Development and Industrial Application of Multi-Domain Security Testing Technologies

Case Study Experience Sheet
Automotive Case Study from Dornier Consulting
Bluetooth connectivity module for mobile devices that allows direct communication between car’s head unit and a mobile phone

Security challenges:
- Access to the car’s infrastructure by malfunctioning or hostile mobile phones or by misuse of the Bluetooth interface
- Modification of the Bluetooth module in order to interfere with the car’s normal operation and its security and safety

Technical challenges:
- Simulation of Bluetooth device/mobile phone and integration of CAN bus
- Specialized Bluetooth stack for security testing
Automotive Case Dornier Consulting
Testing approach: risk-based security testing
Automotive Case Dornier Consulting
Testing approach: data fuzzing

- Fuzzing Library developed by Fraunhofer FOKUS
- Library is called by FuzzingContainer to inject fuzzed test data
- Improved fuzzing heuristics based on Peach and Sulley
- Interface uses XML for requests and generated fuzz test data
- Example: Device name and PIN was fuzzed within this case study

Generators:

- String (default)
- SQL
- Path
- Filename
- Hostname
- Delimiter
- RegExValid
- RegExInvalid
- Number
- Command
- Date
- Time
- IPAddress

© DIAMONDS Consortium 2010-2013
So far, about 150 test cases have been executed.

Test purposes:
- break Bluetooth connectivity module
- compromise the head unit by anomalous Bluetooth messages

Until now, a few anomalies were found:
- need further investigation

Metrics:
- several vulnerabilities resulted from risk analysis were covered
- further metrics have to be found
- CORAS method for risk analysis has been proved of value
  - graphical modelling
  - specification of assets to be protected

- Model-based security test case generation as a complement to static analysis

- Saved resources due to reuse of functional test cases for non-functional security testing

- Standardization of DIAMONDS results increases customer’s confidence in the security of tested product
Automotive Case Dornier Consulting
Summary

- Improvement gains according to DIAMONDS STIP:

![Diagram showing improvement gains across various categories such as Risk assessment, Static testing, Monitoring, Test execution automation, Fuzzing, Test identification, Automated generation of test models, and Test generation. The diagram compares Dco to DIAMONDS.](image-url)