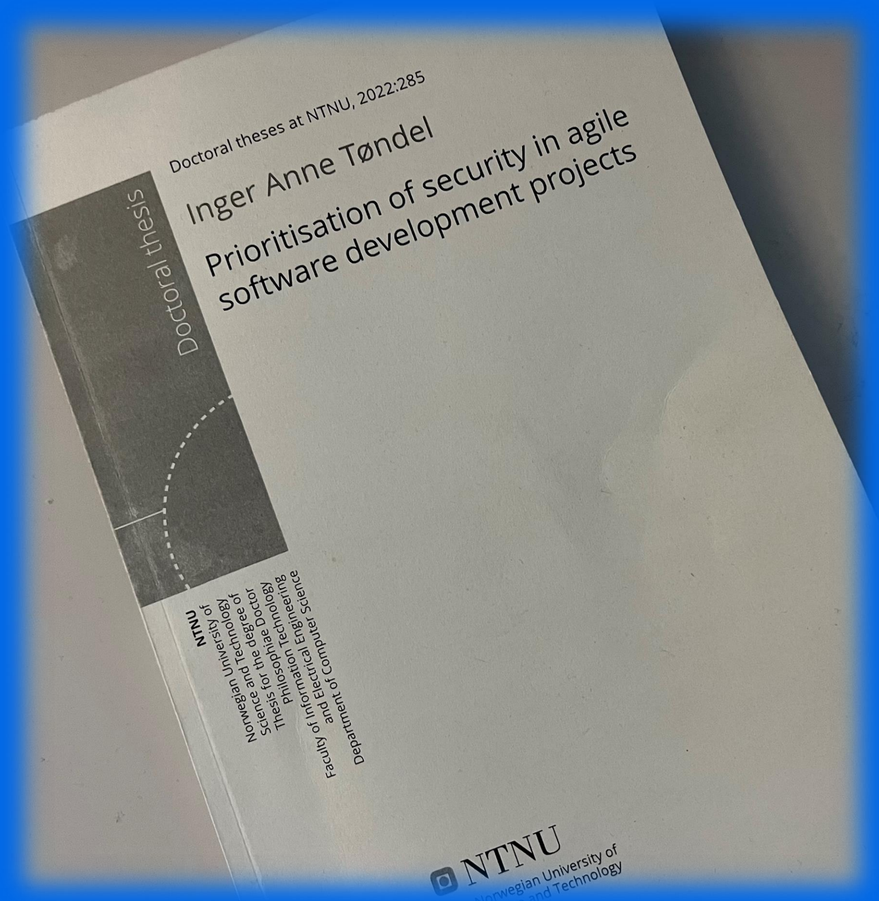
Direktoratet for e-helse

Sikkerhet og smidig utvikling - kan man stole på at utviklerne fikser sikkerheten?

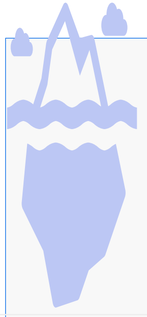
Inger Anne Tøndel
Seniorrådgiver

Normkonferansen 2022



Vi kan alle være enige om …

Programvare kan utsettes for angrep. Motstandsdyktighet må bygges inn!



Dette handler om mer enn kryptering og tilgangskontroll – vi trenger programvare som ikke er full av sårbarheter og designfeil som kan utnyttes av angripere

Når systemer endrer seg så kan også sikkerhetsforutsetninger og –behov endre seg

Sikkerhet må gis prioritet gjennom hele utviklingsprosessen!

Områder som påvirker sikkerhetsprioriteten i et utviklingsprosjekt

- Noen som tar initiativ og pusher på for sikkerhet mot de ulike rollene som er involvert

Drivkraft

- Påminnelser i en travel hverdag
- Synlighet i krav, i design, i arbeids-prosessene, i rollene

Synlighet

- Motivasjon hos utviklere ++
- Motivasjon for sikkerhet fra kunde, ledelse, lovverk, mm.

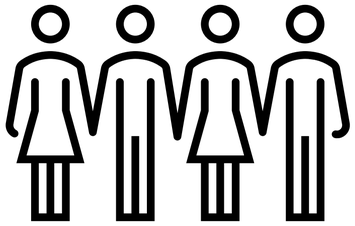
Motivasjon

- Nødvendig tid, budsjett og kompetanse til å gjøre noe med sikkerhet

Handlingsrom

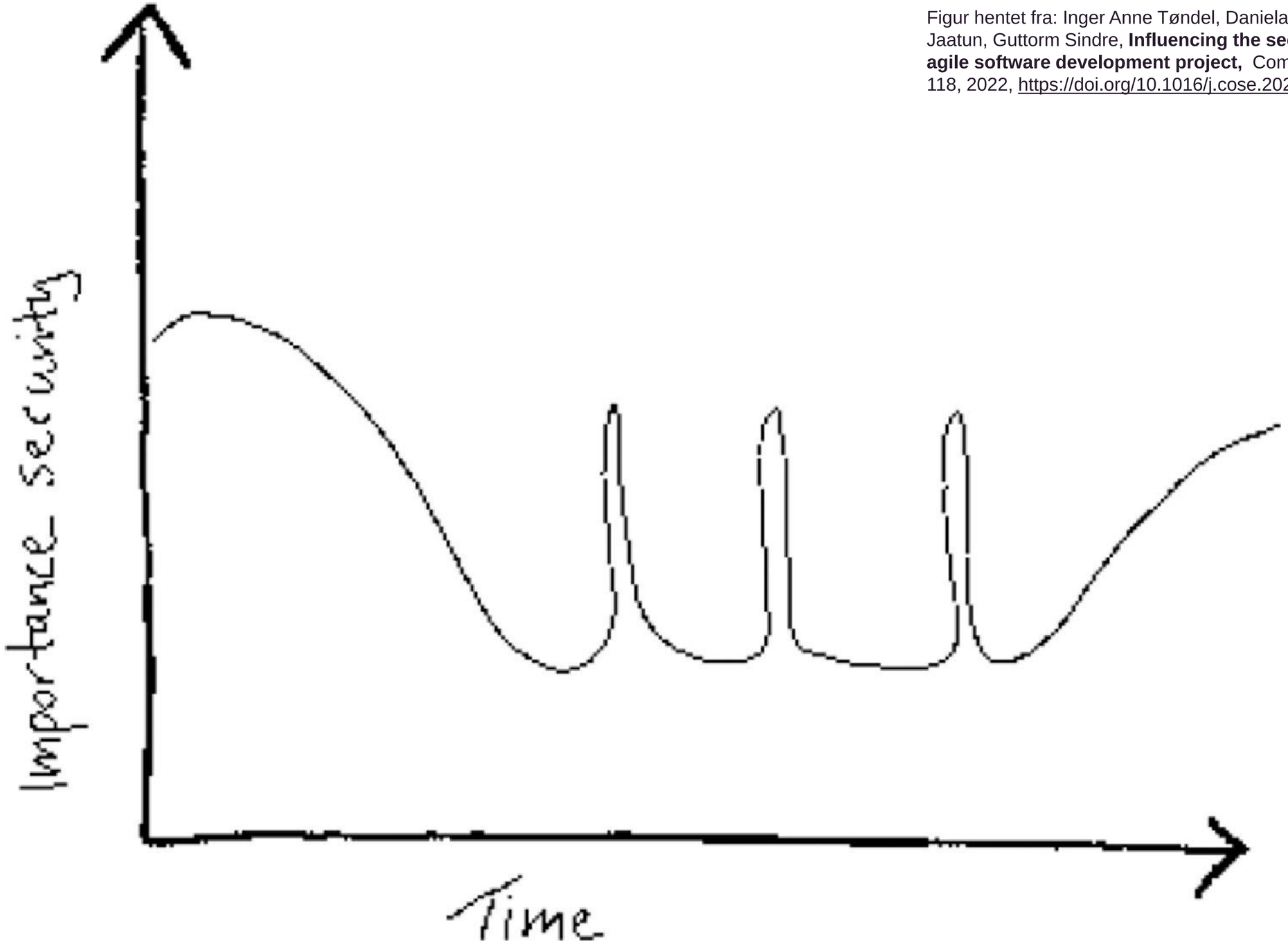
- Hvordan man jobber ellers passer med hvordan man forventes å jobbe med sikkerhet

Prosess-match

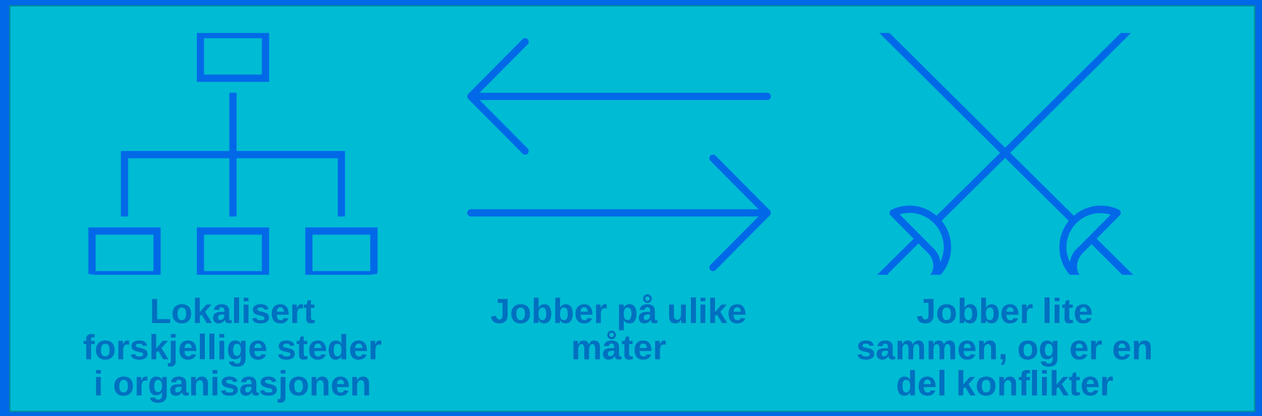


Hva har dette å si for oss som jobber med informasjonssikkerhet og personvern?

Figur hentet fra: Inger Anne Tøndel, Daniela Soares Cruzes, Martin Gilje Jaatun, Guttorm Sindre, **Influencing the security prioritisation of an agile software development project,** Computers & Security, Volume 118, 2022, https://doi.org/10.1016/j.cose.2022.102744.



IT-sikkerhet er fra Mars, programvaresikkerhet er fra Venus



Vi trenger interaksjonskompetanse!

Verdier i smidig utvikling

- **Individer og interaksjoner** *er viktigere enn* prosesser og verktøy
- **Programvare som virker** *er viktigere enn* omfattende dokumentasjon
- **Samarbeid med kunde** *er viktigere enn* kontraktsforhandlinger
- **Å respondere på endringer** *er viktigere enn* å følge en plan

Hva har dette å si for hvordan smidige utviklingsprosjekter jobber med krav?

Cao, L., & Ramesh, B. (2008). Agile requirements engineering practices: An empirical study. *IEEE software*, *25*(1), 60-67.

Kommunikasjon ansikt til ansikt heller enn skriftlige spesifikasjoner

Arbeid med krav skjer iterativt, endringer i krav håndteres gjennom jevnlig re-planlegging

Ekstrem i prioriteringen av de ulike kravene


Vi blir ikke invitert!

Emerging

Prescribed

- Mindre oversikt, mindre sentral kontroll, mer opp til autonome team – avhengig av at de har kompetanse og tar ansvaret.
- Ansvarliggjør teamet. Teamet kan finne måter å jobbe på som passer for dem.

- Mer kontroll og lettere å følge opp.
- Risikerer at sikkerhet blir «noe ekstra» og at det ikke passer med resten. Kan møte mer motstand.

Smidig-manifestet

Bygg prosjekter rundt motiverte individer. Gi de miljøet og støtten de trenger og stol på at de gjør jobben.

Hvordan kan det legges til rette – i omgivelsene, i støtten som gis – for at teamet prioriterer sikkerhet?

Drivkraft

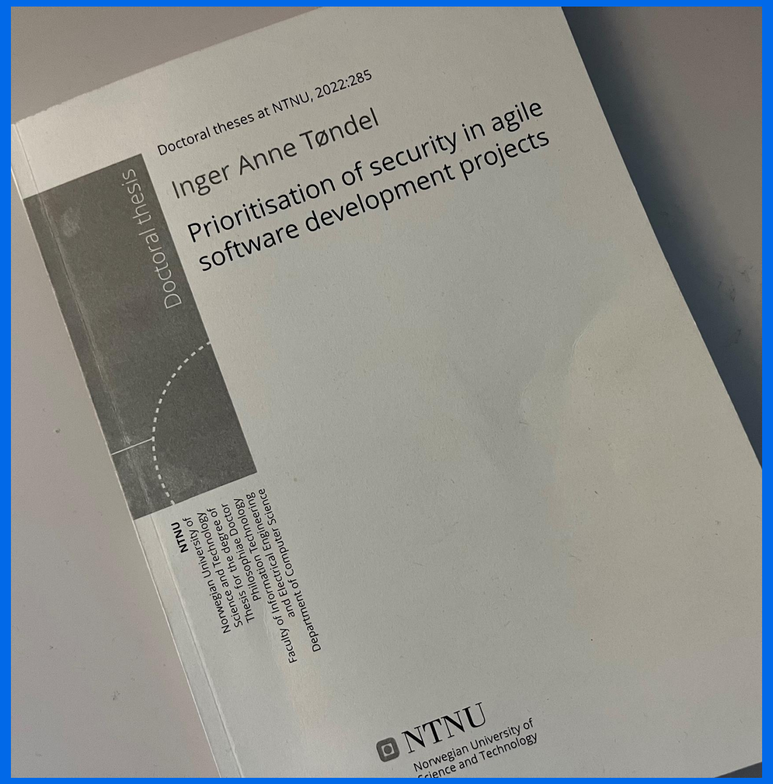
Synlighet

Motivasjon

Handlingsrom

Prosess-match

Direktoratet for e-helse



Mer å lese?

Inger Anne Tøndel, Daniela Soares Cruzes, Martin Gilje Jaatun, Guttorm Sindre,
Influencing the security prioritisation of an agile software development project,
Computers & Security, Volume 118, 2022,
https://doi.org/10.1016/j.cose.2022.102744.

Inger Anne Tøndel, Martin Giljje Jaatun, Daniela Soares Cruzes,
IT security is from Mars, software security is from Venus.
IEEE Security & Privacy, 18(4), 48-54. 2020.
https://doi.org/10.1109/MSEC.2020.2969064