# Kun televisio vakoilee ja jääkaappiin tehdään tietomurto

Ari Turunen

**Oulun yliopiston tietotekniikan osasto tekee kansainvälisesti merkittävää tutkimusta konenäössä, biosignaalien käsittelyssä sekä tietoturvassa. Tietoturvan merkitys on alkanut korostua entisestään, koska uusia verkkovakoilutapauksia tulee ilmi lähes viikoittain. Verkkovakoilu ja identiteettivarkaudet ovat suuria uhkia, mutta tekniikan kehittyessä on pidettävä huolta myös jääkaapista.**

Puhutaan laitteiden internetistä (*Internet of Things*), jossa laitteet kytkeytyvät tietoverkkoon ja keskustelevat keskenään. Mitä jos et enää pääse vaikuttamaan tähän keskusteluun?

– Verkottuneisuuden leviäminen joka paikkaan, kodinkoneista ajoneuvoihin on tietotekniikan kehityksen seuraava luonnollinen askel, johon mekin paneudumme, toteaa tietoturvatutkija Pekka Pietikäinen.

Kalifornian ja Washingtonin yliopiston tutkijat onnistuivat murtautumaan kahden automerkin hallintajärjestelmiin. He onnistuivat sammuttamaan moottorin ja poistamaan jopa jarrut toiminnasta. Tämä kerrotaan vuoden 2011 tutkimusraportissa, jonka julkaisi Center for Automotive Embedded Systems Security. Koska tulevaisuudessa kaikki kytkeytyy kaikkeen, luo se valtavia tietoturvariskejä.

– Yksityisyys on varsin uhattuna, kun jokapaikan tietotekniikkaa käyttämällä tuotetaan lukuisia määrä näennäisesti harmittomia tiedonpalasisia, joista voidaan yhdistellä varsin kattava kokonaisuus henkilöstä. Turvalliset, mutta täysin anonyymit tavat tunnistautua eri palveluihin ovat tulevaisuudessa tarpeen.

Pietikäinen on ollut kiinnostunut tietoturvaasioista, koska työssä pääsee soveltamaan varsin laaja-alaista osaamista.

– Pitää tietää kaikesta vähän aina rautatasosta ohjelmistokehitysprosesseihin. On kiehtovaa seurata teknologian kehitystä ja pyrkiä ymmärtämään, miten erilaisia järjestelmiä on rakennettu. Se vaatii ajattelua hieman laatikon ulkopuolella, jotta voisi huomata millaisia heikkouksia tietojärjestelmien rakenteessa on. Myös tulosten yhteiskunnallinen vaikutus voi olla merkittävä.

Pietikäisen mukaan suomalaisen tietoturvatasotutkimuksen taso on korkea. Hyvää työtä tehdään tutkimuslaitoksissa, alan yrityksissä ja valtiollisissa toimijoissa, ja yhteistyömahdollisuudet niiden välillä ovat erinomaiset. Yhtenä esimerkkinä on vuonna 2013 päättynyt Digilen ja Tekesin Cloud Software -ohjelma, jonka veturiyrityksenä oli suomalainen tietoturvajätti F-Secure. Ohjelmassa oli oma tietoturvaan erikoistunut kokonaisuus, jota johtivat Suomen Ericsson ja Oulun yliopisto.

Sadat miljoonat ihmiset käyttävät tietämättään pilviteknologiaa hyödyntäviä palveluja verkon yli. Pilviteknologian myötä rajapintojen ja sitä kautta riskitekijöiden määrä lisääntyy. Se asettaa suuret vaatimukset myös tulevaisuuden tietoturvalle. Ongelmana on se, että mahdollisuus tietoturvan räätälöintiin on yleensä pilvipalveluissa vähäinen, eikä käyttäjälle aina anneta takeita tiedon säilyvyydestä tai ohjelmistojen tietoturvasta. Olennaista on, että käyttäjä tietää palvelun olevan turvallinen ja tunnettu sekä käyttäjä todennetaan oikeaksi henkilöksi.

Cloud Software -ohjelman aikana Ericsson ja F-Secure kehittivät omat pilvipalvelunsa. Ericssonin virtuaalinen pilvipalvelualusta on optimoitu televerkkoyritysten kommunikointipalvelujen tarpeisiin. F-Securen pilvipalvelu on

riippumaton laiteympäristöstä ja siinä on mukana mm. virustorjunta. Olennaista molemmille palveluilla on se, että niiden tietoturvaan kiinnitetään paljon huomiota.

– Kansainvälisesti suomalaiset ovat tunnettuja mm. haavoittuvuuksien löytämisessä, haavoittuvuustiedon koordinoinnissa, tietoturvallisuustilannekuvan luomisessa ja haittaohjelmilta suojautumisessa.

Oulun yliopiston tietoturvaryhmä löysi internet-selaimista yli sata haavoittuvuutta alkuvuodesta 2013. Se oli pienimuotoinen sensaatio ja paransi huomattavasti selainten tietoturvaa. Firefox on kokonaan ja Google Chrome enimmäkseen avoimen koodin projekti, jotka käyttävät paljon jaettuja kirjastoja. Tällöin korjatut haavoittuvuudet auttavat yleensä parantamaan tietoturvaa. Suurin osa löydetyistä haavoittuvuuksista on Oulun tietoturvatiimin professori Juha Röningin mukaan epäsuorasti parantanut melkein kaikkien Applen laitteiden, Android-puhelinten ja älytelevisioiden turvallisuutta.

Kaikki haavoittuvuudet raportoitiin valmistajille, jotta ne korjattiin mahdollisimman nopeasti. Haavoittuvuuksia löytyi myös antivirusohjelmista ja paljon käytetyistä kuva- ja ääniformaateista.

– Selaintestaus pohjautuu työhömme protokollatestauksen parissa, Pietikäinen kertoo.

Oulun yliopisto aloitti vuosituhannen vaihteesta PROTOS-nimisen projektin, jonka pohjalta tutkimusryhmä sai uutta osaamista haavoittuvuuksien syvimmästä olemuksesta, automaattisesta tiedon rakenteen päättelystä ja mahdollisimman hyvien testitapausten luomisesta.

–Työssämme sovellamme esim. tietojenkäsittelyteorian ja bioinformatiikan perustutkimusta erittäin käytännöllisten lopputulosten, turvallisten ohjelmistojen, aikaansaamiseksi.

Pietikäinen korostaa, että tietoturvaan ei riitä yksi työkalu tai ohjelma. Eri työkaluja pitää koko ajan kehittää ja käyttää samanaikaisesti.

– Tietoturva ei saa olla jälkikäteen ohjelmistoon liitettävä kilke, vaan se tulee ottaa huomioon koko ohjelmistokehityksen elinkaaren ajan. Ryhmämme lähtökohtana on, että turvallisuus täytyy rakentaa ohjelmistoihin sisään, millään erityisellä tietoturvaohjelmalla sitä ei saada aikaan. Niinpä tuotamme työkaluja, joilla olemassa olevien ohjelmistojen turvallisuutta voidaan parantaa tai niiden toimintaa ymmärtää paremmin.

Yksi sellainen on Radamsa, jolla pystyttiin tunnistamaan lukuisat haavoittuvuudet internet-selaimissa. Oulun yliopiston kehittelemä Radamsa on tehokas ja automatisoitu työkalupakki tietoturva-asiantuntijoille. Avoimeen lähdekoodiin perustuvaan sovellukseen on koottu parhaita ominaisuuksia aiemmin kehitellyistä automatisoiduista tietoturvan testaustyökaluista. Yrityspartnereina ovat olleet Ericsson, Nokia, F-Secure, Google, Mozilla Foundation ja WebKit.org. Radamsa tarjoaa apua tietoturvakehitystyön testaukseen. Sen avulla voi testata ohjelman kykyä toimia ja sietää vihamielisiä syötteitä. Pietikäisen mukaan avainsana on järjestelmällisyys. Tietoturvaa tarkastellaan koko ohjelmistokehityksen elinkaaren ajan, niin että se on mukana jo vaatimusmäärittelyssä. Aina kun pätkä koodia valmistuu, se testataan automaattisesti.

Pietikäisen mielestä Radamsa on työkaluna ainutlaatuinen.

– Vastaavien työkalujen käyttö vaatii usein huomattavan määrän työtä, tai työkalut ovat ”liian yksinkertaisia” ollakseen tehokkaita. Radamsa on suunniteltu olemaan helppokäyttöinen, mutta silti erittäin tehokas.

Pietikäisen mielestä olennaista on luoda tietoturvallisuudesta tilannekuva, analysoida se ja päättää minkälaisia välineitä käytetään. Pietikäisen mukaan toinen esimerkki suomalaisesta innovaatiosta tietoturvan parantajana on Kyberturvallisuuskeskuksen (entinen CERT-FI) HAVARO-järjestelmä.

Viestintäviraston ja Huoltovarmuuskeskuksen kanssa toteutetun järjestelmän tuottaman tiedon avulla pyritään havaitsemaan tietoturvauhat mahdollisimman varhain. Näin suojaus voidaan aloittaa ajoissa. Yritykset voivat liittyä mukaan, jolloin ne voivat tarkkailla oman sisäverkkonsa tilannetta. HAVARO tunnistaa poikkeavaa verkkoliikennettä, joka on lähtöi-

sin yrityksen verkosta ja suuntautuu siihen. Osa havainnoista saadaan Viestintäviraston CERTFI:n yhteistyöverkoston kautta.

Oulun yliopistosta on syntynyt myös tietoturvaloukkaustietoon erikoistunut firma Clarified Networks. Toimintaan kuuluu tiedon kerääminen, analysointi, visualisointi ja raportointi.

– Suomi on haittaohjelmatilastoissa pärjännyt erinomaisesti ja mallimme on vähitellen siirtynyt käyttöön muuallakin, kuten Virossa, Belgiassa ja Islannissa. Erityisesti Autoreporter ja HAVARO ovat herättäneet kiinnostusta kansainvälisesti ja ennen kaikkea toimintatavat, jossa vähillä resursseilla ja sopivilla työkaluilla saadaan mahdollisimman paljon aikaan.

Tästäkin huolimatta Pietikäisen mielestä suurimmat tietoturvauhat suomalaisissa yrityksissä ovat haittaohjelmat eri muodoissa.

– Haittaohjelmat tulevat taloon esim. sähköpostista, webistä tai muistitikulta, ja niiden monimuotoisuus on nykyisin valtava. Myös työntekijöiden älypuhelimet ovat houkuttelevia kohde hyökkäyksille. Liiketoiminnan jatkuvuuden varmistaminenkin pitäisi muistaa, pilviaikakautenakin. Miten kommunikoidaan, jos ulkoistettu sähköposti on nurin koko päivän? Kuinka nopeasti palvelut pystyttäisiin siirtämään toiselle palveluntarjoajalle ja mistä ne varmuuskopiot lopulta löytyvät?

## Opas tietoturvasta

Pietikäinen toimitti yhdessä Juha Röhningin kanssa opaskirjan tietoturvasta. Se julkaistiin viime tammikuussa ja se kokoaa Cloud Software -ohjelman kokemukset tietoturvan parantamiseksi. Kirjassa esitellään lyhyiden artikkeleiden muodossa parhaiksi osoittautuneita käytäntöjä turvallisuuden ja yksityisyyden suojan varmistamiseen ketterissä ohjelmistoprojekteissa. Lisäksi annetaan neuvoja ohjelmistojen toimintavarmuuden testaukseen, turvallisuusmetriikoihin ja luottamuksen hallintaan.

– Tutkimusprojektien tulokset jäävät usein vaikeasti lähestyttäviksi akateemisiksi julkaisuiksi ja yritysten sisäiseksi osaamiseksi. Cloud Software -ohjelmassa halusimme tuoda tulokset helposti lähestyttävässä muodossa laajemmalle yleisölle (esim. PK-yritykset), ja niinpä kokosimme työstämme *Handbook of the Secure Agile Software Development Life Cycle* -kirjan.

Voisiko Suomesta tulla tietoturvan Sveitsi? Maa, johon kannattaa tallentaa dataa?

– Ei se mahdotonta ole, yhteiskuntamme on vakaa, osaamispohja erinomainen ja sijaitsemme edelleen lännen ja idän välissä.

## Kirjallisuutta


PROTOS-projekti: https://www.ee.oulu.fi/research/ouspg
PROTOS ja media esim.: http://www.computerworld.com/s/article/68932/SNMP_Vulnerability_Offers_3_200_Reasons_to_Worry
Haittaohjelmatilasto: http://www.f-secure.com/weblog/archives/00001806.html
http://www.autosec.org/publications.html
https://www.ee.oulu.fi/research/ouspg/Radamsa



**Kirjoittaja on tiedetoimittaja ja tietokirjailija.**