Safety versus Security in the Quality Calculus - DTU Orbit (09/11/2017)

Safety versus Security in the Quality Calculus

Safety and security are both needed for ensuring that cyber-physical systems live up to expectations, but often an intelligent trade-off is called for, because sometimes it is impossible to obtain optimal safety at the same time as optimal security. In the context of the Quality Calculus we develop a type system for checking the extent to which safety and security goals have been met. Safety goals include showing that certain error configurations are in fact not reachable and hence do not require intelligent error handling. Security goals include showing that highly trusted communications can only be performed in highly trusted contexts. This is potentially too demanding and the Quality Calculus is therefore extended with a primitive for endorsing data to a higher trust level (accepting violations of the explicit flow) and for temporarily asserting a higher trust in the context (accepting violations of the implicit flow). This is illustrated on a worked example taken from the automotive sector and we conclude with a discussion of the theoretical properties of the type system.

General information

State: Published
Organisations: Department of Applied Mathematics and Computer Science , Language-Based Technology
Authors: Nielson, H. R. (Intern), Nielson, F. (Intern)
Pages: 285-303
Publication date: 2013

Host publication information

Title of host publication: Theories of Programming and Formal Methods : Essays Dedicated to Jifeng He on the Occasion of His 70th Birthday
Publisher: Springer
ISBN (Print): 978-3-642-39697-7
ISBN (Electronic): 978-3-642-39698-4

Series: Lecture Notes in Computer Science
Volume: 8051
ISSN: 0302-9743
Main Research Area: Technical/natural sciences
Automotive industry, Embedded systems, Optimization, Calculations
DOIs:
10.1007/978-3-642-39698-4_18
Source: dtu
Source-ID: n::oai:DTIC-ART:compendex/391909796::31850
Publication: Research - peer-review › Book chapter – Annual report year: 2013