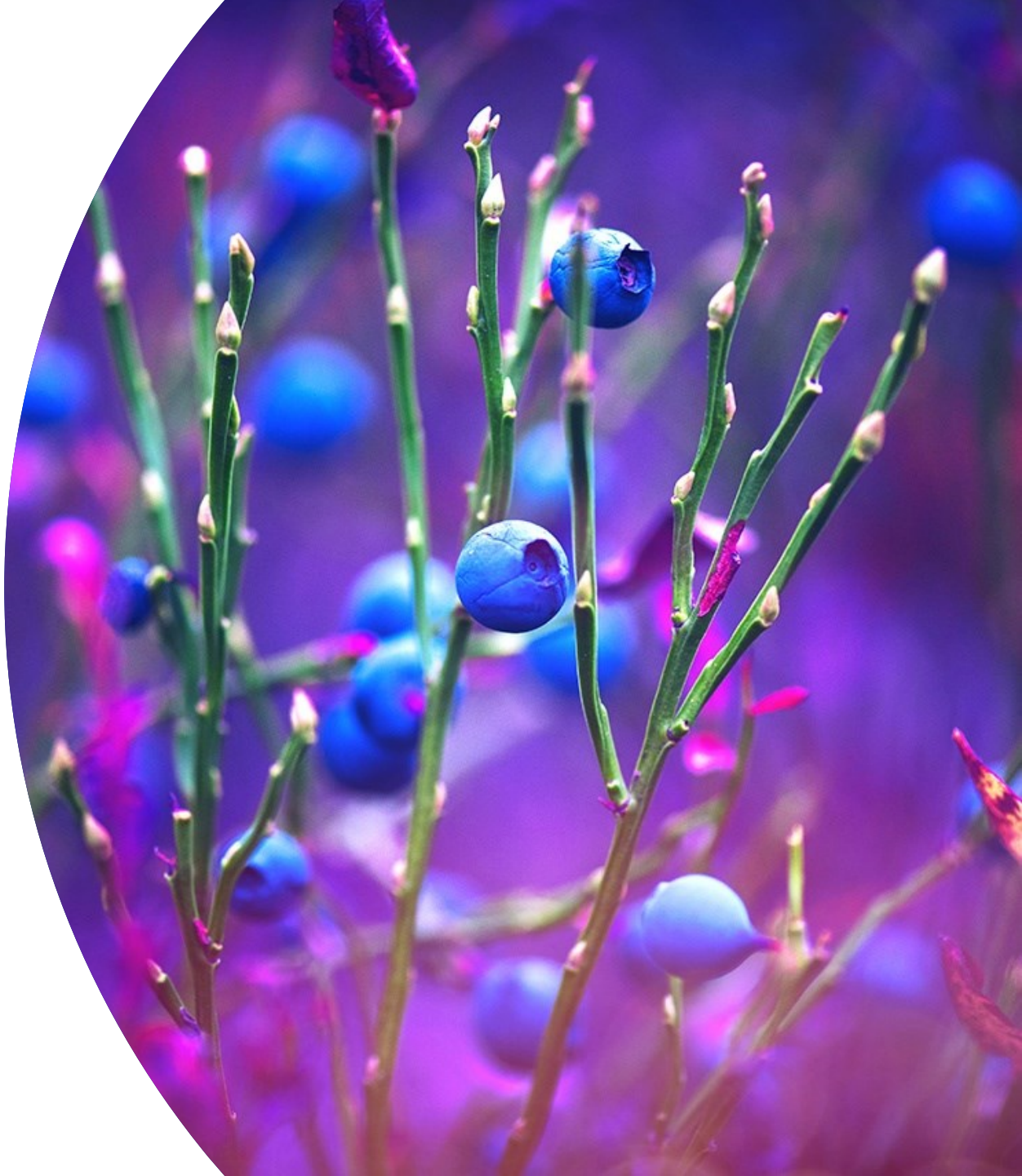
TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Tulevaisuuden tietoturvallinen ohjelmistokehitys

Jussi Eronen



Tulevaisuuden visio

- Suomalainen ohjelmistoteollisuus erottuu laadulla
  - Turvallisuus ⇔ laatu
- Yritykset ymmärtävät vastuunsa tietoturvan toteuttamisesta
  - Turvallinen ohjelmistokehitys on itsestäänselvyys
- Tietoturvan toteuttaminen on helppoa

Sisältö

Nykytila

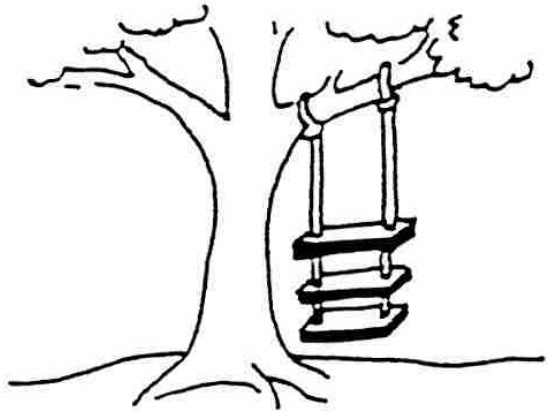
Ohjelmistotuotannon monet muodot

Turvallisen ohjelmistotuotannon kulmakiviä

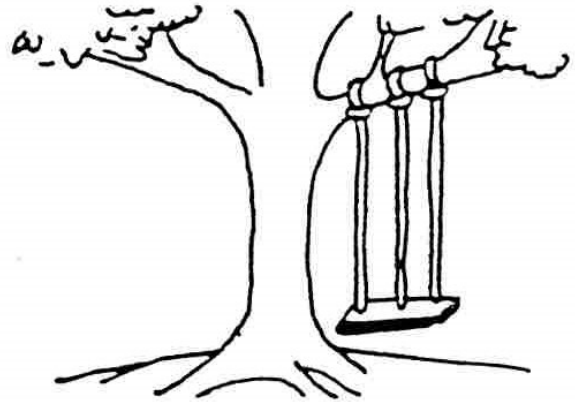
Tulevaisuudesta

Ohjelmistoturvallisuuden nykytila

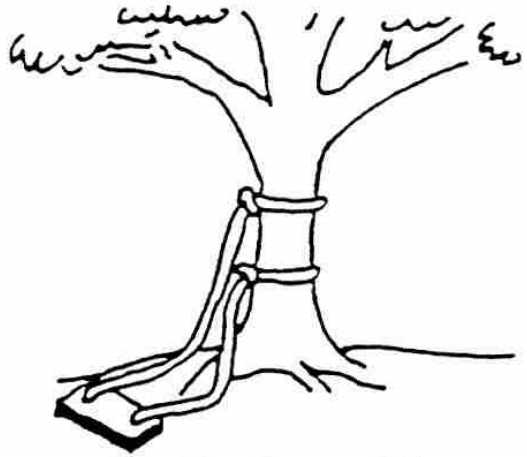
- Ala on jatkuvassa muutoksessa ja muutosnopeus on valtava.
- Turvallisuuden taso on noussut, mutta teknologia muuttuu nopeasti.
- Osaaminen on polarisoitunut.
- Tietoisuus ohjelmistoturvallisuuden merkityksestä on kasvanut.
- Asiakkaat ja yritysjohto ovat alkaneet vaatia ohjelmistoturvallisuutta.
- Kaikki eivät osaa vaatia.



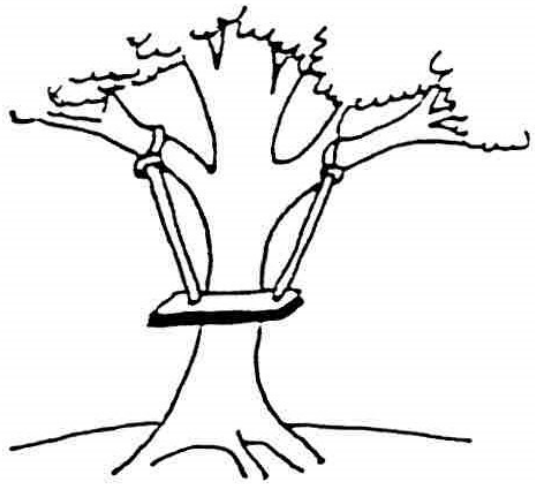
As proposed by the project sponsors



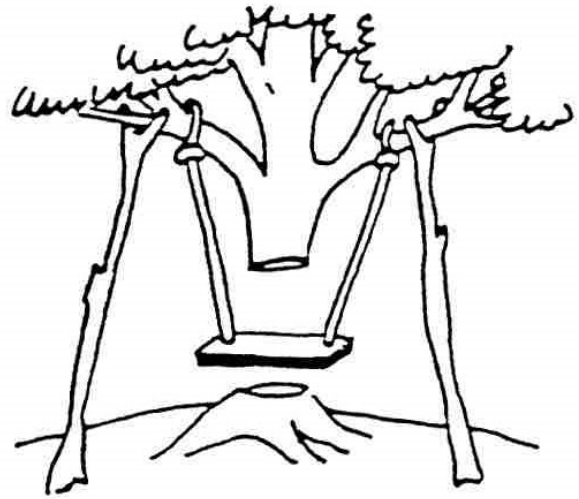
As specified in the project request



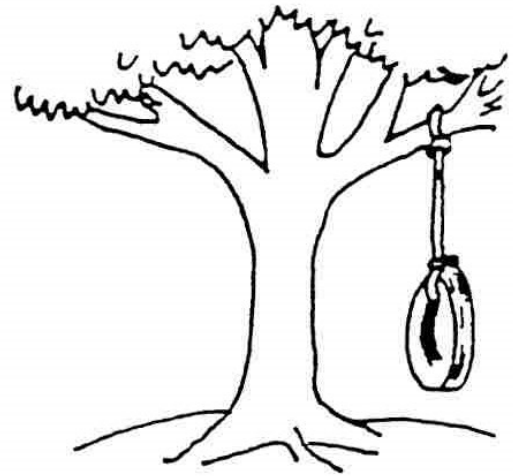
As designed by the senior analyst



As produced by the programmers

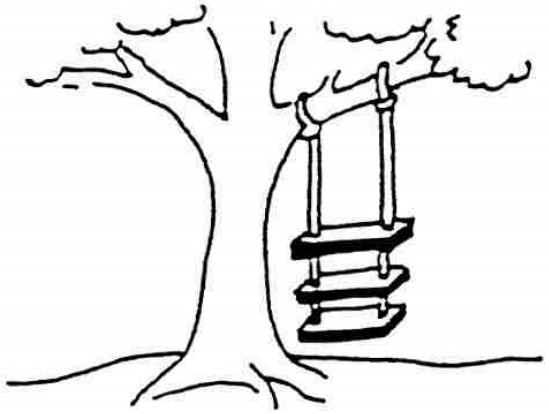


As installed at the user's site

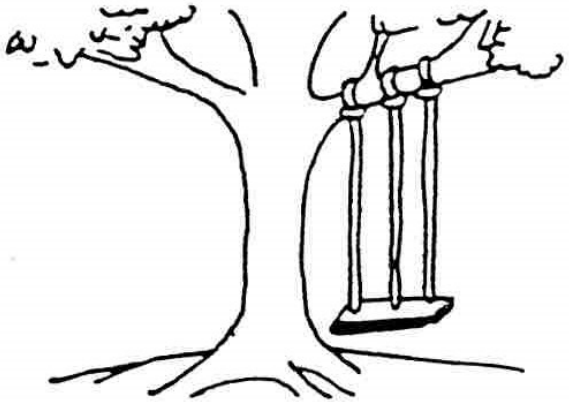


What the user wanted

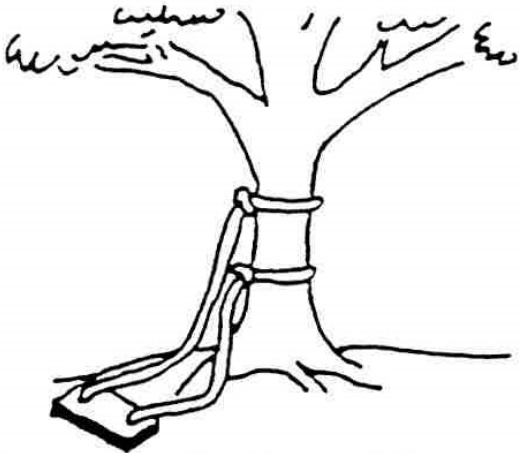
Tree Swing graphic by S Høgh 1993 - from Businessballs.com/treeswing.htm 2013



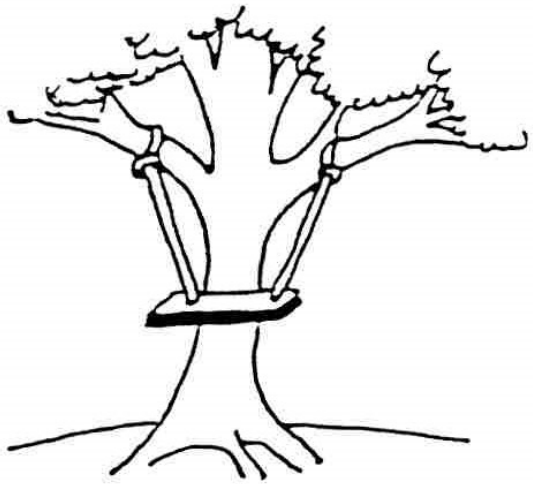
Virallinen projektiohjeistus



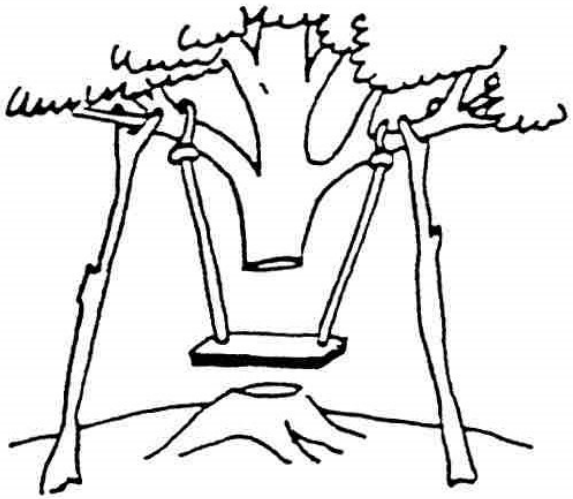
Hankittu räätälöity järjestelmä



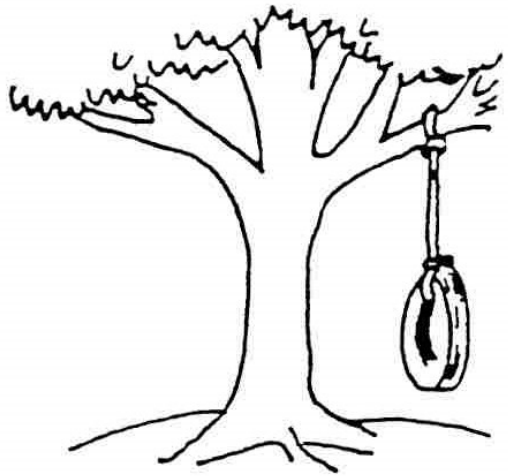
Hankittu valmisjärjestelmä



Alihankinta



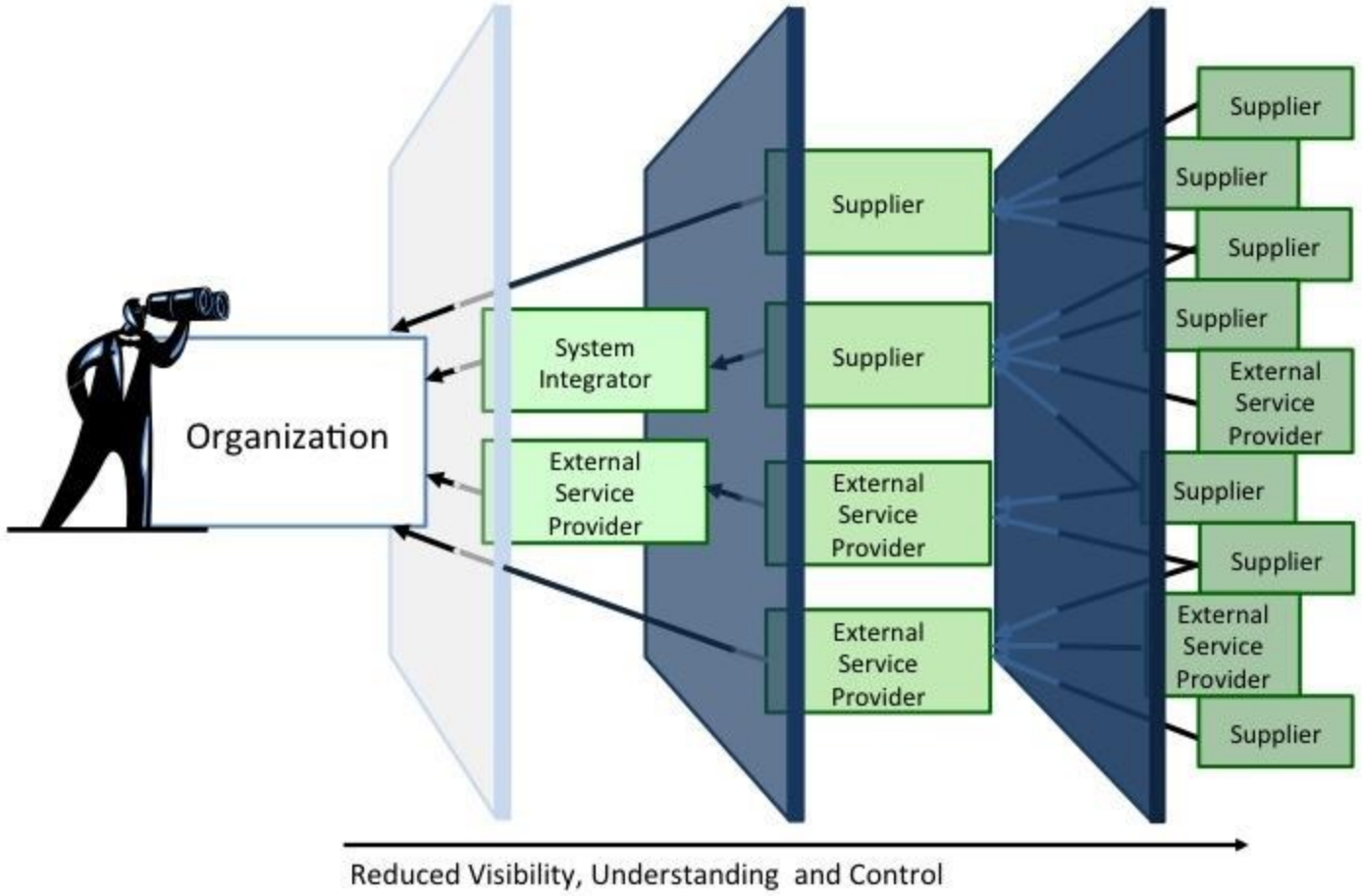
Oma skriptaus



Tavoitetila

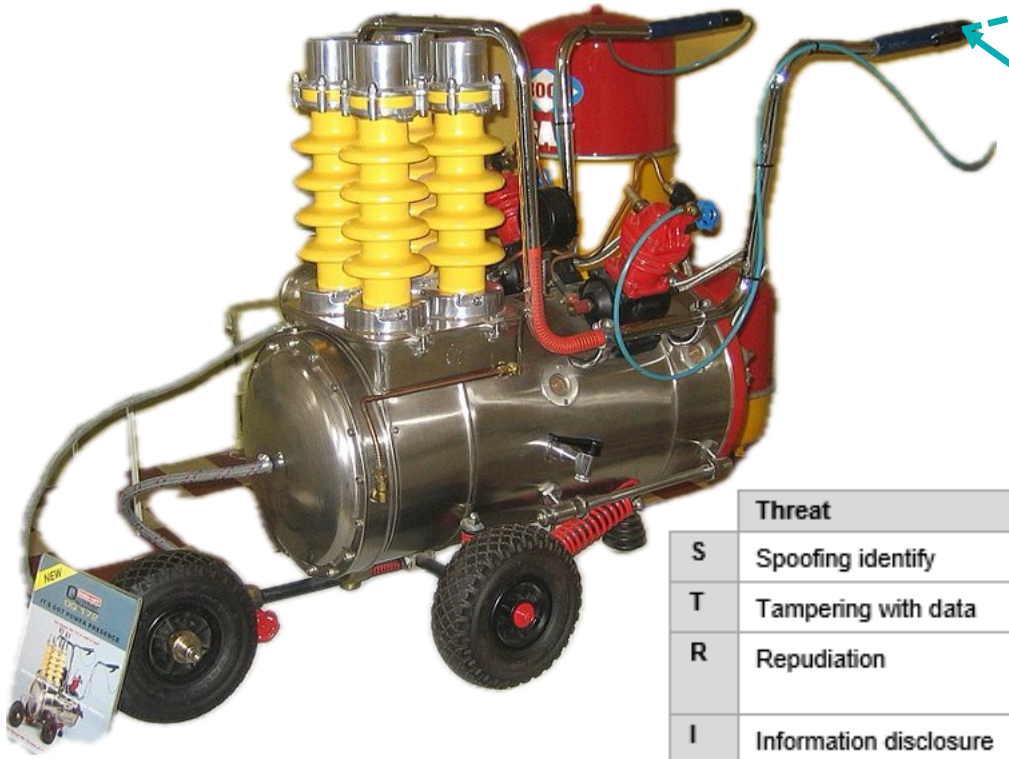
Tree Swing graphic by S Høgh 1993 - from Businessballs.com/treeswing.htm 2013

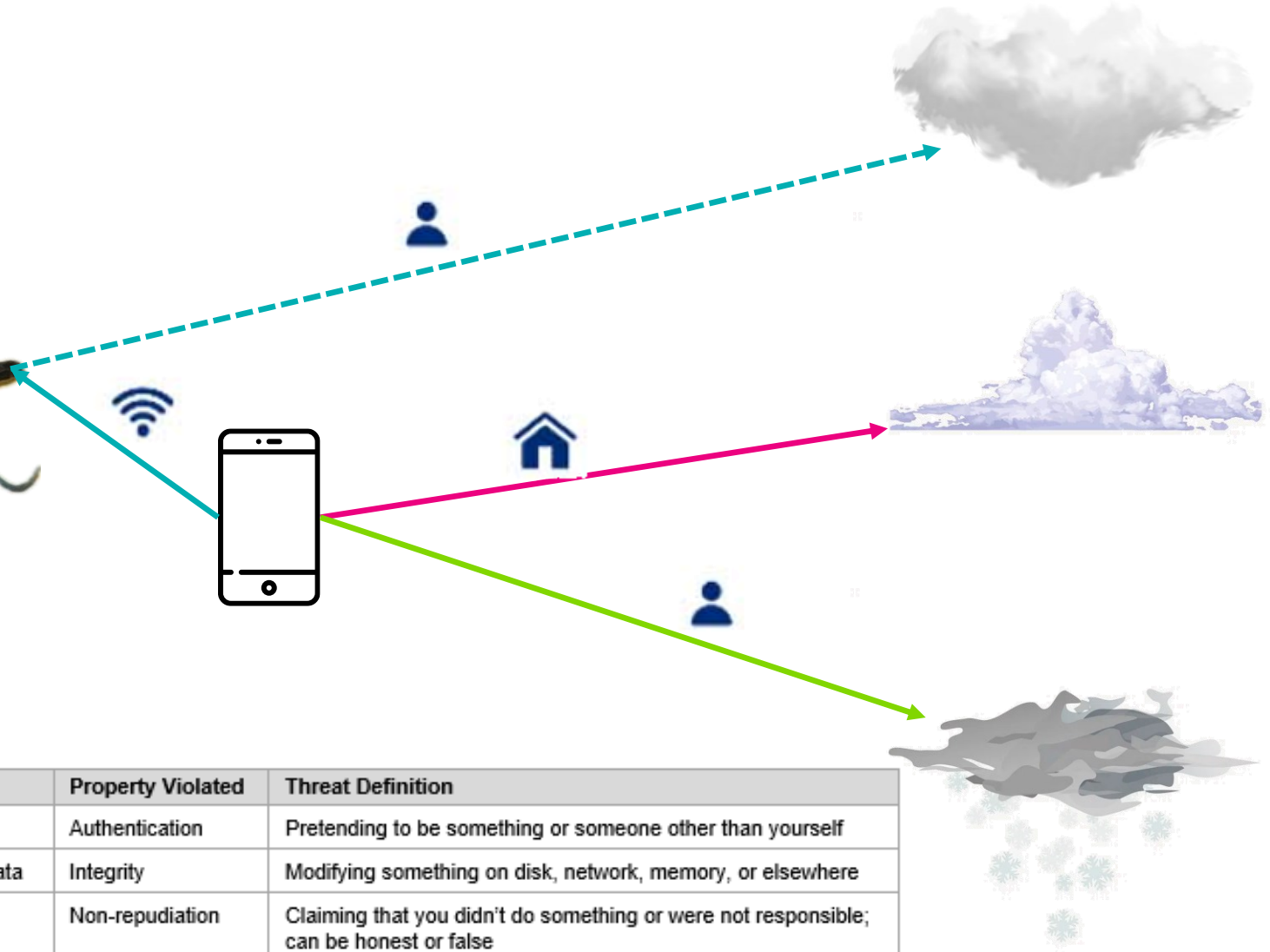
Toimitusketjujen hallinta



https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-161.pdf

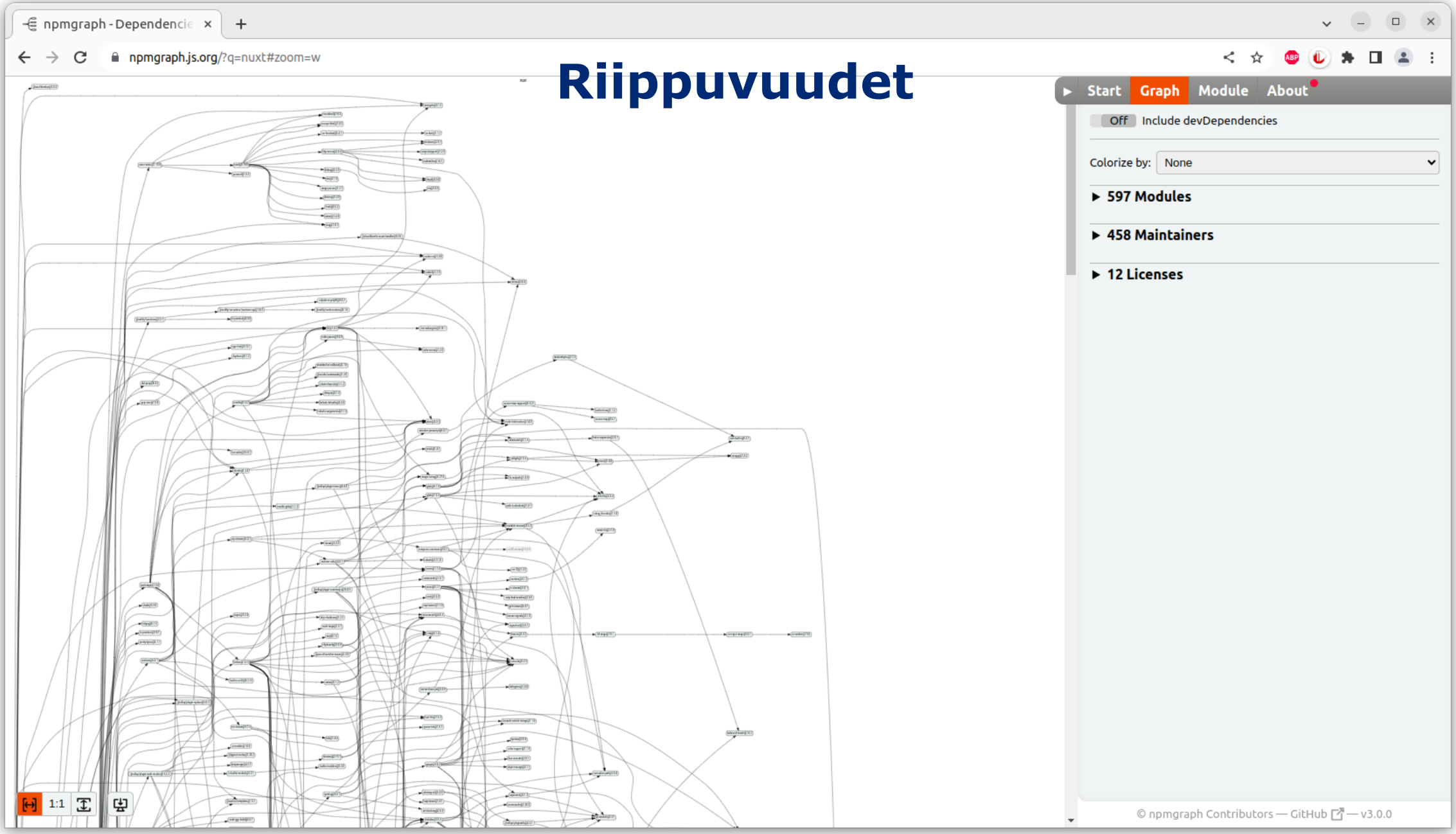
Uhkamallinnus



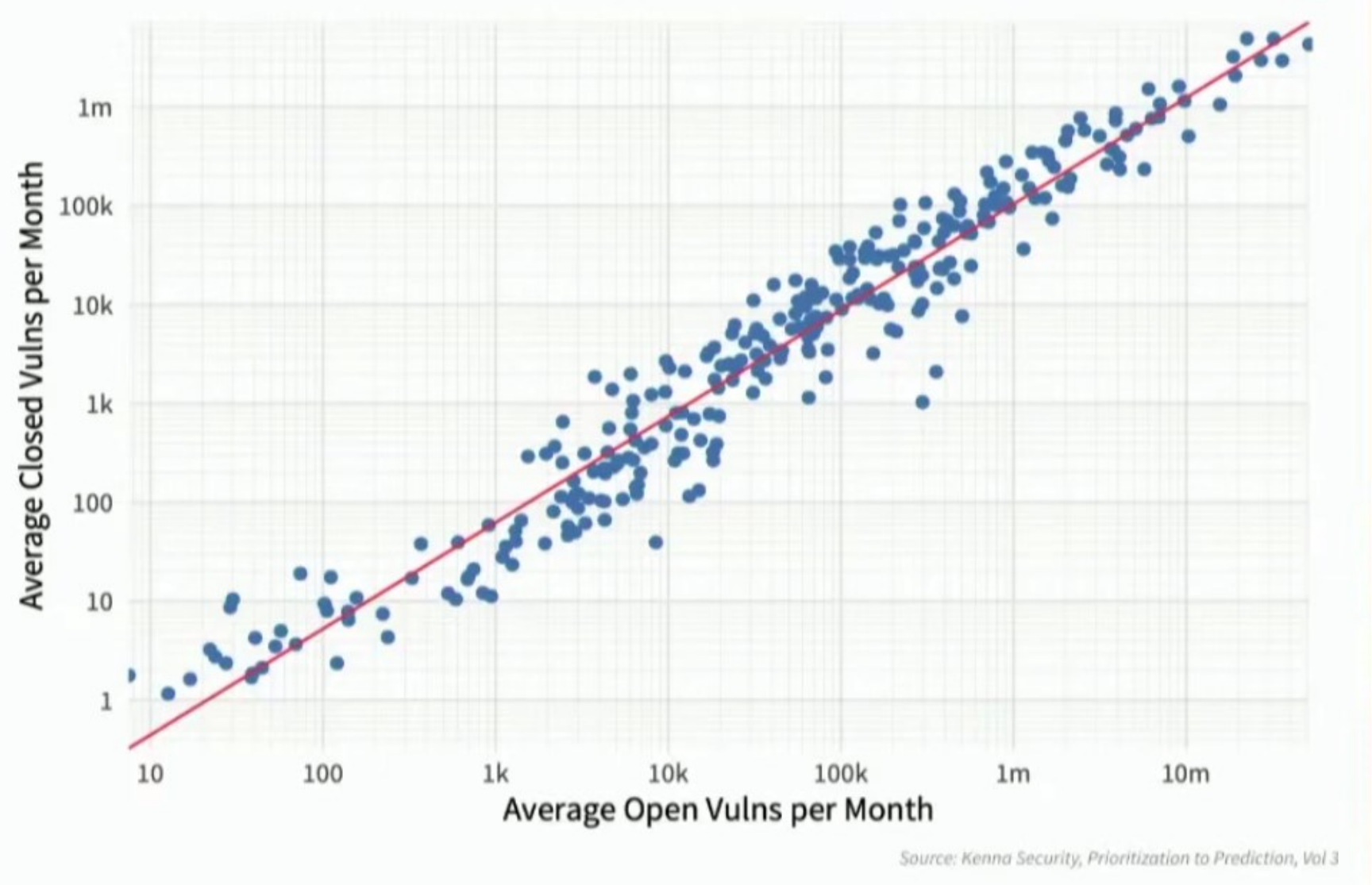


	Threat	Property Violated	Threat Definition
S	Spoofing identify	Authentication	Pretending to be something or someone other than yourself
T	Tampering with data	Integrity	Modifying something on disk, network, memory, or elsewhere
R	Repudiation	Non-repudiation	Claiming that you didn't do something or were not responsible; can be honest or false
I	Information disclosure	Confidentiality	Providing information to someone not authorized to access it
D	Denial of service	Availability	Exhausting resources needed to provide service
E	Elevation of privilege	Authorization	Allowing someone to do something they are not authorized to do

Riippuvuudet



Haavoittuvuuksien hallinta



Tekninen velka

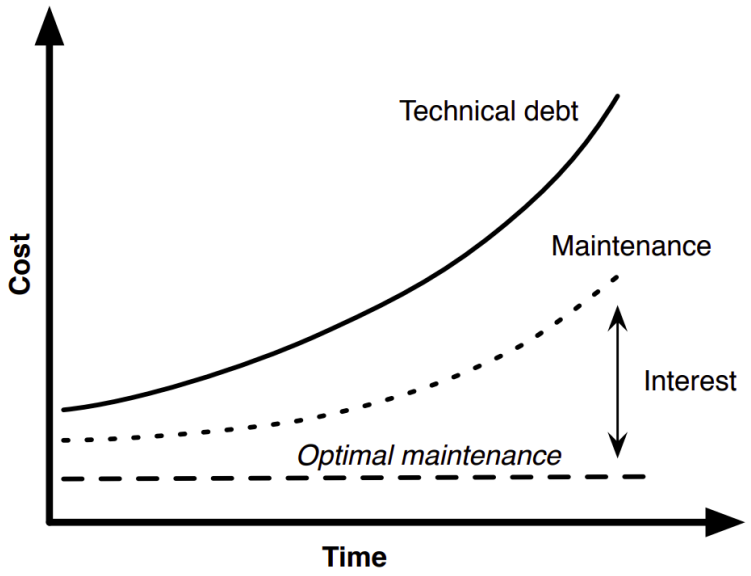
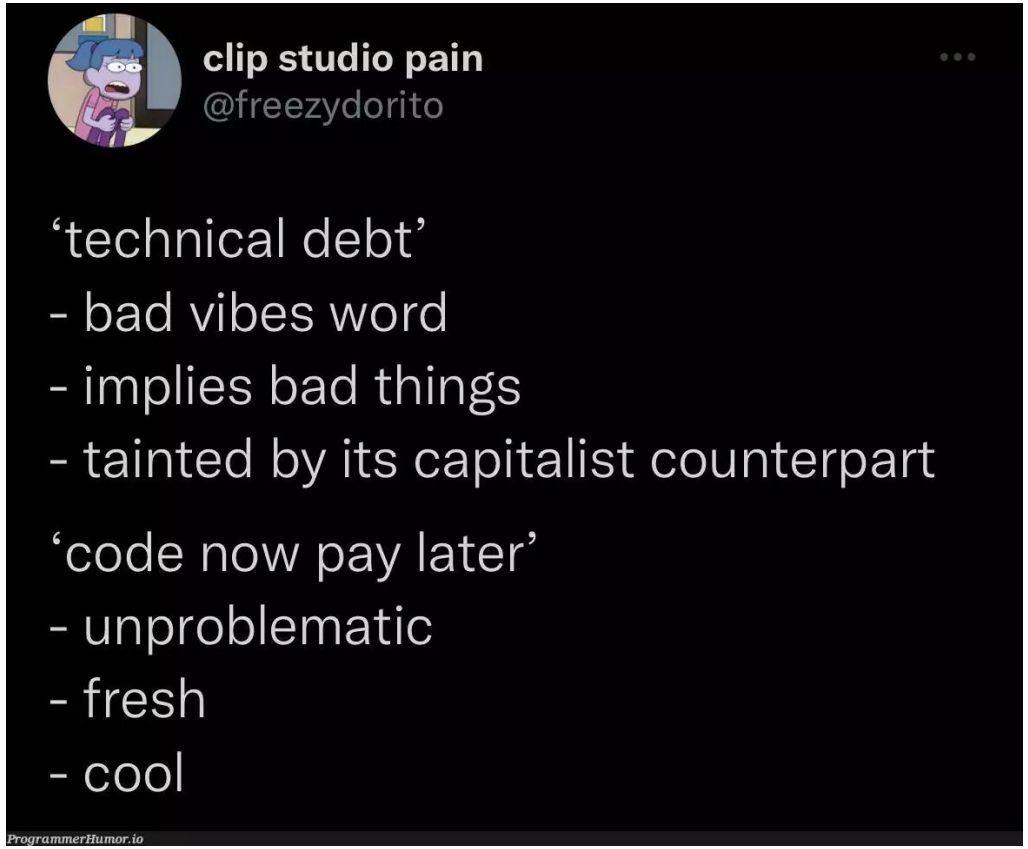


Figure 1: Technical debt and its interest grow over time if not resolved

An Empirical Model of Technical Debt and Interest
Nugroho, Ariadi and Visser, Joost and Kuipers, Tobias
MTD '11: Proceedings of the 2nd Workshop on Managing Technical Debt
https://doi.org/10.1145/1985362.1985364



Valittuja perusasioita

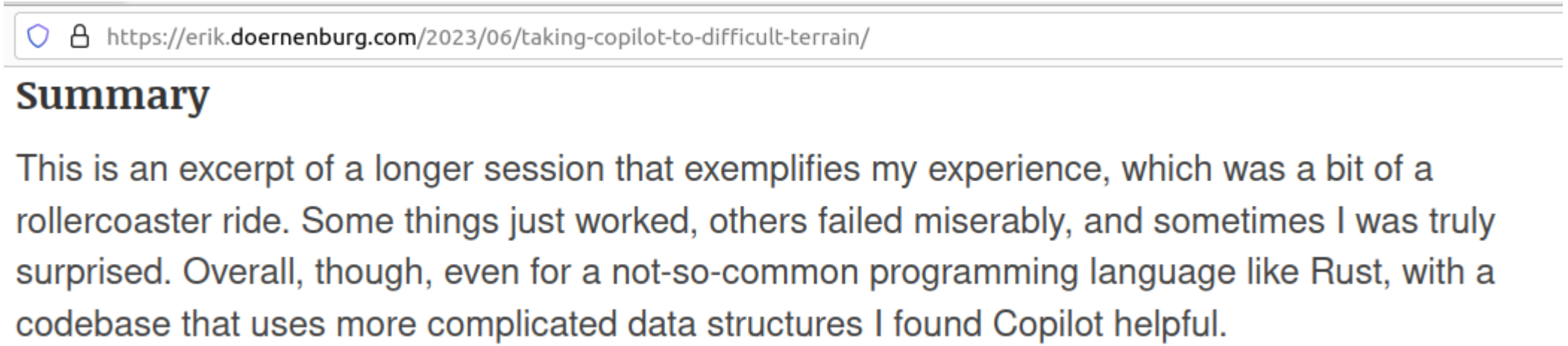
- Turvalliset kehityskielet
- Koodikäytännöt
- Versionhallintamalli
- xAST
- CI/CD

ML ja AI

- Todella paljon lupausta helpottamaan ohjelmistotuotannossa
  - Koodarin apuri rutiinitehtävissä
  - Yksikkötestien luomisessa
  - Koodin ja bisneslogiikan ymmärtämisessä
  - Hyökkäyspolkujen mallintamisessa
  - Koodin iteroinnissa ja uudelleenkirjoittamisessa

ML ja AI

- Todella paljon lupausta helpottamaan ohjelmistotuotannossa
  - Koodarin apuri rutiinitehtävissä



  - Koodin iteroinnissa ja uudelleenkirjoittamisessa

Regulaatio

Strategy for Data

- Open Data Directive
- Data Act (proposal)
- Data Governance Act (DGA)

Cybersecurity Strategy

- Cybersecurity Act (CSA)
- NIS 2 Directive
- Cyber Resilience Act (proposal)
- Digital Operational Resilience Act (DORA)
- Cyber Solidarity Act (proposal)

Digital Privacy

- GDPR
- e-Privacy Regulation (proposal)

AI Strategy

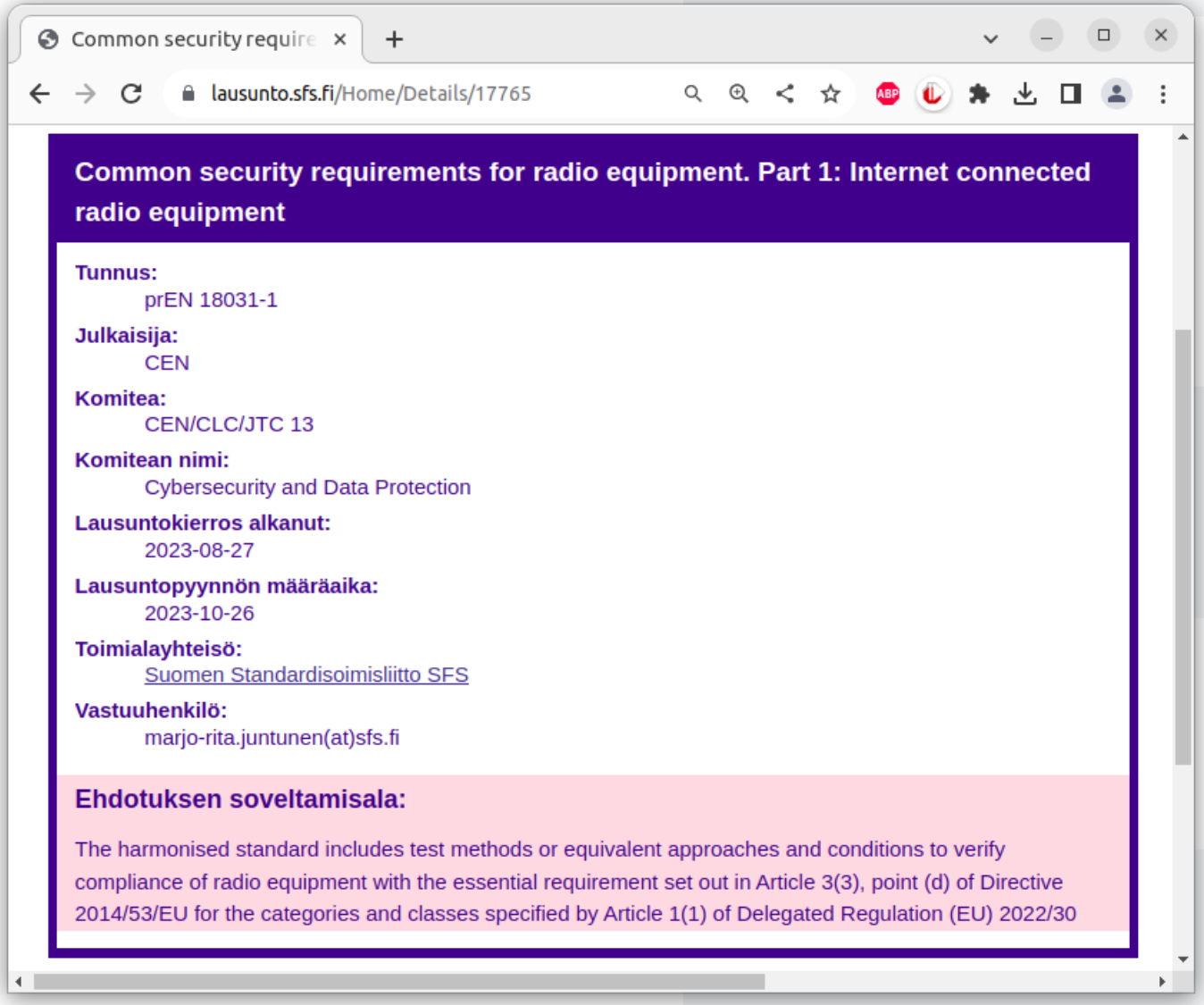
- AI Act (proposal)
- AI Liability Directive (proposal)

Digital Services Package

- Digital Services Act (DSA)
- Digital Markets Act (DMA)

https://digitaldecade.hannessnellman.com/

Regulaatio



Strategy for Data

- Open Data Directive
- Data Act (proposal)
- Data Governance Act (DGA)

- Cybersecurity Act (CSA)
- NIS 2 Directive
- Cyber Resilience Act (proposal)
- Digital Operational Resilience Act (DORA)
- Cyber Solidarity Act (proposal)

- GDPR
- e-Privacy Regulation (proposal)

- AI Act (proposal)
- AI Liability Directive (proposal)

- Digital Services Act (DSA)
- Digital Markets Act (DMA)

Digital Services Package

https://digitaldecade.hannessnellman.com/

TRAFICOM

Johdon vastuu - Millaisen kyberpoikkeaman yrityksesi kestää?

- Liiketoimintajohto näkee ohjelmistojen turvattomuuden jopa eksistentiaalisena riskinä – tämä ei kuitenkaan välttämättä näy toiminnassa ja kehittäjien arjessa.
- Eri organisaatioiden tietoturvan taso on polarisoitunut.
- Nopeasti muuttuva teknologiaympäristö haastaa tietoturvan organisointia ja vastuuttamista.
- Tuleva sääntely pakottaa organisaatiot kiinnittämään huomion kyberturvallisuuteen.

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kiitos

Ohjelmistoturvallisuuden tila 2023

Nykytilaraportti

Timo Kiravuo
Päivi Timlin
Karoliina Kemppainen
Juhani Eronen
Saana Seppänen