Katavisto Sami

AJONEUVON ULKOISEN TIETOLIIKENTEEN TIETOTURVA

Insinöörityö
Kajaanin ammattikorkeakoulu
Tekniikka ja liikenne
Tietotekniikka
Kevät 2012

KAJAANIN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ
TIIVISTELMÄ

Koulutusala Tekniikka ja liikenne	Koulutusohjelma Tietotekniikka
Tekijä(t) Sami Katavisto	
Työn nimi Ajoneuvon ulkoisen tiedonsiirron tietoturva	
Vaihtoehtoiset ammattiopinnot Tietoturvateknologia	Ohjaaja(t) Jukka Heino
	Toimeksiantaja Joona Tolonen
Aika 3. Huhtikuuta 2012	Sivumäärä ja liitteet 27 sivua, 1 liite

Kajaanin ammattikorkeakoulun ajoneuvojärjestelmäkoulutukseen liittyy opetuskäyttöön hankittu ajoneuvo, jonka tietojärjestelmään käytetään hyväksi järjestelmän keräämän tiedon analysointiin ja lähettämiseen edelleen tietosäilöön tallennettavaksi. Insinöörityön tavoitteena oli tutkia tiedonsiirtojärjestelmän tietoturvallisuutta sekä etsiä keinoja mahdollisten tietoturvariskien huomioimiseksi ja soveltamiseksi. Nykyisen järjestelmän tietoturvallisuutta tutkittiin eriyttämällä tietoturvan heikkoudet ja riskit tietoturvan eri osa-alueisiin. Näille osa-alueille etsittiin lähdemateriaalista menetelmiä, joilla olemassa olevia käytänteitä voidaan parantaa.

Tietoturvan osa-alueisiin kuuluvat tiedon saavutettavuus, luotettavuus, eheys ja kiistämättömyys. Ajoneuvon ulkoiseen tiedonsiirtoon sovellettuna nämä tarkoittavat, että ajoneuvo lähettää tietoa katkottomasti, vastaanottava palvelin on käytettävissä, lähetettävä tieto ei muutu matkalla, sekä vastaanottava että lähettävä osapuoli on vahvasti tunnistettu ja kolmas osa puoli ei pysty salakuuntelemaan tietoliikennettä.

Järjestelmän nykytilaa tarkasteltaessa havaittiin, että jo käyttöön otetuissa menetelmissä oli otettu huomioon tietoturvaan liittyviä seikkoja. Toteutus oli nykytilassa ylläpidon kannalta yksinkertainen ja selkeä eikä ylimääräisiä tietoturvaan liittyviä tekniikoita käyttöönottamalla saavutettaisi kuin nimellistä lisähyötyä. Jos tietoturvatasoa kuitenkin halutaan kohottaa, on käytettävissä useita menetelmiä, jotka liittyvät niin saavutettavuuteen, luotettavuuteen, tiedon eheyteen kuin tiedon kiistämättömyyteenkin.

Kieli	Suomi
Asiasanat	Tietoturva, ajoneuvotietokone, tietoliikenne
Säilytyspaikka	☐ Verkkokirjasto Theseus ☐ Kajaanin ammattikorkeakoulun kirjasto

KAJAANIN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

THESIS
ABSTRACT

School School of Engineering	Degree Programme Information Technology
Author(s) Sami Katavisto	
Title Information Security of the External Data Transmission Output of Vehicle	
Optional Professional Studies Information Security	Instructor(s) Jukka Heino
	Commissioned by Joona Tolonen
Date March 28, 2012	Total Number of Pages and Appendices 27 pages, 1 Appendix

This Bachelor's thesis introduces various issues that should be considered while constructing a system that includes data transmission from a vehicle to the data storage. The vehicle collects data from various sources, including the vehicle's own measurement units and probes that gather data such as speed, temperature, revolutions and GPS location. This collected data is then sent over a mobile network to a static data source, in this case server that runs a database.

The first issue is availability. Data is not available if the mobile data connection is broken or the database server is not online. Also if the hardware containing data breaks down, the data will be lost. The second issue is integrity. There must be techniques to ensure that the data being transmitted comes through exactly the same than it was sent. The third issue is securing the gateway so that no third party can eavesdrop what is being transmitted.

The thesis firstly introduces several techniques that could be implemented when improving the security of data transmission is desired. The thesis then studies the architecture of the current data transmission gateway and ponders how implementing additional techniques will affect the security and complexity of the current system and if implementing is even meaningful.

As the conclusion, it is argued that current security over 3G mobile networks is adequate and additional measures are available but not required.

Language of Thesis	Finnish
Keywords	Information security, vehicle data system, communication
Deposited at	☐ Electronic library Theseus ☐ Library of Kajaani University of Applied Sciences

ALKUSANAT

Tietoturva on viime aikoina ollut enemmän kuin paljon esillä niin keskusteluissa kuin mediassakin. Useimpien asiaan perehtymättömien henkilöiden mielissä tietoturva on tiedon piilottamista, salaamista, palomuureja ja virustorjuntaohejmistoja. Nämä ovat kuitenkin vain osa tietoturvaa, jonka tavoite on myös taata tiedon saatavilla oleminen tarvittaessa.

Tätä lopputyötä on yritetty tehdä monipuolisista näkökulmista ottaen kantaa niin tietojen turvalliseen säilytykseen, asiattoman pääsyn karsimiseen kuin tiedon saavutettavuuteenkin.

SISÄLLYS

TERMIT JA SELITYKSET

GPS	Global Positioning System. Satelliittiverkosta muodostuva paikannusjärjestelmä
retina	Silmän ulkopinnan verisuonistosta muodostuva kuvio, joka on jokaisella ihmisellä yksilöllinen sormenjälkien tapaan
RFID	Token-luokan älysirutyyppi, jolla käyttäjä voidaan langattomasti tunnistaa
USB	Universal Serial Bus. Tiedonsiirtoväylä lisälaitteiden liittämiseksi tietokoneeseen

JOHDANTO

Kajaanin ammattikorkeakoululla on ajoneuvojärjestelmien opetuskäyttöön hankittu ajoneuvo. Ajoneuvon on tarkoitus kerätä ajoneuvoon liittyvää tietoa ja lähettää tieto internetin läpi tietovarastoon, jossa se tallennetaan.

Tämän insinöörityön aihe valikoitui useiden ajoneuvojärjestelmiin liittyvien insinööritöiden joukosta tietoturvaan liittyvän aihealueensa johdosta. Työn tilaajaksi päätyi lehtori Joona Tolonen, joka oli insinöörityön luomisen aloitushetkellä ajoneuvojärjestelmien koulutuksen projektipäällikkö.

Tämän insinöörityön tarkoituksena on ottaa kantaa tiedonsiirtoyhteyden muodostamiseen tietoturvan näkökulmasta. Työssä tutkitaan tiedonsiirron eri vaiheita, puututaan mahdollisiin tietoturvaseikkoihin, vertaillaan erilaisia tietoturvamenetelmiä ja suositellaan käytettäväksi näistä parasta.

Työn kirjoittamisen aikana luodaan toimiva tiedonsiirtoväylä ajoneuvosta tietovarastoon. Työ ottaa kantaa luotavan väylän tietoturvaan.

TIETOTURVA KÄSITTEENÄ

1.1 Historia

Tietoturvan voidaan sanoa olevan ollut käsitteenä olemassa aina siitä saakka, kun ihmisillä on ollut hallussaan tärkeää tietoa. Tämän voidaan olettaa saaneen alkunsa luku- ja kirjoitustaidon kehittymisestä. Vaikka varhaiset kirjoitustavat olivat jo itsessään kryptografisia ja niiden ymmärtäminen oli oppineen ylhäisön etuoikeus, ensimmäiset salakirjoitustavat kehittyivät varsin pian ensimmäisten kirjoitusmerkkien jälkeen. Vaikka tietoturvaan liittyy paljon muutakin kuin salakirjoitus, se on luettava ensimmäiseksi tietoturvaan liittyvän tekniikan käyttämiseksi.

1.2 Tietoturvan osa-alueet

Tässä insinöörityössä tiedonsiirron tietoturvaa tarkastellaan seuraavien osa-alueiden kautta.

1.2.1 Saavutettavuus

Tiedon saavutettavuus on ominaisuus, joka ilmentää sitä, kuinka varmasti järjestelmä, laite, ohjelma tai palvelu on tarvittaessa käytettävissä [1]. Hyvää saavutettavuutta vaaditaan esimerkiksi pankkien verkkopankkipalveluissa. Tässä insinöörityössä keskitytään ajoneuvon tiedonlähetysmekanismin saavutettavuuteen, vastaanottavan palvelinjärjestelmän saavutettavuuteen sekä tallennetun tiedon saavutettavuuteen säilytyksen näkökulmasta.

Tietojärjestelmien saavutettavuuden turvaamiseksi on kartoitettava riskit, jotka uhkaavat saavutettavuutta. Näitä riskejä voivat olla esimerkiksi sähkökatko, tulipalo ja laitteiston rikkoontuminen. Riskien toteutuessa on todennäköistä (riippuen riskin vakavuudesta), että palvelu on pois käytöstä jonkin aikaa. Toipumissuunnitelmassa tuleekin määrittää toimenpiteet, joilla käyttökatko eliminoidaan tai ainakin minimoidaan ajallisesti.

Lähetettäessä tietoa langattoman tiedonsiirtoväylän yli on todennäköistä, että tiedonsiirtoyhteys välillä katkeaa. Yhteyden katkeamista ei voida radioteknisistä syistä välttää kaikissa tilanteissa ajoneuvon ollessa liikkeessä. Järjestelmässä täytyy siis varautua yhteyden

katkeamiseen ottamalla se riskien kartoituksessa huomioon todennäköisesti toteutuvana riskinä. Jotta tallennettu tieto olisi onnistuneen tallennuksen jälkeen jatkuvasti saatavilla ja turvassa, se tulee myös varmuuskopioida säännöllisesti.

Ulkoiselle medialle varmuuskopioitaessa on otettava huomioon haluttu tiedon säilyvyyden kesto. Optinen media (CD- ja DVD-levyt) ei kestä säilytystä yhtä hyvin kuin nauhavarmistusaseman nauhat. USB-muistitikkujen tiedon säilyvyydestä ei ole vielä tarpeeksi pitkäaikaista kokemuspohjaa, jotta niitä voitaisiin suositella pitkäaikaiseksi tiedon säilytyspaikaksi. Kaikissa tapauksissa ulkoiselle medialle otettu tieto on säilytettävä mahdollisimman kaukana alkuperäisestä kohteesta sähkö-, palo- ja vesivahinkojen sekä varkauden varalta.

1.2.2 Eheys

Tiedon eheydellä tarkoitetaan sitä, että tieto ei ole muuttunut sen jälkeen, kun tiedon todennettu luoja on sitä viimeksi käsitellyt [1]. Tiedonsiirron eheys tarkoittaa näin ollen sitä, ettei tieto ole muuttunut lähettämisen ja vastaanoton välillä. Tiedon muuttuminen voi olla tahallista tai tahatonta. Tahallisessa muuttumisessa joku hakkeri voi ohjata tiedonsiirron omaan väärennettyyn tallennuspisteeseen, josta tieto lähetetään muunnettuna eteenpäin. Tahattomassa muuttumisessa jokin vika tietoliikennelaitteessa aiheuttaa datan muuttumisen.

Tiedon muuttumista ei välttämättä havaita heti. Muuttunut tieto voi sattumalta näyttää odotetulta, mutta olla silti väärää. Tiedon eheyttä tarkistettaessa ei voida siis olettaa, että määrämuotoinen, odotetuissa raja-arvoissa oleva tieto olisi automaattisesti muuttumatonta.

1.2.3 Luottamuksellisuus

Tiedon luottamuksellisuudella tarkoitetaan sitä, että tietoon pääsevät käsiksi vain ennalta määritellyt tahot. Tässä insinöörityössä asiaa käsitellään käyttöoikeuksien näkökulmasta. Tietoa saa kerätä, lähettää ja tallentaa vain ennalta määritellyt toimijat, ja tallennettuun tietoon pääsevät käsiksi vain ne, joilla on siihen oikeus.

Käyttöoikeuksien myöntäminen palveluihin tapahtuu perinteisesti kolmella tavalla:

- ”Kuka sinä olet” (biometrinen tunnistus eli esim. sormenjäljet tai retina)
- ”Mitä sinä tiedät” (käyttäjätunnus-salasanapari)
- ”Mitä hallussasi on” (esim. älykortit tai rfid-sirut)

Tunnistautumisessa on kyse tiedosta, jonka tunnistautuja sekä tunnistautumisen hyväksyjä tietävät, mutta joka ei ole kolmannen osapuolen hallussa.

Kun kyseessä on internetin yli tapahtuva tunnistautuminen, käytössä on käytännössä vain keskimmäinen vaihtoehto. On kuitenkin olemassa hiukan kolmatta vaihtoehtoa muistuttava tunnistautuminen, jossa hallussa ei ole niinkään fyysinen esine, vaan ohjelmallinen tunniste, jota kutsutaan sertifikaatiksi. Jos käyttäjän interaktiota eli näppäimistön painamista ei tarvita (tai automatisoidussa tunnistautumisessa se ei ole edes mahdollista), sertifikaattiin perustuva tunnistautuminen on paras vaihtoehto.

Luottamuksellisuutta voidaan parantaa myös salakirjoittamalla tieto. Salakirjoituksella ei pyritä piilottamaan tietoa, vaan sen tarkoitus [2, s. 24]. Salaus ja sen purkaminen vaatii kuitenkin aina jonkin verran laskentatehoa. Siksi onkin harkittava, onko tiedon joutuminen vääriin käsiin niin suuri riski, että tiedon salakirjoitus on mielekästä.

1.3 Salakirjoituksen teoriaa

Kuten edellä on mainittu, salakirjoituksen (kryptografia) tarkoitus ei ole piilottaa itse viestiä, vaan viestin tarkoitus. Toisin kuin kryptografia, steganografia pyrkii viestin piilottamiseen. Piilottamisen voi toteuttaa esimerkiksi upottamalla digitaaliseen kuvaan tai äänitteeseen viestin hienovaraisilla bittitason muutoksilla, jotka eivät ole aistein havaittavissa [2, s. 22 - 24].

1.3.1 Salakirjoituksen historiaa

Yksi tunnetuimmista salakirjoituksen vanhoista kuvauksista löytyy Herotodoksen *Historia*-teoksesta. 400-luvulle eKr sijoittuvassa kertomuksessa Demeratos-niminen kreikkalainen haluaa varoittaa spartalaisia Kserkseen valloitussuunnitelmista. Ongelmana oli lähettää viesti niin, etteivät persialaiset sotilaat saisi sitä käsiinsä. Demeratos keksi peittää kirjoitustaulun kirjoituksen vahalla, jolloin taulu näytti tyhjältä. Vaikka tievartijat ja osa taulun tarkoitetusta vastaanottajistakaan ei hoksannut etsiä tekstiä vahan alta, ”Kleomeneen tytär Gorgo, Leonidaan vaimo”[2, s. 21] oli sattumalta keksinyt kaapia vahan pois. Kreikkalaiset alkoivat nyt aseistautua tämän varoituksen ansiosta. Kserkseksen yllätyksen etu oli menetetty ja persialaisten hyökkäys torjuttiin. Salakirjoitus siis pelasti Kreikan joutumasta Kserkseen vallan alle [2. s. 20 - 21].

Salakirjoitus on siis jo tuhansia vuosia vanha käytäntö siirrettäessä tietoa, jonka ei haluta joutuvan vääriin käsiin. Salakirjoitukseen on käytetty yksinkertaisia, niin kirjainten korvaukseen perustuvia menetelmiä kuin erityisesti tätä tarkoitusta varten rakennettuja laitteitakin. Useimmat salakirjoitukset on kuitenkin murrettu sen toimesta, keneltä viesti on pyritty salaamaan. Menetelmää on käytetty erityisesti vakoilussa ja sodissa. Taistellessaan Japanin armeijaa vastaan Yhdysvallat keksi käyttää Navajo-intiaaneja radisteina. Navajo-kielen harvinaisuuden takia japanilaiset eivät onnistuneet selvittämään viestien sisältöä. Aiheesta tehtiin vuonna 2002 Hollywood-elokuva ”Windtalkers”, ja sitä tähditti Nicholas Cage.

1.3.2 Symmetristen avainten salakirjoitustavat

Symmetrisessä salakirjoituksessa salakirjoitettu viesti avataan samalla avaimella, millä se on salakirjoitettukin. Viesti voidaan salakirjoittaa esimerkiksi muuttamalla viesti ensin ASCII-taulukon avulla binääriseen muotoon. Tämän jälkeen viestille tehdään bitti bitiltä XOR-operaatio salakirjoitusavaimen bittien kanssa. Avainta luonnollisesti toistetaan, kunnes pituus vastaa viestin pituutta. Salakirjoitusta purettaessa riittää, että täsmälleen sama XOR-operaatio tehdään salakirjoitetulle viestille käyttäen samaa avainta.

Ongelmana tässä menetelmässä on avaimen toimittaminen viestin vastaanottajalle. Avainhan on samanlainen välitettävä salaisuus kuin salakirjoitettu viestikin.

1.3.3 Epäsymmetristen avainten salakirjoitustavat

Vuonna 1977 Rivest, Shamir ja Adleman kehittivät RSA-algomitmin [2, s. 367], jonka toiminta perustuu epäsymmetristen avainten menetelmään. Yksinkertaisimmillaan selitettynä algoritmi hyödyntää sitä matemaattista faktaa, että kun kahdesta suuresta alkuluvusta otetaan tulo, saadusta tulosta on hyvin vaikea selvittää, mitkä kaksi alkulukua kerrottiin keskenään.

Epäsymmetrisessä salauksessa viestin salakirjoitukseen ja salakirjoituksen purkamiseen käytetään eri avaimia. Avaimia kutsutaan julkisiksi (public) ja yksityisiksi (private). Viestin lähettäjä salakirjoittaa viestin sen vastaanottajan julkisella avaimella. Salakirjoitettu viesti voidaan avata vain viestin vastaanottajan salaisella avaimella. Viestin lähettäjällä täytyy siis olla tiedossaan viestin vastaanottajan julkinen avain eikä viestinvälitystä voida spontaanisti aloittaa ennen vastaanottajan avainten luomista.

1.4 HTTPS

HTTPS (Hypertext Transfer Protocol Secure) on salattu versio HTTP-protokollasta. HTTPS-protokollaa käytetään haluttaessa siirtää tietoa suojatusti WWW:ssä. Tietojen salauksessa käytetään ennen lähettämistä SSL-protokollaa tai uudempaa TLS-protokollaa. SSL-salausta käytettäessä tarvitaan varmenne. Jos varmenne on aito (ts. luotettavan tahon myöntämä), voi käyttäjä olla varma siitä, että palvelin, jolle tietoa lähetetään tai josta tietoa vastaanotetaan, on se mikä se väittää olevansa.[3.]

1.5 SSL ja TSL

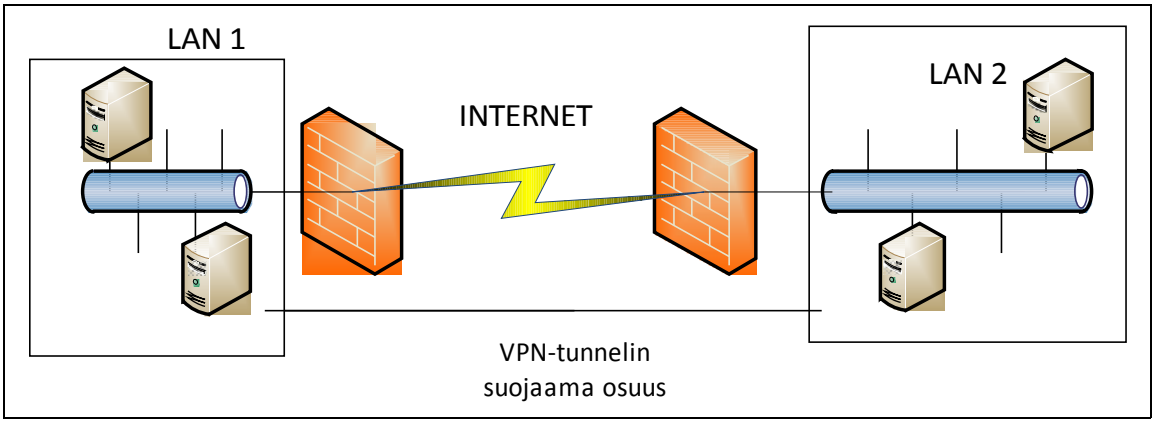
Kuten aikaisemmin mainittiin, SSL (Secure Sockets Layer) ja TSL (Transport Layer Security) ovat HTTPS-protokollan käyttämiä protokollia. SSL-protokolla on TSL-protokollan edeltäjä ja nykyisin käytössä onkin pääsääntöisesti TSL-protokolla sen paremman tietoturvan takia. Protokollat eivät toimi ristiin, mutta jos TSL-protokolla ei ole tuettu, voidaan siirtyä käyttämään SSL-protokollaa, jos yhteyden osapuolet niin sopivat.

Yhteydenmuodostus alkaa osapuolten välisellä kättelyllä (engl. handshake). Kättelyssä sovitaan käytettävistä salausmenetelmistä, vaihdellaan puolin ja toisin salakirjoitettuja satunnaislukuja ja lopulta päätetään aloittaa salakirjoitettu viestintä. Edistyneemmässä tiedonsiirrossa myös asiakkaan (engl. client) identiteetti varmistetaan.

1.6 VPN

VPN (Virtual Private Networking) tarkoittaa yhteydenmuodostustapaa, jossa halutaan luoda suojattu yhteys suojaamattoman yhdeyden yli. VPN-yhteyttä käytetään esimerkiksi, kun halutaan yhdistää yrityksen kahden toimipisteen tietoverkot internet-palveluntarjoajan yhteyden läpi. Tällaista yhteyttä kutsutaan VPN-tunneliksi. Tunneloinnissa käytettäviä protokollia ovat IpSec, L2TP (Layer 2 Tunneling Protocol) ja PPTP (Point-to-Point Tunneling Protocol). Suojattaessa yhteys tunneloimalla on huomioitava, mikä osa verkon tiedonsiirrosta on suojattu. Jos VPN-tunnelointi ulottuu pelkästään VPN-palomuureihin, on sisäverkkojen sisäinen liikenne yhä salaamatonta. Jos sisäverkon jokin työasema on

saastutettu jollakin verkon salakuunteluohjelmalla, on lähiverkon sisäinen liikenne suojaamatonta ja näin salakuunneltavissa. VPN- tunnelin toimintaperiaate on ilmaistu kuvassa 1.



Kuva 1. VPN-tunnelin toimintaperiaate

1.7 SSH ja SCP

SSH (Secure Shell) on salattuun tiedonsiirtoon tarkoitettu protokolla. SSH:n yleisin käyttötapa on ottaa etäyhteys SSH-asiakasohjelmalla SSH-palvelimeen, jotta päästään käyttämään toista konetta merkkipohjaisen konsolin kautta. SSH:lla voidaan myös suojata FTP-, HTTP- tai muuta liikennettä, joka toimii samalla tasolla. SSH1:n kehitti alun perin espoolainen Tatu Ylönen. Tässä jo hieman vanhentuneessa suojauksessa käytettävät algoritmit kuten RSA ja muut ovat osoittautuneet erittäin hyviksi. Myöhemmin SSH1:n yksinkertaista tiedon oikeellisuuden (CRC) tarkistamista on pidetty suojaustasoltaan heikkona. Tämä on kuitenkin kehittynyt SSH2:ssa, jota nykyään suositellaan käytettäväksi.[4.]

SCP (Secure Copy) on SSH- protokollaan perustuva suojattu tiedostonsiirtoprotokolla. Sitä käytetään komentoriviltä samannimistä tiedonsiirto-ohjelmaa käyttäen pitkälti samalla tavalla kuin suojaamatonta tiedonsiirtoyhteyttä käyttävää ftp-siirto-ohjelmaakin. SCP-ohjelmasta on Windows-käyttöjärjestelmälle graafista käyttöliittymää käyttävä ilmainen Martin Prikrylin julkaisema WinSCP.

1.8 3G- ja GPRS-siirtotavan salaus

GSM-verkossa puheen ja tietoliikenteen salaus perustuu kolmeen matemaattiseen algoritmiin. A3-algoritmilla tunnistetaan käyttäjä, A8-algoritmilla luodaan salausavaimet ja liikenne salataan A5-algoritmilla. Käytettävä A5/1–algoritmi on kuitenkin varsin heikko. Salaus murrettiinkin joulukuussa 2009 [5].

Kolmannen sukupolven matkapuhelinverkot (3G) käyttävät UMTS-matkapuhelinteknologiaa. Siinä tietoturvaa ja etenkin salausta on parannettu huomattavasti kehittämällä yhteyden osapuolten tunnistusta ja salausalgoritmeja. Salausalgoritmeja on useita ja niiden toimintaperiaate on julkista, mikä parantaa niiden luotettavuutta. Salausavainten pituutta on myös kasvatettu.[6.]

TIEDONSIIRRON EHEYDEN VARMISTUSMENETELMÄT

Tiedonsiirron eheydellä tarkoitetaan sitä, että lähetetty tieto on pysynyt samana koko tiedonsiirron ajan. Tässä tarkistuksessa ei oteta kantaa siihen, onko tieto mahdollisesti muuttanut muotoaan tahattomasti tai tahattomasti. Tahallinen tiedon muutos voi olla tapahtunut ulkopuolisen tietohyökkäyksen toimesta, tahaton taas esimerkiksi yksinkertaisesti huonon kaapeliliitoksen aikaansaamana.

Tarkistussummat ja tiivistefunktiot

Tarkistussummat ovat yksinkertaisia virheentarkistusmenetelmiä, joista tutuin esimerkki on henkilötunnuksen viimeinen merkki, joka lasketaan henkilötunnuksen muista luvuista. Tarkistussummat ovatkin käteviä pienten tiedonsiirtomäärien virheentarkistukseen ja lasketut summat liitetäänkin usein lähetettavan datan perään.

Tiivistefunktiot ovat menetelmiä, joissa tarkistettavasta tiedosta otetaan ennen lähetystä tarkistussumma tai tiiviste lähes yksisuuntaisilla algoritmeilla. Tiedonsiirron ohessa lähetetään myös tarkistussumma tai tiiviste. Vastaanottopäässä luodaan samoja algoritmeja käyttäen tarkistussumma tai tiiviste, ja lähetyspään tuotoksia verrataan näihin uusiin tuotoksiin. Jos eroa ei ole, tieto ei ole todennäköisesti muuttunut matkalla.

Tiivisteitä otetaan yleensä kerralla suuremmasta tietokokonaisuudesta, kuten kokonaisista tekstidokumenteista. Yksisuuntaisuus algoritmeissa tarkoittaa sitä, ettei kerran otetusta tiivisteestä voida enää palauttaa takaisin alkuperäistä tietoa. Vaikka voidaan valita ääretön määrä lähdemateriaalia, jotka tuottavat saman tiivisteen, ei voida enää valita lähdemateriaalia, josta nimenomainen tiiviste on luotu. Käänteisfunktio ei näin ollen ole yksiselitteinen.

CRC

CRC (Cyclic Redundancy Check) on yksinkertainen tiivistefunktio, joka soveltuu hyvin pienten tietomäärien tarkistamiseen. CRC-tarkisteen laskeminen ei vaadi paljoa laskentatehoa ja se voidaan suorittaa myös laitetasolla.

MD5

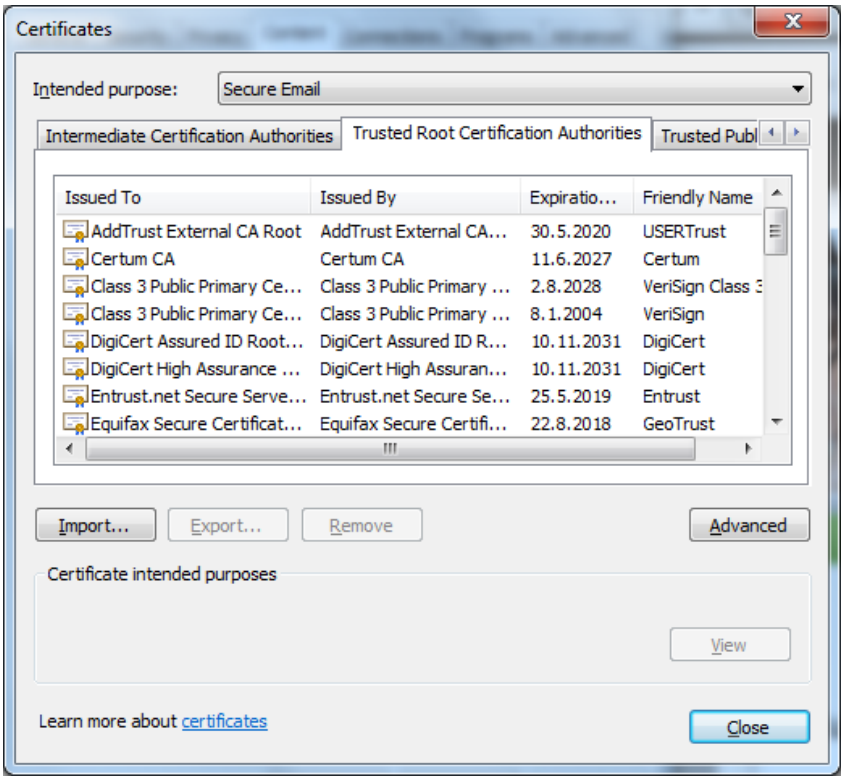
MD5 tuottaa pidemmän tarkisteen (tiivisteen) kuin CRC, joten sitä voidaan käyttää tietomäärissä, joissa kahden identtisen tarkisteen riski on suurempi. MD5 tuottaa 128 bitin pituisen tiivisteen. MD5:stä on kuitenkin löydetty vuonna 2004 kaksi eri lähdemateriaalia, jotka tuottavat saman tiivisteen. Tämä kutsutaan törmäykseksi ja tämän takia MD5:tä pidetään vanhentuneena ja ei-suositeltavana tiivistefunktiona.

SHA-1

SHA-1 on SHA-algoritmin käytetyin versio. SHA-1 on parannettu versio MD5-algoritmista. SHA-1-algoritmi tuottaa 160-bittisen tiivisteen. Myös algoritmin tuottaman tiivisteen ennakoimattomuutta ja tiivisteiden jakaantumista on parannettu. Vaikka algoritmi murrettiin vuonna 2005, se on yhä laajasti käytössä.

1.9 Varmenteet ja ”web of trust”

Varmenteet perustuvat siihen, että luottamusverkostossa on aina myöntäjä, joka toimii ylemmällä tasolla ja on luotettu. Windows–käyttöjärjestelmään on asennettu maailmalla yleisesti luotetuksi tunnettuja varmenteiden myöntäjiä. Tästä käyttöjärjestelmä tietää, että varmentee,t joiden myöntämisketju ulottuu juurisertifikaatteihin, ovat luotettavia. Kuvassa 2 on esitetty Windows-käyttöjärjestelmään asennettuja juurisertifikaatteja, jotka tulevat käyttöjärjestelmän mukana valmiina.



Kuva 2. Windows-käyttöjärjestelmän juurisertifikaatit

1.10 Sähköinen allekirjoitus

Dokumentin sähköinen allekirjoitus perustuu epäsymmetristen avainten kryptografiaan ja tiivistefunktioihin. Dokumentin lähettäjä ottaa dokumentista tiivisteen ja salaa sen omalla yksityisellä avaimellaan. Dokumentin vastaanottaja saa viestin auki lähettäjän julkisella avaimella. Jos hän saa dokumentin auki ja tiiviste täsmää hänen ottamaansa tiivisteeseen,

vastaanottaja voi varmistua sekä viestin kiistämättömyydestä että lähettäjän identiteetistä, koska viestiä ei ole voinut salata kukaan muu kuin yksityisen avaimen haltija.

1.11 PKZIP

ZIP on tiedon pakkaamiseen käytetty työkalu. Pakkaamisella ei tässä yhteydessä tarkoiteta paketoimista (vrt. TCP/IP) vaan tiedon tiivistämistä pienempään tilaan niin, että se saadaan palautettua (purettua) takaisin alkuperäiseen muotoonsa.

ZIP käyttää tiedon pakkamiseen ja purkamiseen DEFLATE-algoritmia. Tiedon eheyden varmistamiseen käytetään CRC-32:tä. Tiedostopaketit voidaan suojata myös salasanalla, mutta tämä ominaisuus tunnetaan olevan suojaukseltaan heikko [7.].

1.12 MySQL

MySQL on relaatiotietokantojen hallintaohjelmisto. MySQL:ää kehittää ruotsalainen MySQL AB. Sun Microsystems osti yrityksen 16. tammikuuta 2008. Tietokantahjelmistoyritys Oracle Corporation osti Sun Microsystemsin huhtikuussa 2009. Tässä yhteydessä MySQL:n omistus siirtyi Oraclelle. MySQL on saatavissa vapaalla GNU GPL (General Public Lisence)-lisenssillä tai kaupallisella lisenssillä, mikäli asiakas ei halua käyttää GPL-lisensoitua ohjelmistoa.

MySQL-tietokanta on erittäin suosittu web-palveluiden tietokantana ilmaisuutensa ansiosta. MySQL-tietokannan päälle rakennettava toiminnallisuus tehdään usein Perl-, PHP- tai Python-ohjelmointikielellä, sivut julkaistaan Apache-webpalvelimella, joka edelleen toimii Linux-käyttöjärjestelmän päällä.[8]

1.13 PHP

PHP (lyhenne sanoista PHP: Hypertext Preprocessor) on ohjelmointikieli, jota käytetään erityisesti Web-palvelinympäristöissä dynaamisten web-sivujen luonnissa. Ohjelmointikielen lisäksi PHP-ympäristössä on laaja luokkakirjasto. PHP on komentosarjakieli, jossa ohjelmakoodi tulkitaan vasta ohjelman suoritusvaiheessa. PHP:tä voidaan käyttää useilla eri alustoilla ja käyttöjärjestelmillä.

PHP:n ensimmäinen versio julkaistiin vuonna 1995, ja nykyisin PHP on vertailuissa johtava dynaamisten web-palveluiden tuottamiseen tarkoitettu kieli.[8]

Syötteen tarkistuksen tarkoituksena on estää sellaisen tiedon välittämisen yritys, joka tahallisesti tai tahattomasti voi vahingoittaa tietoa varastoivaa järjestelmää tai myöntää hyökkääjälle käyttöoikeuksia, joita hänelle ei kuulu. Järjestelmässä, joka tallentaa tietoa tietokantaan, syötteen tarkistus on tärkeää varsinkin, jos tietoa lähettävä ja tallentava järjestelmä ovat etäällä toisistaan. Käytettävällä ohjelmointikielellä ei sinänsä ole väliä. Tässä luvussa on otettu esimerkiksi PHP-kieli siksi, että kyseistä kieltä on käytetty olemassaolevan järjestelmän prototyyppiasteen kehittelyssä eikä syytä tästä toteutustavasta ole syytä muuttaa. Olemassaolevassa järjestelmässä syötteen tarkistukseen tulee kiinnittää lisähuomiota sekä tiedonsiirrossa tapahtuvien virheiden varalta että mahdollisten tahallisten tietoturvahyökkäysten varalta.

Syötteen määrämuotoisuutta tarkistettaessa keskitytään yleensä syötteen pituuteen ja muotoon. Syötteen pituuden tarkistukseen PHP-funktio strlen on toimivin vaihtoehto. Esimerkki funktion käytöstä on koodissa 1.

Koodi 1. Merkkijonon pituuden tarkistaminen

```
<?PHP
$data = ”merkkijono”; // tarkistettava merkkijono
$pituus = 10; // pituus joka merkkijonolla tulisi olla
if(strlen($data) == $pituus) {
jatka(); } // merkkijono läpäisi tarkistuksen
else {
virhe(); } // merkkijono ei ollut halutun pituinen
?>
```

Tarkistettaessa merkkijonon määrämuotoisuutta voidaan tutkia merkkijonon numeraalisuutta is_numeric –funktiolla edellä mainittuun tapaan. Jos määrämuotoisuus vaatii tarkempaa tutkimista (esim. tutkittaessa onko merkkijono säännönmukainen sähköpostiosoite), on syytä käyttää säännöllisiä lausekkeita (engl. regular expressions). Esimerkki säännöllisten lauseiden käytöstä sähköpostiosoitteen oikeellisuuden tarkistamisessa on koodissa 2.

Koodi 2. Merkkijonon säännönmukaisuuden tarkistaminen

```
<?PHP

$saanto = ”\b[A-Z0-9._%-]+@[A-Z0-9.-]+\.[A-Z]{2,4}\b”;

$email = ”testi@osoite.net”;

if(preg_match($saanto,$email)){

jatka(); // sähköpostiosoite täytti säännön ehdot

} else {

virhe(); // sähköpostiosoite oli virheellinen

}
```

TIETOLIIKENNEYHTEYDEN MUODOSTAMISEN VAIHTOEHDOT

Haluttaessa käyttää mobiilia tietoliikenneyhteyttä on muodostettava yhteys valtakunnalliseen matkapuhelinverkkoon. Tämä tapahtuu päätelaitteen välityksellä. Päätelaitteena on perinteisesti käytetty 3G-modeemin sisältävää matkapuhelinta tai ilman puhelinominaisuuksia päätelaitteena toimivaa mobiilimodeemia, ”mokkulaa”. Jälkimmäistä käytettäessä ei kuitenkaan voida käyttää perinteisiä tietoliikennerajapintoja, vaan 3G-yhteyttä käyttävä puhelinverkkoyhteysrajapinta on ohjelmoitava erikseen. On kuitenkin olemassa menetelmiä, joilla yhteyden muodostamista tiedonsiirtoa varten voidaan yksinkertaistaa.

Uusimmissa kännyköissä on ominaisuuksia, jotka mahdollistavat niiden datayhteyden jakamisen joko langattomasti tai langallisesti. Langallinen vaihtoehto tarkoittaa tässä yhteydessä datayhteyttä USB-kaapelin kautta. Normaalitilanteessa internet-yhteyden jakaminen vaatii erillisen ohjelmiston ja monimutkaistaa ohjelmointia, mutta esimerkiksi Samsung Galaxy S 2 –puhelin osaa näyttäytyä siihen liitetylle tietokoneelle tavallisena verkkokorttina, kunhan asianmukaiset ajurit on asennettu. Tämä mahdollistaa sen, että ohjelmoinnissa internet-yhteyttä käytetään kuin laitteisto olisi liitetty internetiin suoraan, ilman 3G–rajapintaa.

Toinen vaihtoehto muodostaa internet-yhteys on tehdä kännykästä WLAN-tukiasema. Tämäkin vaihtoehto mahdollistaa yhdistämisen tietokoneen WLAN-sovittimella langattomaan lähiverkkoon suoraan eikä vaadi monimutkaista rajapintaohjelmointia. Myös tämä ominaisuus löytyy edellä mainitusta kännykkämallista ja monesta muusta uudemmasta kännykkämallista.

Kajaanin ammattikorkeakoulun insinöörikoulutuksen koulutusohjelmat ovat tietotekniikka, rakennustekniikka sekä kone- ja tuotantotekniikka. Tietotekniikan koulutusohjelmassa suuntautuminen ajoneuvojen tietojärjestelmiin tuli mahdolliseksi valita vuonna 2009. Samassa yhteydessä oppilaitos hankki opetuskäyttöön Volkswagen-merkkisen henkilöauton, jonka tietojärjestelmää oli tarkoitus käyttää hyväksi tulevien tietotekniikan insinöörien koulutuksessa. Ajoneuvon tiedonkeruujärjestelmää tutkittiin insinöörien toimesta ja onnistuttiin selvittämään ne käytännöt joilla ajoneuvo välitti keräämäänsä tietoa eteenpäin soveltaviin käyttökohteisiin kuten moottorin ohjaukseen ja mittaristoihin.

1.14 Laitteisto

Esimerkkilaitteistona toimii Sunit Oy:n valmistama ajoneuvotetokone, joka koostuu keskusyksiköstä, kosketusnäytöstä, näppäimistöstä ja osoitinlaitteena toimivasta kosketuslaatasta. Laitteisto on suunniteltu keräämään tietoa ajoneuvon tietojärjestelmästä. Laitteisto ei ole asennettuna ajoneuvoon.

Vastaanottopäässä toimii Dellin valmistama palvelinyksikkö. Palvelimessa on käytetty levyjärjestelmissä RAID-5–varmistustekniikkaa. Palvelimen virransaanti on suojattu UPS-järjestelmän avulla katkottomaksi ja häiriöttömäksi.

1.15 Ohjelmisto

Ohjelmisto koostuu lähetinpään curllib-kirjastoa käyttävästä ohjelmistosta, joka lähettää tietoa siirtoväylän yli. Vastaanottavassa päässä ohjelmisto koostuu Linux-pohjaisesta käyttöjärjestelmästä, WWW-palvelinohjelmistosta, PHP-tulkista, PHP-kielisestä sovelluksesta sekä MySQL-tietokantaohjelmistosta.

1.16 Toiminta

Ajoneuvon tietojärjestelmä kerää lähetettävää tietoa. Tieto pakataan ZIP-paketteihin ja lähetetään HTTPS-yhteyttä hyväksikäyttäen 3G-mobiiliverkon yli palvelimelle. Palvelin on Linux-pohjainen, ja sen päällä toimivat ohjelmistot Apache sekä MySQL, jotka toimivat WWW-palvelimena ja tietokantasovelluksena. Apache-palvelinohjelmiston yhteyteen on asennettu PHP-ohjelmointikielen tulkki, joka mahdollistaa PHP-kielisten sovellusten ajamisen. Palvelimelle on kirjoitettu PHP-kielinen sovellus, joka ottaa vastaan ajoneuvon lähettämät tietopaketit, purkaa ne ja tallentaa vastaanotetut tiedot tietokantaan.

1.17 Kehitystyön tavoite ja tarkoitus

Tavoitteena on parantaa nykyjärjestelmän tietoturvaa. Käsiteltävänä ovat nyt käytössä olevat menetelmät ja tekniikat sekä niiden tietoturvaan liittyvät ominaisuudet. Tietoturvan eri osa-alueita verrataan niihin menetelmiin ja tekniikoihin, jotka on päätetty ottaa käyttöön järjestelmän nykytilaa suunniteltaessa. Käytettävissä olevilla menetelmillä voidaan mahdollisesti parantaa järjestelmän tietoturvaa, mutta voi olla, että työn tilaajan kannalta tietoturvatason kasvattaminen ei ole mielekästä.

JÄRJESTELMÄN RISKIKARTOITUS

Tietojärjestelmään ja tietoturvaan sisältyy aina tiettyjä riskejä. Nämä riskit kannattaa tunnistaa, ja jos mahdollista, ennaltaehkäistä niiden toteutuminen. Jos toteutumista ei voida täysin estää, on syytä suunnitella toipuminen niistä vaikutuksista, joita riski toteutuessaan aikeuttaa.

Riskejä miettiessä on hyvä yrittää ennakoida niitä ympäristöjä ja olosuhteita, joissa ajoneuvo mahdollisesti liikkuu. Toimintasäde voi olla hyvinkin laaja ja kattaa taajamien lisäksi myös syrjäseudut, jonne tiedonsiirtoon käytettävän mobiiliverkon peittoalue ei välttämättä yllä.

Tietoteknisissä laitteissa on aina rikkoutumisen vaara, varsinkin kun on kyse komponenteista, joissa on liikkuvia osia, kuten kiintolevyt ja tuulettimet. Laiterikot aiheuttavat aina keskeytyksiä toimintaan, mutta niihin voidaan varautua tiedostamalla herkimmin rikkoutuvat osat ja hankkimalla etukäteen varaosia, jolloin toimintakatkos saadaan ajallisesti minimoitua. Säännöllisillä varmuuskopioilla estetään tietojen menetys.

Ajoneuvo saattaa liikkuessaan joutua alttiiksi tilanteisiin, joissa on vaara sille, että joku haluaa varastaa auton. Tällainen tilanne on esimerkiksi sellainen, jossa auto jätetään pysäköitynä parkkipaikalle ja jätetään valvomatta. Ensimmäinen askel varkauden estämiseen on olla tekemättä ajoneuvosta kohdetta. Tämä tarkoittaa sitä, ettei autosta tehdä niin erikoisen näköistä, että se herättäisi varkautta suunnittelevan henkilön mielenkiintoa. Ajoneuvon sisältämät erikoiset laitteet kannattaa yrittää peittää niin, etteivät ne ikkunasta sisään katsoessa herätä mielenkiintoa. Jos varkausyritys kuitenkin tapahtuu, tulee autossa olla asianmukaiset hälyttimet. Jos tämäkään ei estä ajoneuvoon sisäänpääsyä, ajoneuvossa tulee olla ajonestojärjestelmä, joka estää auton käynnistymisen ilman auton omaa avainta.

Jos autoon murtaudutaan ja tietojärjestelmiä varastetaan, on huolehdittava siitä, ettei arkaluontoista tietoa joudu vääriin käsiin. Tästä tulisi huolehtia salakirjoitusmekanismien avulla. Ajoneuvoon voidaan myös luoda salakirjoitettu kiintolevyosio TrueCrypt-ohjelmistolla. Tämä estää tehokkaasti luottamuksellisen tiedon hyväksikäytön siinä tapauksessa, että auton tietojärjestelmä joutuu varkauden kohteeksi.

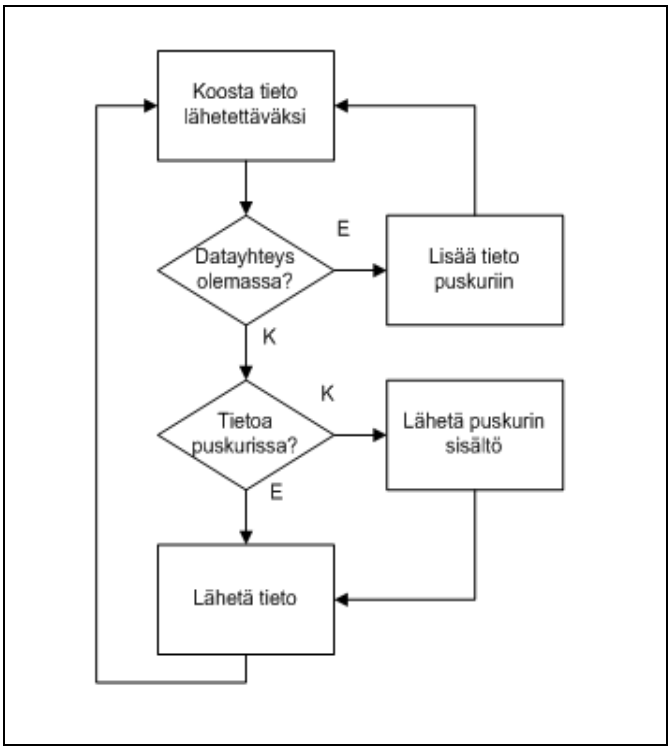
Ajoneuvoon voi kesken ajon iskeä jokin sähköinen vika, joka aiheuttaa ajoneuvossa tulipalon. Tätä varten autossa kannattaa olla jonkinlaista sammutuskalustoa, kuten jauhesammutin. Tarpeeksi ripeällä toiminnalla suuremmat laitevahingot ja tietojen

menettäminen voidaan estää. Auto voidaan tosin sytyttää palamaan myös ilkivaltaisesti. Tällöin auton lähettyvillä ei todennäköisesti ole muita kuin ilkivallan aiheuttaja.

Riskit on lueteltu asianmukaisessa riskianalyysissä liitteessä 1.

1.18 Tiedon lähetys

Jotta kaikki tieto saataisiin lähetetyksi ja talteen, voidaan harkita tiedonlähetysmekanismia, joka on esitetty kuvassa 3.



Kuva 3. Tiedonlähetysmekanismi

Mekanismissa on otettu huomioon tiedonvälityksen katkeaminen. Katkoksen aikana tieto tallennetaan puskuriin. Datayhteyden taas palauduttua puskurin sisältö lähetetään.

Järjestelmän nykytilassa tiedonsiirron katkeaminen on otettu huomioon ja tietoa puskuroidaan katkoksen ajan. Haluttaessa lisäturvaa tiedon saavutettavuuteen voidaan mobiiliyhteys kahdentaa kahden USB-väyliin kytketyn mobiililaitteen avulla.

1.19 Yhteyden osapuolten autentikointi

Yhteyden kummatkin osapuolet voidaan autentikoida varmenteiden avulla. Varmenteille täytyy saada luotettava myöntäjä. Myöntäjäksi voidaan asettaa Kajaanin ammattikorkeakoulu,

jonka juurivarmenne asennetaan sekä lähettävään että vastaanottavaan päähän. Molemmat päät tarkistavat toistensa varmenteet ja voivat varmistua toistensa aitoudesta.

1.20 Tiedon eheyden varmistaminen

Järjestelmän nykytilassa tieto lähetetään ZIP-paketeina. Paketti sisältää itsessään CRC32-tarkistussumman. Purettaessa pakettia purku epäonnistuu, jos tarkistussumma ei täsmää. Tiedon eheys on jo nykytilassaan varmistettu. Jos halutaan lisäturvaa, voidaan järjestelmää kehittää toisella tarkistussummalla tai tiivisteillä.

Ennen tiedon lähettämistä siitä otetaan tiiviste. Tiiviste pakataan mukaan lähetettävään ZIP-pakettiin. Vastaanottopää purkaa paketin, ottaa tiedosta tiivisteen ja vertaa tiivisteitä keskenään. Jos tiivisteet eivät täsmää, pyydetään lähettämään paketti uudestaan ja vastaanotettu paketti hylätään.

1.21 Tiedonsiirtoväylän turvaaminen

Tiedonsiirtoväylä on jo itsessään varsin turvallinen käytettäessä 3G-mobiiliyhteyttä. Jos lisäturvaa kuitenkin kaivataan, lähetettävä paketti voidaan salakirjoittaa vastaanottopään julkisella avaimella. Salakirjoitusalgoritmiksi kannattaa valita AES256 sen turvallisuuden ja tehokkuuden vuoksi. Siirtoväylä voidaan lisäksi suojata VPN-tunneloinnilla, tällöin tunnelien päät muodostuvat palomuureista eivätkä päätelaitteista.

3G-yhteyden katkottomuutta ei voida taata. Yhteyden olemassaolo tuleekin tarkistaa ennen tiedon lähettämistä ja lähettämistä on lykättävä siihen asti, kun yhteys on taas muodostettu. Yhteyden muodostusta odotettaessa kerätty tieto tallennetaan kiintolevylle.

1.22 Varmuuskopiointi

Varmuuskopioinnin keinot ovat tietovarastojen kahdentaminen tai varmuuskopioiden ottaminen ulkoiselle medialle. Tietovarastojen kahdentaminen voidaan toteuttaa fyysisesti kahdentamalla koko tietovarasto, käyttämällä RAID-varmistustekniikoita tai tallentamalla

tieto kahdesti samalle tallennusvälineelle. Yhdistämällä kaksi ensimmäistä saavutetaan usein vähintäänkin riittävä suoja tietojen katoamista vastaan. RAID-5–varmuuskopiointitekniikka ei edellytä kaksinkertaista tallennustilaa, vaan ainoastaan yhden ylimääräisen (mutta vähintään kolme) kiintolevyn.

Ulkoiselle medialle varmuuskopioitaessa on otettava huomioon haluttu tiedon säilyvyyden kesto. Optinen media (CD- ja DVD-levyt) ei kestä säilytystä yhtä hyvin kuin nauhavarmistusaseman nauhat. USB-muistitikkujen tiedon säilyvyydestä ei ole vielä tarpeeksi pitkäaikaista kokemuspohjaa, jotta niitä voitaisiin suositella pitkäaikaiseksi tiedon säilytyspaikaksi. Kaikissa tapauksissa ulkoiselle medialle otettu tieto on säilytettävä mahdollisimman kaukana alkuperäisestä kohteesta sähkö-, palo- ja vesivahinkojen sekä varkauden varalta.

Edellämainittuja varmuuskopiointimenetelmiä ei kannata soveltaa itse ajoneuvossa. Ajoneuvon tietojen varmuuskopionti kannattaa toteuttaa ns. etävarmuuskopiointina, jossa tieto siirretään tietoverkon yli varmuuskopiontipalveluun, joka soveltaa em. tallennuskeinoja.

YHTEENVETO

Tietoturva on ollut käsitteenä olemassa satoja, ellei tuhansia vuosia. Viime vuosikymmeniin saakka tiedon määrä ja asema tuotteena ei ole ollut niin merkityksellinen että tietoturvaan olisi kiinnitetty niin suurta huomiota kuin se nykyaikana vaatii.

Kajaanin ammattikorkeakoulun insinöörikoulutuksen opetusohjelmaan on kuulunut suuntautuminen ajoneuvotietokoneisiin vuodesta 2009 lähtien. Koulutusta varten on hankittu henkilöauto Volkswagen Scirocco, jonka tietoja keräävään järjestelmään on järjestetty mahdollisuus päästä koululla työskentelevien insinöörien toimesta.

Tämän insinöörityön aiheena oli koululle hankitun ajoneuvon tietojärjestelmän tietoturva. Järjestelmän tarkoitus on lähettää mitattua tietoa mobiiliverkon yli koululla sijaitsevalle palvelimelle, joka tallentaa tiedon tietokantaan.

Tässä tössä tutkittiin erilaisia tietoturvamenetelmiä ja pohdittiin niiden soveltuvuutta tiedonsiirron tietoturvan parantamiseksi. Todettiin, että osa olemassaolevista ja käyttöön suunnitelluista menetelmistä tarjosi jo varsin hyvän tietoturvan tiedonsiirtojärjestelmälle, mutta haluttaessa lisäturvaa on tekniikoita olemassa ja saatavilla.

LÄHTEET

1. Tietotekniikan termitalkoot. Julkaistut suositukset. Päivitetty 14.12.2007, luettu 15.4.2011 [WWW-dokumentti]. http://www.tsk.fi/tsk/termitalkoot/fi/haku-266.html

2. Singh, S., Koodikirja : salakirjoituksen historia muinaisesta Egyptistä kvanttikryptografiaan. Helsinki: Tammi 1999. ISBN 951-31-1544-5

3. Rescorla, E. "HTTP over TLS", request for comments –dokumentti, Huhtikuu 2000, luettu 16.4.1011 [WWW-DOKUMENTTI], http://www.ietf.org/rfc/rfc2818.txt

4. SSH, Secure Shell, Wikipedia 16.4.2012, luettu 16.5.2011 [WWW-DOKUMENTTI], http://fi.wikipedia.org/wiki/SSH

5. O'brien, Kevin J., "Cellphone Encryption Code Is Divulged", New York Times, 28.12.2009 [WWW-DOKUMENTTI], http://www.nytimes.com/2009/12/29/technology/29hack.html

6. Perttula, K-P, " Security of Communication Protocols", Helsingin Yliopisto, 15.4.2003 [WWW-DOKUMENTTI], http://www.netlab.tkk.fi/opetus/s38153/k2003/Lectures/g42UMTS_security.pdf

7. ——: .ZIP File Format Specification A , 29.9.2006 PkWare Inc., [WWW-DOKUMENTTI], http://www.pkware.com/documents/APPNOTE/APPNOTE-6.3.0.TXT

8. Heinisuo, Rami. PHP ja MySQL : tietokantapohjaiset verkkopalvelut, 4.painos, Helsinki: Talentum 2007, ISBN 978-952-14-1092-5

LIITTEET

1. Riskianalyysi

RISKIANALYYSI

Riski nro 1	**Tietoliikenneyhteyden katkeaminen**
Todennäköisyys	Erittäin todennäköinen
Seuraus	Toiminnan keskeytyminen. Lähetys palvelimelle katkeaa
Ennaltaehkäisy	Mobiiliyhteyden kahdentaminen
Toipuminen	Kerätään tieto puskuriin ja lähetetään yhdeyden taas muodostuttua
Riski nro 2	**Lähettävän pään laiterikko**
Todennäköisyys	Todennäköinen
Seuraus	Toiminnan keskeytyminen
Ennaltaehkäisy	Komponenttien ja laitteiden laadukkuus hankittaessa. Tietojen varmuuskopiointi
Toipuminen	Korjaus, sisällön palautus varmuuskopioista
Riski nro 3	**Autovarkaus**
Todennäköisyys	Epätodennäköinen
Seuraus	Toiminnan keskeytyminen. Kaluston, ohjelmiston sekä kerätyn tiedon joutuminen vääriin käsiin
Ennaltaehkäisy	Auton murtosuojaus hälyttimineen ja ajonestojärjestelmineen. Kohteen tekeminen epäkiinnostavaksi. Vakuutusten ajan tasalla pitäminen. Luottamuksellisen aineiston salakirjoittaminen. Varmuuskopiointi
Toipuminen	Jos varastettua kaluastoa ei saada takaisin, uuden kaluston hankinta. Laiteasennukset, palautukset varmuuskopioista
Riski nro 4	**Tulipalo**
Todennäköisyys	Pieni
Seuraus	Toiminnan keskeytyminen.

	Laitteistovahinkoja. Tietojen menetys.
Ennaltaehkäisy	Vakuutusten ajan tasalla pitäminen. Sammutusvälineistön sijoittaminen ajoneuvoon. Varmuuskopiointi.
Toipuminen	Kaluston uusiminen. Palautus varmuuskopioista