Redan för 16 år sedan presenterades en rapport som gjordes i den amerikanska delstaten Kalifornien. Denna visade på  att de mest omstridda frågor som rör webbaserade röstning, kommer från oron över webbsäkerheten[8]. Olika säkerhetsutmaningar presenteras av webbaserade röstning jämfört med papper röstning. Till exempel kan överföring av röstningsdata presenterar möjligheten att systemet attackeras vilket i sin tur kan leda till att val manipuleras.

Flera studier har genomförts i Sverige och utomlands. Resultatet av den senaste stora utredningen i Sverige kom 2013 och den rapporten var positiv till webbaserat valsystem men bara som ett komplement till det traditionella valsystemet[5].

2014 gjordes en SIFO-undersökning för att se hur svenska folket ställde sig till frågan om webbaserad röstning. 67% var positiva till röstning genom webben och 58% skulle rösta genom webben om den möjligheten fanns[10].

# 3 Metod

Här presenteras en beskrivning av metoden som ska användas i uppsatsen, samt vilken typ av faktakällor som ska användas och vilka avgränsningar som gäller för dem. För att besvara uppsatsens frågeställning används en litteraturstudie.

En litteraturstudie är en studie där man går igenom tidigare forskning för att på så sätt besvara sin fråga. Syftet med en litteraturstudie är att visa läsaren att det finns endjupare förstålse om ett visst ämne. literaturen man tar del av kan vara i valfritt format, inklusive källor på nätet. Det kan vara böcker, andra upsattser, rapporter eller avhandling inom ämnet man valt.

Det är viktigt att notera att litteraturstudien inte bör vara en återberättande text av vad andra har publicerat eller sammanfattning av en vis raport. Genom att gå igenom tidigare forskning tar man lärdom av de erfarenheter, iakttagelser och misstag som kan ha gjorts i liknande eller relaterade arbeten[11]. Litteraturstudien går ut på att studera flera källor och föra en kritisk diskussion för att visar insikt och medvetenhet om olika argument, teorier och tillvägagångssätt. samt efter analys av den relevanta literaturen, hitta svar på uppsatafrågan eller visa att den literatur man läst inte kunde ge svar på uppsatfrågan.

I det här fallet kommer jag att fokusera på studier som utförts på beställning/uppdrag av olika stater för eventuellt införande av webbaserade röstningssytem. Fakta som presenteras och antaganden som görs ska inte ske i ett vakuum, utan det ska byggas på forskning inom området och ämnet[12].

## 3.1 Data

Denna litteraturstudie ska vara kvantitativ, för att vara exakt kommer fem olika forskningsrapporter studeras. För att datan som samlas in ska återspegla de tekniska problem som råder just nu så kommer forskningsrapporter inom området som är äldre än 7 år, samt forskningsrapporter som bara berör den etiska aspekten av webbaserad röstning exkluderas

För att validera och öka trovärdigheten i studien så kommer forskningsrapporterna som studeras ha varit gjorda på uppdrag av statsmakter eller större organisationer som till exempel EU. För att hitta relevant data så ska sökningar göras i olika databaser och Googel.

För att få en djupare förståelse över ämnet så kommer datainsamling ske från officiella dokument, allmänna forskningsrapporter, publicerade artiklar och böcker om ämnet. Data som samlas in ska utvärderas för att komma fram till dess värde och giltighet.

## 3.2 Sökord

Följande sök ord har använts: internet voting, internet voting eu rapport, internet voting UK rapport, internet voting norge rapport, internet voting australian rapport, e-röstnings, A Comparative Assessment of Electronic Voting, Internet Voting in Canada, internet voting finland rapport, e voting danmark rapport

Följande platser har använt för sökning: linneuniversitet Databaser och Googel

## 3.2 Metoddiskussion

I denna litteraturstudie kommer inte de etiska aspekterna av webbaserade röstningssystem att behandlas, utan studien kommer koncentreras runt tekniska säkerhetsaspekter. Syftet med litteraturstudien är att besvara frågan om säkerhetsrisker med en webbaserad röstningstjänst därför är det lämpligt att filtrera bort information som inte har med den teknisksäkerheten att göra.

De ställningstaganden som görs och de slutsatser som dras ska baseras på fakta och en saklig argumentation. Personer som skulle vilja återskapa denna litteraturstudie ska kunna göra det genom att använda metoden och källorna som använts, detta skapar en validitet i litteraturstudien.

# 4 Rapporter

För att besvara uppsatsen övergripande fråga ” Vad finns det för tekniska säkerhetsrisker med en webbaserad röstningstjänst?” så har jag valt ut 5 olika rapporter utifrån de avgränsningar som presenterat i Metod kapitlet. Det är rapporter som är oberoende av varan, men alla bekräftar samma data eller förklaring som riktig. I och med detta kan vi hysa större tillit till de valda källorna. För att säkra oberoendet mellan rapporterna så har det varit viktigt att de har olika författare, är utgivna av olika länder, samt att de undviker att referera till varandra.

## 4.1 2013, E-röstning och andra valfrågor[5]

En utredning som gjordes av Vallagskommittén på uppdrag av svenska regeringen. Där man under sökt fördelarna och nackdelarna med webb baserad röstning, rapporten har några allmänna skrivningar om att e-röstning skulle bli säkrare, enklare och snabbare. Samt att utredningen gör bedömningen att införandet av val med modern informations teknik ökar tillgängligheten vilket bland annat kan medföra ett ökat valdeltagande. De gör också bedömningen att det kan reducera kostnaderna för val på lång sikt.

Enligt utredningen finns det fördelar med e-röstning via Internet, den främsta att flerar skulle kunna röst och personer med vissa funktionshinder då kan genomföra sin valhandling på egen hand. Vallagskommittén förslår att Sverige ska införa försök med e-röstning och i första hand förordat försök med e-röstning via Internet i okontrollerade miljöer, men med en utformning så att det även kan tillämpas i vallokaler och röstningslokaler.

### 4.1.1 Säkerhet

I rapporten E-röstning och andra valfrågor[5, S. 75-77] så tar man upp följande tekniska säkerhetsrisker virusangrepp, Överbelastning angrepp och Dataintrång.

I en webbaserad röstningstjänst kan virusangrepp användas för att komma åt användarens login information och ändra användarens vall av kandidat, samt att viruset kan hindra användaren från att rösta[5,S.75].

Överbelastning kan användas för att över belasta röstningstjänst och hålla legitima väljare från att rösta[5,S.76].

Dataintrång är attacker avsedd att öka den obehöriga användarens åtkomstprivilegier utöver de som beviljats av en systemadministratör[5,S.76].

## 4.2 2013, Internet voting in Australian election systems[16]

En utredning som gjort av den Australiska val myndigheten AEC (Australian Electoral Commission). Där man undersökt en rad viktiga frågor som är relevanta för att Australierns valkommitté ska kunna ta ställning till frågan om vilken roll internet röstning ska ha i Australien. Utredningen gör det genom att studera länder där man infört webb baserade röstning tjänster, samt genom att identifiera risker med dessa system och några områden där Internetröstning kan ha positiv inverkan på demokratin och val deltagandet.

### 4.2.1 Säkerhet

I rapporten så tar man upp att det finns 3 risk moment i en webb baserat röstningens tjänst [16,S.9].

Den första risken är att privat ägda internet uppkopplade enheter står inför en mängd potentiella attacker och måste skyddas så att inte obehöriga användare kan kränka valets integritet eller stjäla en väljare autentiseringsbevis.

Den andra risken är autentiserings av väljare, olika tekniken finns men kan vara svåra eller dyra att distribuera. Sam att äldre privat ägda enheter kan sakna den nödvändiga säkerhetsskydden samt sakna kompabilitet som krävs för att använda smartkortsläsare för kryptografisk autentisering.

Den tredje risken är insyn och möjlighet att granska valet efter att det avslutats. På grund av svårigheten att validera och verifiera om server data modifierats.

## 4.3 2012, International Experience with E-Voting[17]

Norges webb baserade röstnings tjänst granskades av IFES( International Foundation for Electoral Systems). Rapporten fokuserar till stor del på Norges erfarenheter kring Internetröstning, samt att den också granska länder som har använt internet röstning tidigare.

### 4.3.1 Säkerhet

Rapporten lyfter framförallt fram risken med överföring av data genom webben, tjänsten kan attackeras och falska resultat införas[17,S.87]. Följande moment anses vitala för att ett webbaserat röstnings tjänst ska anses pålitligt[17,S.29].

Autentisering av väljare - syftar till att säkerställa att endast legitima väljare kan rösta och att det är den registrerade väljaren som faktiskt röstar.

En röst en väljare - Den webb baserade röstnings tjänsten måste se till att väljare endast kan lägga en röst.

Systemsäker - röstningstjänsten måste säkerställa röstning transaktionerna så att den inte kan manipuleras eller övervakas. Det för att skydda servrarna som har väljarnas uppgifter och rösterna som lagts i valet.

kryptografiska protokoll - val data som överför genom webben bör krypteras för att säkerställa att röst data inte kan fångas upp och valintegriteten kränks. Samt att uppgifter som sparas på servrar bör krypteras för att se till att uppgifterna inte kan nås utan nödvändig dekrypteringsnyckel.

Krypteringsnyckelkontroll - en viktig funktion som bör skyddas är generering och innehav av krypteringsnyckeln som behövs för att dekryptera valdata.

## 4.4 2011, E-public, e-participation and e-voting in Europe [18]

En undersökning som gjorts på uppdrag av Europaparlamentet. Rapporten är resultatet av forsknings om den potentiella effekten av Internetbaserade politiska deltagande och vad det kan ha för konsekvenser på demokratin i Europa. I rapporten presenteras en analys av den aktuella utvecklingen inom området e-demokrati. Rapporten kommer också fram till att e-röstning i Europa för närvarande inte rekommenderas. Skälen till detta är främst lönsamhets överväganden, tekniska frågor och politisk legitimitet.

### 4.4.1Säkerhet

Rapporten lyfter fram tre oros moment med webb baserad röstning, attacker riktade mot servern, klienten eller kommunikationsvägen. internet uppkopplade privat ägda enheter kan påverkas av skadliga program/virus, olika attacker kan riktas mot val data servern och data som skickas mellan server och privat person kan attackeras för att förfalskas och manipuleras[18,S.113].

## 4.5 2011, Discussion Paper: Internet Voting

En rapport i ämnet Internetröstning framställd av Elections BC. Elections BC är en oberoende och lagstiftande organisation ansvaret för att administrera valprocesser i den kanadasiska provinsen British Columbia(B.C). I rapporten sammanfattas läget av Internetröstning i Kanada och runt om i världen samt att den belyser olika etiska och tekniska frågor.

### 4.5.1 Säkerhet

Rapporten lyfter fram att det svåraste att skydda är väljares dator och mobil enheter. Efter som det är utan för valmyndighetens kontroll[19,S.27]. Väljare registrera och röstar på sina privata enheter som ofta är dåligt skyddade mott attacker. Webbläsare är sårbara för skadlig kod som kan laddas ner av en inte ont anande väljarna. När en enhet är infekterat så kan en obehörig användare se vad väljaren har röstat på, samt visa väljaren att röstningen processen har gått rätt till medans den ändrar rösten som lagts utan väljarens till medgivande eller kunskap[19,S.28].

Kommunikationen mellan en väljares dator och servern kan attackeras för att av lyssna data och ändra röster samt att kommunikationen till servern kan blockeras på grund av överbelastning. En DOS-attacker skulle göra valet servern otillgänglig genom att överbelasta det med illegitima serviceärenden[19,S.29]. En röstnings tjänst är beroende

av val servern tillgänglighet  för att tillåta väljare autentisering och mottagande av digitala valsedlar.

# 5 Resultat

Resultat delen i detta arbete har som mål att ge tydlig och kortfattad översikt över de risker som är förknippade med webb baserat röstning. Den kommer dessutom ge exempel på möjliga attacker genom att presentera dem, samt att arbetet är riktade till både tekniskt insatt och nya som vill koma in i ämnet. Arbetet kommer därför hållas på teknisk nivå som är övergripande.

Vid bedömningen av möjliga attacker som kan riktas mott röstnings tjänster, är det nödvändigt att identifiera de mål som kan utsättas för attacker. Efter sammanställning av säkerhets risker som de olika rapporterna presenterat i ovanstående sidor. Kan man I en webbbaserad röstningstjänst konstatera att det är klienten, servern och kommunikation vägen som kan utsättas för attacker.

## 5.1 Internetröstning

Internetröstning definieras som röstning genom Internet med hjälp av en dator som inte nödvändigtvis ägs och drivs av valmyndigheter[18,S.111]. Internetröstning skulle inte kräva att väljarna går någonstans för att rösta och det kan genomföras från privata platser såsom hem, skola eller kontor. Denna typ av röstning möjliggör röstning från praktiskt taget var som helst och när som helst. Men Internetröstning presenterar också en uppsättning unika utmaningar jämfört med röstning i en kontrollerad miljö som en vallokal, såsom säkerhet, tillgänglighet, autentisering, anonymitet, kontrollerbarhet, öppenhet och sekretess[18,S.113].

## 5.2 Klienten

Hot mot klienten är programvara/virus som har som mål att skada röstningstjänsten. För att en sådan attack ska varar genomförbar så tar en obehörig användare hjälp av virusprogram. ett virus är ett skadligt datorprogram som reproducerar sig och fäster sig till andra datorprogram, det sker utan samtycke eller kunskap av datoranvändaren[13]. Det gör det på ett sådant sätt att dess instruktioner aktiveras när det infekterade programmet startas.

Skadligaprogram kan till exempel överföras till klienten eller server genom e-postbilagor, nedladdningar av filer genom Internet eller genom att utnyttja säkerhetsbrister i webbläsaren. Virus kan vara godartad som till exempel de som visar trevliga meddelanden, eller elakartad som en fullständig sjukdomsspridning, såsom de som förstör datafiler och system. En obehörig användare som kommer åt klient eller server, kan med hjälp av skadligt program beröva väljares röst rätt samt ändra röster[18,S.129].

En attack som också lyfts fram är bedrägerier, en obehörig användare kan ha kapat en användares webbläsare eller skickat ett e-mail med en länk som tar en till röstningstjänsten, men i själva verket tar den användaren till en falsk sida som är identiskt med originalet[18,S.129]. Med hjälp av en sådan attack så kan en obehörig användare komma åt login data.

Exempel på virus typer:
Resident-Virus är en typ av datorvirus som döljer och lagrar sig i datorns minne, som sedan gör det möjligt att infektera alla filer som körs av datorn, beroende på viruset programmering uppgift[20]. Den aktiverar när operativsystemet startat eller när användaren startar en specifik funktion.

Non-resident Virus är ett virus som endast aktiveras när det infekterade programmet startas. De lagras inte i datorns minne[20]. När den startas söker den omedelbart efter andra program den kan infekteras, den består av en sökare modul och en replikeringsmodul. Sökar modulen är ansvarig för att hitta nya filer att infektera. För varje ny körbar fil sökaren modulen möter, kallar den replikering modul för att infektera den filen.

Macro-Virus är ett datorvirus som infekterar Microsoft Word eller liknande program och gör så att en sekvens av skadlig kod körs automatiskt när det infekterade programmet startas[20].

## 5.3 Server

Servern hottas då en obehörig användare bryter sig in i ett webbaserat system för att stjäla, ändra eller förstöra information, ofta genom att utsätta tjänst för skadlig kod, eller en kommandosekvens som utnyttjar en bugg, tekniskt fel eller sårbarhet i det webb baserade systemet. En sårbarhet kan orsaka oavsiktlig eller oförutsedda beteende i en röstningstjänst.

Här nere presenteras några exempel dataintrång tekniker som kan användas mot en webb baserad tjänst.

SQL Injection är en teknik där en obehörig användare skapar eller förändrar befintliga SQL-kommandon för att exponera dolda data eller för att utföra farlig systemnivå kommandon på webbsidan databas[15,S.6]. Detta kan låta en obehörig användare kringgå åtkomstkontroller och därigenom kringgå standard autentisering och auktoriseringskontroller för ett system.

Bruten autentisering och sessionshantering
Om applikationsfunktioner som rör autentisering och sessionshantering är fel implementerade i systemet. Kan det leda till att obehörig användare kommer åt lösenord, nycklar, eller session token för att med hjälp av dem kunna ta över en användares identitet[15,S.8].

XSS(Cross-site Scripting)
Webbapplikationer tar i mot opålitliga data och skickar det till webbläsaren utan ordentlig validering. Det kan låta en obehörig användare köra skript i offrets webbläsare som kan kapa användarsessioner, vanställa webbplatser, eller omdirigera användaren till skadliga webbplatser[15,S.9].

CSRF (Cross-Site Request Forgery)
Webbläsare tillåter HTTP-begäran som kan göras mellan olika webbplatser, CSRF attack användes för att kom åt eller förstöra känslig data. När en användare besöker en skadlig webbsida som gör så att besökarens webbläsare kör en POST begäran till en webbsida som den själv inte avsåg. Det inloggat offrets webbläsare skickar då en

HTTP-begäran, som in håller offrets sessions cookie och autentiseringsinformation[15,S.14]. Detta kan i sin tur göra det möjligt för angripare att ta över offrets identitet och befogenheter i systemet.

## 5.4 Kommunikationsvägen

Hott mott kommunikationsvägen i det här arbetet definieras som ett intrång på din nätverksinfrastruktur. Där en obehörig användare samlar in information för att utnyttja de befintliga öppna portar eller sårbarheter. Vilket kan innebära att obehörig får åtkomst till en användares kommunikationsväg för att antingen samla, förändrar, inaktiverar, hindra eller förstör resurser eller data.

Här presenteras två attacker som kan riktas mot kommunikationsvägen.
DOS(denial of service) attack lyft fram som en av de främsta hoten mot kommunikationsvägen mellan klient och server[18,S.127]. Det är en attack där angriparna försök förhindra legitima användare från att komma åt tjänsten. I en DOS attack, skickar angriparen ett överflöd av förfrågningar som har ogiltiga returadresser till servern som i sinn tur kommer hålla servern upptagen[14]. Servern kommer inte kunna hitta avsändaradressen vilket gör att servern väntar innan den stänger anslutningen. När servern stänger anslutningen så upprepar angriparen processen vilket håller servern upptagen medan legitima användare hindras från att kom åt tjänster på servern.

En avancerad version av DOS attack är DDoS (distributed denial-of-service), det är en attack där flera datorer är infekterad av ett skadligt program som ökar möjlighterna av en DOS attack efter som servern blir angripen från flera datorer som samarbetar[18,S.129]. Attacken översvämmar kommunikationen mellan klienten och servern med fler förfrågningar än den kan hantera. Skulle en val server utsättas för en DOS/DDOS attack så riskerar den att bli avskuren från Internet och resultera i att väljare berövas sin rösträtt och beroende på hur länge attacken på går så kan det delegitimera hela valet[18,S.129].

Samlings namn för attacker som skulle kunna lyssna av data är MITM (man in the middle). Det är attacker som på olika sätt utnyttja kryptografisk svaghet i SSL/TLS-protokoll. I en MITM attack, placerar en angripare sig i mellan en klient och en webbplats server, angriparen härmar båda. I denna attack, tror klientens webbläsare att den talar till servern på en krypterad kanal och servern tro att den talar till klientens webbläsare, men de båda pratar med angriparen som sitter i mitten[21]. All trafik passerar genom angriparen, som kan läsa och ändra data som skickas.

Känsliga uppgifter såsom kreditkortsnummer, skatte ID och autentiseringsuppgifter kan avlyssnas för att användas eller manipuleras för otillåtna ändamål. Dessa uppgifter kan leda till skadliga brott som personbedrägerier och identitetsstöld, samt att det kan leda till att valtjänsten pålitlighet ifråga sätts.

# 6 Diskussion

Webbaserad röstning ses ofta av allmänheten som ett verktyg för att göra valprocessen mer effektiv, korrekt implementering av ett sådant system kan påskynda behandlingen av resultaten och göra röstningen lättare. I denna del av arbetet beskrivs faktorer som kan påverka framgången för webbaserat röstning.

Den mest uppenbara fördelen med Internetröstning är bekvämlighet för väljaren[19,S.18]. Genom att göra valdeltagandet lika enkelt som att logga in på en webbplats, kryssa i några rutor i ett formulär och klicka på att rösta knappen så har man under lättat för väljaren. För oavsett hur bra vallokalerna är så är det mer bekvämt att rösta från hemmet.

Om Internetröstning infördes som ett alternativ vid sidan av mer traditionella röstningen metoder, skulle det expanderar tillgängligheten av röstsystemet i allmänhet. Det skulle göra att väljare röstar när det passar dem, via hemmet, på arbetsplatsen eller offentliga internetterminaler. Detta i sin tur skulle var en betydande kostnadsbesparing[19.S,19].

Trots den omfattande spridningen och användningen av Internet banker och andra känsliga transaktioner, måste det betonas att garantera säkerheten för röstning via internet är ett fundamentalt svårare problem på grund av två viktiga skäl[18,S.128].

Till skillnad från finansiella transaktioner där man kan koppla en transaktion till en användare så ska det inte vara möjligt i val att koppla en väljare till hans eller hennes röst, registrering och granskningsfunktioner som är standard i den finansiella världen är därför inte tillämpligs bar i ett webbaserat röstningen system[19,S.6]. För det andra kan upptäckten av avvikelser eller fel i överföring eller registrering av röster inte sannolikt leda till en korrigering av dessa resultat i efterhand[19,S.5]. I bästa fall kan en sådan upptäckt endast leda till ogiltigförklaring av de röster som påverkas, i värsta fall i ogiltigförklara själva valet. I ett sådant fall kan resultat få katastrofala följder i form av allmänhetens förtroende för legitimiteten i hela processen.

De eventuella fördelarna med Internetröstning måste vägas mot de risker som denna röstning metod utsett för. Samt att den bör uppfylla grundläggande principer för sekretess och anonymitet, rättvisa, noggrannhet och öppenhet. Dem potentiella risker som finns uppstår på grund av säkerhetsbrister som kan finnas i både användarens dator och nätverksanslutningen genom vilken den ansluter till den centrala val servern. Säkra förbindelsen mellan väljarens hemdator och den centrala servern är problematiskt, men i detta område kan korrekt användning av kryptering tillåta en grad av förtroende för integriteten för denna kommunikationsväg. kryptering kan använda för att förhindra så kallade MITM (man in the middle) attacker[5.S,77]. men även om denna teknik används på rätt sätt, är det fortfarande sårbara för andra typer av attacker, som en DOS attacker eller bedrägeri attacker så kallad spoofing attacker.

En överbelastningsattack kan inte ändra eller störa innehållet i data som skickas till servern, men den kan förhindra kommunikationen från att äga rum. vanligtvis genom att överbelasta den ena eller andra slutpunkten för kommunikationen.

En bedrägeri attack uppstå när en av de kommunicerande parterna luras att öppna en säker anslutning till en webbplats som kontrolleras av en angripare. Det kan vara ett e-postmeddelande som innehåller en länk till en webbplats som har skapats för att helt

efterlikna ett särskilt webbplats för att komma åt känsliga personuppgifter som kreditkortsnummer, lösenord, m.m.

# 7 Slutsats

Webbaserade röstningssystem är fortfarande i en allmän utvecklings fas, för närvarande så är ingen av de befintliga systemen perfekta. From rapporterna som studerats i det här arbetet så får man fram att det i nu läget inte finns en standard för röstningssystem. De system som användas i olika länder varierar i storlek och omfattning. Inte heller finns det enighet om hur en sådan perfekt röstningssystem skulle kunna se ut. Länder som i nu läget har Webbaserade röstningssystem implementerar det som bäst passar de lokala förhållandena i fråga om behov, brådska, kostnader och tidsplan. Även om systemen varierar så kan många fallgropar undvikas genom att studera de system som redan används i olika länder.

Om vi pratar om Sverige så är frågan inte längre om Webbaserade röstningssystem en dag kommer införas utan frågan är när kommer det att in föras. Ett tryck för att möjliggöra Internetröstning i val växer starkare tillsammans med framsteg inom den underliggande tekniken.

webbaserade röstningssystem är fundamentalt annorlunda. På grund av kravet på rösternas sekretess måste samband mellan väljarens identitet och rösten den lagt undvikas. Genom att bryta sambandet mellan väljare och den man röstat på så kan inte externa kontrollanter bevisa att varje röst verkligen är räknad samt att de inte ändrats vid räknings till fället. Detta är utmaning som standard webbaserade tjänster inte tampas med för att de har en inbyggd funktion som spåra och övervaka transaktioner som sker på dem.

Om en kund inte litar på en banks elektroniska banksystem, kan han eller hon kontrollera deras kontoöversikt och bekräfta att alla transaktioner avspeglas på rätt sätt. Om ägaren till en bil inte litar på elektroniken i bilen, så är varje start av motorn en möjlighet att testa systemet.

Trots betydande framsteg i teknikens de senaste åren, är informationen i datorer mer sårbara än någonsin. Varje steg man tar i den tekniska utvecklingen av webbaserade tjänster för med sig nya säkerhetshot som kräver nya säkerhetslösningar.
Men naturligtvis finns det hopp, även om man aldrig kan veta om ett system är helt säker, så tror jag att man kan bygga ett system på ett sätt som kommer att göra en attack så svårt, riskfyllt och dyrt att attacken inte kommer att vara värt ansträngningen.

När det arbete startades så var målet att identifiera de tekniska säkerhetsriskerna som fins med en webbaserad röstningstjänst. Genom arbetet har Jag konstatera att det är i klienten, servern och kommunikation vägarna som säkerhetsriskerna finns. Jag har identifierat 3 områden som kan utsätta för attacker av varierande slag.

Säkerhetsaspekten är den viktigaste delen i ett webbaserat röstningssystem, utan ett säkert system för skapande, överföring och lagring av kritiska data och personuppgifter så kan inget sådant system implementeras. Det finns olika uppfattning om hur skyddad data är när den skickas mellan två punkter, den mest pessimistiska säger att det finns alltför många problem i datorer och nätverk vilket gör att man inte kan skapa ett säkert

röstningssystem. Detta är delvis sant, det finn inget system som kan garantera absolut säkerhet, även klassiska pappersbaserade vall har en viss risk.

Ett visst mått av bedrägeri förekommer i pappers baserade valsystem men det tolereras eftersom det inte finns något alternativ.  Samt att det är mycket osannolikt att ett bedrägeri skulle kunna vara rikstäckande  efter som systemet är distrikt baserat. Allmänhetens uppfattning är att systemet fungerar, även om det kan finnas några veck i det här och där.

Kanske är det viktigaste inte om webbaserat röstningssystem kan vara helt säkert utan att utvärdera om de risker som finns  är acceptabla och hur man kan minska dem till ett minimum. Ett webbaserat röstningssystem kan bara fungera om alla inblandade med andra ord medborgare, politiker och myndigheter har tillräckligt förtroende i systemet och i teknik som används.

Även om det fortfarande krävs utveckling inom området så går det inte att stoppa den tekniska utvecklingen. Som jag sa tidigare så är frågan inte längre om utan när vi kommer kunna rösta på webben.

# Referenser


[1] Karlskrona2 - den digitala staden: Nya mötesplatser för demokratin? [Karlskrona2: The Digital City. New Fora for Democracy?], Per Zetterfalk, https://humanit.hb.se/article/view/154/158

[2] Post - och telestyrelsen Konsumentundersökning om Internetsäkerhet, 2012 - 02 - 14, Per Nellevad, https://www.iis.se/docs/PTS_-ER-2012_3-Internetsa%CC%88kerhet_Rapport.pdf

[3] It i människans tjänst – en digital agenda för Sverige, Produktion: Näringsdepartementet, oktober 2011. http://www.regeringen.se/contentassets/6136dab3982543bea4adc18420087a03/it-i-manniskans-tjanst---en-digital-agenda-for-sverige-n2011.12

[4] e-tjänster för ett enklare och öppnare samhälle, 15 december 2005 http://www.regeringen.se/contentassets/ed45c63feb064ff1a9a015bc25048b66/e-tjanster-for-ett-enklare-och-oppnare-samhalle

[5] E-röstning och andra valfrågor, SOU 2013:24 Slutbetänkande av 2011 års vallagskommitté Stockholm 2013 http://www.regeringen.se/contentassets/50146d1ac81d45318fb1a2c1e8679e90/e-rostning-och-andra-valfragor-sou-201324

[6] Svenskarna och internet, 2015 års undersökning av svenska folkets internetvanor, IIS, Olle Findahl & Pamela Davidsson, https://www.iis.se/docs/Svenskarna_och_internet_2015.pdf

[7] Svenskarna och internet 2015 Utdrag om sociala medier https://www.iis.se/docs/Svenskarna_och_internet_2015_Sociala_medier.pdf

[8] California Internet Voting Task Force A Report on the Feasibility of Internet Voting January, 2000, Bill Jones Secretary of State, http://www.umic.pt/images/stories/publicacoes1/final_report.pdf

[9] Council of Europe Publishing L EGAL , OPERATIONAL AND TECHNICAL STANDARDS FOR E - VOTING, adopted by the Committee of Ministers of the Council of Europe on 30 September 2004, http://www.coe.int/t/dgap/democracy/Activities/Key-Texts/Recommendations/Rec%282004%2911_Eng_Evoting_and_Expl_Memo_en.pdf

[10] Svenskarna positiva till att internetrösta i valet, David Bismark, http://www.internetstatistik.se/artiklar/svenskarna-positiva-till-att-internetrosta-i-valet/

[11] Higher Education Research Methodology-Literature Method, Guijuan Lin http://files.eric.ed.gov/fulltext/EJ1065734.pdf

[12] KTHB Den kreativa och kritiska litteraturstudien https://www.kth.se/polopoly_fs/1.308099!/Menu/general/column-content/attachment/Litterarurstudie-booklet.pdf

[13] OWASP-projektet, virus
https://www.owasp.org/index.php/Computer_Viruses

[14] OWASP-projektet, Denial of service
https://www.owasp.org/index.php/Application_Denial_of_Service

[15] OWASP-projektet, The Most Critical Web Application Security Risks
http://owasptop10.googlecode.com/files/OWASP%20Top%2010%20-%202013.pdf
[16] Internet voting in Australian election systems
http://www.ecanz.gov.au/research/files/internet-voting-australian-election-systems.pdf

[17] International Experience with E-Voting Norwegian E-Vote Project
https://www.parliament.uk/documents/speaker/digital-democracy/IFESIVreport.pdf

[18] 2011, E-public, e-participation and e-voting in Europe - prospects and challenges
http://www.europarl.europa.eu/RegData/etudes/etudes/join/2011/471584/IPOL-JOIN_ET(2011)471584_EN.pdf

[19] 2011, Discussion Paper: Internet Voting
http://www.elections.bc.ca/docs/Internet-Voting-Discussion-Paper.pdf

[20] Security 1:1 - Part 1, Viruses and worms
http://www.symantec.com/connect/articles/security-11-part-1-viruses-and-worms

[21] OWASP-projektet, Man-in-the-middle attack
https://www.owasp.org/index.php/Man-in-the-middle_attack