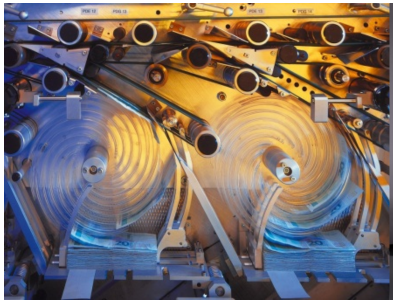
DIAMONDS

Development and Industrial Application of Multi-Domain Security Testing Technologies

Case Study Experience Sheet
Automotive Case Study from Dornier Consulting



ITEA 2
INFORMATION TECHNOLOGY FOR EUROPEAN ADVANCEMENT

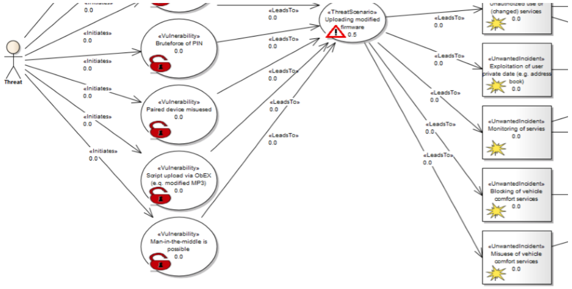
Automotive Case Dornier Consulting

Case study characterization

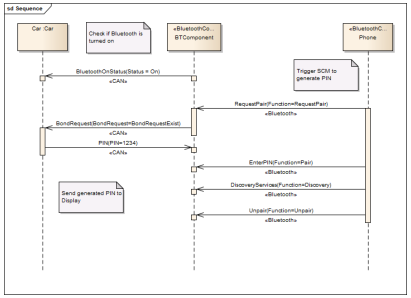
- Bluetooth connectivity module for mobile devices that allows direct communication between car’s head unit and a mobile phone
- Security challenges:
  - Access to the car’s infrastructure by malfunctioning or hostile mobile phones or by misuse of the Bluetooth interface
  - Modification of the Bluetooth 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

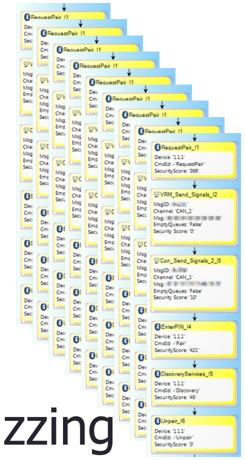
Testing approach: risk-based security testing



Security Risk Analysis


sd Sequence
Car :Car
Check if Bluetooth is turned on
«BluetoothCo...
BTComponent
«BluetoothC...
Phone
Trigger SCM to generate PIN
BluetoothOnStatus(Status = On)
«CAN»
RequestPair(Function=RequestPair)
«Bluetooth»
BondRequest(BondRequest=BondRequestExist)
«CAN»
PIN(PIN=1234)
«CAN»
EnterPIN(Function=Pair)
«Bluetooth»
DiscoveryServices(Function=Discovery)
«Bluetooth»
Send generated PIN to Display
Unpair(Function=Unpair)
«Bluetooth»

Functional test cases


RequestPair_I1
Device: '1.1.1'
CmdId: -'RequestPair'
SecurityScore: '366'

VRM_Send_Signals_I2
MsgID: [redacted]
Channel: 'CAN_1'
Msg: [redacted]
EmptyQueues: 'False'
Security Score: '0'

Con_Send_Signals_2_I3
MsgID: [redacted]
Channel: 'CAN_1'
Msg: [redacted]
EmptyQueues: 'False'
Security Score: '10'

EnterPIN_I4
Device: '1.1.1'
CmdId: -'Pair'
SecurityScore: '421'

DiscoveryServices_I5
Device: '1.1.1'
CmdId: -'Discovery'
SecurityScore: '45'

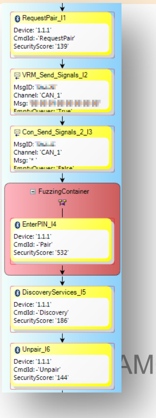
Unpair_I6
Device: '1.1.1'
CmdId: -'Unpair'
SecurityScore: '0'

Fuzzing techniques

System Model

Test Model

Security Test Case Templates


RequestPair_I1
Device: '1.1.1'
CmdId: -'RequestPair'
SecurityScore: '139'

VRM_Send_Signals_I2
MsgID: [redacted]
Channel: 'CAN_1'
Msg: [redacted]
EmptyQueues: 'True'

Con_Send_Signals_2_I3
MsgID: [redacted]
Channel: 'CAN_1'
Msg: '* '
EmptyQueues: 'False'

FuzzingContainer

EnterPIN_I4
Device: '1.1.1'
CmdId: -'Pair'
SecurityScore: '532'

DiscoveryServices_I5
Device: '1.1.1'
CmdId: -'Discovery'
SecurityScore: '186'

Unpair_I6
Device: '1.1.1'
CmdId: -'Unpair'
SecurityScore: '144'

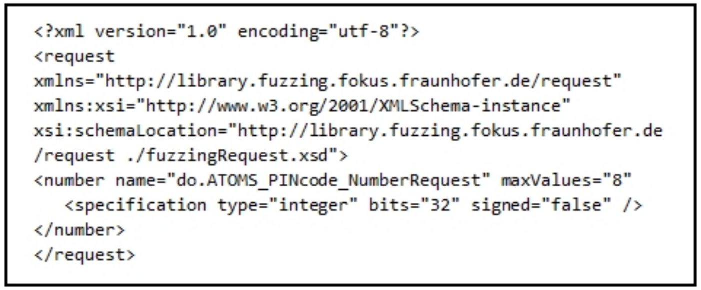
Automotive Case Dornier Consulting

Testing approach: data fuzzing

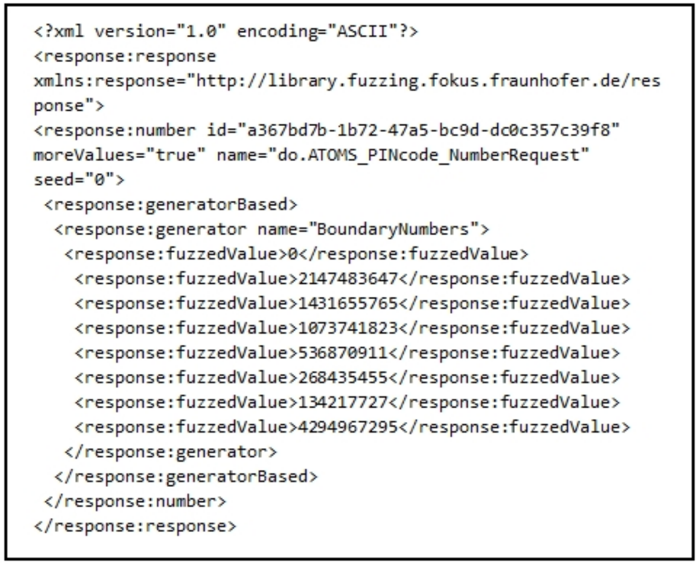
- Fuzzing Library developed by Fraunhofer FOKUS
- Library is called by FuzzingContainer to inject fuzzed test data
- Improved fuzzing heuristics based on Peach and Sulley
- Interface uses XML for requests and generated fuzz test data
- Example: Device name and PIN was fuzzed within this case study

- Generators:

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



```xml
<?xml version="1.0" encoding="utf-8"?>
<request
xmlns="http://library.fuzzing.fokus.fraunhofer.de/request"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://library.fuzzing.fokus.fraunhofer.de
/request ./fuzzingRequest.xsd">
<number name="do.ATOMS_PINcode_NumberRequest" maxValues="8"
   <specification type="integer" bits="32" signed="false" />
</number>
</request>
```



```xml
<?xml version="1.0" encoding="ASCII"?>
<response:response
xmlns:response="http://library.fuzzing.fokus.fraunhofer.de/res
ponse">
<response:number id="a367bd7b-1b72-47a5-bc9d-dc0c357c39f8"
moreValues="true" name="do.ATOMS_PINcode_NumberRequest"
seed="0">
 <response:generatorBased>
  <response:generator name="BoundaryNumbers">
   <response:fuzzedValue>0</response:fuzzedValue>
    <response:fuzzedValue>2147483647</response:fuzzedValue>
    <response:fuzzedValue>1431655765</response:fuzzedValue>
    <response:fuzzedValue>1073741823</response:fuzzedValue>
    <response:fuzzedValue>536870911</response:fuzzedValue>
    <response:fuzzedValue>268435455</response:fuzzedValue>
    <response:fuzzedValue>134217727</response:fuzzedValue>
    <response:fuzzedValue>4294967295</response:fuzzedValue>
   </response:generator>
  </response:generatorBased>
 </response:number>
</response:response>
```

Automotive Case Dornier Consulting
Results

- So far, about 150 test cases has 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

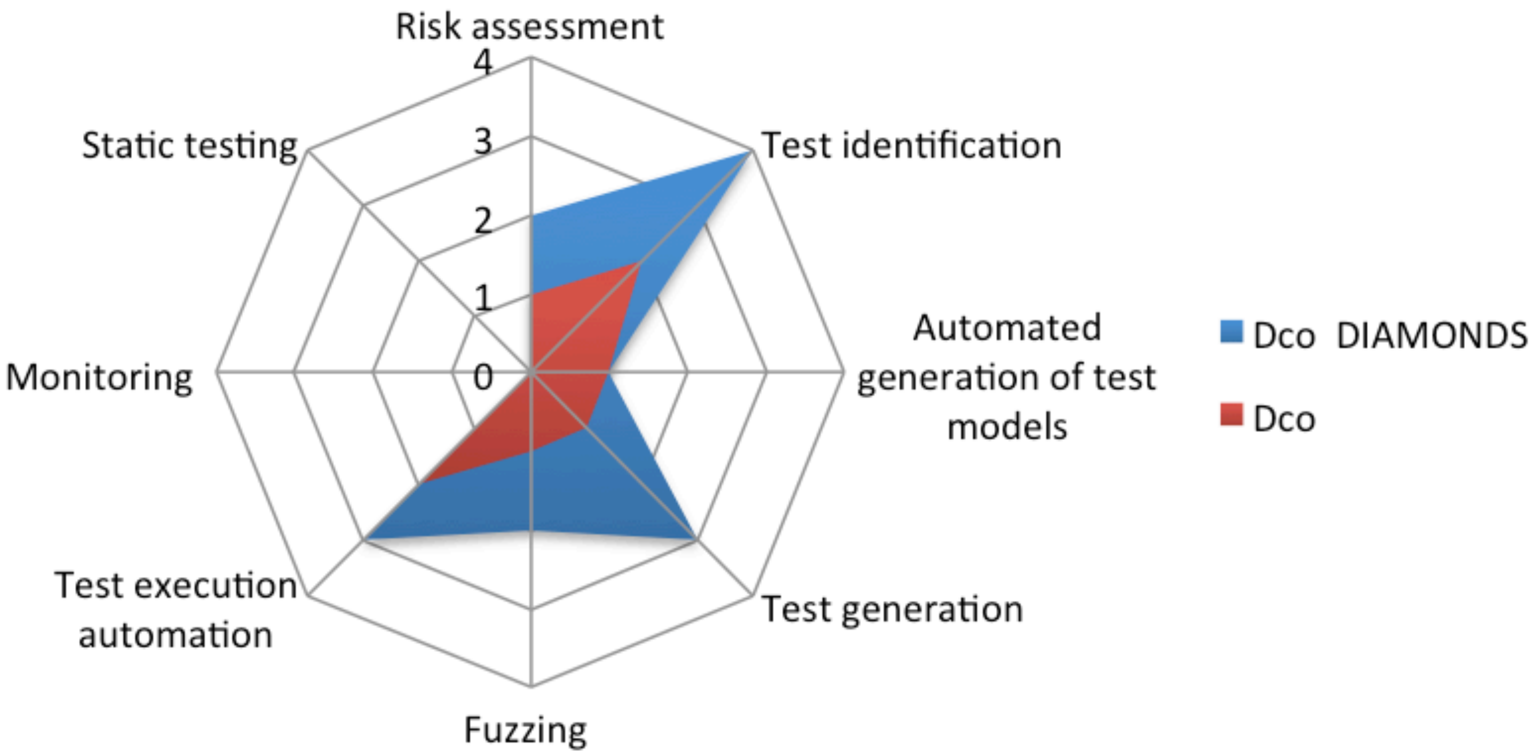
Automotive Case Dornier Consulting

Exploitation

- 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:**


Risk assessment
Test identification
Automated generation of test models
Test generation
Fuzzing
Test execution automation
Monitoring
Static testing
🟦 Dco DIAMONDS
🟥 Dco