Lääketieteellisten tuotteiden kyberturvan arviointi: Haasteet ja ratkaisut

Rauli Kaksonen

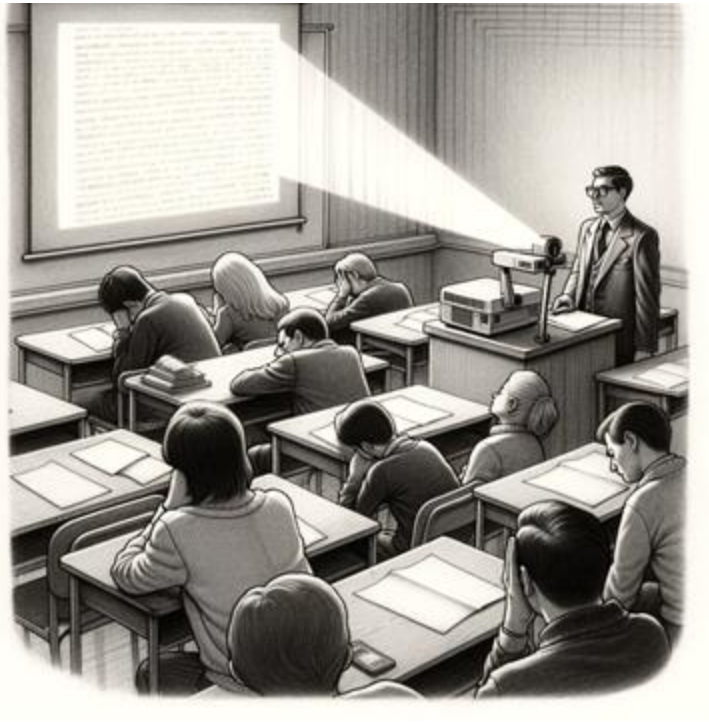
UNIVERSITY OF OULU

Puhuja

- **Rauli Kaksonen, Tek. lis.**
- **Oulu university, OUSPG**
- **Väitöskirjatutkija**
  - "Transparent and *tool-driven security assessment for sustainable IoT security*"
- **Työhistoria:**
  - Oulun yliopisto, erityisasiantuntija, tietoturva
  - Synopsys, Group director
  - Codenomicon, Teknologiajohtaja, perustaja
  - VTT, Tutkija
- **rauli.kaksonen@oulu.fi**

Esityksen sisältö

1. Tietoturva, kyberturva
2. Haavoittuvuudet
3. Tietoturvallisuuden arviointi
4. Standardit ja regulaatio
5. Yhteenveto



Mitä ~~tietoturva~~ on?
kyberturva

- **Tietoturvalle on monia määritelmiä**
- **Paljon käytetty on ns. "CIA" malli**
  - Tietoturvallinen järjestelmä säilyttää C-I-A ominaisuudet
  - C = Confidentiality eli luottamuksellisuus
  - I = Integrity eli eheys
  - A = Availability eli saatavuus
- **Tai yksinkertaisesti**
  - Tietoturvallisuus on sitä että järjestelmää käytetään ainoastaan sen käyttäjien ja muiden sidosryhmien eduksi
  - …eikä ainakaan heidän vahingokseen

Lääketieteen tekniikka ja tietoturva

- **Lääketieteen alalla korostuvat:**
  - Turvallisuus (eng. *safety*), viat ja ongelmat voivat johtaa vammoihin tai pahempaan
  - Yksityisen tiedon suojaus
  - Helppokäyttöisyys, käyttäjät eivät ole IT-alan ihmisiä
  - Yhteistoiminta, tiedon pitäisi kulkea järjestelmien välillä
- **Mutta samat tekniset ratkaisut toimivat eri aloilla**

Tietoturvan puutteen seurauksia

- **Vastaamo 2020**
- **Helsingin kaupunki 2024**
- **Lockbit-kiristyshaittaohjelma Saksassa 2023**
- **Jne.**

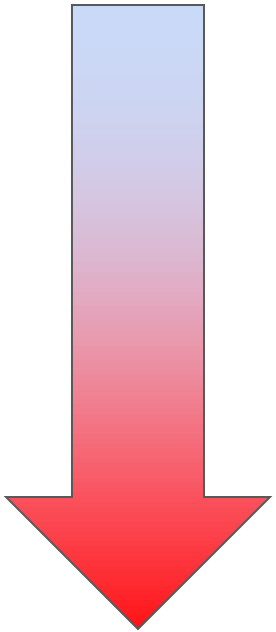
> *"From 2016 to 2021, we estimate that ransomware attacks killed between 42 and 67 Medicare patients." — McGlave, Neprash, and Nikpay; University of Minnesota School of Public Health*[1]

https://www.emsisoft.com/en/blog/44987/the-state-of-ransomware-in-the-u-s-report-and-statistics-2023/

Tietoruutu: "Ransu"

- **Kirityshaittaohjelmat (*ransomware eli ransut*) ovat haitallisimpia tai ainakin näkyvimpiä ongelmia tällä hetkellä**
- **Kiristyshyökkäyksen vaiheet**
  - Tietomurto, esim. sähköpostin välityksellä
  - Hyökkääjän oikeuksien korotus järjestelmän haavoittuvuuksien avulla
  - Kiristyshaittaohjelman suoritus, tiedot salataan ja/tai varastetaan
  - Vaatimusten esittäminen
  - Toipuminen; järjestelmän palautus / lunnaiden maksu
- **Järjestelmien tietoturva osaltaan vaikuttaa haittaohjelmien leviämiseen**

Termistöä



Tietoturva

- Järjestelmä on suojassa

Heikkous

- Heikko kohta joka voi ehkä mahdollistaa hyökkäyksen

Haavoittuvaisuus

- Ominaisuus jolla järjestelmän voi murtaa

Hyväksikäyttö

- Haavoittuvuuden avulla suoritettu hyökkäys

Tietomurto

- Tietoturva on menetetty

Missä tietoturva-aukot ovat?

Yrityksen tai organisaation järjestelmissä (tai prosesseissa)

Käytetyssä IT-tuotteessa

- ***Tässä esityksessä keskitytään tähän kategoriaan***

Yhteistyökumppanilla

Hyökkäysrajapinnat

Hyökkäysrajapinta on kohta jossa ulkopuolinen hyökkääjä pääsee käsiksi järjestelmän sisäosiin

- Internet
- Langattomat verkot
- Yritys- ja kotiverkot
- Pilvipalvelut ja muut ulkopuoliset palvelut
- Sähköposti
- Tekstiviestit
- Fyysisten laitteiden verkkoliittymät sekä USB ja muut portit
- Tekoälymallit, esim. opetusdata
- Ihmiset

Salaus- ja tunnistusmekanismit

IT-tuotteet siirtävät usein tietoa epäluotettavien verkkojen yli

- **Esim. internet, langaton verkko, sisäverkko**
- **Suojattujen verkkojen käyttö on liian kallista ja mahdollista vain erityssovelluksissa, esim. sotilaskäyttö**

Tämä luo ongelmia:

- **Osapuolet tulee tunnistaa eli autentikoida**
- **Tieto tulee suojata, esimerkiksi salaamalla**
- **Pitää sietää tilannetta jossa tieto ei kulje**
  - Pitää sietää palvelunestohyökkäyksiä

Vanhat ja haavoittuvat ohjelmistot

Ohjelmistoissa on "parasta ennen" aika

- **Tietoturva-ala kehittyy ja vanhat ratkaisut eivät enään anna riittävää suojaa**
- **Tietoturva-aukkoja löydetään ja ohjelmistoista pitää päivittää turvallisiin versioihin**

Vanhat ja haavoittuvat ohjelmistokomponentit ovat yksi keskeisimmistä syistä tietomurtoihin

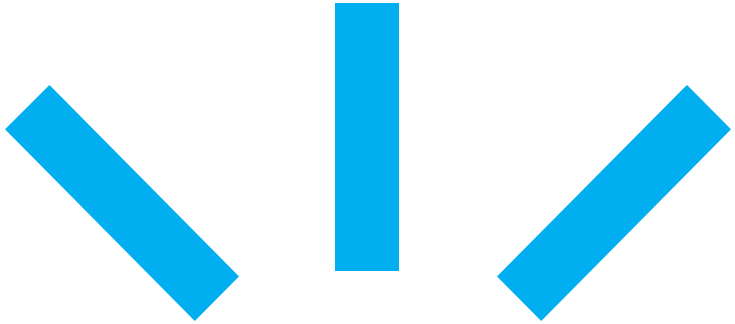
Yksityinen tieto tietoturvaongelmana

Tietojärjestelmien keräämä yksityinen tieto on osaltaan tietoturvaongelma

- **Vaikka kerääjä itse olisi vastuullinen ja huolellinen**

Ongelma on että tieto välitetään tai vuotaa eteenpäin

- **Alkuperäinen tiedon luovuttaja menettää kontrollin tietoonsa**
- **Tietoa voidaa käyttää väärin**



IT-tuotteiden tietoturvan tason nostaminen

Kyberturvallisen tuotteen kehittäminen

"On vain kaksi tapaa kehittää tietoturvaa, oikea ja väärä"

- **Oikea tapa on rakentaa tietoturva mukaan tuotteeseen**
  - Tunnistetaan riskit jo suunnitteluvaiheessa
  - Valitaan sopivat tietoturvamekanismit
  - Toteutetaan tietoturvaominaisuudet tuotetta kehitettäessä
  - Koulutetaan niin kehittäjät kuin käyttäjätkin
  - Testataan tietoturvaominaisuudet muun testauksen ohessa
  - Rakennetaan **prosessi** tietoturvalliselle toiminnalle ja poikkeustilanteiden käsittelylle
- **Väärä tapa**
  - Mietitään tietoturvaa vasta kun pitäisi saada sertifiointi tai joudutaan vastaamaan asiakkaan kysymyksiin
  - Reagoidaan tietoturvaongelmaan korjaamalla (vain) ongelmakohta
  - Kohdellaan tietoturvaa lisäosana

Tietoturvan arviointi

- **Itsearviointi on osa tuotekehitystä**
  - Lähtökohta on että valmistaja arvioi tuotteensa turvallisuutta joka vaiheessa
- **Valmistajasta riippumaton tietoturvan arviointi on välttämätön**
  - Saatetaan valmistajat samalle viivalle
  - Nostetaan tietoturvan tasoa
- **Arviointi voidaan tehdä eri vaiheissa**
  - Suunnittelu- tai tarjouskilpailuvaiheessa
  - Tuotteen kehityksen aikana
  - Valmista järjestelmää tutkimalla ja muita tietolähteitä seuraamalla
- **Arvoinnin tulisi jatkua koko tuotteen elinkaaren ajan**
  - Tuotteen päivitykset voivat vaikuttaa tietoturvaan
  - Löydetyt tietoturvaongelmat pitää korjata
  - Tietoturvatilanne muuttuu eikä aiemmin riittävä suojaus päde loputtomiin

Kuka arvioinnin tekee?

- **Itsearviointi**
  - Valmistaja itse tietoturvansa arvioi jonkin arviointikehikon pohjalta
  - Helppo suorittaa koska tiedon ei tarvitse liikkua
  - Tuloksiin pitää suhtautua varauksella
- **Asiakkaan suorittava arviointi**
  - Tuotteen asiakas arvioi riittääkö tietoturva
  - Voidaan keskittyä juuri asiakkaan käyttämiin ominaisuuksiin
    - JOS että muut ominaisuudet ovat "pois päältä" eivätkä osa hyökkäysrajapintaa
  - Haastellista, vaatii osaamista ja valmistajan pitää toimittaa riittävästi tietoa
- **"Kolmas" osapuoli**
  - Ulkopuolinen tietoturvan arviointi (ei itsearviointi eikä asiakas)
  - Osaamista helpompi löytää, mutta edelleen valmistajan pitää antaa tietoa
  - Kallista tai pintapuolista
  - Ei välttämättä vastaa asiakkaan käyttöä

Haavoittuksien etsimistä vai testausta?

- **Usein tietoturvatestaus mielletään vain *haavoittuvuuksien* etsimiseksi**
  - Valitettavasti (?) haavoittuvuuksia on vaikea löytää
  - Iso osa jää yleensä aluksi löytymättä
  - Löydöksien puute tulkitaan turvallisuudeksi vaikka testaus on vain tehotonta
- **Tehokkaampaa on varmistaa että tuote käyttää tietoturvallisia ratkaisuja ja on laadukas**
  - Eli etsitään järjestelmästä **heikkouksia**
  - Tehokkaampaa kun tuote on *testattava* ja hyvin dokumentoitu
- **Ongelma on usein valmistajien asenne**
  - "Älä korjaa jos ei ole rikki"
  - Resurssien säästämisen nimissä puututaan vain haavoittuvuuksiin vaikka turvallisuuden vuoksi olisi parempi poistaa jo heikkouksia

Tietoturvastan-dardit ja -ohjeet

Laitteiden tietoturvaongelmat on laajalti tunnistettu

Tämä on johtanut suureen määrään erilaisia

- **Tietoturvaohjeistuksia, esim.**
  - Traficom "*Sosiaali- ja terveydenhuollon hankintojen tietoturva- ja tietosuojavaatimukset*"
- **Tietoturvastandardeja**
  - Erilaiset ISO-standardit, IEC 62304, …
- **Lakeja ja määräyksiä**
  - Medical Device Regulation (MDR)
  - Cyber Resilience Act (CRA)
  - Kanta-liitynnän tietoturvavaatimukset

Tietoturvavaatimukset

- **Tietoturvavaatimusten, -ohjeiden, ja -määräysten vertailu[2] osoittaa että ylätasolla vallitsee konsensus toimenpiteistä:**
  - Tuotteen tietoturva-arkkitehtuuri on määriteltävä
  - Hyökkäysrajapinta pitää vahvistaa
  - Dataa pitää suojata
  - Käyttäjät ja komponentit pitää tunnistaa
  - Järjestelmää pitää voida päivittää
  - Yksityistä tietoa on käsiteltävä vastuullisesti
- **Vaatimukset pyrkivät poistamaan järjestelmien heikkouksia**
  - Käytännön tietoturvatyö edelleen usein keskittyy haavoittuvuuksien etsimiseen
- **Valitettavasti vaatimusten yksityiskohdat vaihtelevat eri lähteiden välillä**
  - Valmistajalle on työlästä noudattaa useampaa standardia tai ohjetta
  - Vaatimusten harmonisointi olisi toivottavaa

Oma tutkimukseni

Esineiden internetin (*Internet of Things, IoT*) tietoturva

- **IoT tietoturvavaatimukset**
- **Haavoittuvuudet**
- **Työkalupohjainen tietoturvatestaus**

Väitöskirjatutkimus

- **IoT tuotteen tietoturvan kuvaus (*security statement*)**
- **Kuvauksen tarkistus automaattisesti tietoturvatyökaluilla**
  - Itsearviointina
  - Asiakkaan toimesta
  - Kolmannen osapuolen arviointina
- **Kuvauksen käyttö riskiarvioihin ja sertifiointeihin**

Tuloksia:

- **IoT tietoturvaa voidaan mitata automaattisesti**
  - Valmistajan on kuvattava järjestelmän ominaisuudet
  - Kattavuus on 80% vaatimuksista, jotka valitaan tehokkuuden mukaan
- **Tietoturvastandardien täyttämistä voidaan mitata osittain**
  - Kattavuus laskee, koska vaatimukset eivät sovellu automaatiolle
  - Koejärjestelmässä toteutettiin 45% kattavuus tietoturvaa suoraa mittaaville testeille
- **Automaatiolla voidaan nostaa IoT tietoturvan tasoa koko elinkaaren ajalta**

Yhteenveto

- Tietoturvan puute aiheuttaa taloudellisia tappioita ja inhimillisiä kärsimystä
- Tietoturvaongelmia esiintyy IT-tuotteiden eri osissa
- Valmistajien tulisi ottaa tietoturva huomioon tuotekehityksen joka vaiheessa
- Tietoturvan taso on arvioitava riippumattomasti ja kattavasti, jotta paine tehdä turvallisia tuotteita on riittävä
- Eri tahot ovat luoneet kirjavan joukon standardeja ja määräyksiä
- Huomio pitäisi kiinnittää heikkouksien poistamiseen koska haavoittuvuuksia on vaikea löytää ennen julkaisua

Väitöskirjani osajulkaisut

1. Kaksonen, R., Järvenpää, T., Pajukangas, J., Mahalean, M., & Röning, J. (2021). "100 Popular Open-Source Infosec Tools", IFIP.
2. Kaksonen, R., Halunen, K., & Röning, J. (2022). "Common Cybersecurity Requirements in IoT Standards, Best Practices, and Guidelines", IoTBDS
3. Kaksonen, R., Halunen, K., & Röning, J. (2023). "Vulnerabilities in IoT Devices, Backends, Applications, and Components", ICISSP.
4. Kaksonen, R., Halunen, K., Laakso, M., & Röning, J. (2023). "Transparent Security Method for Automating IoT Security Assessments", ISPEC
5. Kaksonen, R., Halunen, K., Laakso, M., & Röning, J. (2024). "Automating IoT Security Standard Testing by Common Security Tools", ICISSP