EndCryptor

Versio 2.5.5 www.endcryptor.com. Valmistaja Enternet Oy.
Vinkki: Käytä kirjainmerkkejä liikkumiseen tässä dokumentissa.

Contents

Tämän documentin päiväys: Elokuu 25, 2020

Yleiskuvaus

Erinomainen suoja nykyajan hyökkäyksiä vastaan

EndCryptor suojaa vanhat salatut viestit vaikka hakkeri saisi haltuunsa nykyiset salausavaimet. Jokin aika sitten havaittiin tietokoneviruksia (jotka olivat olleet toiminnassa vuosikymmenen), jotka varastivat tunnettujen sähköpostin salausohjelmien salausavaimia – näin mahdollistaen näillä tuotteilla salattujen aikaisempien viestien avaamisen. EndCryptor on suunniteltu suojaamaan ennen hakkerointia muodostettu salattu liikenne ja myös toipumaan hyökkäyksestä – näin hakkeri menettää kyvyn avata uusia saapuvia viestejä.

Helppokäyttöinen

Käyttäjän ei tarvitse olla salaustekniikan ammattilainen. Ohjelman käyttöliittymä on samanlainen kuin tavanomaisessa sähköpostiohjelmassa. Käyttäjän nykyistä sähköpostitiliä käytetään salattujen sähköpostien lähettämiseen ja vastaanottamiseen.

Päästä päähän salattu

Viesti salataan lähettäjän koneella ja salaus avataan vastaanottajan koneella. Vain oikea vastaanottaja voi avata viestin.

Kvanttihyökkäyksen kestävä

Saattaa olla mahdollista, että ennen vuotta 2030 on kvanttitietokoneita, jotka voivat avata klassiset julkiset avaimet. EndCryptor käyttää klassisten julkisten avainten lisäksi uusia kvanttihyökkäyksen kestäviä avaimia. On otettava huomioon, että nykyinen salattu liikenne on helppo kopioida ja tallettaa odottamaan kvanttikoneiden valmistumista ja niiden avulla tapahtuvaa salauksen avausta. On vastuullista suojautua tältä mahdollisuudelta. Kun kaksi henkilöä kommunikoi, alkaa kvanttisuojaus toisesta vaihdetusta viestistä se mukaanlukien, jos henkilöt viestivät vuorotellen.

Patentoitu teknologia, nykyaikainen salausmenetelmä ja julkiset avaimet

Salausprotokolla on patentoitu USA’ssa. Symmetrisen salausmenetelmän ja julkisten avainten toteutus perustuu julkisesti nähtävillä ja saatavilla olevaan koodiin, jonka ovat tehneet tekniikat suunnitelleet tiedemiehet.

Vertailu EndCryptorin ja S/MIME ja PGP-perheen (PGP, OpenPGP, GnuPG, ...) välillä tilanteessa, jossa uhrin kaikki nykyiset salausavaimet ovat paljastuneet.

	EndCryptor	**S/MIME ja PGP -perhe**
Ovatko viestit, jotka lähetetty uhrille ennen hyökkäystä, suojattuja?	KYLLÄ	EI
Toipuminen hyökkäyksestä tapahtuu	Kun seuraava viesti uhrilta on avattu. Kvanttihyökkäyksessä kun seuraava kvanttihyökkäyksen kestävä Diffie-Hellman vaihto on tehty.	Kun uusi julkinen avain saatu uhrilta. Tämä tapahtuu useimmiten sovituin ajanjaksoin - kuukausien tai vuosien välein. Ei suojaa kvanttikoneita vastaan.
Identiteettivarkaus huomataan	KYLLÄ	EI

Salausavaimia on varastettu mm. Hacking Team vakoilu-yritykseltä, tunnettuja virusohjelmia ovat Sauron, APT30, Red October, Team Spy ja Mask - jotka toimivat noin 5, 10, 5, 10 ja 7 vuotta - ja varastivat mm. salausavaimia. Pääkohteina olivat: hallitusten organisaatiot, diplomaatit / lähetystöt, energia, öljy ja kaasualan yritykset, tuskimuslaitokset, sijoitusyritykset, aktivistit.

Vertailussa EndCryptor ja selainpohjaiset ratkaisut

	EndCryptor	**Selaimeen perustuvat**
Suoja MITM hyökkäystä vastaan, jos vihamielinen juurivarmenne on asennettu käyttäjän koneeseen	KYLLÄ	EI

Jos hyökkääjän juurivarmenne on asennettu (esim. viruksen, pakottamisen, 'ilkeän' kotiapulaisen tai ilkeän tullivirkailijan avulla tai yrityksen politiikan seurauksena) käyttäjän koneeseen, niin selainpohjaisen salauksen ominaisuuksien vuoksi liikenne voidaan avata. Esimerkiksi yritykset käyttävät tätä tekniikkaa avatakseen kaiken yrityksestä lähtevän SSL liikenteen (sisältää selainliikenteen) - motivaationa on virusten etsintä. Salauksen avaus tehdään uhrin ja web palvelimen välissä, siitä luokittelu 'man-in-the-middle' (MITM) hyökkäykseksi.

Joskus selainpohjaiset sähköpostin salausratkaisut tekevät selaimessa javascriptillä viestin salauksen (esim. PGP). Tämä ei tuo suojaa MITM hyökkäystä vastaan - hyökkääjä muuttaa javascript koodia ennenkuin lähettää sen uhrille esim. niin, että käytetyn salausmenetelmän salausavain välitetään hyökkääjälle (esim. PGP:n yksityinen avain). Lue lisää selainpohjaisten ratkaisujen riskeistä luvusta ’SSL:n ja selainpohjaisen salauksen riskit ¨.

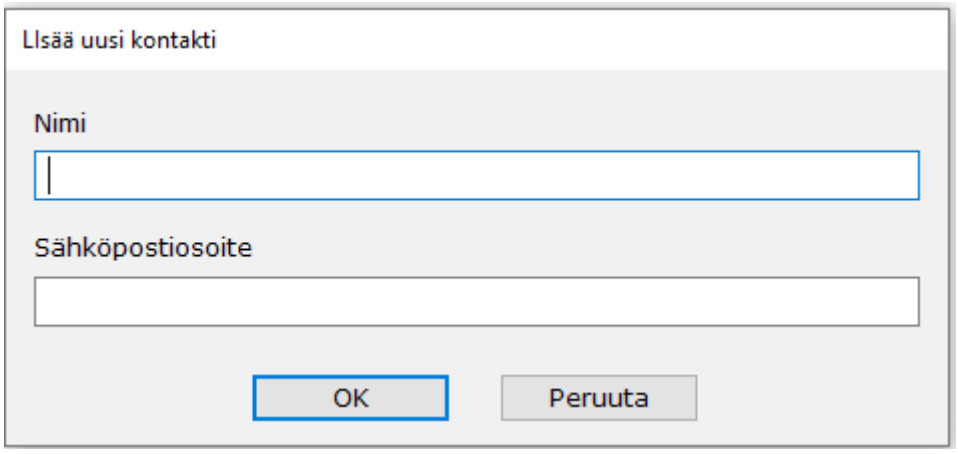
Pikaohje

Asenna EndCryptor. Kun olet lähettänyt yhden ja vastaanottanut kaksi tarkastus-sähköpostia, voit aloittaa salattujen sähköpostien lähettämisen ja vastaanottamisen.

Youtube video asennuksesta ja käytöstä:

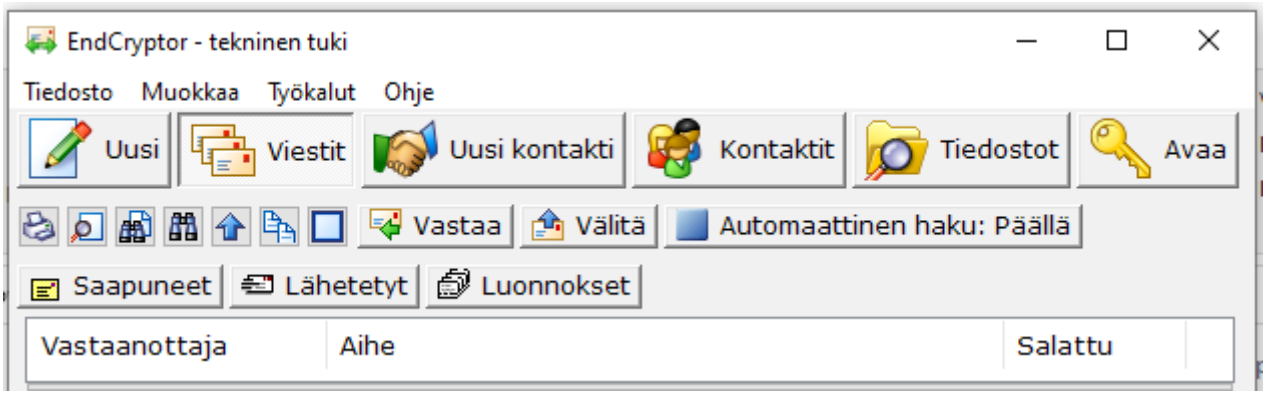
https://www.youtube.com/channel/UCAiIkQf2kRmcULg86GIQWRA

Tarkastus-sähköpostit varmistavat, että hallitset sähköpostiosoitetta. Tarkastuksen jälkeen sähköpostiosoite ja siihen liitetty julkinen avain laitetaan Web Hakemistoon. Jos joku haluaa lähettää sinulle salatun viestin, tulee hänen tietää vain sähköpostiosoitteesi – sen perusteella Web Hakemisto palauttaa sähköpostiosoitteeseen liitetyn julkisen avaimen.

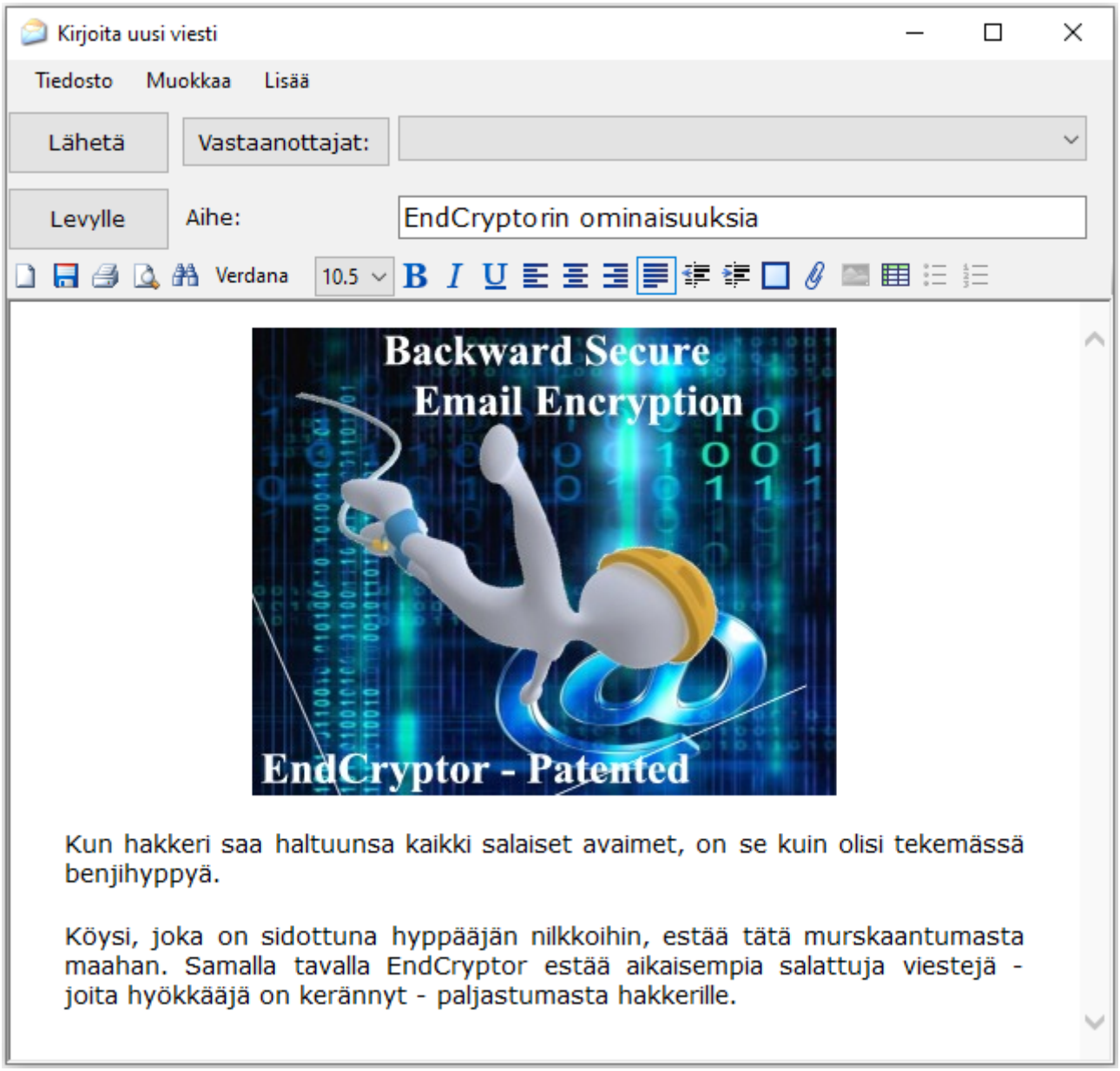


Web Hakemiston käyttö oman julkisen avaimen jakamiseen ei ole pakollista. Tällaisessa tapauksessa kontaktien on jotenkin saatava tietoonsa vastaanottajan julkinen avain (sen voi julkaista esim. sosiaalisessa mediassa tai web sivulla).

Esimerkki pääikkunasta, kun uusi salattu viesti on saapunut:

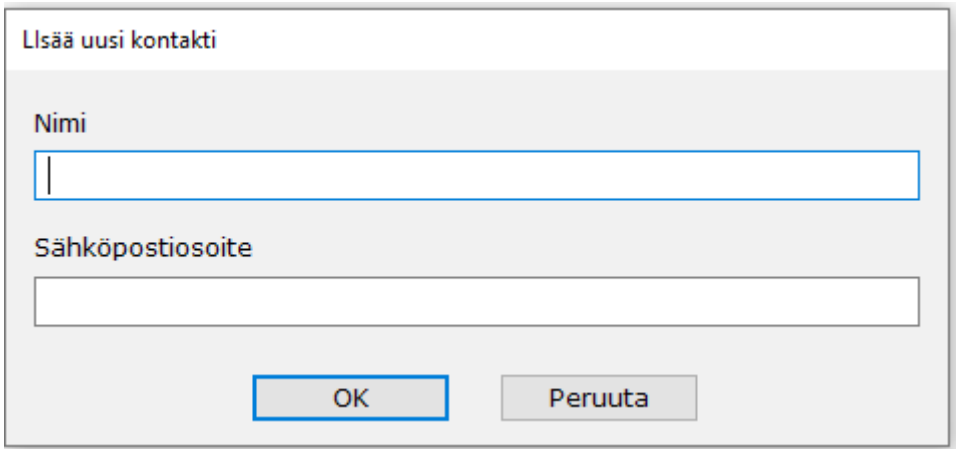


Esimerkki uuden viestin kirjoittamisesta:



Lisää uusi kontakti

Jos käytät oletusasetuksia eli Web Hakemistoa, niin uuden kontaktin lisäys tapahtuu seuraavalla näytöllä:

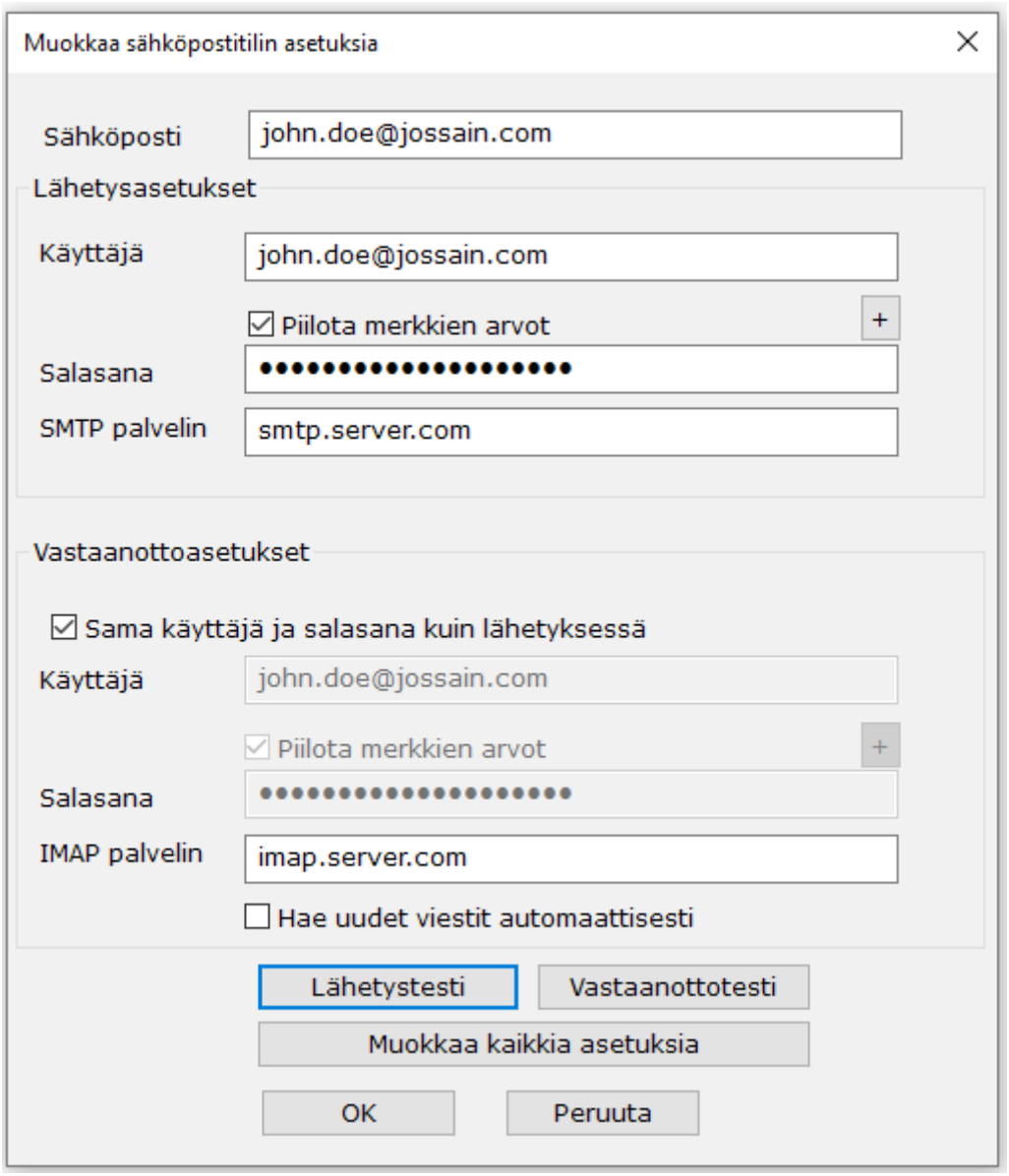


Kun OK nappulaa on painettu, Web Hakemistosta haetaan annettua sähköpostiosoitetta vastaava julkinen avain ja kontakti on valmis ottamaan vastaan lähetyksiä.

Kun vastaanotat ensimmäisen viestin henkilöltä, joka ei ole kontaktiesi joukossa, saat tiedot hänen julkisesta avaimestaan saapuneesta viestistä. Jos viestin lähettäjä on Web Hakemistossa, sisältää viesti digitaalisesti allekirjoitetun todistuksen (jonka ohjelma tarkastaa), että lähettäjän sähköpostiosoite on liitetty lähettäjän julkiseen avaimeen ja tähän viestiin.

Lähetys ja vastaanotto

Alla esimerkki sähköpostitilin asetuksista. Käyä menun Työkalut→Sähköpostitilit valintaa.



Vastaanota käyttäen omaa sähköpostiohjelmaa:

Jos EndCryptoria ei ole konfiguroitu vastaanottamaan sähköposteja, voit avata sähköpostin liitteenä olevan salatun viestin (.ndd päätteisen tiedoston) jollain seuraavalla tavalla:

- *Tuplaklikkaa liitettä.*
- *Tallenna liite ja raahaa ja pudota se Resurssienhallinasta EndCryptoriin.*
- *Tallenna liite ja valitse liite EndCryptorin Tiedostot nappulan kautta*.
- *Tallenna liite ja tuplaklikkaa liitettä Resurssienhallinnassa.*

Lähetä itse käyttäen Levylle nappulaa

Rastita Työkalut→Optioista joko ‘Lähetä itse levyltä’ tai ‘Valitse lähetysaikana’. Tällöin uudessa viestissä on esillä ‘Levylle’ nappula, mikä tallettaa lähetettävän viestin levylle. Viesti on .ndd loppuinen tiedosto, jonka voit toimittaa vastaanottajalle haluamallasi tavalla. Tämä on tarkoitettu tilanteisiin, jossa internet yhteyttä pidetään tietoturvariskinä. Salattu viesti siirretään esim. USB tikulla toiseen tietokoneeseen, joka on yhteydessä internettiin. Tuo .ndd tiedosto voidaan myös raahata ja pudottaa ‘Lähetetyt’ kansiosta tartumalla siihen sen nimestä otsikon oikeassa kulmassa.

Lähetä käyttäen omaa ohjelmaa

Voit käyttää jotain nimeämääsi ohjelmaa viestin lähetykseen. EndCryptor antaa ohjelmalle parametrina viestitiedoston ja sen vastaanottajat. Parametrit kuvataan tämän dokumentin Optiot osassa.

Optiot

Viestin allekirjoitus

Teksti, joka tulee viestin loppuun – tyypillisesti lähettäjän nimi ja yritys.

Näytä kuvat

EndCryptor näyttää viestit käyttäen Microsoftin MSHTML moottoria. Viestissä olevat kuvat ovat viestin mukana. Joskus MSHTML:n käyttämissä kuvankäsittelyohjelmissa on virheitä. Tämä voisi avata hyökkäysmahdollisuuden viallisen ja pahantahtoisen kuvan avulla. Kun Windows Update päivittää ko. ohjelmat, on ongelma poistunut. Myös MSHTML päivittyy Windows Update'n kautta. Jos kuvia ei näytetä -valinta on päällä ja kuvallinen viesti välitetään toiselle henkilölle, ovat kuvat mukana välitettävässä viestissä, niiden näyttäminen vastaanottajalle riippuu hänen asetuksestaan kuvien näyttämiselle.

Viestejä vastaanotettaessa älä talleta liitteitä selväkielisenä

Salatun viestin saapuessa sen liitteet talletetaan vain salattuina. Selväkielinen versio saadaan avaamalla liite haluttaessa myöhemmin.

Käytä piilokopio kenttää piilottamaan vastaanottajia

Uuden viestin vastaanottajien ensimmäinen henkilö tulee lähtevän sähköpostin ‘Vastaanottajat’ kenttään. Jos vastaanottajina on vain ryhmiä tulee joku vastaanottajista tuohon kenttään.

Salattuun viestiin lisättävien satunnaisten tavujen määrä

Tavuja lisäämällä voidaan piilottaa viestin todellinen pituus – salatut viestit ovat eri pituisia vaikka niiden sisältö on sama.

Viestin pakkauksen lisäasetuksia

Asetus ‘Huomaa pakkautumattomuus automaattisesti’ merkitsee, että isohkot liitetiedostot, jotka eivät pienene niitä tiivistettäessä, jätetään pakkaamatta. Voit myös antaa lisää tiedostotyyppejä, joita ei pakata.

Lähetä

Konfiguroi lähetyksen eri vaihtoehtoja.

Rastitus ‘Poista juuri lähetetty viesti levyltä’ tarkoittaa, että onnistuneen lähetyksen jälkeen tiedosto poistetaan mutta sitä ei ylikirjoiteta.

Jos valinta ‘Käyttäen tätä ohjelmaa’ on rastitettu, niin nimettyä ohjelmaa kutsutaan, kun viesti lähetetään. Kun EndCryptor kutsuu ohjelmaa, sille annetaan Unicode merkkijono, jossa parametrien arvot erotetaan toisistaan ‘*’ merkillä:

*3*C:\ProgramData\Enternet\EndCryptor\Instance_1\files\outgoing_123.ndd

Ensimmäinen parametri on numero ja toinen on tiedostopolku lähetettävään tiedostoon. Käytettävät numerot:

3 – salattu viesti,
5 – lisenssin tilaus, salattu

Mahdollisia tulevia muutoksia varten suunnittele ohjelma niin, että se hyväksyy enemmän kuin kaksi ‘*’ merkillä erotettua arvoa. Ohjelmaa kutsuttaessa levyllä on 2 tiedostoa, joista toinen on lähetettävä tiedosto ja toinen .txt loppuinen mutta muuten samanniminen sisältäen vastaanottajat. Tiedostot ovat ulosmenevien tiedostojen kansiossa.

Tarkkaile tähän kansioon tulevia .ndd tiedostoja

EndCryptor käynnistää ohjelman 'efw.exe' - EndCryptor File Watcher - joka pyytää käyttöjärjestelmää kertomaan aina kun uusi .ndd loppuinen tiedosto tulee tähän kansioon. Ohjelma myös itse tarkastaa kansion 5 minuutin välein. Uusi tiedosto siirretään oletus sisääntulokansioon ja käyttäjää informoidaan.

Jos kansio on pilvessä, ei pilven ohjelmisto ehkä informoi käyttöjärjestelmää eikä EndCryptor tällöin saa tätä tietoa. Myös pilvi voi näyttää tiedoston olevan kansiossa ennenkuin se on kokonaan saatavilla - tästä voi koitua ongelmia kun 'efw.exe' yrittää siirtää tiedoston sisääntulokansioon.

Kun 'efw.exe' on käytössä, on tehtäväpalkin ilmaisinalueella pieni EndCryptor File Watcher'in kuvake.

Ohjelman, joka kirjoittaa tiedoston tarkkailtavaan kansioon kannattaa nimetä tiedosto niin, että sillä on aluksi .tmp tiedostopääte. Kun tiedosto on kokonaan kirjoitettu, tulee se nimetä .ndd loppuiseksi.

Poista 14 vrk vanhemmat viestit ‘processed’ kansiosta

Nämä tiedostot ovat avattuja viestejä, jotka on avattu onnistuneesti. Niitä ei voi avata enää uudestaan. Tiedostoja ei ylikirjoiteta, ne poistetaan.

Työkalut

Selaa

Windowsin versioissa Vista, Windows 7 , 8 ja 10 kansio

C:\ProgramData\Enternet\EndCryptor\Instance_1\files\
sisältää nämä kansiot:

Kansio	**Käyttö**
erroneous	Vastaanotetut, mutta virheellisiksi havaitut viestit
incoming	Saapuneet uudet viestit
outgoing	Ulosmenevät sekä lähetetyt
processed	Saapuneet ja onnistuneesti avatut viestit

Saatat haluta joskus poistaa tiedostoja outgoing, processed ja erroneous kansioista. Optioissa voi rastittaa valinnan, jonka mukaan juuri lähetetty tiedosto poistetaan outgoing kansiosta. Älä poista tiedostoa incoming kansiosta, ellei ole olemassa jotain virhetilannetta, joka vaatii sitä. Jos samassa koneessa on eri identiteettejä eli instansseja niin ne nimetään seuraavasti: Instance_1, Instance_2, …

Viennin asetuksia

'Tarkasta onko muutettu' valinnan avulla voi tarkastaa, onko vietyjä viestejä muutettu niiden viennin jälkeen.

'Eristä tiedoston tunniste' lukee salatusta .ndd tiedostosta merkkijonon, joka on vastaavassa selväkielisessä viedyssä viestissä nimellä 'Tiedoston tunniste'. Näin salattua viestiä vastaava selväkielinen viesti voidaan etsiä sähköpostin arkistointisovelluksesta. Lue 'Vie (export) selväkieliseen muotoon' osio tästä dokumentistä saadaksesi lisää tietoa koskien vientiä selväkieliseen muotoon.

'Hallitse Export avaimia' valinnassa voi luoda uuden henkilökohtaisen Export avaimen ja tuoda yrityksen Export avaimen.

'Hallinnoinnin työkaluja' valinta on tarkoitettu henkilölle, joka luo uuden yrityksen/osaston Export avaimen ja jakaa sen julkisen avaimen muille.

Osio 'Varmistus ja palautus' antaa lisätietoa Export avaimista.

Vastaanotetut varmenteet

EndCryptor tallettaa sähköpostipalvelimilta saadut varmenteet ja laskee niiden käyttökerrat ja näyttää varmenteiden ominaisuuksia. On mahdollista vaatia, että varmenne sisältää Certificate Transparency SCT-luettelo osan. Tällöin esimerkiksi estetään muiden kuin julkisesti hyväksyttyjen Varmentajien (Certificate Authority) myöntamien varmenteiden käyttö, joita saatetaan käyttää liikenteen avaamiseen.

Varmenteita voidaan tuoda ja viedä. On mahdollista sallia ja kieltää varmenteita. Tietyn varmenteen salliminen/kieltäminen on hyvin kehittynyt optio ja edellyttää käyttäjältä asiaan paneutumista. Syynä varmenteen salli/kielto -option tarjoamiseen on varmenteiden eli SSL/TLS salauksen infrastruktuuriin liittyvät ongelmat – tästä kerrrotaan enemmän eglanninkielisessä teknisessä dokumentaatiossa. Tässä todetaan, että mikäli hyökkäys pahantahtoisella varmenteella onnistuu, hyökkääjä ei voi avata salattua viestiä mutta saa haltuunsa sähköpostitilin tunnuksen ja salasanan.

Lukijan on hyvä tietää, että jos lukija käyttää tavanomaista sähköpostiohjelmaa – joissa ei yleensä ole suojausta pahantahtoisia varmenteita vastaan – on mahdollista, että hän joutuu alttiiksi tälle hyökkäykselle.

EndCryptor laskee varmenteiden käyttökerrat ja vaikka käyttäjä ei käyttäisikään varmenteiden salli/kielto -optiota, hän kuitenkin tunnistaa hyökkäyksessä käytetyn varmenteen sen käyttökertojen perusteella. Esimerkiksi käyttäjä matkustaa ulkomaille ja joutuu siellä hyökkäyksen kohteeksi. Myöhemmin havaitaan, että jotakin varmennetta, jota sähköpostipalvelimen hallinnoija ei tunnista, on käytetty vain kerran.

Proxy asetukset

Jos proxya käytetään EndCryptor ohjaa lähetys ja vastaanotto liikenteen proxylle.

Proxy voi olla tässä tietokoneessa (osoitteessa '127.0.0.1') tai jossain verkossa. Proxya voidaan käyttää tarkkailemaan ohjelman toimintaa tai ohjaamaan liikenne haluttua reittiä sähköpostipalvelimille. Joskus proxeja käytetään anonymisaation saavuttamiseksi: käyttäjä yrittää piilottaa kohdepalvelimen tarkkailijalta, joka on lähellä käyttäjää ja piilottaa käyttäjän IP osoitteen tarkkailijalta, joka on lähellä palvelinta. Tässä tapauksessa käytetään tyypin socks5 proxya, esimerkiksi voidaan käyttää Tor anonymisaatioverkkoa (asetus socks5 proxy osoitteessa 127.0.0.1, portti 9150) ja asennetaan 'Tor Browser Bundle'. EndCryptor tekee yhden perusjutun estääkseen kohdepalvelimen paljastumisen - DNS kyselyä kohdepalvelimen IP osoitteen saamiseksi ei tehdä.

Tietoturva-asiantuntijat näyttävät olevan sitä mieltä, että absoluuttista anonymisaatiota on hyvin vaikea saavuttaa vaikka käytettäsiin hyvin erikoistuneita ohjelmia. Esimerkiksi sähköpostin ollessa kyseessä niin kun se lähtee lähettäjän palvelimelta niin monessa tapauksessa käytössä ei ole edes SSL/TLS suojausta

vastaanottajan palvelimeen ja lähettäjän ja vastaanottajan sähköpostiosoitteet ovat näkyvillä.

On huomioitava, että EndCryptorin palvelinvarmenteen oletus tarkastusoptio (Kumoamistarkastus verkossa) voi paljastaa kohdepalvelimen. Jos tätä valintaa käytetään, Windows voi ladata verkosta uusia juurivarmenteita ja palvelimen varmenteen sulkulistan, varmenteen tarkastus voi myös lähettää sen sarjanumeron varmenteen myöntäjälle - tämä 'Online Certificate Status Protocol' liikenne voi paljastaa käyttäjän ja kohdepalvelimen IP osoitteen osaavalle tarkkailijalle. Tämän tilanteen välttämiseksi valitse menussa Työkalut->Vastaanotetut varmenteet ja rastita valinta 'Hyväksy jos sallittu ja voimassaoleva' (sinun tulee ehkä tuoda ko. varmenne saataville ensin). Lukijan, joka on äärimmäiseen asti tietoturvatietoinen on hyvä tietää, että kun varmennetta katsotaan Windowsissa, se tarkastetaan ja tämä voi käynnistää paljastavan liikenteen.

Liikenne Web Hakemistoon ei kulje proxyn kautta.

Varmistus ja palautus

Varmistusten näkökulmasta EndCryptor koostuu tietokannasta ja tallennetuista viesteistä. Tietokannassa ovat mm. salausavaimet ja muu tieto, jota tarvitaan ohjelman toimintaan. Sekä tietokannan tiedot että levyllä olevat viestit on salattu. Salattuja viestejä voi lukea ohjelman kautta, kun oikea sisäänkirjautumisen salasana on annettu – tämä on normaali tapa lukea viestejä. Toinen tapa on käyttää Export avaimia ja varmistettuja salattuja viestejä ja viedä (export) viestit selväkieliseen muotoon tiedostoiksi – näin viestit voidaan aina lukea vaikka edes tietokannan varmistusta ei olisi saatavilla, on vain oltava Export avaintiedosto ja levylle talletetut viestit (tai niiden kopiot varmistuksessa). Henkilökohtainen Export avaintiedosto talletetaan ohjelman ensimmäisessä käynnistyksessä.

EndCryptor voi ottaa varmistukset tietokannasta ja viesteistä. Toinen vaihtoehto on, että yrityksen varmistusohjelmisto tekee tämän.

Kun EndCryptor käynnistyy, eikä olemassaolevaa tietokantaa löydy, niin yhtenä vaihtoehtona annetaan mahdollisuus palauttaa tietokanta varmistuksesta. Tämä tapahtuu esimerkiksi ensimmäisessä käynnistyksessä. Jos haluat simuloida tilannetta, niin nimeä kansio, jossa tietokanta on (EndCryptor_store) uudestaan (EndCryptor_store_org) ja käynnistä EndCryptor.

Kun tietokanta varmistetaan se voidaan vielä erikseen salata henkilökohtaisella Export avaimella.

Kun tietokanta on palautettu varmistuksesta, kysytään varmistettujen viestien sijaintia – tämän jälkeen kopioidaan tietokannan indeksoimat viestit niiden oikeaan paikkaan.

Viestit voidaan varmistaa, kun EndCryptor sulkeutuu tai välittömästi silloin kun viesti kirjoitetaan levylle. **Täten on mahdollista aina avata jokainen lähetetty ja vastaanotettu viesti, vaikka käyttäjän kovalevy hajoaisi (mikäli varmistukset ovat muualla).**

Tietyn tyyppisten yritysten tai palveluiden on lain mukaan joissakin maissa pystyttävä näyttämään jokainen käsitelty sähköposti.

Varmistukset konfiguroidaan Työkalut→Varmistuksen asetukset valinnasta.

Export avaimia on kahdenlaisia: käyttäjän henkilökohtainen ja yrityksen avain. Yrityksen avaimen käyttö edellyttää sen erillistä asentamista käyttäjän toimesta. Kun eri käyttäjät asentavat yrityksen Export avaimen, voi tuon avaimen luoja avata kaikkien näiden käyttäjien talletetut viestit.

Viestien avaus varmistetuista viesteistä tehdään menusta Tiedosto→Vie varmistuksesta.

Mikäli yrityksen oma ohjelmisto tekee varmistukset (kanta ja viestit) seuraava kansio ja sen alikansiot tulee varmistaa:

C:\ProgramData\Enternet\EndCryptor

Jos käyttäjä on sijoittanut tietokannan muualle kuin oletuspaikkaan, on tämä huomioitava. Käytä menun 'Työkalut→Selaa→Tietokannan kansiota' nähdäksesi missä tietokanta on.

Jos EndCryptor varmistaa tietokannan, siitä tehdään yksi tiedosto ohjelman sulkeutuessa. Tämä varmistus voidaan salata henkilökohtaisella Export avaimella. Jokaista päivää kohti säilytetään 5 viimeisintä varmistusta ja korkeintaan 2 edellistä varmistuspäivää talletetaan. Jos näiden sääntöjen perusteella varmistustiedostoa ei säilytetä, se ylikirjoitetaan ja poistetaan. Varmistuksen sisältävä kansio voi olla verkkokansio.

Viestit ovat seuraavassa kansiossa:

C:\ProgramData\Enternet\EndCryptor\Instance_X\EndCryptor_store\emsgs

ellei käyttäjä ole sijoittanut tietokantaa muualle kuin oletuskansioon. Ylläolevassa 'Instance_X' tarkoitaa Instance_1, Instance_2 jne. eri identiteettien lukumäärän mukaisesti.

Viestejä voi varmistaa koska tahansa, myös ohjelman ollessa käynnissä.

Vie (export) selväkieliseen muotoon

Kun viesti lähetetään tai vastaanotetaan, se salataan uudestaan levylle talletusta varten (käyttäen eri salausavaimia kuin .ndd viestissä). Nämä paikallisesti tallennetut viestit voidaan varmistaa kopioimalla ne sopivalle medialle. Ne voidaan myöhemmin avata eli viedä (export) näistä kopioista ilman tietokantaa käyttäen henkilökohtaista tai yrityksen Export avainta.

Kun EndCryptor käynnistetään ensimmäisen kerran, se tallettaa henkilökohtaisen (salasanalla suojatun) Export avaimen. Lisäksi käyttäjä voi asentaa erillisen yrityksen Export avaimen. Yrityksen Export avaimen avulla voidaan avata usean eri käyttäjän viestejä – tämän voi tehdä tuon yrityksen avaimen luoja. Yrityksen ei tarvitse välttämättä käyttää samaa avainta kaikille käyttäjille, voidaan käyttää esimerkiksi osastokohtaisia avaimia.

Export avaimet kannattaa tallettaa siirrettävälle medialle, esimerkiksi USB muistille.

Oletusarvoisesti viestit ovat kansiossa:

C:\ProgramData\Enternet\EndCryptor\Instance_1\EndCryptor_store\emsgs

Yksittäiset salatut tiedostot näyttävät tältä:

10_1885387336_a_1663277279_789AF06969FC0275.dat on itse viesti
10_1885387336_b_1984071552_789AF06969FC0275.dat on viestin liite

Viesti viedään eml formaattiin, jota esimerkiksi sähköpostin arkistointijärjestelmät ymmärtävät. Ne voidaan myös raahata ja pudottaa tavanomaisten sähköpostiohjelmien paikallisiin kansioihin. Viety selväkielinen viesti sisältää itse viestin ja sen liitteet.

Tallennetut viedyt tiedostot allekirjoitetaan viennissä digitaalisesti ja jos niitä muutetaan myöhemmin, niin se voidaan havaita menun ‘Työkalut→Viennin asetuksia→Tarkasta onko muutettu’ avulla. Digitaalinen allekirjoitus tehdää aina samalla allekirjoitusavaimella, joka on vientiä tekevän käyttäjän tietokannassa, sen julkinen avain sisältyy vietyihin viesteihin. Tarkastettaessa useita viestejä muutosten varalta, kerrotaan myös eri viejien lukumäärä (eri julkisten avainten lkm). Jos viejä on viesteillä sama, tulee eri viejienkin lukumäärän olla yksi. Allekirjoitusavain on tietokantakohtainen, kannan tuhoamisesta seuraa avaimen vaihtuminen.

Jos yritys käyttää sähköpostin arkistointiohjelmaa, jokainen lähtevä ja saapuva viesti tallennetaan sinne. Oletetaan, että arkistointijärjestelmässä on salatun .ndd liitteen sisältävä viesti ja halutaan jostain syystä tietää, onko järjestelmään myös tuotu sen avattu sisältö. EndCryptorissa on työkalu (‘Työkalut→Viennin asetuksia→Eristä tiedoston tunniste’), joka eristää .ndd tiedostosta tunnisteen (Tiedoston tunniste),

joka on myös viedyssä selväkielisessä viestissä. Näin voidaan käyttää arkistointijärjestelmän etsintäominaisuuksia.

Esimerkki selväkielisestä .eml tiedostosta tavanomaisen sähköpostiohjelman näyttämänä:

Viestin tunniste : 7A9DD8CFC757ACDD366BAC2681EB2C2603C678C7C5F6EC13

Lähettäjä :	John Doe	John.Doe@somewhere.com	own_DE7419E54EEC0DFE_
Vastaanottaja :	Jane Doe	Jane.Doe@somewhere.com	s2r_BABDBE4E10F559E7_

Luotu: 2010-04-03 10:25:28 (UTC 2010-04-03 07:25:28)
Tiedosto: _314_216_122.ndd, Tiedoston tunniste: E6A16A56285EBCC6DB82D830304E70E04C9BBAC137187412
Tiedoston numero: 59
Viejä: 29F732E7EE7FD700FB01458CB3E7813F52AE55676310AEA5
Aihe: Testi

Tämä on testiviesti.

Arvo, joka alkaa ‘own_’ merkeillä, on ‘Owner’ tunniste. Löytääksesi kaikki John Doen lähettämät ja vastaanottamat viestit etsi arkistointijärjestelmästä merkkijonoa ‘own_DE7419E54EEC0DFE_’. Arvo, joka alkaa merkeillä ‘s2r_’ on ‘Sender to Receiver’ tunniste. Löytääksesi kaikki John Doen lähettämät viestit Jane Doelle etsi käyttäen merkkijonoa ‘s2r_BABDBE4E10F559E7_’. Jane Doella on tämä sama merkkijono omassa ‘From:’ sarakkeessaan. Kentän ‘Viestin tunniste’ arvo on sama, kun kyseessä on sama viesti lähettäjällä ja vastaanottajalla. ‘Tiedosto’ on sen tiedoston nimi, joka sisälsi viestin. ‘Tiedoston tunniste’ on arvo, joka voidaan eristää .ndd tiedostosta. ‘Tiedoston numero’ on John Doen lähettämän viestin järjestysnumero Jane Doelle. Tätä arvoa ei voi näyttää lähettävässä päässä, jos viestillä on useita eri vastaanottajia, koska numerot ovat jokaisella omansa. Ota huomioon, että jos käyttäjä poistaa kontaktin ja luo tämän uudestaan, niin ‘s2r_’ arvo muuttuu.

Esimerkki, jossa kahden vastaanottajan viesti on viety yhden vastaanottajan toimesta:

Viestin tunniste: 1BE0708B6C66EB42FE1B1CBE1A0C1D3BE2B77B8F695A6E0F

Lähettäjä:	John Doe	John.Doe@somewhere.com	s2r_BABDBE4E10F559E7_
Vastaanottaja:	Jane Doe	Jane.Doe@somewhere.com	own_CE4B8EF1A2034840_
Vastaanottaja:	Tuntematon nimi	Tuntematon_osoite@ei.ole	s2r_435282EFA93363F7_

Luotu: 2010-05-06 14:09:38 (UTC time 2010-05-06 11:09:38)
Tiedosto: _361_877_810.ndd, Tiedoston tunniste: FE7BC9BEA8FEEB421D55663F75B849BD7467DCEC21765DBB
Tiedoston numero: 60
Viejä: 52DCDC88A60EFFD50A65EE605B006F8C6EA8D8D3E6C02057
Aihe: Testi

Tämä on testiviesti.

Vastaanottaja Jane Doe on vastaanottanut ylläolevan viestin. Toisen vastaanottajan nimeä eikä sähköpostiosoitetta ei tiedetä (siksi muoto ’Tuntematon_osoite@ei.ole’), näitä tietoja ei ole viestissä. Kun viestejä viedään, niin EndCryptor pitää kirjaa siitä, mitkä viestit on viety.

Siirrä tietokanta

Käyttäjän tietokone voi sisältää useita eri EndCryptorin instansseja. Tyypillisesti vain yhden, mutta jos henkilöllä on erilaisia organisatoorisia rooleja voi hänellä olla eri EndCryptor tietokanta jokaiselle eri identiteetille. Voi tulla tilanne, jossa organisatoorinen rooli siirtyy toiselle henkilölle ja siihen liittyvä instanssi tietokantoineen tulee siirtää toiseen tietokoneeseen.

Siirrä tietokanta ja tallennetut viestin toiseen tietokoneeseen USB tikun avulla:

Menetelmä 1.

1. Aktivoi siirrettävä instanssi ja paikallista tietokanta menusta 'Työkalut→Selaa→Tietokannan kansiota'. Sulje tämä instanssi ja laita hiiri kansion 'EndCryptor_store' päälle ja tee oikean hiirinäppäimen klikkaus. Valitse 'Lähetä kohteeseen' ja ota kohteeksi USB tikku. Windows kopioi tietokannan ja tallennetut viestit muistitikulle.
2. Nimeä tietokoneellasi oleva kansio 'EndCryptor_store' nimellä 'EndCryptor_store_vanha'.
3. Käynnistä EndCryptor kohdetietokoneessa. Jos tämä on EndCryptorin ensimmäinen käynnistys kohdekoneessa, niin 'Määritä tietokanta' ikkuna tulee esille. Mene kohtaan 5.
4. Jos 'Määritä tietokanta' ikkuna ei tule esille, on ensimmäisessä esille tulevassa ikkunassa 'Lisää identiteetti' nappula oikeassa yläkulmassa. Paina sitä nappulaa. Anna identiteetille nimi (sen organisatoorisen roolin mukainen) ja paina 'Lisää' nappulaa. Odota kunnes ikkuna 'Määritä tietokanta' tulee esille.
5. Ikkunassa 'Määritä tietokanta' valitse **'Lisää olemassaoleva kanta'** ja paina OK. Valitse sitten USB tikulla oleva sinne kopioitu 'EndCryptor_store' kansio ja paina OK. EndCryptor kopioi nyt tietokannan ja viestit oikeaan paikkaan kohdekoneessa. Kopioinnin jälkeen EndCryptor sulkeutuu automaattisesti.
6. Käynnistä EndCryptor kohdekoneessa ja valitse juuri luotu instanssi, joka on valmis käyttöön.

Oletetaan nyt, että haluat käyttää samaa identitettiä kahdelta eri tietokoneelta – kuten esimerkiksi toimiston ja kodin tietokoneelta. Tässä tapauksessa tietokannan on oltava pysyvästi USB tikulla tai vastaavalla medialla, joka liitetään aina kulloinkin käytettävään tietokoneeseen ennenkuin EndCryptor käynnistetään.

Siirrä tietokanta ja viestit USB tikulle, käytä sitä 2 eri koneelta A (nykyinen, kanta tässä) ja B:

Menetelmä 2.

1. Tee edellisen Menetelmä 1:n askeleet 1 ja 2. Muista nimetä A:n kovalevyllä oleva kanta nimellä 'EndCryptor_store_vanha'.
2. Käynnistä EndCryptor koneessa A. Jos ikkuna 'Määritä tietokanta' tulee esille mene kohtaan 4.
3. Jos ikkuna 'Määritä tietokanta' ei tule esille, niin ensimmäisen esille tulevan ikkunan oikeassa yläkulmassa on nappula 'Lisää identiteetti'. Paina sitä. Anna identiteetille nimi ja paina 'Lisää' nappulaa. Odota kunnes ikkuna 'Määritä tietokanta' tulee esille.
4. Ikkunassa 'Määritä tietokanta' valitse **'Paikallista olemassaoleva kanta'** ja paina OK. Valitse USB tikulla oleva sinne juuri kopioitu kansio 'EndCryptor_store' ja paina OK. Tämä EndCryptorin instanssi käyttää nyt USB tikulla olevaa kantaa. Tarkasta, että voit lukea tallennettuja viestejä.
5. Sulje EndCryptor koneessa A ja liitä USB tikku toiseen tietokoneseen B.
6. Käynnistä EndCryptor koneessa B. Jos ikkuna 'Määritä tietokanta' tulee esille, mene kohtaan 8.
7. Jos ikkuna 'Määritä tietokanta' ei tule esille, niin ensimmäisen esille tulevan ikkunan oikeassa yläkulmassa on nappula 'Lisää identiteetti'. Paina sitä. Anna identiteetille nimi ja paina 'Lisää' nappulaa. Odota kunnes ikkuna 'Määritä tietokanta' tulee esille.
8. Ikkunassa 'Määritä tietokanta' valitse **'Paikallista olemassaoleva kanta'** ja paina OK. Valitse USB tikulla oleva sinne juuri kopioitu kansio 'EndCryptor_store' ja paina OK. Tämä EndCryptorin instanssi käyttää nyt USB tikulla olevaa kantaa. Tarkasta, että voit lukea tallennettuja viestejä.

Ota huomioon, että ei ole mahdollista käyttää USB tikulla olevaa kantaa ja sitten alkaa taas käyttämään koneessa A olevaa vanhaa kantaa. Kun viestejä vaihdetaan tietokantaa päivitetään sisältämään uusia klassisia ja kvanttihyökkäyksen kestäviä avaimia. Tämä saatu tieto menetetään, jos vanhaa versiota kannasta käytetään. Jos haluat siirtää kannan USB tikulta tietokoneeseen tee Menetelmä 1:n askeleet 3-6.

Unohdettu salasana

Vain oikea sisäänkirjautumisen salasana mahdollistaa tietokannan ja siten ohjelman käytön.

Mikäli viestien liitteitä on selväkielisenä, ovat ne kansiossa:
…EndCryptor_store\pltxt_files

Voit viedä tallennetut viestit selväkieliseen muotoon

Voit käyttää Export avaimia ja viedä viestit selväkieliseen muotoon. Tarvitset avaintiedoston ja sen salasanan. Henkilökohtainen Export avaintiedosto tallennettiin ohjelman ensimmäisen käynnistyksen yhteydessä. Sinun tulee luoda uusi identiteetti, jotta voi käyttää ohjelmaa sen kautta ja viedä sen identiteetin viestit selväkielisiksi, jonka salasana on unohtunut. Tallennetut viestit ovat levyllä, tyypillisesti kansiossa:

C:\ProgramData\Enternet\EndCryptor\Instance_1\EndCryptor_store\emsgs

Ylläolevassa kansiopolussa identiteettien vaihtuminen muuttaa Instance_1 osaa (Instance_1, Instance_2, …).

Toimi seuraavasti:

1. Nimeä nykyinen kansio ‘EndCryptor’ uudestaan nimellä ‘EndCryptor_vanha’ niin että polku siihen on C:\ProgramData\Enternet\EndCryptor_vanha\
2. Käynnistä EndCryptor ja valitse ‘Aloita 60 päivän koeaika’ ja asenna uusi EndCryptor. Tarkoituksena on mahdollistaa viestien vienti tämän instanssin avulla. Voit käyttää myös jotain toimivaa instanssia, jos sellainen on olemassa, tällöin ylläolevaa askelta 1 ei tarvita.
3. Kun EndCryptor on käynnissä valitse menusta ‘Tiedosto→Vie varmistuksesta’.
4. Valitse kansio: C:\ProgramData\Enternet\EndCryptor_vanha\Instance_X\ EndCryptor_store\emsg, missä X on unohdetun salasanan instanssi.
5. Valitse kansio, johon viestit viedään.
6. Noudata annettuja ohjeita.

Jos käytössäsi on useita eri identiteettejä nimeä ‘EndCryptor_vanha’ takaisin nimellä ‘EndCryptor’, jotta voit taas käyttää niitä.

Lisää tietoja tämän dokumentin osiossa ‘Vie (export) selväkieliseen muotoon’.

Kovalevyn hajoaminen

EndCryptor vaihtaa jatkuvasti uusia julkisia avaimia kontaktien kanssa viestejä vaihdettaessa – tämä edellyttää synkronisaatiota kontaktien välillä. Jos vanha tietokanta, jossa ei ole uusimpia muutoksia, palautetaan varmistuksesta, voi sattua, että jonkin viestin vastaanottaja ei saakaan saapunutta viestiä avattua. Tällöin on molempien osapuolten poistettava toisensa kontakteista. Kontaktin deletoiminen ei vaikuta jo avattujen viestin näkymiseen ohjelmassa. Sitten toinen osapuoli lisää toisen takaisin kontakteihin ja lähettää viestin. Sen avauduttua vastaanottajalla voidaan luottaa siihen, että kaikki viestit osapuolten välillä taas avautuvat.

Lisensointi

Ohjelma lopettaa lähetyksen ja vastaanoton kun 60 päivän koeaika on päättynyt ellei lisenssiä ole. Tämä tapahtuu myös, jos aikaperusteinen lisenssi umpeutuu. Tallennettuja viestejä voi aina katsella.

Jokainen tietokone, jossa on EndCryptorin tietokanta, tarvitsee lisenssin. Samassa tietokoneessa voi olla useita eri EndCryptor instansseja eli tietokantoja eli käyttäjän identiteettejä (käyttäjän eri rooleja varten) - vain yksi lisenssi tarvitaan yhtä tietokonetta kohti. Sama lisenssi tulee asentaa kaikkiin samassa koneessa oleviin eri instansseihin. Tietokone, jossa on vain ohjelmakoodi (ei kantaa) ei tarvitse lisenssiä - tällöin siihen liitetään tarvittaessa esim. USB muistitikku, jossa kanta on.

Siirrettävä USB muistiväline, joka sisältää kannan tarvitsee lisenssin, muistiväline voi sisältää useita eri identiteettejä eli kantoja mutta vain yksi lisenssi tarvitaan.

Jos tietokone on verkon palvelin niin jokainen palvelimella oleva EndCryptor kanta tarvitsee oman lisenssin (emme suosittele kannan sijoittamista palvelimelle).

Lisenssejä voi tilata ohjelman kautta tai websivulta www.endcryptor.com. Jos tilaus tehdään ohjelman kautta, on maksutapa ennakkomaksu pankkisiirrolla. Websivulta tilatut ja samalla maksetuksi tulevat lisenssit toimitetaan tilauksen yhteydessä sähköpostilla.

Jos tilaus tehdään ohjelman kautta ennakkomaksulla voi tilauksen käsittely kestää yhden työpäivän. Yksi henkilö vastaanottaa sähköpostilla lisenssitiedoston, joka voi sisältää oikeuden useisiin lisensseihin (sisältää siis maksetun lukumäärän). Tämä tiedosto annetaan organisaatiossa niile, jotka lisenssiä tarvitsevat.

Lisenssejä on kahdenlaisia: aikaperusteisia ja versioon perustuvia.

Aikaperusteinen lisenssi antaa oikeuden käyttää uusinta versiota lisenssin loppumiseen saakka. Uudista aikaperusteinen lisenssi, kun on alle 1 kuukausi sen loppumiseen. Tällöin uuden lisenssin aikaan lisätään vanhan käyttämätön osuus. Muissa tapauksissa lisenssin alkamispäivä on sen myöntämispäivä. Versioperusteinen lisenssi antaa oikeuden käyttää tiettyä versiota ajasta riippumatta. Lisenssi esimerkiksi versiolle 2 on lisenssi kaikille ohjelman versioille 2.x, kaikilla x:n arvoilla. On mahdollista muuttaa aikaperusteinen lisenssi versioperusteiseksi. Yhden vuoden vuosimaksu vähennetään tällöin versioperusteisesta hinnasta. Edellytyksenä on siis, että laitteessa on aikaisempi aikaperusteinen lisenssi.

Maksutiedot ennakkomaksussa:

Enternet Oy
Finland
Alv tunnus: FI 08210504

Pankki: Nordea Bank Finland Plc, Helsinki
SWIFT: NDEAFIHH
IBAN numero: FI08 1220 3000 2499 00

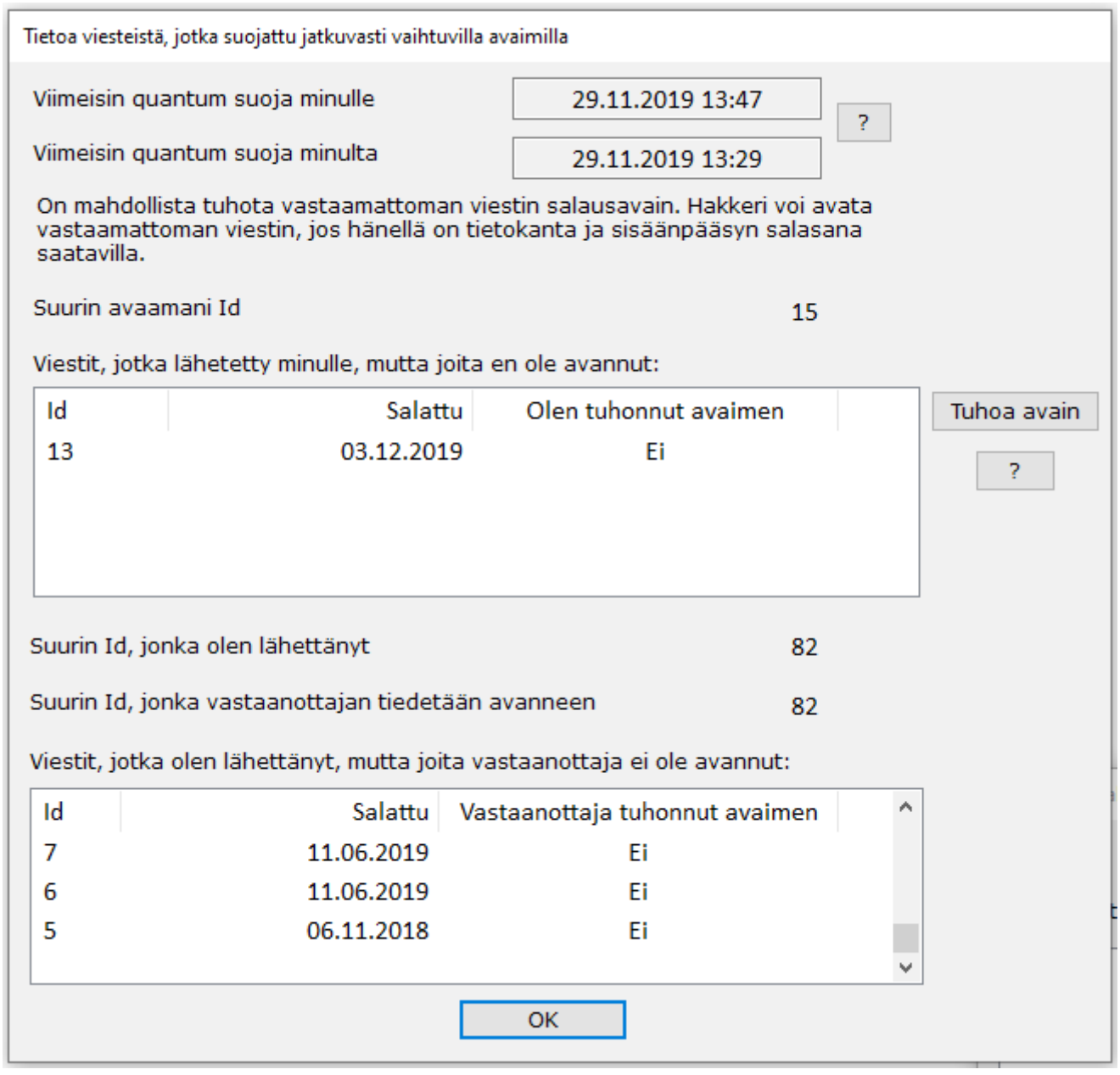
Tekninen huomautus:

Yksittäiset salatut viestit eivät sisällä sellaisia tietoja, joiden perusteella Enternet Oy voisi päätellä viestin olevan tietyn lisenssinhaltijan lähettämä.

Kontaktin lisätiedot

Tuhoa saapumattoman viestin salausavain

Paina ‘Kontaktit’ valitse kontakti ja paina ‘Lisätiedot’ ja valitse ‘Vaihtuvia avaimia käytettäessä’. Esille tulee:



Hakkeri voi kopioida viestin internetisssä ja estää sinua saamasta sitä tehden viestin avaamisen mahdottomaksi. Jos sitten hakkeri onnistuu varastamaan EndCryptorin tietokannan koneeltasi ja onnistuu esim. näppäimistökaappauksen avulla saamaan salasanasi, hän voi avata aikaisemmin kopioimansa viestin. Voit estää tällaisen tilanteen tuhoamalla tällaisen avaamattoman viestin salausavaimen. Viestin

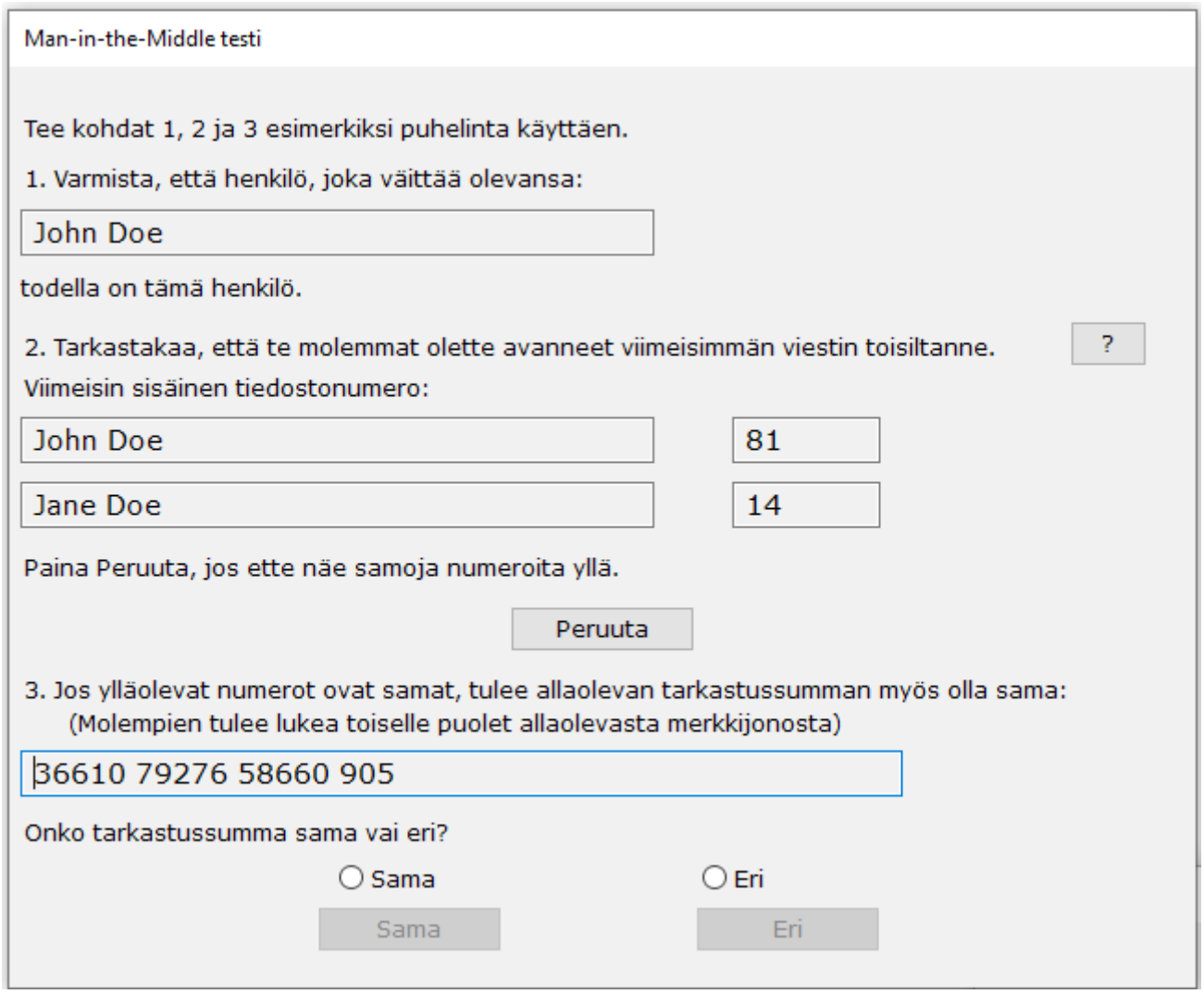
avaamiseen tarvittavat tiedot poistetaan tietokannasta. Jos viestiä yritetään avata, annetaan samanlainen ilmoitus, kuin jos viesti olisi jo aikaisemmin avattu.

Ota huomioon, että jos olet juuri vastaanottanut useita viestejä, jotka eivät ole salausjärjestyksessä, ja avaat viimeiseksi salatun, niin muut näkyvät tässä listassa. Tee salausavaimen tuhoaminen vasta huolellisen harkinnan jälkeen.

Lista ‘Viestit, jotka olen lähettänyt, mutta joita vastaanottaja ei ole avannut’ perustuu viimeisimmässä häneltä saadussa viestissä olleisiin tietoihin.

Man In The Middle hyökkäyksen paljastaminen

Tämä testi tarkastaa, onko molemmilla osapuolilla sama sisäinen tila salausprotokollassa. Jos tilanne on se, että sisäinen tila on sama, ei käynnissä ole 'man-in-the-middle' hyökkäystä.



Julkisten avainten perustiedot

Julkisiin avaimiin perustuva salaustekniikka on nykyaikaisen suojatun viestinnän perusta. Tässä esitetään lyhyesti ilman teknisiä yksityiskohtia näiden avainten perustiedot. Samalla kerrotaan suojausmekanismeistamme tunnettuja hyökkäyksiä vastaan.

Käytämme julkisia avaimia seuraavista syistä:

- Muodostaaksemme jaetun salaisuuden
- Toipuaksemme hyökkäyksestä
- Muodostaaksemme digitaalisen allekirjoituksen

Tärkeimmät hyökkäystavat:

- Yksityisen avaimen varkaus
- Man-in-the-middle hyökkäys ensimmäisessä avainten vaihdossa

Julkiset avaimet mahdollistavat jaetun salaisuuden muodostamisen.

Kun osapuolet vaihtavat julkisia avaimia, he voivat laskea arvon, jonka vain he voivat tietää. Kolmas henkilö, joka näkee vaihdetut julkiset avaimet ei voi laskea tätä arvoa. Tätä laskettua arvoa kutsutaan jaetuksi salaisuudeksi ja siitä voidaan muodostaa itse salausavain, jota käytetään viestin salaukseen. Tällaista menetelmää kutsutaan Diffie-Hellman avaintenvaihdoksi sen keksijöiden Whitfield Diffien ja Martin Hellmanin mukaan.

Tämä ratkaisee hyvin tärkeän ongelman: kuinka kommunikoida turvallisesti salausavain toiselle henkilölle? Lähettämällä ja vastaanottamalla julkinen avain.

Jokaisella julkisella avaimella on vastaava yksityinen avain. Julkisen avaimen luoja tietää automaattisesti sen yksityisen avaimen. Jaettu salaisuus lasketaan tämän yksityisen avaimen ja toisen osapuolen julkisen avaimen avulla.

Julkiset avaimet mahdollistavat toipumisen hyökkäyksestä.

Nyt kolmas henkilö, joka tarkkailee julkisten avainten vaihtoa ei pysty laskemaan jaettua salaisuutta, koska häneltä puuttuu jommankumman julkisen avaimen yksityinen avain. Tilanne kuitenkin muuttuu, jos hän onnistuneesti lähettää vakoiluohjelman, joka varastaa yksityisen avaimen tietokoneesta. Tällöin hän voi laskea jaetun salaisuuden ja voi avata kaikki ne viestit, joissa tuota jaettua salaisuutta on käytetty.

Meillä on nyt ongelma: kuinka toipua yksityisen avaimen paljastumisesta? EndCryptor ratkaisee tämän luomalla uusia julkisia avaimia ja lähettämällä ne.

Hyökkääjän täytyy taas pystyä varastamaan yksityinen avain – jos hän ei siinä onnistu, hän ei voi enää avata uusia viestejä.

Jotkut julkisiin avaimiin perustuvat järjestelmät käyttävät samaa julkista avainta vuosia. Jos sen yksityinen avain paljastuu esimerkiksi hakkeroinnin seurauksena kaikki tämän avaimen avulla salatut viestit voidaan avata. On havaittu tietokoneviruksia, jotka pyrkivät löytämään yksityisiä avaimia.

EndCryptor muodostaa paljon julkisia avaimia. Ensimmäiset viestit käyttävät pitkän ajan julkista avainta, jonka käyttäjä on julkistanut aikaisemmin kaikille. Tämän jälkeen jokainen viesti sisältää uusia lyhytaikaisia julkisia avaimia. Ne on tarkoitettu vain tämän vastaanottajan kanssa tapahtuvan viestinnän suojaamiseen. Niitä kutsutaan lyhytaikaisiksi avaimiksi, koska niitä käytetään vain lyhyen aikaa, esimerkiksi vain yhden viestin suojaamiseen. Kun henkilö, jonka yksityinen avain on paljastunut, lähettää uuden viestin ja se on vastaanotettu, voidaan muodostaa uusi jaettu salaisuus – hyökkäjä on menettänyt mahdollisuutensa avata uhrille tulevia viestejä.

On vielä olemassa ongelma: kuinka suojata aikaisempia viestejä, jotka on vastaanotettu ennen yksityisen avaimen paljastumista?

On otettava huomioon, että henkilö on voinut vastaanottaa useita viestejä lähettämättä viestejä takaisin, kun sitten yksityinen avain varastetaan. Kuinka suojata näitä viestejä, jotka on vastaanotettu Diffie-Hellman avaintenvaihdon jälkeen ja ennen yksityisen avaimen paljastumista? Vastaus edellyttäisi koko salausprotokollan tarkkaa kuvausta (voit lukea patentin tarvittaessa), joten annamme tuloksen:

Niitä salattuja viestejä, jotka vastaanottaja on avannut ennen hyökkäystä, ei voida avata hyökkääjän toimesta.

Julkiset avaimet mahdollistavat digitaalisen allekirjoituksen.

Jokaisen viestin lopussa on digitaalinen allekirjoitus. Se muodostetaan laskemalla kryptologinen tiivistearvo salatusta viestistä ja sitten yksityisen avaimen avulla muodostetaan digitaalinen allekirjoitus.

Henkilö, joka vastaanottaa viestin, tarkastaa allekirjoituksen aikaisemmin saamansa julkisen avaimen avulla.

Jos viestiä tai allekirjoitusta on muutettu, se havaitaan.

Tämä ratkaisee ongelman: kuinka estää viestien muuttaminen niiden liikkuessa internetissä ja kuinka estää lähettäjän identiteetin väärentäminen?

Man-in-the-middle hyökkäys

Tämä hyökkäys voidaan tehdä, kun henkilö lähettää julkisen avaimensa toiselle henkilölle viestinnän alussa. Kryptologiassa tämä hyökkäys kuvataan kolmen henkilön avulla: Alice, Bob ja Mallory. Alice ja Bob haluvat kommunikoida suojatusti ja Mallory haluaa avata heidän viestinsä.

Alice lähettää julkisen avaimensa Bobille, mutta Mallory sieppaa sen ja luo oman avaimensa ja lähettääkin sen Bobille muka Alicen avaimena. Bob luo oman vastauksensa, jossa on hänen julkinen avaimensa ja lähettää vastauksen Alicelle. Taas Mallory sieppaa viestin ja korvaa Bobin avaimen omalla avaimellaan. Nyt Mallory voi esiintyi kumpanakin henkilönä.

Man-in-the-middle hyökkäys: Alice ← → Mallory ← → Bob.

Alice ja Bob eivät tiedä, että on olemassa Mallory, joka vaihtoi heidän julkiset avaimensa omiinsa. Nyt Mallory avaa jokaisen Alicen ja Bobin lähettämän viestin, ja sitten taas salaa sen uudestaan omien salausavaintensa avulla ja lähettää sen viestin vastaanottajalle.

Tältä hyökkäykseltä suojautuakseen EndCryptorissa voi käyttää Web Hakemistoa oman julkisen avaimensa tallettamiseen ja jakamiseen muille. Käyttäjän julkinen avain allekirjoitetaan avaimella, josta on olemassa allekirjoitusketju julkiseen avaimeen, johon EndCryptor luottaa. Kun käyttäjän julkinen avain haetaan Web Hakemistosta tai vastaanotetaan ensimmäinen viesti kontaktilta, tämä allekirjoitus tarkastetaan. Käyttäjä voi myös tarkastaa, että tiedot Web Hakemistossa vastaavat hänen julkista avaintaan ja sähköpostiosoitettaan.

On myös mahdollista paljastaa tämä hyökkäys viestien vaihdon alettua: esimerkiksi puhelinkeskustelussa vertaillaan tarkastussummia. EndCryptor myös tallettaa ensimmäisten viestien julkisten avainten tarkastussummat tietokantaansa – käyttäjä voi tarkastella niitä myöhemmin.

EndCryptor, PGP ja S/MIME vertailussa

Tarkastelemme tässä yksityisen avaimen paljastumista

Lukijan tulee tietää, että yksityisen avaimen paljastuminen hyökkääjälle mahdollistaa kaikkien niiden viestien avaamisen, mitkä käyttävät tämän yksityisen avaimen avulla muodostettua jaettua salaisuutta.

S/MIME sähköpostin suojaustekniikka käyttää julkisten avainten infrastruktuuria, jossa on Varmentaja (Certificate Authority) joka allekirjoittaa digitaalisesti jokaisen uuden julkisen avaimen. Käyttäjillä on tietokoneessaan tämän Varmentajan julkinen avain ja he käyttävät sitä tarkastamaan saamansa varmenteen (certificate) allekirjoituksen. Kun käyttäjä ottaa käyttöön uuden julkisen avaimen, se täytyy ensin varmentaa Varmentajalla ja sitten toimittaa (esimerkiksi viestin yhteydessä) käyttäjille.

S/MIME ja PGP järjestelmissä julkinen avain vaihdetaan aikajaksolla, joka on vuosi tai vuosia.

EndCryptorissa käytetään viestinnän alussa osapuolten pitkän ajan julkisia avaimia. Vaihdettaviin viesteihin laitetaan uudet lyhytaikaiset julkiset avaimet, joita käytetään patentoidussa protokollassa, joka jatkuvasti vaihtaa uusia julkisia avaimia. Nämä lyhytaikaiset avaimet ovat vastaanottajakohtaisia. Pitkän ajan ja lyhyen ajan avaimet ovat samanlaisia, vain käyttöaika on erilainen.

Oletetaan nyt, että Alice aloittaa viestinnän Bobin kanssa ja lähettää viestin Bobille käyttäen Bobin pitkän ajan julkista avainta. Saatuaan tämän viestin, Bob avaa sen ja vastaa siihen. Myöhemmin hyökkääjä saa selville Bobin yksityisen avaimen. EndCryptorin ollessa kyseessä hyökkääjä voi lukea vain Alicen ensimmäisen viestin, mutta perinteisissä järjestelmissä hyökkääjä voi lukea kaikki Alicen viestit Bobille, jotka on lähetetty käyttäen Bobin pitkän ajan avainta - tässä voi olla usean vuoden viestit.

EndCryptorin tekniikassa julkisia avaimia vaihdetaan useammin: jos osapuolet viestivät vuorotellen, yhtä julkista avainta käytetään vain kerran. Paljastuneella yksityisellä avaimella on tässä ratkaisussa hyvin lyhyt käyttöaika. Julkisten avainten vaihto ei aiheuta myöskään kustannuksia.

Käytettäessä S/MIME tai PGP järjestelmää julkinen avain voi olla käytössä vuosia.

SSL:n ja selainpohjaisen salauksen riskit

Tämä osa käsittelee selainpohjaisen salauksen (SSL/TLS/https) riskejä - tätä tekniikkaa käytetään salattaessa yhteys web palvelimeen (tyypillisesti selain näyttää lukon osoitekentässä yrittäen näin vakuuttaa käyttäjän yhteyden turvallisuudesta). **Tämän sivun tulisi kiinnostaa tahoja, joille markkinoidaan sähköpostin salausratkaisuja, jotka perustuvat selaimiin ja jotka eivät siten tarvitse mitään ohjelmien asennusta käyttäjän koneeseen.**

Maaliskuussa 2017 Wikileaks julkaisi vuotoja koskien CIA:n hakkerointiaineistoa. Eräissä näistä dokumenteista on ohjeita CIA:n omille viruskirjoittajille: 'DO NOT solely rely on SSL/TLS to secure data in transit. Numerous man-in-middle attack vectors ... ' eli **'Älä luota yksinomaan SSL/TLS 'ään turvataksesi liikkuvaa tietoa. Lukuisia man-in-middle hyökkäystekniikoita ja julkistettuja vikoja protokollassa.'** ja **'Koska tämä uloin kerros voidaan avata hyökkääjän toimesta (esim. man-in-the-middle tekniikalla), jokainen tällainen salaus tulee tehdä vain tiedon sulauttamiseksi eikä sen turvaamiseksi'** - **CIA:n mukaan SSL/TLS/https kelpaa siis vain siihen, että se saa tiedon näyttämään tavanomaiselta internet liikenteeltä.**

Aikaisemmin marraskuussa 2011 Wall Street Journal julkaisi 'Surveillance Catalog' -luettelon ja Wikileaks julkaisi listan kansainvälisistä tiedusteluryityksistä ja heidän laitteistaan 'WikiLeaks Spy Files' -julkaisussa. Ohessa joitakin esimerkkejä esitteistä, joissa kuvataan laitteiden ominaisuuksia: "Laite voi myös purkaa SSL salauksen, jos se on asennettu 'man-in-the-middle' konfiguraatioon ...'; "Tarkkaile epäillyn salattua viestintää Gmailiin, Hush mailiin jne., tarkkaile epäillyn pankkisiirtoja jne.". **"Sieppaa mikä tahansa liikenne, joka käyttää SSL'ää tai TLS'ää. Kun asennettu, laitteet voivat mennä liikenteen väliin mihin tahansa SSL tai TLS yhteyteen ... käyttäjät ovat tuudittautuneet väärään turvallisuuden tunteeseen, jota tarjoavat selaimen. sähköpostin tai VoIP salaukset";. "Mutta 'man-in-the-middle' tekniikalla voidaan siepata liikenne ja aito varmenne ja korvata se väärällä varmenteella ja saada tietokone luulemaan, että liikenne sujuu normaalisti".**

Kuinka tämä on mahdollista?

Kun selain ottaa yhteyden HTTPS - SSL tai TLS palvelimeen, lähettää palvelin selaimelle varmenteen, joka todistaa käyttäjälle, että hän todella on yhteydessä haluttuun palvelimeen. Miten varmenne voi tehdä tämän? Palvelimen omistaja on - ennenkuin on aloittanut toimintansa - ottanyt yhteyttä Varmentajaan (Certificate Authority), ja todistanut tälle, että hän omistaa ja hallitsee palvelinta. Palvelimen omistaja on lähettänyt Varmentajalle palvelimen julkisen avaimen ja Varmentaja on allekirjoittanut tämän omalla avaimellaan.

Kaikissa tietokoneissa, jotka käyttävät SSL/TLS'ää, on varasto, jossa on eri julkisten Varmentajien julkiset avaimet. Nämä julkiset avaimet ovat varmenteissa, joita kutsutaan juurivarmenteiksi. Kun palvelimelta tuleva varmenne tarkastetaan, sen

aitous rippuu viime kädessä tästä juurivarmenteesta - tulee olla oikea digitaalinen allekirjoitusketju juurivarmenteesta palvelimelta tulevaan varmenteeseen.

Nyt jokainen, joka tietää juurivarmenteen julkisen avaimen yksityisen avaimen, voi esiintyä minä tahansa web palvelimena, purkaa niiden salauksen ja muuttaa liikenteen sisältöä käyttäen 'man-in-the-middle' tekniikkaa - tämä selitetään myöhemmin. Siis, varmenteiden infastruktuurista johtuen jokainen julkisesti hyväksytty Varmentaja voi - jos se kääntyy 'ilkeäksi' - tehdä tämän jokaiselle SSL/TLS'ää käyttävälle tietokoneelle. Varmentaja yksinkertaisesti myöntää varmenteen palvelimelle ja antaa käytetyn julkisen avaimen yksityisen avaimen hyökkääjälle - joka voi nyt voi avata ja muuttaa tähän yksittäiseen palvelimeen kohdistuvan liikenteen. Ilkeäksi muuttunut Varmentaja voi myös antaa juurivarmenteen yksityisen avaimen hyökkääjälle - joka voi nyt hyökätä jokaista SSL/TLS palvelinta vastaan myöntämällä itse tarvittaessa varmenteen uhriksi valitulle palvelimelle.

Voidaan argumentoida, että jos suojattava tieto on riittävän sensitiivistä, on liian iso riski siihen, että jokin noin 600 julkisesta Varmentajasta kääntyy 'ilkeäksi' tai pakotetaan jonkin hallituksen toimesta siihen tai sillä on lahjottu työntekijä tai se joutuu hakkeroiduksi. On huomattava, että viime vuosina on kehitetty ns. 'Certificate Transparency' projekti, joka koittaa minimoida tämän kaltaisia mahdollisuuksia - tästä myöhemmin.

Varmentaja Trustwave myönsi helmikuun 4 päivä 2012, että he olivat antaneet yhdelle yksityiselle asiakkaalle juurivarmenteen yksityisine avaimineen erillisen laitteen sisällä ('man-in-the-middle' laite), joka generoi tarvittaessa varmenteen halutulle palvelimelle. Tämä tehtiin, jotta voitaisiin avata ja tarkkailla kaikkea yrityksen SSL/TLS liikennettä, katso https://www.theregister.co.uk/2012/02/14/trustwave_analysis/ .

Nyt siis jokainen tietokoneen varmennevarastossa oleva varmenne tekee tyhjäksi tälle tietokoneelle tapahtuvan SSL/TLS liikenteen, jos varmenteen yksityinen avain joutuu vääriin käsiin.

Hyökkääjä voi asettaa oman varmenteensa tähän varastoon esim. pakottamalla käyttäjän asentamaan sen, tai 'ilkeä' kotiapulainen (ns. evil maid hyökkäys), ilkeä tullivirkailija tai tietokonevirus voi tehdä sen. Jotkut antivirus tai lasten tietokoneen käyttöä valvovat ohjelmat asentavat omat juurivarmenteensa tähän varastoon voidakseen avata ja tarkastaa SSL/TLS liikenteen. On ollut tilanteita, joissa tällaisen juurivarmenteen yksityinen avain on ollut kaikille ko. ohjelman käyttäjille sama - tällöin käyttäjä etsii omasta tietokoneestaan tuon yksityisen avaimen ja voi sen avulla avata kaikkien muiden ko. ohjelman käyttäjien liikenteen.

Tekniikka, jossa virus asentaa varmenteen varmennevarastoon mainitaan **Hacking Team** yritykseltä vuodetuissa materiaaleissa. Tuo yritys myy vakoiluohjelmia hallituksille ja lain täytäntöönpanoviranomaisille. Tällaiset tahot pystyvät helposti määräämään internet palvelujen tarjoajat asentamaan vaadittavat laitteet liikenteen

avaamiseksi. On huomattava, että myös erilaiset wifi pisteet ja internet kahvilat voivat avata käyttäjän liikenteen, jos niillä on tarvittava yksityinen avain (tai niillä on laite, jossa vaadittava yksityinen avain on).

Heinäkuussa 2019 Kazakhstan alkoi toteuttaa politiikkaa, jossa osaa internetin käyttäjistä pakotettiin asentamaan hallituksen toimittama varmenne tietokoneisiinsa, kun he selaimen avulla menivät tietyille salatun yhteyden vaativille websivuille. Asiasta julkaistun raportin (https://censoredplanet.org/kazakhstan) mukaan salaus purettiin mm. seuraavilta kohteilta: Gmail, Google, Facebook, Messenger, mail.ru, translate.google.com, Instagram ja Youtube.

Voi olla myös hyvin vaarallista käyttää tuntemattoman tietokoneen selainta ottamaan yhteyttä web palvelimeen - tuossa koneessa voi olla hyökkääjän asentama juurivarmenne ja kone voi helposti ohjata liikenteen man-in-the-middle laitteeseen.

On olemassa hyökkäys, joka käyttää internetin DNS järjestelmää: hyökkääjä onnistuu muuttamaan joidenkin internetin DNS palvelinten tietueita. Tämän jälkeen hyökkääjä pyytää joltain Varmentajalta uusia varmenteita hyökkäyksen kohteena olevalle palvelimelle. Tämän jälkeen se voi matkia tätä palvelinta käyttäjälle. Tällainen hyökkäys paljastui marraskuussa 2018, se kohdistui 50 Lähi-idässä olevaan yritykseen ja hallitusten virastoihin. Lisätietoa saa haulla 'DNSpionage' ja Brian Krebsin selonteosta osoitteesta https://krebsonsecurity.com/2019/02/a-deep-dive-on-the-recent-widespread-dns-hijacking-attacks/

Mielenkiintoinen on myös tilanne, jossa palvelimen yksityinen avain on paljastunut. Yksityinen avain voidaan hakkeroida, vuotaa ilkeän työntekijän toimesta tai se voidaan vaatia luovuttamaan viranomaisille. Jos palvelimen SSL/TLS liikennettä ei ole määritelty käyttämään ns. 'Perfect Forward Secrecy (PFS)' asetuksia voidaan yksityisen avaimen avulla avata aikaisemmat nauhoitetut yhteydet. Jos PSF on määritelty, vaaditaan man-in-the-middle tekniikka yhteyden aikana, jotta salaus saadaan avattua - se onnistuu, koska palvelimen yksityinen avain on tiedossa. Tämä ei vaadi mitään ylimääräisiä varmenteita uhrin koneessa.

U.S.A 'n hallitus vaati salatun sähköpostin tarjoaja Lavabit -yritystä luovuttamaan palvelimen SSL/TLS varmenteen yksityisen avaimen todennäköisesti kerätäkseen todisteita Edward Snowdenia vastaan, katso https://www.wired.com/2013/10/lavabit_unsealed/ .

Suositussa OpenSSL ohjelmassa havaittiin **Heartbleed** haavoittuvuus huhtikuussa 2014, se paljasti palvelimen muistin hyökkääjälle. Virhe oli koodissa 2 vuotta, mutta myös vanhemmat nauhoitetut SSL yhteydet (ilman PSF'ää) saadaan avattua muistista haetun yksityisen avaimen avulla. "Hyökkäsimme itseämme vastaan ulkopuolelta jättämättä jälkiä. Käyttämättä mitään ylimääräisiä oikeuksia pystyimme varastamaan itsellemme salatut avaimet, joita käytettiin X.509 varmenteissamme, käyttäjien nimiä ja salasanoja, pikaviestejä, sähköposteja ja liiketoiminalle kriitisiä dokumentteja ja viestintää."

Tammikuun 14, 2020 Microsoft ilmoitti, että kriittinen haavoittuvuus on havaittu varmenteiden tarkastusohjelmassa. Havainnosta Microsoftille ilmoitti NSA, katso https://media.defense.gov/2020/Jan/14/2002234275/-1/-1/0/CSA-WINDOWS-10-CRYPT-LIB-20190114.PDF . NSA:n mukaan "esimerkkejä missä vaikutukset voivat ilmetä: **HTTPS yhteydet, allekirjoitetut tiedostot ja sähköpostit** ja allekirjoitettu käyttäjän koodi. **NSA arvio haavoittuvuuden olevan vakavan ja että kehittyneet kybertoimijat ymmärtävät allaolevan vian hyvin nopeasti ja että jos haavoittuvuutta hyväksikäytetään, tulevat edellämainitut osa-alueet olemaan perustavanlaatuisesti haavoittuvia.**". Tämä tarkoittaa, että hyökkääjä, joka käyttää tätä vikaa, voi aloittaa 'man-in-the-middle' hyökkäyksen ilman tietoa yksityisistä avaimista. USA:n Cert koordinaattori (https://kb.cert.org/vuls/id/849224/) sanoo "Hyväksikäyttämällä tätä haavoittuvuutta hyökkääjä saattaa voida onnistua huijaamalla luomaan oikealta näyttävän allekirjoitusketjun haavoittuvassa Windows järjestelmässä. Tämä saattaa mahdollistaa erilaisia jatkotoimia sisältäen, muttei rajoittuen TLS-salatun liikenteen sieppaamiseen (avaamiseen, suom. huom.) ja muuttamiseen ja huijattujen Authenticode allekirjoitusten luomiseen.". Haavoittuvien versioiden joukossa on Windows 10, joka julkaistiin heinäkuun 29 päivä 2015.

Muistatko vielä mitä vuodetuissa CIA'n papereissa sanottiin: 'Älä luota yksinomaan SSL/TLS'ään turvataksesi liikkuvaa tietoa. Lukuisia man-in-middle hyökkäystekniikoita ja julkistettuja vikoja protokollassa.'

Kuinka 'man-in-the-middle' (MITM) tekniikka toimii? Tämä hyökkäys voidaan tehdä käyttäjän tietokoneen ja palvelimen välillä sellaisen hyökkääjän toimesta, joka tietää sopivan yksityisen avaimen (joko juurivarmenteen tai palvelimen). Kun käyttäjä aloittaa yhteyden palvelimeen hyökkääjä esiintyy palvelimena. Palvelimelle taas hyökkääjä esiintyy käyttäjänä.

MITM hyökkäys: Käyttäjä ↔ Hyökkääjä ↔ Palvelin.

Useat yritykset käyttävät erityisiä laitteita avaamaan oman SSL/TLS liikenteensä. Tämän mahdollistamiseksi yritys asentaa käyttäjien tietokoneiden varmennevarastoihin oman juurivarmenteensa. Nyt esim. tietynlaiset palomuurilaitteet voivat avata ja taas uudestaan salata käyttäjille menevän liikenteen. Tarkoituksena on esim. etsiä viruksia tietovirrasta. Citizen Lab'in raportissa "Planet Blue Coat: Mapping Global Censorship and Surveillance Tools, January 2013" (from https://citizenlab.ca/publications/) kuvataan kuinka tällaisia laitteita käyttävät myös valtiot, joilla on historiaa ihmisoikeuksien loukkaamisessa.

MITM hyökkäystä voidaan käyttää SSL/TLS pohjaisiin sähköposti ja webmail -ratkaisuihin. On myös olemassa VPN ratkaisuja, jotka käyttävät selainta. Selainpohjaiset salausratkaisut yleensä käyttävät markkinointiargumentteina sitä, ettei käyttäjän tarvitse asentaa mitään muita ohjelmia tietokoneeseensa - vain selain riittää.

Joskus selainpohjaiset sähköpostin salausratkaisut tekevät selaimessa javascriptillä viestin salauksen (esim. PGP). Tämä ei tuo suojaa MITM hyökkäystä vastaan - hyökkääjä muuttaa javascript koodia ennenkuin lähettää sen uhrille esim. niin, että käytetyn salausmenetelmän salausavain välitetään hyökkääjälle (esim. PGP:n yksityinen avain).

EndCryptor käyttää TLS'ää ottaessaan yhteyttä käyttäjän sähköpostipalvelimeen, sähköpostipalvelimet edellyttävät sitä. EndCryptor salaa viestin ennenkuin palvelimeen muodostetaan yhteys - onnistunutkaan MITM hyökkäys ei voi paljastaa viestin sisältöä. EndCryptorin kyseessä ollen hyökkääjä voi saada vain sähköpostin käyttäjätunnuksen ja salasanan haltuunsa. EndCryptor myös tallettaa kaikki saamansa varmenteet, ne voidaan myöhemmin analysoida, jos epäillään hyökkäystä. EndCryptor voidaan konfiguroida niin, että se hyväksyy palvelimelta vain tietyn varmenteen, tämä estää väärien varmenteiden käytön. Tämä on tunnettu tekniikka ja siitä käytetään nimitystä 'certificate pinning'.

Googlen kehittämä Certificate Transparency project (https://www.certificate-transparency.org/) yrittää parantaa varmenteiden infrastruktuuria. Tässä projektissa yritetään tallettaa kaikki maailmassa julkisten Varmentajien toimesta myönnetyt varmenteet, jotta havaittaisiin tietylle palvelimelle myönnetyt vihamieliset varmenteet. Suurimmat julkiset Varmentajat ovat siinä mukana ja myös hakukoneet voivat lähettää havaitsemiaan varmenteita projektille. Huhtikuun 30, 2018 jälkeen myönnettyjä varmenteita ei enää hyväksytä Chrome selaimessa ellei niiden mukana ole projektin vaatimaa lisäosaa (Signed Certificate Timestamp eli SCT), joka todistaa, että varmenne on toimitettu projektille. Google: "Erityisesti Certificate Transparency mahdollistaa sellaisten varmenteiden havaitsemisen, joita on virheellisesti myönnetty Varmentajien toimesta tai pahantahtoisesti saatu moitteettomilta Varmentajilta. Se myös mahdollistaa sellaisten Varmentajien tunnistamisen, jotka ovat alkaneet toimia vilpillisesti ja myöntävät pahantoisia varmenteita.".

Jos julkisesti hyväksytty Varmentaja myöntää varmenteen palvelimelle, se tulee tallettaa läpinäkyviin logeihin. Domainin (palvelimen) omistaja voi tehdä kyselyjä logeihin ja tarkastaa, että palvelimelle on myönnetty vain hänen haluamansa varmenteet. Väärää varmennetta voidaan käyttää MITM hyökkäyksissä kunnes se havaitaan ja kumotaan ja käyttäjät saavat tiedon kumoamisesta. Tällaisesta järjestelmästä voidaan tehdä johtopäätös, että on täytynyt tapahtua vakavia väärinkäytöksiä, koska tarvitaan näin iso systeemi.

Projekti sanoo https://www.certificate-transparency.org/benefits: "Todella, välikohtauksia, joita aikaisemmin on peitelty ja vähätelty ja jotka itse asiassa aiheuttivat kokonaisen Varmentajan sulkemisen, voidaan paljastaa paljon aikaisemmin ja korjata yksinkertaisesti kumoamalla yksittäinen varmenne.".

Certificate Transparency järjestelmään lisäämistä ei tehdä paikallisille ei-julkisen Varmentajan myöntämille varmenteille ja jotka on lisätty käyttäjän varmennevarastoon käyttäjän tai jonkin ohjelman kuten antivirus, palomuuri, virus jne. toimesta. Selain, joka ei hyväksy julkisen Varmentajan varmennetta puuttuvan

SCT osan vuoksi, hyväksyy varmenteen, jos se ei ole julkisen Varmentajan myöntämä. Selain olettaa tällöin, että varmennetta käytetään paikallisesti tai esim. SSL/TLS liikenteen avaamisen virustarkastuksen vuoksi.

Salausratkaisut, jotka käyttävät SSL/TLS'ää ilman selainta, eivät välttämättä noudata selainten käytäntöä ja vaadi CT lisäosaa.

Tekniset tiedot

Perusteellisemmat tiedot ovat englanninkielisessä dokumentissa EndCryptor_features.pdf.

Käytetyt julkiset avaimet ovat elliptisiin käyriin perustuvia, sillä niillä saadaan vahvempi suoja vaikka käytetään pienempiä avainkokoja. Varsinkin klassisten elliptisiin käyriin perustuvien avainten käsittely on hyvin nopeaa, tämä mahdollistaa niiden runsaan käytön ja hyökkäyksistä tapahtuvan nopean toipumisen.

Klassiset avaimet ovat Edwards avain Ed25519 ja vastaava avain Curve25519, jota käytetään mm. selaimissa. Edwards avainta käytetään digitaaliseen allekirjoitukseen ja Curve25519 avainta Diffie-Hellman laskentaan. Tuon Curve25519 avaimen klassinen turvataso on 128 bittiä.

Kvanttihyökkäyksen kestävät avaimet ovat ’supersingular isogeny SIDH (p751)’ versio 3.3 avaimia, jotka ovat Microsoftin suunnittelemia. Tammikuussa 2019 SIKE, jossa SIDH on ydinosana, hyväksyttiin kierrokselle 2 NIST'in Post-Quantum kryptologian standardointi prosessiin. NIST on National Institute of Standards and Technology (USA). Nykyisin arvioidaan SIDH p751 avaimen täyttävän NIST'in Quantum turvatason 5 (vahvin, paras) - sen arvioidaan olevan samaa luokaa kuin AES 256 symmetrisen avaimen. Heinäkuun 22, 2020 SIKE hyväksyttiin kierrokselle 3 vaihtoehtoisena kandidaattina, katso https://doi.org/10.6028/NIST.IR.8309 ja https://www.nist.gov/news-events/news/2020/07/nists-post-quantum-cryptography-program-enters-selection-round .

Vertaa klassisia turvatasoja:

Symmetrinen	Elliptinen	DH tai RSA
80	163-223	1024
112	224-255	2048
128	256-383	3072
192	384-511	7680
256	512+	15360

Curve25519 turvataso on 128 bittiä ja se vastaa 3072 bitin pituista RSA/Diffie-Hellman julkista avainta. Kannattaa huomata, että 256 bitin symmetrinen turvataso vastaa 15360 bitin pituista RSA/Diffie-Hellman avainta. Yleensä kryptologisen

rakenteen turvallisuus arvioidaan sen heikoimman lenkin perusteella - tämä on tavallisesti julkinen avain.

Tuo taulukko on NIST'in julkaisussa Special Publication 800-57 ajalta heinäkuu 2012 nimeltään 'Recommendation for Key Management – Part 1: General(Revision 3)'.

Jos osapuolet viestivät vuorotellen, on ensimmäisen viestin turvataso 128 bittiä, sen jälkeen on klassinen turvataso 256 bittiä. Kvanttisuoja alkaa toisesta viestistä, se mukaanluettuna. Patentoitu protokolla alkaa, kun toinen viesti on vastaanotettu. Tämän jälkeen jokainen uusi viesti sisältää lähettäjän uudet klassiset avaimet. Kvanttihyökkäyksen kestävien avainten käsittely on laskennallisesti enemmän resursseja vievää, joten niitä vaihdetaan kerran viikossa, jos osapuolet viestivät säännöllisesti.

Symmetrinen salaus tehdään Chacha20'llä ja 256 bittisellä avaimella. Kryptotekstin digitaaliset allekirjoitukset käyttävät Keccak-256 tiivistettä, joka muodostetaan käyttäen kuvausta, joka voitti SHA3 kilpailun (bitrate on 1088 ja capacity on 512). Poly1305 tarkastussummaa käyttään selväkielisen osan tarkastukseen.

Ed25519, Curve25519, Chacha20 ja Poly1305 toteutus käyttää SUPERCOP'in ja NaCl kirjaston (European Network of Excellence in Cryptology II projecteja, rahoittajana European Commission) referenssitoteuksia. SIDH avainten toteusprojekti on GitHup'issa: PQCrypto-SIDH.

Curve25519 kuten muut klassiset DH tai RSA julkiset avaimet voidaan murtaa kvanttitietokoneella, jos sellaisia onnistutaan rakentamaan.

Kvanttihyökkäyksessä arvioidaan karkeasti, että symmetrinen salaus (AES, ChaCha20) menettää turvatasoaan seuraavasti: N bitin turvatasosta, joka saadaan N bitin avaimella, tulee N/2 bitin turvataso. EndCryptorin Chacha20 käyttää 256 bitin avainta ja niinpä kvanttihyökkäyksessä sen turvataso on 128 bittiä.

Otetaan nyt tavoitteeksi rikkoa Chacha20'n symmetrinen salaus kvanttikoneella. Tämä tarkoittaa, että tarvitaan noin 2^128 kvanttioperaatiota salausavaimen löytämiseksi.

Kuinka kauan sitten yksi tällainen kvanttioperaatio kestäisi - luultavasti se vaatii enemmän aikaa kuin yksi klassinen salausoperaatio.

Tarkastellaan asiaa bitcoin verkon avulla. Se tekee (3 heinäkuuta, 2018) alle 50x10^18 hajautus (tiivistys) operaatiota sekunnissa (katso https://www.blockchain.com/charts/hash-rate). Oletetaan, että bitcoin verkko voisi tehdä salausoperaatiota 100 kertaa nopeammin eli 50x10^20 operaatiota sekunnissa. Tällöin se pystyisi murtamaan 128 bitin turvatason

2^128/50x10^20/31536000 = 107 902 830 708 vuodessa.
Voit tarkastaa laskelman Windowsin laskimella.

Tarkastellaan nyt bitcoinin energian kulutusta. Sen arvioidaan nyt olevan 18TWh ja TWh välillä (katso https://digiconomist.net/bitcoin-energy-consumption).

Jos otamme alhaisimman arvon 18 TWh/vuosi ja kerromme sen tarvittavilla vuosilla, saamme:

107902830708 x 18 Twh = 1 942 250 952 744 TWh

mikä on 128 bitin turvatason murtamiseen tarvittava energiamäärä. Vuonna 2015 maailman kokonaisenergian kulutus oli 20 201,31 TWh (International Energy Agency'n mukaan).