Axel Rennoch, Sascha Hackel, Dorian Knoblauch

2nd Int. Workshop on Verification and Validation of Adaptive Software Systems, IEEE Int. Conference on Software Security and Reliability (QRS), 18th July 2018, Lisbon
Digital Transformation from A to Z

Transfer Centers:
- IoT
- 5G Testbed
- Industrie 4.0
- Hardware for CPS Lab

Experience
Learning
Consulting
Development
Testing
Solutions

lab tours
qualification & training
digital strategy
workshops
business models
technology advisory

modeling
pilot solutions
implementation
software licensing

engineering
system integration
testing & QC

Industry Forum
AGENDA

• IoT Testing
  – Challenges and scope
  – IoT test language: TTCN-3

• Project IoT-T
  – Eclipse IoT-Testware
  – Standardization & Certification

• Summary and outlook
• **Mirai botnet**, October 2016:
  - botnet using *insecure configured* IoT-devices (~100,000)
  - attack causes *blackout* and *disruption*
    (e.g. Amazon, Netflix, Twitter, Github)
• **Wannacry**, May 2017
  - ransomeware affecting the whole world (e.g. hospitals in the U.K.)
• **KRACK**: Key Reinstallation Attack, October 2017
  - Replay attack on Wi-Fi Protected Access protocol
• **Spectre** and **Meltdown**, January 2018
  - **Spectre**: vulnerability that allows observable side effects from mispredicted speculative executions
  - **Meltdown**: hardware vulnerability that allows to read all memory
TRENDS IN IOT

Top IoT Concerns / Trends 2016–2018

Copyright (c) 2018, Eclipse Foundation, Inc. | Made available under a Creative Commons Attribution 4.0 International License (CC BY 4.0).
IOT ARCHITECTURE

The Three Software Stacks Required for IoT Architectures, Eclipse IoT Working Group, September 2016
STARTING: TEST OBJECTS

- **IoT devices**,  
  - Mikrocontroller (**MCU**),  
  - **Gateways** (Bosch XDK, IoT starterkits)

- **IoT platforms**  
  - RIOT, relayr, Thread, mbed…  
  - service layer (oneM2M, FiWare)

- **IoT protocols**  
  - Constrained Application Protocol (**CoAP**)  
  - MQ Telemetry Transport (**MQTT**)  

**IoT challenges:** complexity, asynchronism, resource constraints, long operation phase
After the acceptance and system tests there will be a long operation phase => **new test phase „operation“**
TECHNICAL SCOPE

- Wide portfolio of competences required
  - Devices (sensors, HW, embedded SW)
  - Platforms (Cloud, platform domain knowledge)
  - Applications (SW, dashboard, business logic)

- IoT platforms
  - 360+ worldwide

- IoT protocols
  - Rich selection
  - IP-based
  - non-IP based

- Connectivity options
  - Throughput
  - Latency
  - Power efficiency
  - Packet size
INTEGRATION OF SEVERAL TESTING APPROACHES

- IoT Testing
- Security Testing
- Test Automation
- Protocol Testing
- Software Testing
- System Testing
• Less resources needed (time and money)
• Avoid human mistakes due to manually testing
• During test development and execution
• Speed-up of regression tests and product time-to-market
MULTIPLE TEST CONFIGURATION (SAMPLES)
TESTWARE

• **Toolset** (*selection of available means*)

  - **Protocol tester/monitor** (Eclipse *Titan*, *Wireshark*)
  - **Test devices** (*RFID* kit, *Bluetooth* test device)
  - **GUI tester** (*Selenium*, *SikuliX*, Chrome headless)
  - **Web services tester** (*soapUI*)

  ...

• **Public Testsuites** (*in development*)
  - Application of a *standardized* notation
  - Abstract and *platform-independent*
Did you know that **YOUR PHONE**...

...has been **tested** using ETSI specifications written in **ETSI**?
• TTCN-3 is the **Testing and Test Control Notation**
• **Internationally standardized** testing language for formally defining test scenarios.
• Designed **purely for testing**

```plaintext
testcase Hello_Bob () {
    p.send("How do you do?");
    alt {
        []p.receive("Fine!");
            {setverdict( pass )};
        [else]
            {setverdict( inconc )}  //Bob asleep!
    }
}
```
DESIGN PRINCIPLES OF TTCN-3

• One test technology for different tests
  – Distributed, platform-independent testing
  – Integrated graphical test development, documentation and analysis
  – Adaptable, open test environment

• Areas of Testing
  – Conformance and functional testing
  – Interoperability and integration testing
  – Real-time, performance, load and stress testing
  – Security testing
  – Regression testing

• Used for system and product qualification and certification
THE IOT-T PROJECT

Eclipse IoT-Testware

Fraunhofer FOKUS
Take available software and tools …

... and adding public testuites as a result of insights from IoT testing:

https://projects.eclipse.org/projects/technology.iottestware
THE ECLIPSE PROJECT

• Supplement to running and active Eclipse projects
  – Paho, OM2M, Titan

• New project at Eclipse Foundation: https://projects.eclipse.org/projects/technology.iotestware
  – TTCN-3 test suites for CoAP, MQTT, OPC-UA, LoRa?

• Assured licenses for users

• Currently in cooperation with
  relAYr GmbH, Ericsson, LAAS/CNRS, itemis AG, Spirent Communications, Easy Global Market, Iskratel/Sintesio, …
SAMPLE TESTSUITE STRUCTURE: MQTT

- Broker as SUT
  - All mandatory message data fields
    - Regular and illegal data
      (Fixed/variable header, payload)
  - Protocol features
    - General
    - Connect/disconnect (session)
    - Subscribe/unsubscribe
    - Immediate publish
    - Last will and Testament (LWT)
    - Heartbeats keepAlive values
    - Topic
    - Error handling
- Client as SUT
  - ...
TEST DEVELOPMENT SAMPLE: MQTT

✓ Test configurations

✓ Test Suite Structure

✓ Test purpose (catalogue)

✓ Test implementation (TTCN-3)

<table>
<thead>
<tr>
<th>TP-ID</th>
<th>TP_MQTT_Broker_CONNECT_001</th>
</tr>
</thead>
<tbody>
<tr>
<td>Selection</td>
<td>PIC_Broker</td>
</tr>
<tr>
<td>Summary</td>
<td>The IUT MUST close the network connection if fixed header flags in CONNECT Control Packet are invalid</td>
</tr>
<tr>
<td>Reference</td>
<td>[MQTT-2.2.2-1], [MQTT-2.2.2-2], [MQTT-3.1.4-1], [MQTT-3.2.2-6]</td>
</tr>
</tbody>
</table>

Test purpose

Ensure that the IUT

on receipt of an CONNECT message containing header_flags := ‘1111’B

sends no RESPONSE message

and closes the Network Connection

Comments
# MQTT Broker Evaluation (Conformance, April 2018)

<table>
<thead>
<tr>
<th>Broker</th>
<th>PASS</th>
<th>FAIL</th>
<th>INCONCLUSIVE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>#</td>
<td>%</td>
<td>#</td>
</tr>
<tr>
<td>HiveMQ</td>
<td>39</td>
<td>86.67%</td>
<td>4</td>
</tr>
<tr>
<td>Mosquitto</td>
<td>38</td>
<td>84.44%</td>
<td>5</td>
</tr>
<tr>
<td>VerneMQ</td>
<td>37</td>
<td>82.22%</td>
<td>5</td>
</tr>
<tr>
<td>EMQ</td>
<td>35</td>
<td>77.78%</td>
<td>8</td>
</tr>
<tr>
<td>Iannister</td>
<td>31</td>
<td>68.89%</td>
<td>12</td>
</tr>
<tr>
<td>ActiveMQ</td>
<td>29</td>
<td>64.44%</td>
<td>14</td>
</tr>
<tr>
<td>aedes</td>
<td>26</td>
<td>57.78%</td>
<td>17</td>
</tr>
<tr>
<td>RSMB</td>
<td>26</td>
<td>57.78%</td>
<td>17</td>
</tr>
<tr>
<td>RabbitMQ</td>
<td>19</td>
<td>42.22%</td>
<td>26</td>
</tr>
<tr>
<td>Mosca</td>
<td>19</td>
<td>42.22%</td>
<td>24</td>
</tr>
<tr>
<td>HBMQTT</td>
<td>0.9</td>
<td>37.78%</td>
<td>28</td>
</tr>
<tr>
<td>Moquette</td>
<td>0.10</td>
<td>35.56%</td>
<td>29</td>
</tr>
</tbody>
</table>
TESTWARE: SECURITY

• Vulnerability scanner:
  – in particular for web applications, zero-day/fuzzing, consideration of data bases, traffic/network analyser, program code scanner

• Penetration tester, e.g. “SQL injection”

• Intrusion detection tools

• Load test/Scalability

• Further utilities: Model-based testing (UML testing profile) and risk modelling
FUZZING APPROACH

ATS: Abstract Test Suite
ETS: Executable TS

FUZZINC

Fuzzed Data

CoAP ATS

TTCN-3

CoAP ETS

IoT TESTWARE

TITAN

eclipse

Fraunhofer FOKUS
Results for CoAP:
- Initially, 4421 fuzzed test data for CoAP were generated
- After sending the data to a (local) CoAP server, it crashed after date “1107”

https://www.fokus.fraunhofer.de/de/sqc/security_testing
THE IOT-T PROJECT

Standardization & Certification
• **New Working Group (TST)** will develop IoT test catalogues and specifications (not covered elsewhere)

• The **types of testing** include conformance, interoperability, security and performance testing

• The initial technical **focus** will be:
  - IoT **network layer**
    (communication protocols, node connectivity, edge computing etc.),
  - **Basic security** of IoT devices
## ETSI ACTIVE WORKING ITEMS

<table>
<thead>
<tr>
<th>Work item number</th>
<th>Version</th>
<th>Current status</th>
<th>Next status</th>
<th>Rapporteur name</th>
<th>Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>DTS/MTS-TST8 (TS)</td>
<td></td>
<td>TB adoption of WI (2018-05-24)</td>
<td>Start of work</td>
<td>Wardaschka Andre</td>
<td>IEC 62443-4-2</td>
</tr>
<tr>
<td>DTS/MTS-TSTCoAP-1 (TS 103 596-1)</td>
<td>0.0.1</td>
<td>Early draft (2018-05-18)</td>
<td>Stable draft</td>
<td>Hackel Sascha</td>
<td>CoAP</td>
</tr>
<tr>
<td>DTS/MTS-TSTCoAP-2 (TS 103 596-2)</td>
<td></td>
<td>Start of work (2018-01-24)</td>
<td>Early draft</td>
<td>Hackel Sascha</td>
<td></td>
</tr>
<tr>
<td>DTS/MTS-TSTCoAP-3 (TS 103 596-3)</td>
<td></td>
<td>TB adoption of WI (2018-01-24)</td>
<td>Start of work</td>
<td>Hackel Sascha</td>
<td></td>
</tr>
<tr>
<td>DTS/MTS-TSTLoRaWAN (TS 103 598)</td>
<td></td>
<td>Early draft (2018-02-28)</td>
<td>Stable draft</td>
<td>AHMAD Abbas</td>
<td>LoRaWAN</td>
</tr>
<tr>
<td>DTS/MTS-TSTMQTT-1 (TS 103 597-1)</td>
<td>0.0.1</td>
<td>Early draft (2018-05-18)</td>
<td>Stable draft</td>
<td>Pintar Bostjan</td>
<td>MQTT</td>
</tr>
<tr>
<td>DTS/MTS-TSTMQTT-2 (TS 103 597-2)</td>
<td></td>
<td>TB adoption of WI (2018-01-24)</td>
<td>Start of work</td>
<td>Pintar Bostjan</td>
<td></td>
</tr>
<tr>
<td>DTS/MTS-TSTSecTM (TS 103 599)</td>
<td></td>
<td>TB adoption of WI (2018-01-23)</td>
<td>Start of work</td>
<td>AHMAD Abbas</td>
<td>Vul. database</td>
</tr>
<tr>
<td>DTS/MTS-TSTSecTM (TS 103 599)</td>
<td></td>
<td>TB adoption of WI (2018-01-23)</td>
<td>Start of work</td>
<td>AHMAD Abbas</td>
<td>Vul. database</td>
</tr>
</tbody>
</table>

*9 WIs, Work in progress, displaying 1 to 9*
IoT-Testlab Scope (basic security level certification)
Putting everything together
SUMMARY

- Advanced testing technology:
  - **Open source** IoT-Testware (code):
  - External (open source) SW
  - **Standardized** IoT test purposes:
(ALMOST) COMPLETE IOT-TESTWARE
OUTLOOK

• Adding more protocols to IoT-Testware
  AMQP, LWM2M, 6LoWPAN, LPWAN

• Increased security level for certification

• Cooperation/liaisons (*in preparation*) with
  ETSI TC Cyber/SmartM2M, oneM2M, OPC Foundation ...
Thank you for your attention!

https://www.fokus.fraunhofer.de/en/sqc