HAAGA-HELIA
ammattikorkeakoulu

Tallentavien äänestyskoneiden ja etä-äänestyksen tieto-turvauhkien selvitys

Miika Portaankorva

Opinnäytetyö
Tietojenkäsittelyn koulutusohjelma
2014

HAAGA-HELIA
ammattikorkeakoulu

Tiivistelmä

26.11.2014

Tekijä(t)
Miika Portaankorva

Koulutusohjelma
Tietojenkäsittelyn koulutusohjelma

Opinnäytetyön otsikko
Tallentavien äänestyskoneiden ja etä-äänestyksen tietoturvauhkien selvitys

Sivu- ja liitesivumäärä
24+1

Opinnäytetyön otsikko englanniksi
Research on Data Security Vulnerabilities of Direct-Recording Electronic Voting Machines and Online Voting

Tämä opinnäytetyö tutkii sähköisen äänestämisen kahden eri tekniikan tietoturvauhkia. Tutkittavat tekniikat ovat äänestyspaikalla sijaitsevat tallentavat äänestyskoneet (engl. direct-recording electronic voting machine, DRE) ja etä-äänestys (engl. online voting), joista viimeksi mainittu voidaan tehdä käyttäen jotain tietoteknistä laitetta kuten tietokonetta tai älypuhelinta. Työ tutkii näitä kahta sähköisen äänestyksen tekniikkaa ja tarkastelee niiden löydettyjä tietoturvauhkia.

Työssä käsitellään äänestyksen historiaa, sähköisen äänestämisen teknistä taustaa ja pureudutaan kahden suositun äänestystavan tietoturvauhkiin. Työssä esitellään tarkemmin esimerkkitapaus, joka on kuvaus amerikkalaisen Dieboldin toimittamasta sähköisestä äänestysjärjestelmästä ja sen tietoturva-aukkojen löydöistä.

Tallentavien äänestyskoneiden ja etä-äänestyksen uhkia tutkittiin lähdeaineiston avulla. Tämä lähdeaineisto koostuu tieteellisistä artikkeleista, julkishallinnon julkaisuista ja tutkimuksista. Tästä työstä on hyötyä ihmisille, jotka haluavat tietoa sähköisen äänestämisen pääperiaatteista ja yleisimmistä tietoturvauhista.

Projektin lopputuloksena syntyy kahden yleisen äänestystekniikan tietoturvauhkien selvitys, mikä kertoo tämän hetken sähköisen äänestämisen turvallisuudesta. Työssä esitellään erilaisia uhkia, kuten haittaohjelmia, ohjelmointivirheitä ja äänten myyntiä, sekä käydään läpi kolmannen osapuolen vaikutusta vaalijärjestelmän toimittajana.

Asiasanat
sähköinen äänestäminen, tietoturvauhka, äänestysjärjestelmä

HAAGA-HELIA
University of Applied Sciences

Abstract

26.11.2014

Author(s)
Miika Portaankorva

Degree programme
Business Information Technology

Report/thesis title
Research on Data Security Vulnerabilities of Direct-Recording Electronic Voting Machines and Online Voting

Number of pages and appendix pages
24+1

This study investigates data security vulnerabilities in the field of e-voting.

The study focuses on data security vulnerabilities of the two widely known electronic voting techniques: direct-recording electronic voting machines and online voting.

This thesis contains a historical perspective of the voting machines, the technical background of the above-mentioned e-voting standards and a research on data security vulnerabilities. This work also includes a deeper investigation of a case study on an American corporation Diebold Inc. and its electronic voting system. This study reveals data security vulnerabilities that were found in the system.

The results of this study offer an insight into the two common e-voting techniques and their data security vulnerabilities and the general level of safety of e-voting. This work goes over a variety of threats such as malware, programming errors and vote selling.

The literature material for this thesis includes scientific articles, public administration's publications and other researches. This study helps understand the main principles of e-voting systems and their most common data security threats.

Keywords
e-voting, data security vulnerability, voting machine

Sisällys

1 Johdanto

Tämän projektin tehtävä on etsiä ja koota sähköisen äänestämisen selvitettyjä ja tutkittuja tietoturvauhkia. Opinnäytetyöprojekti keskittyy tietoturvauhkien selvittämiseen lähdeaineiston avulla. Työssä käsitellään lähinnä 2000-luvun alun Yhdysvaltojen sähköisen äänestämisen ongelmakohtia.

Projektissa on kaksi pääasiallista tutkimuskysymystä: ensimmäinen on tallentavien äänestyskoneiden tietoturvauhat ja toinen on online-äänestämisen tietoturvauhat. Nämä tutkimuskysymykset ovat tämän projektin ydin, ja tämä työ rakentuu niiden ympärille. Työssä etsitään ja esitellään kahden edellä mainitun äänestystekniikan löydettyjä sekä tutkittuja tietoturvauhkia.

Tämä työ ei tuo ratkaisuehdotuksia tallentavien äänestyskoneiden ja etä-äänestämisen tietoturvaongelmiin vaan esittelee noin 15 vuoden aikana havaittuja tietoturvauhkia. Työ esittelee sähköisen äänestämisen tapauksia ja selvittää, mitä tietoturvauhkia on ilmentynyt käyttöönottojen aikana.

1.1 Menetelmät

Tutkimus toteutetaan käyttämällä lähdeaineistoa yhdysvaltalaisista ja eurooppalaisista teoksista. Työ on selvitystyö, joka kokoaa eri sähköisen äänestyksen tutkimuksista tietoturvauhkia. Näistä tutkimuksista etsitään ja käsitellään tietoturvaongelmia, ja ne esitellään tässä työssä. Työhön on valittu lähteiksi tieteellisiä julkaisuja sekä raportointeja sähköisestä äänestyksestä.

Tutkimuksessa on esitelty sähköisen tunnistamisen osuus, joka tukee työssä kuvattuja sähköisen äänestämisen tekniikoita. Työssä on esitelty sähköisen äänestysjärjestelmän tapauskuvaus, joka tuo tutkimukseen tarttumapintaa lähimenneisyydestä ja havainnollistaa seikkaperäisemmin löydettyjä tietoturva-aukkoja.

2 Taustaa

Äänestämisestä on syntynyt kuuma puheenaihe, kun se ynnä monet muut perinteiset asian hoidot, kuten maksaminen ja veroilmoituksen teko, on siirretty sähköiseen muotoon. Tässä opinnäytetyössä tutkitaan kahta yleistä sähköistä äänestystekniikkaa ja selvitetään, mitä uhkia näiden äänestystapojen käyttöönotto on tuonut tullessaan.

Kaikilla sähköisillä äänestysjärjestelmillä on tarkat määritykset, jotta äänestysjärjestelmät pystyisivät palvelemaan valtioidensa kansalaisia sellaisella tavalla, ettei se jättäisi äänioikeutettuja epäuskoiseksi sen toimivuudesta.

Äänestysjärjestelmää koskevat määritykset varmistavat, että vain äänioikeutetut pystyvät äänestämään ja että jokainen äänioikeutettu on tunnistettavissa äänioikeutetuksi. Äänestäjä äänestää vain kerran, ja jokainen vastaanotettu ja laskettu ääni on pätevä ääni. Äänestysjärjestelmä on avoin ja läpinäkyvä, ja se voidaan asettaa tarkastelun kohteeksi. (Mason 2005.)

Sähköisen äänestysjärjestelmän yksi tärkeimpiä lähtökohtia on, että se toisi helpotuksia nykypäivän äänestämiseen. Etä-äänestyksen toteutuessa ei tarvitsisi miettiä liikkumistaan vaalipäivänä. Tämän seurauksena koolle kutsuminen helpottuisi. Ei enää ainaista sunnuntaipäivän viettoa lähikoulussa tai ennakkoäänestämällä posteissa. Ihmiset sen sijaan äänestäisivät kotonaan käyttäen heille sopivinta älylaitetta. Tallentavilla äänestyskoneilla pystyttäisiin karsimaan virheellisiä ääniä, jotka ovat kirjoitettu epäselvästi, ja äänestystuloksen julkistaminen ei kestäisi niin kauaa kuin perinteisillä laskentatavoilla.

Sähköisillä äänestysjärjestelmillä on samat ongelmat kuin muillakin sähköisillä järjestelmillä. On tahoja, jotka haluavat hyötyä järjestelmien heikkouksista, ja tahoja, jotka tiedostamattaan saattavat käyttää järjestelmää väärin ja näin tekemään hallaa lähinnä itselleen.

Ne ihmiset, jotka käyttävät tiedostaen hyväkseen järjestelmän heikkouksia, pystyvät vaikuttamaan järjestelmään suuressa mittakaavassa, kuten esimerkiksi muuttamaan äänestyksen tulosta. Ne ihmiset taas, jotka käyttävät tiedostamattaan äänestysjärjestelmää väärin, johtuen esimerkiksi äänestysjärjestelmän huonosta käytettävyydestä, saattavat äänestää vahingossa toista, ei-mieluisaa kandidaattia. Nämä kuvaukset ovat läsnä 2000-luvun sähköisessä äänestämisessä. Kummatkin esimerkit ovat varteenotettavia, eikä niitä pysty laittamaan loppukädessä tärkeysjärjestykseen.

3 Äänestyksen historiaa

Äänestyslippu, engl. *ballot,* tulee italian kielen sanasta *ballota*. Sanalla viitataan varhaiseen äänestystapaan, missä lipukkeet laitettiin astiaan merkitsemään ääniä. (Lauer 2004, 179.)

Historian aikana ihmisten tapa äänestää on muuttunut useita kertoja. Vaikka perinteinen käsinkirjoitettu paperilippuäänestys onkin säilynyt yleisimpänä tapana äänestää, erilaisia äänestyksen muotoja on kokeiltu sivussa.

Paperilippuäänestystä käytettiin ensimmäisen kerran Roomassa vuonna 139 EAA, ja tapa tuli käyttöön Amerikassa ensimmäisen kerran vuonna 1629, kun erääseen Salem-kirkkoon täytyi valita uusi pastori. Ensimmäiset äänestyslipukkeilla tehdyt äänestykset olivat turvatasoltaan heikkoja, eikä äänestäjän yksityisyyttä pystytty varjelemaan tarpeeksi hyvin, joten niihin kohdistui erilaisia vaalivilppejä. (Jones 2001.)

Nykyaikainen paperilippuäänestys muodostui Australiassa vuonna 1858. Valtio loi standardoidun äänestyslipukkeen, joka jaettiin kansalaisille vaalitoimistossa, ja ihmisiä kehotettiin äänestämään ja heti sen suoritettuaan palauttamaan äänestyslipukkeet vaalivirkailijalle. (Jones 2001.)

Ensimmäisen internetin avulla suoritetun äänestyksen teki astronautti David Wolf vuonna 1997 Texasin vaaleissa. Wolf työskenteli Mir-avaruusaluksella äänestyshetkellä. Äänestyslipuke oli lähetetty sähköpostilla Wolfin lähivaalitoimistosta Johnson-avaruusasemalle ja sieltä edelleen eteenpäin Venäjän avaruusjärjestöön, ennen kuin se oli yhdistetty avaruusasemaan. (Lauer 2004, 180.)

4 Sähköiset tunnistamistavat

Sähköisen äänestämisen edellytyksenä on käyttäjän oikeaoppinen tunnistaminen. Tällä tarkoitetaan henkilön identiteetin todentamista (Perttula 2003, 10). Henkilöllä on oltava yksilöivä ominaisuus, piirre, tieto tai fyysinen tunniste, jonka täytyy olla luettavissa ja todennettavissa sähköisesti (Perttula 2003, 10).

Sähköisessä tunnistamisessa on kaksi menetelmää: henkilön autentikointi ja identifiointi. Autentikoinnissa henkilö vakuuttaa olevansa esittämänsä henkilö ja tämä väite tarkastetaan. Identifioinnin tarkoitus on, että ihmisen henkilöllisyys voidaan tunnistaa ilman henkilön väitettä siitä. Autentikointi on käytössä usein asiointipalveluissa ja identifiointi valvonnassa ja esimerkiksi poliisitutkinnassa. (Perttula 2003, 10.)

Sähköinen tunnistaminen

Sähköisiä tunnistusmenetelmiä käytetään yksilön henkilöllisyyden todentamiseen. Perttulan (2003, 20) mukaan on luotu seuraavat oletukset, joihin menetelmien toiminnallisuus ja luotettavuus perustuu:

> Tunnistettavalla henkilöllä on esittää jokin tieto, jonka vain hän tietää.
> Tunnistettavalla henkilöllä on esittää jokin fyysinen väline, jonka vain hän omistaa.
> Tunnistettavalla henkilöllä on esittää jokin ominaisuus, joka on vain hänellä ja on osa häntä. (Perttula 2003, 20.)

Yllä olevat oletukset ovat luonteeltaan suurpiirteisiä mutta täysin pitäviä. Tunnistustilanteessa luotettavuus kasvaa, kun yhä useampi edellä mainituista oletuksista on otettu huomioon. (Perttula 2003, 20.)

Ensimmäisen oletuksen lähtökohtana on, että tunnistava taho ja tunnistettava henkilö ovat sopineet spesifistä tunnisteesta, joka on vain heidän tiedossa. Tämä tieto voi olla henkilötunnus, asiakasnumero tai vain sitä tarkoitusta varten sovittu tai luotu salasana. Ongelma on sovitun tiedon leviäminen ja näin ollen sen joutuminen ulkopuolisten käsiin. (Perttula 2003, 20.)

Toisen oletuksen lähtökohtana on, että tunnistettavan henkilön täytyy esittää jokin fyysinen väline tai laite, jonka käyttäjä omistaa. Tässä tapauksessa edellisen kohdan sovittu

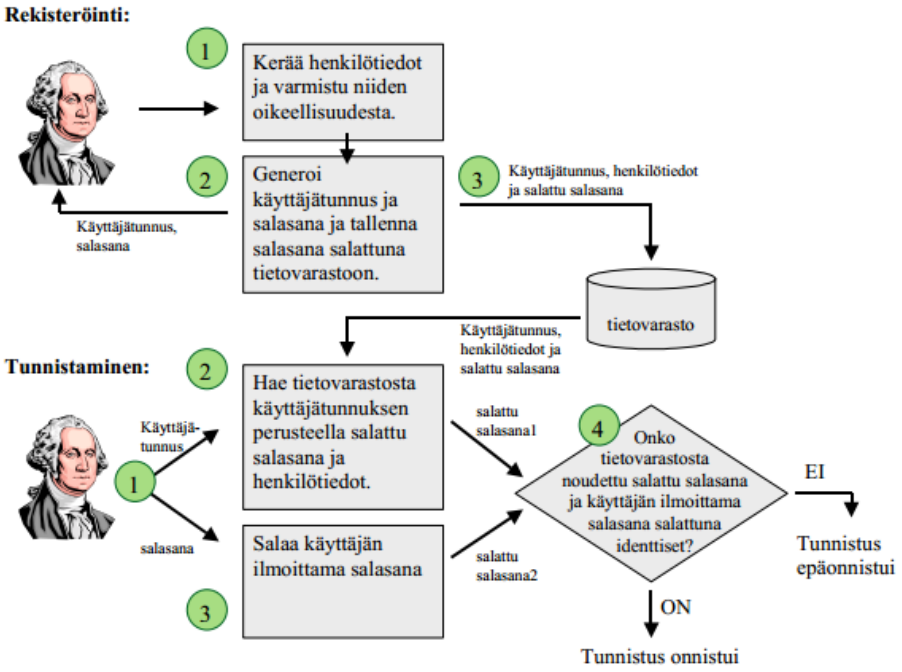
tieto on tallennettuna laitteelle. Menetelmä paranee ainoastaan, jos välineen kopioiminen ja väärentäminen on tarpeeksi vaivalloista. Silloin voidaan olla tarpeeksi varmoja siitä, että väline sekä tieto ovat vain yhden ihmisen hallussa. Tilanteessa, jossa laite häviää tai varastetaan, täytyy sen omistajan huomata sen katoaminen ja ilmoittaa siitä niille osapuolille, jotka ovat kelpuuttaneet sen tunnistusvälineeksi. (Perttula 2003, 20.)

Kolmannen oletuksen lähtökohtana on, että tunnistettava henkilö ei voi jäljentää tai luovuttaa tunnistustapaa, koska se on osa henkilöä. Jos ihminen on kiistattomasti tunnistettavissa tällaisen ominaisuuden kautta, niin kaksi aikaisemmin esitettyä oletusta ei paranna henkilön tunnistusta. (Perttula 2003, 20.)

4.1 Käyttäjätunnus ja salasana

Sähköisten palvelujen ylivoimaisesti käytetyin tunnistustapa on käyttäjätunnuksiin ja salasanoihin perustuva menetelmä. Se perustuu siihen, että tunnistettava ihminen omistaa käyttäjätunnuksen ja salasanan ja tunnistava osapuoli osaa yhdistää tunnuspariin (käyttäjätunnus ja salasana) liittyvät henkilötiedot. (Perttula 2003, 26.)

Generoitu käyttäjätunnus ja salasana on säilötty tietovarastoon. Käyttäjä kirjautuu palveluun tallennetulla tunnuksella ja salasanalla, ja niitä verrataan tietovarastoon aiemmin tallennettuun tunnuspariin. (Perttula 2003, 26.) Tekniikka on avattu Kuvassa 1.

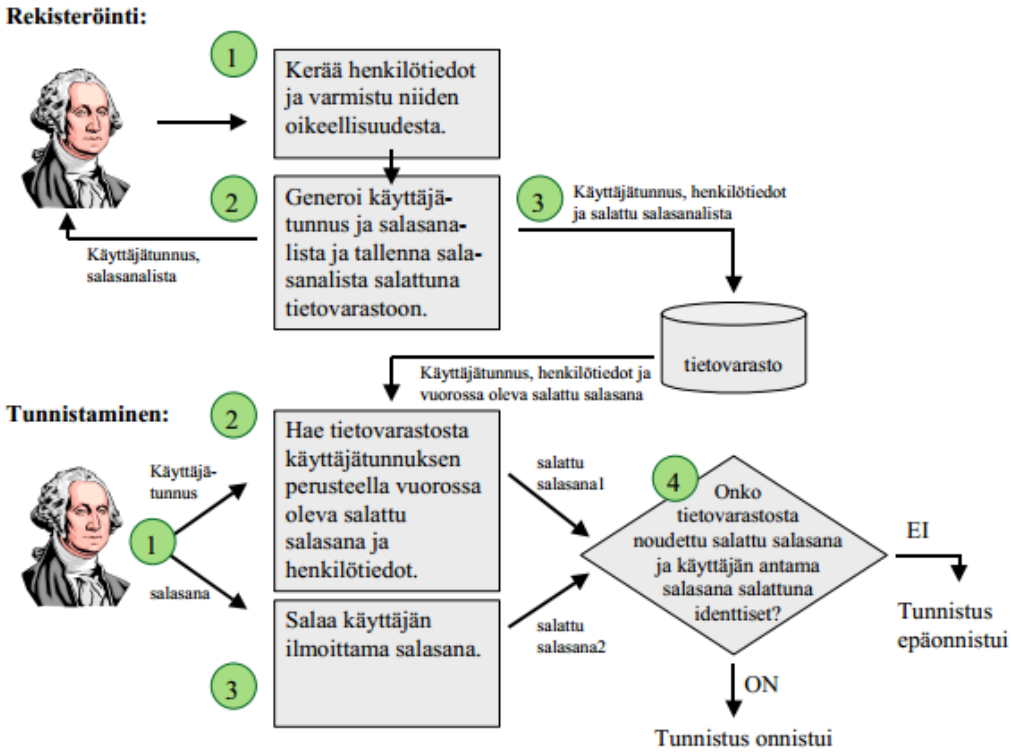


Kuva 1: Käyttäjätunnus ja salasana (Perttula, 2003)

4.2 Kertakäyttöiset salasanat

Kertakäyttösalasanat poistavat tietoturvariskin varastamiseen, jäljentämiseen tai hävittämiseen liittyvissä ongelmatapauksissa. Kertakäyttöisten salasanojen tekniikka perustuu algoritmiin, joka pystyy luomaan satunnaisia, toisiinsa liittymättömiä salasanoja, jotka ovat voimassa vain yhden käyttökerran. (Perttula 2003, 27-28.)

Tietovarastoon on tallennettu henkilön käyttäjätunnus, salasana ja salasanalista. Henkilön kirjautuessa palveluun verrataan tietovarastoon jo aiemmin tallennettua tunnusparia ja seuraavaa vapaana olevaa salasanalistan salasanaa. (Perttula 2003, 27-28.) Tekniikka on avattu Kuvassa 2.



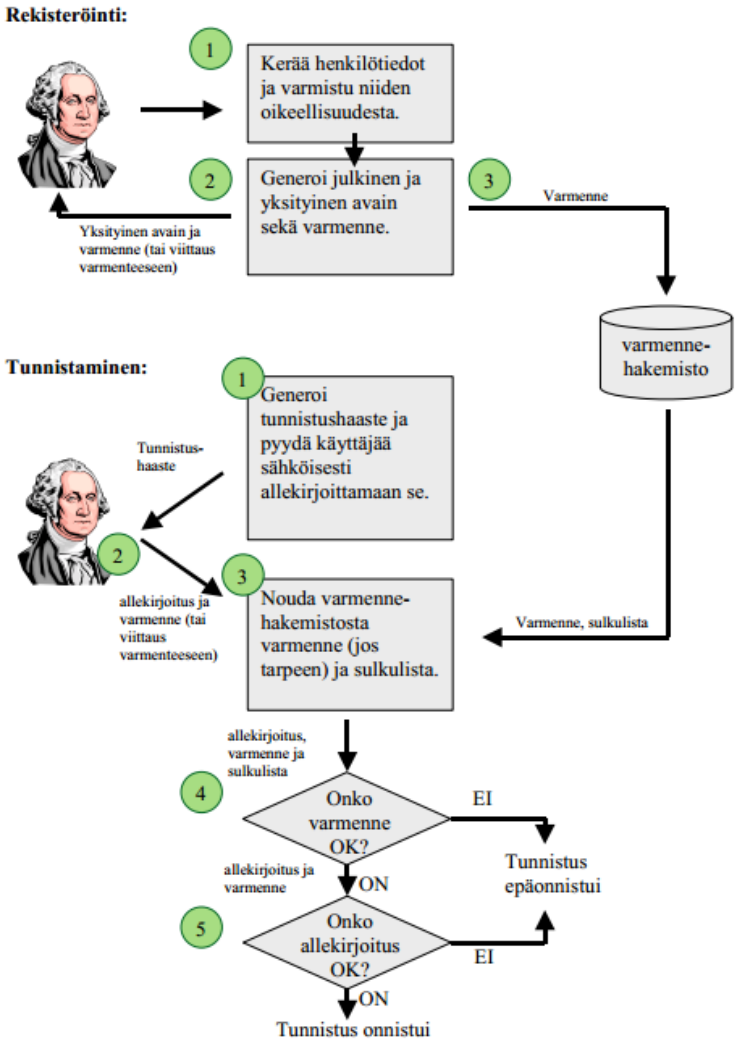
Kuva 2: Kertakäyttösalasanat (Perttula, 2003)

4.3 Varmennetyyppiset tunnistusmenetelmät

Varmennepohjaiset menetelmät pohjautuvat julkisen avaimen menetelmään, PKI:hin (engl. Public Key Infrastructure). Tekniikka perustuu siihen, että käyttäjälle luodaan kahdesta avaimesta rakentuva avainpari. Kun käyttäjä haluaa salata tietoa, salataan se toisella avaimella ja salauksen purku suoritetaan avainparin toisella avaimella. Toinen avaimis-

ta on niin sanottu julkinen avain, joka on julkisesti kaikkien nähtävillä. Sen sijaan toinen avaimista on niin sanottu yksityinen avain, joka on vain omistajansa hallussa. Kun tieto on salattu yksityisellä avaimella ja se on purettu julkisella avaimella, voidaan luottaa, että alkuperäisen datan kryptanneella osapuolella on ollut hallussaan avainparin yksityinen avain. Tätä voidaan myös kutsua sähköiseksi allekirjoittamiseksi ja sen tarkastamiseksi.

(Perttula 2003, 30.) Tekniikka on avattu Kuvassa 3.

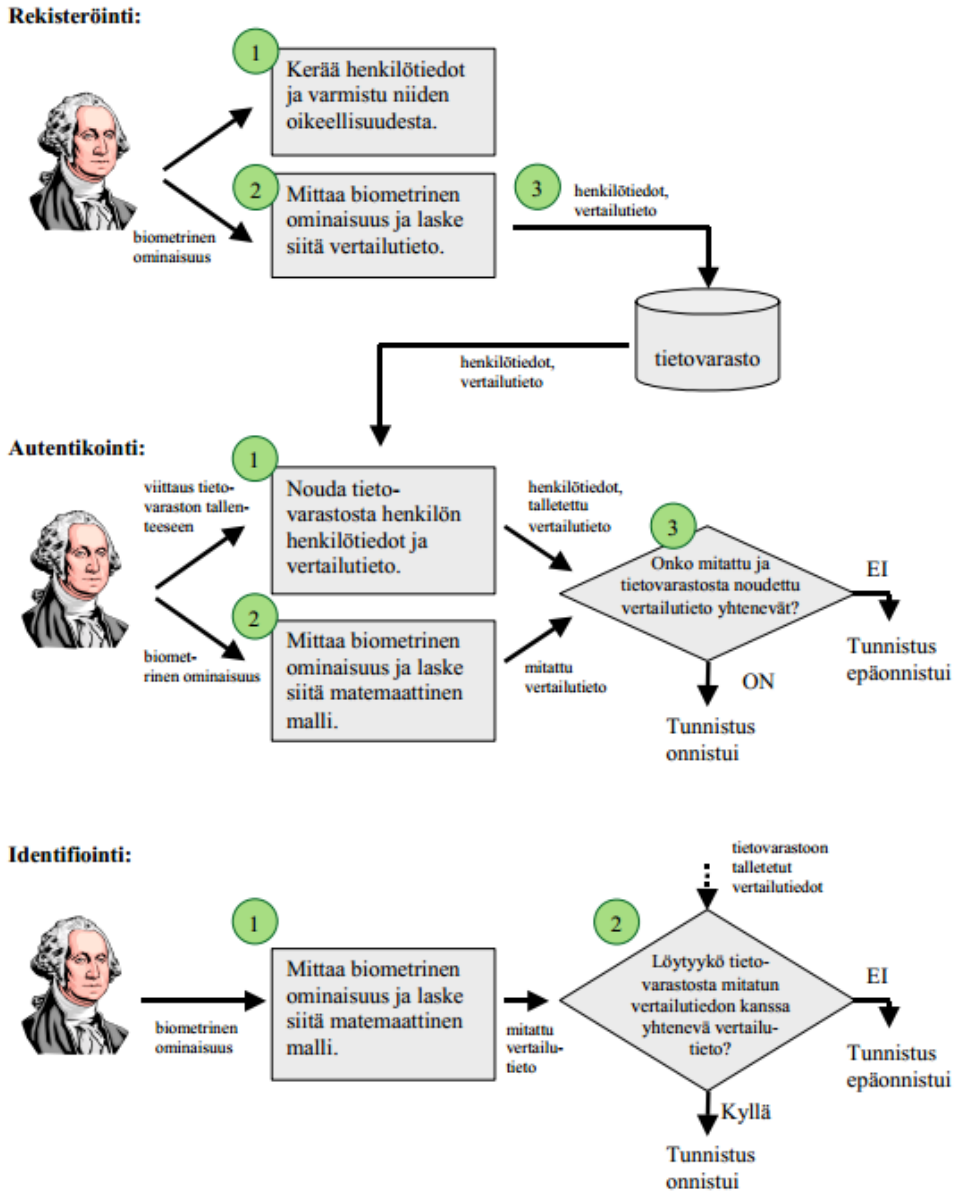


Kuva 3: Varmenteeseen perustuva tunnistus (Perttula, 2003)

4.4 Biometrinen tunnistus

Biometrisessä tunnistuksessa käytetään jotakin tiettyä ihmisen fyysistä ominaisuutta. Henkilöstä otetaan kuvat esimerkiksi sormenjäljistä tai silmän verkkokalvosta, ja ne tallen-

netaan yhdessä henkilötietojen kanssa tietojärjestelmään. Tunnistus tehdään mittaamalla tämä tietty fyysinen ominaisuus uudelleenmittausta vaativassa tilanteessa ja vertaamalla mittaustulosta aiemmin tallennettuun tulokseen. (Perttula 2003, 34.) Tekniikka on avattu Kuvassa 4.



Kuva 4: Biometrinen tunnistus (Perttula, 2003)

5 Äänestysmenetelmät esittelyssä

Tutkimuksen äänestystekniikat ovat tallentavat äänestyskoneet ja etä-äänestys. Tallentavilla äänestyskoneilla äänestäminen tapahtuu yleensä esimerkiksi kouluissa, kunnantaloilla tai siinä paikassa, jossa äänestys halutaan pidettävän. Tallentava äänestyskone sisältää usein tietokoneen, vaalisovelluksen ja käyttöliittymän.
Etä-äänestämistä pystyy tekemään paikasta riippumatta missä vain. Äänestysvälineenä on tarkoitus käyttää jotain henkilön saatavilla olevaa älylaitetta, kuten esimerkiksi tietokonetta tai älypuhelinta.

5.1 Tallentava äänestyskone

Tallentavat äänestyskoneet tulivat suosituksi mikroprosessorien halventumisen myötä, kun komponenteista pystyttiin muodostamaan koneita. Ensimmäiset tallentavat äänestyskoneet kehitti Shoup-yhtiö vuonna 1978. Kyseinen yhtiö oli toinen kahdesta yrityksestä, jotka olivat tehneet niin sanottuja vipukoneita (engl. lever voting machine) jo pitkän aikaa. Shoup-yhtiön kehittelemä sähköinen tallentava äänestyskone oli ulkomuodoltaan vanhanaikainen, jotta ihmisten olisi helppo omaksua uuden äänestyslaitteen käyttö. (Jones 2001.)

Tallentavan äänestyskoneen, DRE:n (engl. direct-recording electronic voting machine) laitteisto pitää sisällään useimmiten Windowsin PC-yksikön. Äänestyskoneessa on mukana kosketusnäyttö, joka on suojattu turvakotelolla, jotta estettäisi hiiren tai näppäimistön liittämisen. Äänestyskone on liitettynä verkkoon, jossa on katkeamaton energiavara. Äänestyskone on asetettu äänestyskoppiin, ja kopissa on sermi, joka estää näkyvyyden sinne. (Lauer 2004, 180.)

Äänestäjät menevät siihen vaalipiiriin, jossa he ovat tunnistettavissa, ja heille annetaan usein PIN-koodi tai älykortti, jonka avulla he saavat pääsyn käyttämään äänestyskonetta. Kansalaisten äänet tallennetaan, ja ne säilytetään äänestyskoneessa ja myöhemmin ladataan vaalitietojärjestelmään. (Lauer 2004, 180.)

Nykyajan tallentavilla äänestyskoneilla on paljon paremmat auditointi- ja turvallisuusominaisuudet kuin vanhoilla vipukoneilla. Tallentavat äänestyskoneet pystyvät säilyttämään sähköisen tallenteen, (engl, *ballot image),* joka tallentaa jokaisen äänen. Aikaisemmin pystyttiin tallettamaan vain äänien loppusumma laitteen sisälle. Sähköinen tallenne pystyy tallentamaan kaiken, mikä liittyy laitteeseen. Näin pystytään näkemään kaikki dokumentointi esivaaleja edeltävästä testauksesta aina äänestyspisteiden sulkemiseen. (Jones 2001.)

5.2 Etä-äänestys

Etä-äänestystä voidaan suorittaa monella eri laitteella. Äänestäjä pystyy käyttämään erilaisia tietoteknisiä laitteita, kuten kannettavaa tietokonetta tai älypuhelinta.

Arizonassa vuonna 2000 käytettiin seuraavanlaista tapaa online-äänestämisessä: Ensin äänestäjä todennettiin oikeaksi (vaalikelpoiselle äänestäjälle postitettiin PIN-koodi). Seuraavaksi suoritettiin äänen salaus julkisella avaimella äänestäjän käyttämään laitteeseen ja laitteen yksityisen avaimen säilytys luotetulla kolmannella osapuolella. Tämän jälkeen ääni siirrettiin www.election.com -palvelimelle käyttäen SSL-salattua tunnelia. (Lauer 2004, 180.)

SSL (engl. Secure Sockets Layer) on standardoitu turvateknologia, joka luo kryptatun yhteyden käyttäjäkoneen ja serverin välillä (Digicert 2014). Lopuksi annettu ääni erotettiin äänestäjän henkilöllisyydestä sijoittamalla tiedot tietokantaan sekä tarkistettiin auditointiloki. Auditointilokin tarkastuksessa tarkastetaan ensin, ketkä ovat äänestäneet, ja toiseksi tietokantaserverit. (Lauer 2004, 180.)

6 Tallentavien äänestyskoneiden tietoturvauhat

Tallentavien äänestyskoneiden uhkien esittely perustuu Thomas Lauerin luomaan kaavaan, Taulukko 3, joka löytyy tämän työn liitteenä.

Lauer (2004, 180) käy julkaisemassaan artikkelissa läpi tallentavien äänestyskoneiden elinkaaren, joka jakautuu neljään päävaiheeseen, ja luettelee niiden pääasialliset haavoittuvuudet. Vaiheet ovat tuotekehitys, asennus ja testaus, äänestystilanne sekä äänten siirtäminen ja laskeminen (Lauer 2004, 180).

Elinkaaren ensimmäinen vaihe sisältää tuotekokonaisuuden, eli tallentavan äänestyskoneen, joka pitää sisällään tavallisen verkkoon yhdistetyn PC-työasemakokoonpanon Windowsin käyttöjärjestelmällä. Äänestyskone sisältää tietyn vaalisovelluksen ja kortinlukijan. Tuotekokonaisuus voi olla vaihteleva, mutta edellä mainittu kokoonpano mahdollistaa tallentavalla äänestyskoneella äänestämisen. Kokoonpanoon liittyvät haavoittuvuudet koskevat tietokoneen laitteistoa ja eri sulautettuja järjestelmiä, kuten tässä tapauksessa kortinlukijaa. (Lauer 2004, 180.)

Ensimmäinen uhka tässä vaiheessa ovat salatut ohjelmat, eli niin kutsutut troijalaiset, jotka ovat jo tuotekehitysvaiheessa asennettu vaalikoneeseen (Lauer 2004, 180). Troijalaiset ovat haitallisia ohjelmia, jotka suorittavat toimenpiteitä, jotka eivät ole saaneet valtuutusta käyttäjältä. Toiminnot voivat olla esimerkiksi tiedon muuntelua tai poistoa. (Kaspersky 2014.) Nämä haittaohjelmat pystyvät muuttamaan ääniä toisiksi. Toisena uhkana on kortinlukijan vikatila, joka sallii luvattomien äänien antamisen tai äänestämisen useammin kuin kerran, ja kolmas uhka on se, että verkon koskemattomuus on uhattuna; tällöin äänestyksen loppusummia voisi muokata. (Lauer 2004, 180.)

Elinkaaren toinen vaihe koskee laitteistoa, testausta ja koulutusta. Toisen vaiheen tärkeimmät huomiot ovat paikallisten vaalitoimistojen henkilökunnan kouluttaminen ja kolmannen osapuolen suorittama testaus ja sertifiointi vaalisovellukselle sekä tarpeeksi turvallisen säilytyspaikan osoittamisen äänestyslaitteistolle. (Lauer 2004, 180.)

Suurin haavoittuvuus elinkaaren toisessa vaiheessa on kolmannen osapuolen testaajan vilpillinen toiminta (Lauer 2004, 180). Tämä näkyisi todennäköisesti siten, että testaaja ei tee tarvittavia turvatestauksia vaalisovellukselle tai laitteistolle ja näin laiminlyö äänestysjärjestelmän tietoturvan, joka olisi sen jäljiltä altis vaalivilpille.

Toisena uhkana on yksilöllisempi ongelma, eli tallentavan äänestyskoneen sähköisen äänestyslipukkeen ulkonäkö (Lauer 2004, 180). Jos äänestyslipukkeen käytettävyys ja muotoilu on suunniteltu huonosti, voi se harhaanjohtaa ihmisen äänestämään jotakin toista, ei-toivottua kandidaattia.

Kolmas mainittava haavoittuvuus on vaalihenkilöstön liian niukka tai pinnallinen koulutus (Lauer, 2004). Tämä voisi johtaa yleiseen epäluottamukseen äänestyspaikalla - tai pahimmassa tapauksessa vaalivirkailijat voisivat vilpillisesti ohjeistaa äänestäjiä äänestämään oman etunsa mukaisesti.

Elinkaaren kolmannessa vaiheessa käsitellään itse äänestämistä äänestyspaikoilla. Äänestyspaikoilla suoritetaan äänestäjän oikeaksi todentaminen kortinlukijoilla, tarkastetaan äänestyslaitteiden tila ja kunto sekä annettujen äänien tallentaminen (Lauer 2004, 180).

Suurin uhka tässä vaiheessa on laitteiston toimintahäiriö äänestyspaikalla. Ensimmäinen haavoittuvuus koskee sulautettuja järjestelmiä, eli kortinlukijaa. Äänestystä ei voida suorittaa, jos kortinlukijan toimintakunnosta ei voida olla varmoja. Riski on, että kortinlukija sallii äänestäjien äänestää useita kertoja, jolloin äänestystulos ei ole enää luotettava.
Toinen riski on, että kortinlukija ei anna äänestämiseen oikeutettujen kansalaisten äänestää, jolloin ihminen ei pääse käyttämään äänioikeuttaan. Kolmantena riskinä on, että vaalikone ei tallenna annettua ääntä järjestelmään. (Lauer 2004, 180.)

Elinkaaren neljäs ja viimeinen vaihe pitää sisällään äänien siirron äänestyskoneista vaalitietojärjestelmään, äänien auditoinnin sekä äänien uudelleenlaskennan (Lauer 2004, 180).

Ensimmäinen riski tässä vaiheessa on kolmannen osapuolen tiedostonsiirron aikana tapahtuva yhteyden hakkerointi (Lauer 2004, 180). Hakkeri pystyisi tekemään palvelunestohyökkäyksen (engl. denial of service) vaalitietojärjestelmän palvelinkoneeseen. Palvelunestohyökkäyksessä hyökkääjä yrittää estää käyttäjien pääsyn käyttämään tiettyä palvelua (US-CERT 2014). Hakkerointi saman aikaisesti kun ääniä siirretään, voi myöhästyttää tuloksien laskentaa tai pahimmassa tapauksessa hävittää tietyn alueen äänimäärät.

Toisena riskinä on, ettei vaalisovellus pysty laskemaan kokonaisäänimääriä oikein ja luottamus siihen vaarantuu. Kolmantena taas, että vaalien auditoinnin suorittava kolmas osapuoli ei enää ole luotettava vaan pyrkii hyötymään vaalien tuloksesta muuttamalla äänien kokonaismääriä. (Lauer 2004, 180.)

Taulukossa 1, Lauer (2004, 181) listaa yleisimpiä uhkia tallentavista äänestyskoneista. Taulukosta on helppo hahmottaa, mitä seurauksia ja vastatoimia eri uhat saavat aikaan.

Taulukko 1: Tallentavien äänestyskoneiden tietoturvauhkia (Lauer, 2004).

Threat	**Consequence**	**Likelihood**	**Countermeasures**
Trojan horse installed by DRE vendor	Wholesale election compromise	Unknown – consider gaming industry as reference	Detection very difficult especially when code obfuscation techniques used
Trojan horse installed by Operating System vendor	Wholesale	No known example, but theoretically possible	See above
Trade secrecy	Prevents examination and adequate testing of software	Certain	Require Open Source system components and vendor source code inspection and testing
Lack of standards	Prevents adequate testing of DRE Voting system	Certain	Develop standards (a slow process)
Lack of configuration oversight	Configuration change could introduce new voting compromises	Known problems with configuration oversight	Stronger legal sanctions – but oversight is expensive
Buggy software	Potential for multiple voting, loss of voter privacy	Unknown	Better testing and certification of DRE voting systems
			The most effective countermeasure for many of the above problems is to use a voter verified audit trail

7 Etä-äänestämisen tietoturvauhat

Etä-äänestäminen (online-äänestys) käsittää kattavan sarjan erilaisia uhkia, jotka on lähes mahdotonta neutralisoida tai pyrkiä edes lähelle sitä. Lauer (2004) kuvaa artikkelissaan erittäin hyvin etä-äänestämisen lukuisia riskejä, joista suurin osa liittyy käytettävään PC-tietokoneeseen ja internetiin.

Lähtökohta etä-äänestämisen riskien kartoitukselle on paikka, eli se lokaatio, missä äänestäjä käyttää esimerkiksi tietokonetta tai älypuhelinta ja äänestää kandidaattiaan. Paikka tekee etä-äänestämisestä erikoisen, koska käytetty laite ja se paikka, mistä kukin äänestää, tekevät siitä vaaliuurnan. Käyttäjien laitteet, tietokoneet, tabletit tai puhelimet voivat siis käytännössä sijaita missä tahansa. Äänestystä ei välttämättä rajoita se, tapahtuuko se kotikoneella tai jollain julkisella tietokoneella - kuten esimerkiksi kirjastoissa tai kahviloissa (Lauer 2004, 181).

Myös suojaamattoman langattoman verkon käyttö voi aiheuttaa riskin etä-äänestämisessä. Oikein valituilla välineillä kenellä tahansa on mahdollisuus seurata laitteen liikennettä, kuten verkkosivuilla vierailuja tai mitä käyttäjätunnuksia ja salasanoja on käytetty (Microsoft 2014).

PC-tietokoneista on todettava ainakin se, että niiden saaminen puhtaaksi kaikista haitta-ohjelmista ja viruksista on käytännössä mahdotonta (Lauer 2004, 181). Jo yksin tämä ongelma asettaa etä-äänestämiselle perustavanlaatuisen riskin.

Etä-äänestämisen haastava ongelma on äänestäjän yksityisyys. Kun äänestys tapahtuu äänestäjän itsensä valvomassa hetkessä, kuten esimerkiksi kotona tai vaikka julkisessa liikennevälineessä, ei synny takeita vaalisalaisuuden paikkansapitävyydestä. Kansalaisten äänestäessä keskenään viranomaisen valvomattomissa tiloissa ei pystytä takaamaan samankaltaista vaalisalaisuutta kuin perinteisesti uurnilla käytäessä (Lauer 2004, 181).

Tämä voi asettaa äänestystilanteen alttiiksi painostukselle: joku ulkopuolinen tai tuttu henkilö voi koettaa vaikuttaa laittomasti jonkun toisen äänioikeuteen ja näin ohjailla äänten antoa. Lauer (2004, 181) toteaa artikkelissaan, että esimerkiksi kahden ihmisen suhteessa, jossa toinen pystyy käyttämään hyväksi toista ihmistä ja siten ohjailemaan tämän tekemisiä, voisi vaaleissakin dominoivampi osapuoli pakottaa heikomman äänestämään vastoin omaa tahtoaan. Kun äänestäminen tapahtuu äänioikeutetun valitsemassa paikassa, on vaikea valvoa eri tahojen vaikuttamista äänestäjien antamiin ääniin. Etä-

äänestäminen voi avata oven laajalle ulottuvalle äänten myynnille (Lauer 2004, 181). Skenaariossa äänioikeutetut voisivat saada vastineeksi esimerkiksi rahaa tai palveluja, kunhan äänestävät tiettyä asiaa, kandidaattia tai puoluetta.

Mielenkiintoisimpia Lauerin (2004, 181) huomioita ovat internetin infrastruktuuriin liittyvät uhat. Uhkakuvat liittyvät äänioikeuden riistoon, joka voisi tapahtua palvelunestohyökkäyksillä. Jokin taho pystyisi tekemään valikoivasti palvelunestohyökkäyksen, joka lamauttaisi äänestäjien laitteet tietyllä asuinalueella äänestyspäivänä. (Lauer 2004, 181.)

Hyökkäys voisi olla erittäin vaikuttava esimerkiksi kunnallisvaaleissa, jossa valitaan kandidaatteja kaupunkien valtuustoihin. Lamauttamalla osan kaupungista, tai jopa täsmentäen sen tiettyyn kaupunginosaan, jossa on taipumusta äänestää tiettyä puoluetta, voisi se kääntää vaakakuppia toisten puolueiden puolelle.

Etä-äänestämisessä ilmaantuu sama ongelma kuin tallentavilla äänestyskoneilla äänestäessä eli kolmannet osapuolet. Ne osapuolet, jotka tuottavat järjestelmän, luovat samalla uhan järjestelmän sisäpuolelta toimimiseen. Samalla, jos järjestelmät ovat suljettuja, käy niiden standardien, testauksen ja sertifikaattien kehitys vaikeaksi suorittaa. (Lauer 2004, 182.)

Taulukossa 2 Lauer (2004, 182) listaa etä-äänestämisen yleisimpiä uhkia. Taulukosta on helppo hahmottaa, mitä seurauksia ja vastatoimia eri uhat saavat aikaan.

Taulukko 2: Etä-äänestämisen tietoturvauhkia (Lauer, 2004).

Threat	Consequence	Likelihood	Countermeasures
Denial of Service	Disenfranchisement	Common, occurred during Canadian Internet election	No simple countermeasures
Trojan horse spyware to change or monitor votes	Vote theft, loss of privacy	Widely available tools for this	Detection difficult. Individual PCs can be protected, but assuring compliance difficult, especially for public PCs.
Automated vote buying	Compromise of election	Likely since there exist organizations set up to do this.	None. Organizations may exist outside country's jurisdiction
Insider attack on voting system	Compromise of election	Insider attacks are common in commercial settings.	Separation of duties, adequate documentation, control over physical assets, independent audits,
Virus specific to Internet voting system	Vote theft, privacy loss, disenfranchisement, compromise of election	Unknown	Very difficult since such a virus would have no prior history
Spoofing	Vote theft,	Common and easy	Can be launched from anywhere. Made difficult by use of encrypted PIN

8 Kolmas osapuoli ja monopolin vaikutus

Aiemmissa kappaleissa olen maininnut kolmannen osapuolen roolin merkittäväksi sähköisen äänestämisen kannalta. Kolmas osapuoli, joka toimii järjestelmän toimittajan roolissa, kantaa vaalien suurimman vastuun. Jos valtio hyväksyy yhden toimittajan luomaan äänestysjärjestelmän ja käyttää sitä järjestelmää tulevaisuudessa, niin monopoli on syntynyt (Jones 2001).

Jones (2001) kuvaa lausunnossaan monopolin syntymistä ja sen vaikutuksia. Tärkeimmäksi ajatukseksi nostan tilanteen, jossa monopoli hyväksyttäisiin, minkä seurauksena äänestysjärjestelmien kehittäminen lakkaisi ja kansalaiset pakotettaisiin hyväksymään järjestelmä, jossa on tunnettuja puutteita. Näin ollen, jos yksi toimittaja ja sen järjestelmä valittaisiin standardiksi, kilpailu toimittajien välillä lakkaisi. (Jones 2001.)

Tietoturvan kannalta on vain järkevää käyttää ja kilpailuttaa mahdollisimman monia toimijoita. Jos jollain taholla on pyrkimys horjuttaa vaalijärjestelmää ja hyötyä siitä, monopolitilanteessa täytyisi vaikuttaa vain yhteen toimijaan. (Jones 2001.)

Seuraavassa kappaleessa tutkitaan tarkemmin kolmannen osapuolen roolia sähköisen äänestysjärjestelmän toimittajana.

8.1 BlackBoxVoting Case: Diebold Precinct-Based Optical Scan 1.94w

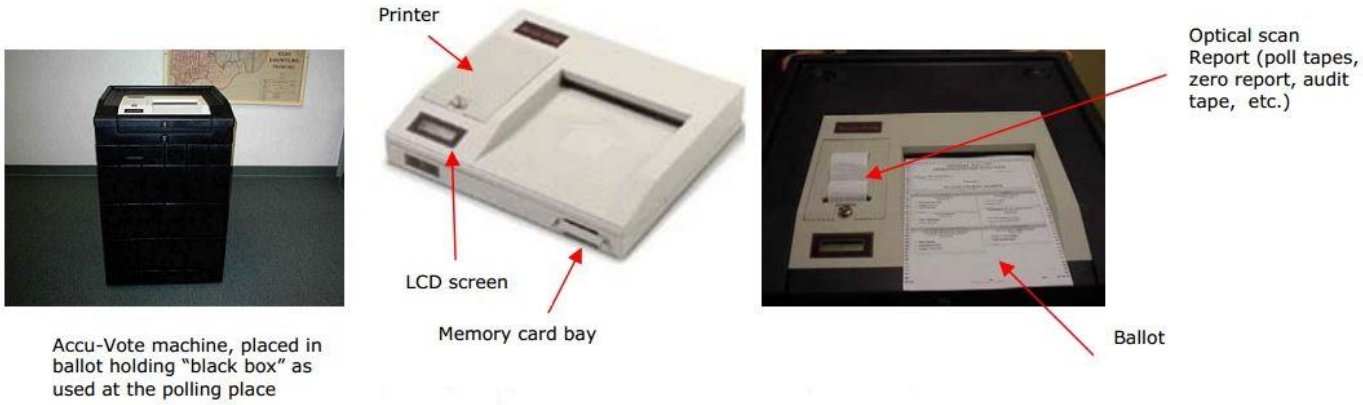
Black Box Voting on puolueeton, ei-kaupallinen tutkiva järjestö, joka tiedottaa ja seuraa Yhdysvalloissa tapahtuvia äänestyksiä. Järjestön perusti kirjailija Bev Harris vuonna 2004. (BlackBoxVoting 2004.)

Diebold, Inc. on yhdysvaltalainen noin 7000 henkilöä työllistävä julkinen osakeyhtiö, joka toimii tietoturvapalveluiden ja sulautettujen järjestelmien tuottajana. (Diebold 2014)

Yhdysvalloissa vuoden 2004 presidenttivaaleihin Dieboldin toimittama järjestelmä piti sisällään kolme komponenttia: optisen lukijan, jota käytetään äänestyspaikalla lukemaan ja tulkitsemaan äänestysdataa; irrotettavan muistikortin, joka säilöö annetut äänet; laskentasovelluksen, joka on PC-sovellus, joka pyörii Windows käyttöjärjestelmän päällä. Tätä sovellusta Diebold kutsuu nimellä ”GEMS”. GEMS kerää ja pitää lukua annetuista äänistä

sen jälkeen, kun ne on ladattu järjestelmään. (BlackBoxReport 2005, 5.) Kuvassa 7 on esitelty edellä mainittuja komponentteja.

Äänestäessä ihmiset asettavat täytetyn vaalilipukkeen optiseen lukijaan, joka osaa tulkita annetut äänet ja säilöö loppusummat mutta ei yksittäisiä ääniä muistikortille. Vaalien jälkeen data siirretään muistikorteilta vaalitietojärjestelmään joko modeemin avulla, tai sitten muistikortit tuodaan piirikunnan vaalitoimistoon, jossa ne siirretään käyttäen kaapelia. (BlackBoxReport 2005, 5.)



Kuva 5: Diebold Optical Scan Voting Machine (BlackBoxReport, 2005)

8.2 Zero report

Black Box Voting –järjestön raportti (2005) keskittyy paljolti yhteen merkittävään tietoturvaongelmaan Dieboldin järjestelmässä. Järjestön tutkiessa muistikortteja huomasivat he, että muistikortteihin pystyi vaikuttamaan lataamalla niihin ääniä ennen äänestystä, ikään kuin esiääniä. Tämä toimenpide ei vaihda ääniä vaan muokkaa äänistä kertovaa raporttia. Kopeloimalla tällä tavalla muistikortteja se säilyttää silti uskottavalta tuntuvan eheyden tekemällä vääriä raportteja vastaamaan vaalitietojärjestelmässä olevia raportteja. (BlackBoxReport 2005, 8.)

Merkittävä huomio BBV:n raportissa oli, että muistikortissa käytettiin 16 bittisiä kokonaislukuja (2 byte) pidempien kokonaislukujen (long integer) sijaan, jotka ovat 2000-luvun ohjelmoinnissa vakio (BlackBoxReport 2005, 19). Tämä mahdollisti muistikortteihin kohdistuvan kokonaisluvun ylivuodon (integer overflow) jälkiä jättämättä (BlackBoxReport 2005, 8).

Äänestyskoneen muistikortti kykenee vastaanottamaan vain tietyn äänimäärän. Kuitenkin, jos muistikortti vastaanottaa oman maksimiäänimääränsä, pyörähtää ääntenlasku nollaan. Kokonaisluvun ylivuodossa ideana on, että äänestyskortti on täynnä jo ennen äänestyksen alkamista, jolloin äänestystilanteessa molempien ehdokkaiden äänien lasku alkaa nollasta mutta äänestyksen jälkeinen raportti huomio myös esiäänet. (BlackBoxReport 2005, 8.)

Esimerkiksi tilanteessa, jossa on kaksi kandidaattia, voi toiselle ladata pienen ja toiselle suuren määrän esiääniä, niin että esiäänien kokonaismäärä on sama, minkä muistikortti voi kokonaisuudessaan ottaa vastaan. Näin esiäänien kokonaisluvuksi tulee nolla ja voi alkaa hyödyntää kokonaisluvun ylivuotoa. (BlackBoxReport 2005, 8.)

Tämän voi havainnollistaa yksinkertaistetulla esimerkillä: Oletetaan, että muistikortti voisi ottaa vastaan 10 ääntä. Kandidaatille A annetaan 8 ja kandidaatille B 2 esiääntä. Kun vaalivirkailija tarkistaa, että muistikortti on koskematon, saa hän raportin, jonka mukaan muistikortilla ei ole ääniä (zero report). Tämä johtuu siitä, että muistikortilla on jo niin paljon ääniä kuin se voi vastaanottaa. Nyt äänestyksessä muistikortti aloittaa laskun nollasta. Kandidaatille A annetaan äänestyksessä 6 ja kandidaatille B 4 ääntä. Mikäli muistikortti olisi koskematon, olisi tuo myös äänestyksen lopullinen tulos. Kuitenkin äänestyksen jälkeinen raportti huomio esiäänet, jotka aiemmin jäivät huomaamatta vaalivirkailijalta. Kandidaatti A:lle plussattaan vaaleissa annetut kuusi ääntä hänen etukäteen saamiinsa kahdeksaan ääneen, jolloin hänen kokonaisäänisaalinsa olisi 11. Muistikortti ei kuitenkaan voi vastaanottaa kuin kymmenen ääntä. Tällöin ehdokkaan saavuttaessa kymmenen äänen rajapyykin, laskuri nollaantuu taas ja vain kymmenen yli menevät äänet lasketaan. Kokonaisäänimäärä on näin ollen 1. Kandidaatilla B oli 2 esiääntä, ja vaaleissa hän saa 4. Hänen kokonaisäänimääräkseen tulee 6.

AccuVote-järjestelmä käytti tarkistealgoritmia (checksum algorithm) sen yksinkertaisuuden takia suojaamaan ääniä sattumanvaraisen tiedon hajoamiselta. Tarkistealgoritmin käyttäminen ei kuitenkaan suojaa järjestelmää tarkoituksenmukaiselta peukaloinnilta. Kokonaislukujen manipulointi osoitti, että on mahdollista lisätä ääniä, jotka kumoavat toisensa lisäämisen jälkeen. (BlackBoxReport 2005, 18.)

BBV:n tekemät testit osoittautuivat poikkeukselliseksi. He pystyivät lataamaan muistikorttiin ääniä ilman, että he modifioivat optisen lukijan raporttia. Äänien lataus ei muodostanut mitään virheilmoitusta, vaikka ladatut äänet olivat keinotekoisesti muutettu, ja raportti käyttäytyi kuin se olisi saanut vain sallittuja ääniä. (BlackBoxReport 2005, 18.)

9 Tulokset

Tutkimuksen valossa tallentavien äänestyskoneiden suurimmat uhat liittyvät kolmannen osapuolen toimittamaan äänestysjärjestelmään. Yksinään kolmas osapuoli voi olla isoin uhka. Järjestelmän toimittajalla on halutessaan parhaimmat mahdollisuudet toimia järjestelmän sisäpuolelta, koska on järjestelmän kehittäjä.

Kehittäjän roolissa kolmannella osapuolella on mahdollisuus laiminlyödä tietoturvatestauksia ja näin jättää järjestelmä haavoittuvaiseksi siten, että siihen on mahdollista asentaa komponentteja, joilla voisi peukaloida vaalitulosta. Kolmas osapuoli kantaa myös suuren vastuun lopputuotteesta, jonka äänestäjät kohtaavat vaaliuurnilla. Jos vaalisovellus ja sen käyttöliittymä ovat sekavia tai esimerkiksi hitaita, voi se vaikuttaa ihmisten antamiin ääniin.

Kolmannelta osapuolelta on hyvä vaatia läpinäkyvyyttä vaalijärjestelmän kehitysvaiheissa. Vaalijärjestelmän täytyy suoriutua turvatestauksista ja auditoinneista, ja näiden toteuttajana olisi parasta olla ulkopuolinen toimija.
Kokonaan ulkopuolinen testaaja tuo uskottavuutta ja läpinäkyvyyttä vaalijärjestelmän tuotannossa. Mitä enemmän vaalijärjestelmän kehitykseen osallistuu eri toimijoita, sitä eheämpänä sitä voidaan pitää.

Etä-äänestämisen suurimmat uhat liittyvät käyttäjiin ja laitteistoon. Isoimpia kysymyksiä on, kuinka varmistaa etukäteen laitteen turvallisuus, jolla äänestys suoritetaan. Äänestyksen suorittava laite voi olla lähtökohtaisesti turvatasoltaan heikko. Jos laite pitää sisällään salaisia ohjelmia, jotka kuuntelevat laitteesta lähtevää liikennettä, ei äänestäjän yksityisyydestä voida olla varmoja.

Äänestäjän yksityisyys ja äänestyspaikka ovat suuria muuttujia. Äänestyspaikka voi vaihdella esimerkiksi kodin ja julkisen kulkuneuvon välillä. Kun paikalla ei ole samanlaista viranomaista kuin vaaliuurnilla, jää äänestäjän vastuulle, onko paikka, missä äänestyksen suorittaa, tarpeeksi turvallinen.

Kaikkien äänestäjien tulisi omien mahdollisuuksiensa mukaan säilyttää oma, henkilökohtainen äänioikeus. Kun valvovaa viranomaista ei ole paikalla äänestyshetkellä, helpottuu toisen henkilön tarkoituksenmukainen ääneen vaikuttaminen radikaalisti. Ihmisillä on entistä paremmat mahdollisuudet käydä kauppaa äänistä ja kiristää toisia äänestämään omien etujensa mukaisesti.

Käyttäjälähtöiset uhat ovat huomionarvoisia vaalisovelluksen käyttöliittymää suunniteltaessa. Käytettävyyden tulisi huomioida yksinkertaisinkin käyttäjä, jolla ei saata olla aiempaa kokemusta käyttöliittymistä, jotta vuorovaikutus koneen kanssa olisi mahdollisimman luontevaa.

10 Yhteenveto

Tutkimuksessa selvisi, että sähköisen äänestämisen tietoturvauhkien pelikenttä käyttäytyy todella moninaisesti. Ei ole olemassa pelkästään ulkopuolisen ihmisen tai tahon luomia uhkia, kuten palvelunestohyökkäykset, vaan uhkia voi ilmetä myös järjestelmän sisältä toimivalta taholta. Myös käyttäjä, eli äänestäjä, on suuressa roolissa kummassakin äänestystavassa. Äänestäjälle annetaan paljon vastuuta, ja äänestäjän omaan harkintakykyyn luotetaan paljon.

Lähtökohtaisesti työn rajaus oli parhaimpia onnistumisia. Rajauksen linjaveto, että parannusehdotuksia löydettyihin uhkiin ei tutkimuksessa tuoda esille, oli koko projektin kannalta hyvä päätös. Tällä tavalla toimiminen tekee lopputuloksesta hyvän kokonaisuuden.

Sähköisen äänestyksen tietoturvauhkien tutkinta on mielenkiintoinen teema. Tutkimuksen aihe oli valittu hyvin ja sopiva kirjoittajalle. Opinnäytetyöprosessi oli sujuva. Vaikka pääasiallinen kirjoittaminen ei jakautunut ajallisesti tasapuolisesti, ylitsepääsemättömiä aikatauluongelmia ei päässyt syntymään.

Projektissa saavutettiin työn ydin: vastaus tutkimuskysymyksiin kahden äänestystekniikan tietoturvauhkista. Lopputulos saavutti tavoitteet, joita alun perin lähdettiinkin tutkimaan. Työssä tuotiin esille sähköisen äänestämisen pääperiaatteet ja selvitys yleisimpiin tietoturvauhkiin.

11 Pohdinta

Tässä osiossa käsitellään tutkimuksen johtopäätöksiä ja esitellään projektissa ilmenneitä tietoturvauhkia yleisesti sekä esitellään tutkimuksen aikana nousseita ajatuksia.

Äänestäminen on demokratian perusoikeuksia, ja äänioikeuden käyttäminen on useille ihmisille kunnia-asia. Sähköinen äänestäminen on houkutteleva idea. Toimivalla sähköisellä äänestysjärjestelmällä voisi mahdollisesti aktivoida äänestäjiä.

Lähdin melko ennakkoluulottomasti tutkimaan sähköisen äänestyksen uhkia, sillä minulla ei ollut oletuksia lukuun ottamatta aiemmin opittua tietoa. Kannatan yleisesti kaikkea, mikä voi helpottaa ihmisten elämää ja mikä alentaa kynnystä toimia. Sähköiset palvelut ovat mielestäni parhaimpia esimerkkejä siitä, miten teknologia muovautuu ihmisten tarpeiden mukaan. Mitä enemmän ihmiset saavat sähköisiä palveluja osaksi omaa elämäänsä, sitä helpommaksi oleminen usein käy.

Sähköisen äänestämisen tietoturva on sen nuoresta iästä johtuen melko vähän tutkittu osa-alue, minkä takia tässä työssä käytettiin pelkästään internetistä löytyviä lähteitä.

Ennen tutkimusta ajattelin, että turvallisuuden takaaminen olisi helppo asia: onhan sähköinen maksaminenkin tehty melko turvalliseksi jo aikoja sitten, ja luulin, että samat lainalaisuudet pätisivät myös sähköisen äänestämisen tietoturvaan. Tutkimuksen kulun aikana tuli kuitenkin yllätyksenä ennen kaikkea se, kuinka laaja kirjo erilaisia epäkohtia liittyy sähköiseen äänestykseen.

Lopputulos on tiivis ja selittää ymmärrettävästi sähköisen äänestyksen tyypillisiä tietoturvauhkia. Työssä on onnistuneesti kuvattu pääasiallisia riskejä ja uhkia, mitkä ovat läsnä sähköisessä äänestämisessä. Onnistuneimpia kappaleita ovat uhkakuvaukset kummastakin äänestystavasta ja seikkaperäisempi kuvaus BlackBoxVoting-yhdistyksen tutkimasta tapauksesta. Äänestysmenetelmien esittelyosuudet olisivat voineet vaatia enemmän tutkintaa ja näkökulmia.

Sähköinen äänestäminen on oiva esimerkki siitä, miten tietoturvallisuuden kaksi pääasiaa, käytettävyys ja turvallisuus, kohtaavat. Palvelukonseptit tasapainoilevat jatkuvasti luontevan käytettävyyden ja tarpeellisten tietoturvakysymysten huomioon ottamisen kanssa.

Lähteet

BlackBoxVoting. 2005. The Black Box Report: Critical Security Issues with Diebold Optical Scan Design. Luettavissa: http://www.blackboxvoting.org/BBVreport.pdf Luettu: 01.09.2014

BlackBoxVoting. 2004. Luettavissa: http://www.blackboxvoting.org Luettu: 01.10.2014

Diebold. 2014. Luettavissa: http://www.diebold.com Luettu: 28.10.2014

Digicert 2014. What Is SSL (Secure Sockets Layer) and What Are SSL Certificates? Luettavissa: https://www.digicert.com/ssl.htm Luettu: 13.11.2014

Jones, D. 2001. Problems With Voting Systems and the Applicable Standards. Luettavissa: http://homepage.cs.uiowa.edu/~jones/voting/congress.html Luettu: 15.09.2014

Kaspersky 2014. What is a Trojan Virus? Luettavissa: http://usa.kaspersky.com/internet-security-center/threats/trojans Luettu: 13.11.2014

Lauer, T. 2004. The Risk of e-Voting. Luettavissa: www.ejeg.com/issue/download.html?idArticle=34 Luettu: 31.4.2014

Mason, S. 2005. Is There a Future For Internet Voting? Luettavissa: http://www.votobit.org/lallave/mason.html Luettu: 08.10.2014

Microsoft 2014. Mistä tiedän, onko langaton verkko turvallinen? Luettavissa: http://windows.microsoft.com/fi-fi/windows/know-wireless-network-secure#1TC=windows-7 Luettu: 19.11.2014

Perttula, J. 2003. Sähköisen tunnistamisen menetelmät ja niiden sääntelyn tarve, Liikenne ja viestintäministeriön julkaisuja, 44/2003. Luettavissa: http://www.lvm.fi/fileserver/44_2003.pdf Luettu: 03.06.2014

Digicert 2014. What Is SSL (Secure Sockets Layer) and What Are SSL Certificates? Luettavissa: https://www.digicert.com/ssl.htm Luettu: 13.11.2014

US-CERT 2014. Understanding Denial-of-Service Attacks. Luettavissa: https://www.us-cert.gov/ncas/tips/ST04-015 Luettu: 13.11.2014

Liitteet

Taulukko 1: Tallentavien äänestyskoneiden elinkaari (Lauer, 2004)