HoliSec

Holistic Approach to Improve Data Security

Topic: Interplay between safety and security
(Live MODIFI demo)

Presenter: Peter Folkesson, RISE
September 7, 2017. Time 11:10 – 11:30
MODel-Implemented Fault Injection tool

- MODIFI is a fault injection tool for Simulink models
  - Useful for early dependability evaluation of software developed as models
  - Provides a large number of fault models, e.g., bit-flip faults and sensor faults
  - Includes support for analyzing and visualizing fault injection results
Injecting faults in Simulink models

- Faults are injected using fault injection blocks inserted into the model
  - Fault injection is triggered based on simulated time
  - No effect on simulated time but some effect on simulation execution time

Original model

Model with fault injection support
HoliSec: Model Implemented Attack Injection

• Attack model in MODIFI:
  – Replay(N,M) attack on signals/CAN bus
  – Replays N values from consecutive time steps, M time steps old (N<=M)

Topic: Interplay between safety and security (Live MODIFI demo)
Presenter: Peter Folkesson, RISE
September 7, 2017. Time 11:10 – 11:30
MODIFI 2.0 – new features

• Support for attack injection
  – Replay\((N,M)\) attack
  – Denial-of-service, Man-in-the Middle, Sybil, Interception, Data and message corruption attacks
  – ...

• Extended support for fault injection
  – Stuck-at-value and Stuck-at-one fault models added

• Support for (attack/fault) injection into signals of alias, enum and fixed-point datatypes
• Support for (attack/fault) injection into individual signals of buses
• Interface improvements
  – Support for FIND (generic Fault/attack INjection Database) SQL database
  – CSV-formatted stimuli files supported for compatibility with tools like Mx-VDev
  – Script control using command line execution to support batch processing (development flows)
• Several bug fixes and improvements made to the source code, GUI and supported file formats
FIND –
generic Fault/attack INjection Database

• MySQL database for storing fault/attack injection data in a generic (tool independent) format
• Speeds up fault/attack injection campaigns and analyses
• Simplifies comparison of results from different fault/attack injection tools at different abstraction levels
• Stores:
  – Campaign configuration information (*injection types, locations, time, ...*)
  – Observed behaviour of nominal system (*golden run*)
  – Observed behaviour of injected system (*experimental runs*)
• Tool independent analysis and visualisation of injection experiments:
  – Generic error classification scripts (SQL-scripts, views and stored procedures)
  – Tool for graphical visualization of experimental results (FIND Analyzer)
MODIFI 2.0

• DEMO!
HoliSec

*Holistic Approach to Improve Data Security*

Thank you for your attention!