DOKTORAND:	Gyrd Brændeland
GRAD:	Philosophiae doctor
FAKULTET:	Det matematisk-naturvitenskapelige fakultet
INSTITUTT:	Institutt for informatikk
FAGOMRÅDE:	Formell spesifikasjon, sikkerhet og risikoanalyse
VEILEDERE:	Ketil Stølen, Jan Øyvind Aagedal
DISPUTASDATO:	15. juli 2011

AVHANDLINGENS TITTEL: *Component-based risk analysis*

Cand. philol. Gyrd Brændeland ved Institutt for informatikk, disputerer fredag 15. juli 2011 for PhD-graden ved Universitetet i Oslo med avhandlingen: ”Component-based risk analysis”. Brændeland har forsket på sikkerhetsrisikoen ved å installere en programvarekomponent i et system. I avhandlingen representeres sikkerhetsrisiko som en egenskap ved en komponent. Risiko er kombinasjonen av sannsynligheten for at en uønsket hendelse inntreffer og konsekvensene i form av skade på verdier, slik som sensitiv informasjon i en database. Regler for å sette sammen risikoer gjør det mulig å bestemme sikkerhetsrisikoen til et system sammensatt av komponenter, som har blitt oppgradert med en ny komponent.

Biler, laptoper, smart-telefoner og mobile produkter generelt selges ikke som ferdige produkter, men inneholder i stadig større grad programvarekomponenter som blir oppgradert flere ganger i løpet av produktets levetid. - Dette gjør slike systemer fleksible, men fører også til sikkerhetsmessige utfordringer som ikke håndteres tilfredsstillende i dag, påpeker Brændeland.

- Problemet er at systemutviklere fokuserer på hva en komponent skal gjøre, mens sikkerheten først tas i betraktning etter at systemet er ferdig bygd. Hvis en ny komponent samvirker med resten av systemet på en måte som ikke var forutsett da den ble installert, kan det være svært vanskelig å finne ut hva feilen skyldes. Et kjent eksempel på dette er Toyotas problemer med å forklare hvorfor gasspedalen hang seg opp i flere av bilene deres. De visste ikke om problemet var rent mekanisk, skyltes elektronikkfeil, programvarefeil eller menneskelige feil, forklarer Brændeland. Til syvende og sist er det ikke forsvarlig med komponentbasert utvikling uten også å ha en komponentbasert forståelse av sikkerhetsrisiko, sier hun.

Avhandlingen beskriver en metode for komponentbasert modellering av sikkerhetsrisiko og en prosedyre for komponentbasert risikoanalyse, det vil si hvordan risikoer kan identifiseres og dokumenters på komponentnivå.

- Ingen komponenter er ment å fungere i ethvert miljø. For eksempel kan en bilprodusent garantere en viss oppførsel når en bil kjøres på motorveien, men ikke hvis den slippes fra et fly i 1000 meters høyde. Det er derfor vanlig å spesifisere komponenter i kontraktsform: Gitt at visse betingelser er oppfylt av omgivelsene til komponenten, gir komponenten visse garantier med hensyn til oppførsel. I avhandlingen formaliseres denne ideen med hensyn til risiko. Gitt visse betingelser i omgivelsen til en komponent, som for eksempel kryptering av passord, vil en komponent ha et visst risikonivå.