Automatisches Erkennen von Sicherheitslücken mit Polyspace

Christian Guß
Cybersecurity – Emerging Topic in the Auto Industry

- Growing communication of on-board systems, sensors and external sites
- Car becomes another node of IoT
- Security of automotive embedded systems increasingly important (possible cyber attacks)

FCA recalls 1.4 Million cars after Jeep hack

Embedded Software Security New Challenge

Source: https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/
Security is on consumers’ mind

82% of customers would never buy from automaker if they had been hacked

85% of automakers admit their organization have been breached in the past 2 years

according to 2016 KPMG Consumer Loss Barometer study
Cybersecurity – Emerging Topic in the Internet of Things

Source:
„Industrial Control Systems (ICS) Cyber Emergency Response Team“ (ICS-CERT)
Embedded Software External Interactions

Control Algorithm, Fault Detection, Supervisory Logic

Utility (I/O Driver, Lookup Table, etc.)

RTOS, Fault Logging, Service Tool Interface

Network
File System
HSM
3rd party software
User Input
Sensors

MATLAB EXPO 2017
Embedded Software Security Concerns

- Incorrect order of network connection operations
- Tainted data
- Execution of a binary/Load of library from a relative path can be controlled by an external actor
- Tainted Data
- TOCTOU
- Vulnerable path manipulation
- Use of non-secure temporary file
- Tainted Data
- Deterministic random output from constant seed
- Vulnerable pseudo-random number generator
- Sensitive heap memory not cleared before release
- Tainted Data
- Tainted Data
- Execution of a binary/Load of library from a relative path can be controlled by an external actor
- Tainted Data
- Deterministic random output from constant seed
- Vulnerable pseudo-random number generator
- Sensitive heap memory not cleared before release
- Tainted Data

Network

File System

HSM

3rd party software

User Input

Sensors
Polyspace helps you to....

Identify and prove absence of critical defects

Enforce coding rules

1. A standard C environment
2. Compilation and build
3. Unused code
4. Code design
5. Identifiers
6. Literals and constants
7. Evaluations and definitions
8. Pointers and arrays
9. Standard libraries
10. Resources

Produce and monitor quality metrics
What is “Tainted Data”?

MATLAB EXPO 2017
Cybersecurity – Industry Activities & Standards

SAE – Vehicle Cybersecurity Systems Engineering Committee

- SAE J3061 - Cybersecurity Guidebook for Cyber-Physical Vehicle Systems
- SAE J3101 - Requirements for Hardware-Protected Security for Ground Vehicle Applications (WIP)
- SAE “Cybersecurity Assurance Testing Task Force” (TEVEES18A1)

Coding standards & practices that we observe at automotive customers

- CERT C
- ISO/IEC TS 17961 – C Secure Coding Rules
- CWE – Common Weakness Enumeration
- MISRA-C:2012 Amendment 1
Polyspace helps you to....

- Enforce **new coding rules**
  (all of them required or mandatory)

- 1 new directive [4.14]

- 13 new rules on
  - Expressions [12.5]
  - Resources [22.7, 22.8, 22.9, 22.10]

- Changes to existing rules [21.8]
Example of new MISRA directive 4.14

```
MISRA C:2012 D4.14 (Required)
The validity of values received from external sources shall be checked.
Division (/) operation operands are from an insecure source. Check for:
- Denominator of zero.
- Numerator of minimum value and denominator of -1.
```

```
1  Formal parameter is a tainted value tainteddata.c  bug_taintedintdivision()  108
2  MISRA C:2012 D4.14 tainteddata.c  bug_taintedintdivision()  109
```

```
/*===============================================*/
/* USING TAINTED DATA AS NUMERATOR IN DIVISION  */
/*===============================================*/

int bug_taintedintdivision(int numerator, int denominator) {
    int r = numerator / denominator; /* Defect: Parameter is not checked before being used as numerator */
    print_int(r);
    return r;
}
```
Summary

Cybersecurity …

- enable new future markets
- entire vehicle lifecycle process
- by design