Protocol Conformance Testing for 4G/5G soft-UEs

Andre Puschmann, Paul Sutton, Ismael Gomez
Agenda

- Introduction
- srsLTE Overview
- srsUE Protocol Conformance Testing
An off-the-shelf handset

- Snapdragon SD838/SD845 16 GB NAND Flash
- Qualcomm WTRX855/LTE/3G/HSDPA/CDMA200/1X/DCS/PCS/GSM/EDGE/GPS/nano-SIM
- Qualcomm QMEM1 power-management IC
- Broadcom BCM4339 5G Wi-Fi combo chip with integrated power and low-noise amplifiers (the updated version of the BCM4335)
- Avago RF333
- Sony (Sensor MPL6551 six-axis Gyro + accelerometer) MEMS MotionTracking device
- Anadi Keenly AMB163 3-axis electronic compass

- SK Hynix HSC9N/NBD4/2G/4G/32N/2GB LPDDR3-1024 RAM
- The Qualcomm 2.26 GHz Snapdragon 805 SoC is layered beneath the SIM
- Qualcomm WCD9320 audio codec
- Analog Devices AD9900 S/PDIF transmission
- Qualcomm PM8961 power-management IC
- Texas Instruments BQ41921IC controlled 4.5 A USB-C power charger
- Avago ACMP-1300

User Conference on Advanced Automated Testing
A Software Defined Radio
The srsLTE Eco-System

- Core 4G/5G library
  - Modular and portable, high-performance library for PHY, MAC, RLC, PDCP, RRC, NAS, S1AP, NGAP, SDAP and GW
  - All bandwidths up to 20 MHz, TM1-4
  - Highly optimized Turbo decoder for Intel SSE4.1/AVX (+150Mbps in TM3/4)
- Applications
  - srsUE: First open-source SDR LTE UE
  - srsENB: A complete SDR LTE eNodeB application
  - srsEPC: A light-weight LTE core network
  - airScope: passive air-interface analyzer (not FOSS)

“Open-source 4G/5G software radio suite”

www.srslte.com
A Full E2E Open-Source Open LTE Solution

Radio Network

Core Network

Internet

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE

UE
<table>
<thead>
<tr>
<th>CVD-Year</th>
<th>ID</th>
<th>Name 1</th>
<th>Institution/URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVD-2018</td>
<td>0007</td>
<td>Altaf Shail</td>
<td>Technical University of Berlin and Kaitaki Labs</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><a href="https://www.isit.tu-berlin.de/security_in_telecommunications">https://www.isit.tu-berlin.de/security_in_telecommunications</a></td>
</tr>
<tr>
<td>CVD-2018</td>
<td>0007</td>
<td>Ravishankar Borgaonkar</td>
<td>SINTEF Digital and Kaitaki Labs</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><a href="https://www.sintef.no/en/cyber-security/">https://www.sintef.no/en/cyber-security/</a></td>
</tr>
<tr>
<td>CVD-2018</td>
<td>0008</td>
<td>David Rupprecht</td>
<td>Ruhr University Bochum and New York University Abu Dhabi</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Katharina Kohls</td>
<td><a href="https://www.alter-attack.net">https://www.alter-attack.net</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Christina Plopper</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Thorsten Holz</td>
<td></td>
</tr>
<tr>
<td>CVD-2018</td>
<td>0012</td>
<td>David Basn</td>
<td>ETH Zurich, Université de Lorraine, CNRS, Inria, University of Dundee</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Luca Hirschik</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sascha Rademirovi</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Reif Saase</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Vincent Stettler</td>
<td></td>
</tr>
<tr>
<td>CVD-2018</td>
<td>0014</td>
<td>Elisa Bertino</td>
<td>Purdue University</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><a href="https://www.cs.purdue.edu/homes/bertino/">https://www.cs.purdue.edu/homes/bertino/</a></td>
</tr>
<tr>
<td>CVD-2018</td>
<td>0014</td>
<td>Omar Chowdhury</td>
<td>University of Iowa</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><a href="http://homepages.divms.uiowa.edu/~comarhader/">http://homepages.divms.uiowa.edu/~comarhader/</a></td>
</tr>
<tr>
<td>CVD-2018</td>
<td>0014</td>
<td>Mitziu Echeveria</td>
<td>University of Iowa</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CVD-2018</td>
<td>0014</td>
<td>Syed Raffiul Hussain</td>
<td>Purdue University</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><a href="https://relentless-warrior.github.io/">https://relentless-warrior.github.io/</a></td>
</tr>
<tr>
<td>CVD-2018</td>
<td>0014</td>
<td>Ninghui Li</td>
<td>Purdue University</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><a href="https://www.cs.purdue.edu/homes/ninghui/">https://www.cs.purdue.edu/homes/ninghui/</a></td>
</tr>
</tbody>
</table>
## GSMA Mobile Security Hall of Fame

<table>
<thead>
<tr>
<th>CVD-2018</th>
<th>0007</th>
<th>Altas Shaik</th>
<th>Technical University of Berlin and Kaitaki Labs</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td><a href="https://www%E4%BF%A1%E6%81%AF%E6%8A%80%E6%9C%AF,secured_communications">https://www信息技术,secured_communications</a></td>
</tr>
<tr>
<td>CVD-2018</td>
<td>0007</td>
<td>Ravishankar Boriaonkar</td>
<td>SINTEF Digital and Kaitaki Labs</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><a href="https://www%E4%BF%A1%E6%81%AF%E6%8A%80%E6%9C%AF,cyber-security">https://www信息技术,cyber-security</a></td>
</tr>
<tr>
<td>CVD-2018</td>
<td>0008</td>
<td>David Rupprecht, Katharina Kohls, Christina Pöpper, Thorsten Holz</td>
<td>Ruhr University Bochum and New York University Abu Dhabi</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><a href="https://www%E4%BF%A1%E6%81%AF%E6%8A%80%E6%9C%AF,attack.net">https://www信息技术,attack.net</a></td>
</tr>
<tr>
<td>CVD-2018</td>
<td>0012</td>
<td>David Basin, Jannik Dreier, Lucca Hirsch, Saša Radosavljević, Reif Sasse, Vincent Stettler</td>
<td>ETH Zurich, Université de Lorraine</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><a href="https://arxiv.org/abs/1806.10360">CNRS, Inria, University of Dundee</a></td>
</tr>
<tr>
<td>CVD-2018</td>
<td>0014</td>
<td>Elisa Bertino</td>
<td>Purdue University</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><a href="https://www%E4%BF%A1%E6%81%AF%E6%8A%80%E6%9C%AF,bertino">https://www信息技术,bertino</a></td>
</tr>
<tr>
<td>CVD-2018</td>
<td>0014</td>
<td>Omar Chowdhury</td>
<td>University of Iowa</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>[<a href="http://homepage.divms.u">http://homepage.divms.u</a> Iowa.edu/~comraider](<a href="http://homepage.divms.u">http://homepage.divms.u</a> Iowa.edu/~comraider)</td>
</tr>
<tr>
<td>CVD-2018</td>
<td>0014</td>
<td>Mitzu Echeverria</td>
<td>University of Iowa</td>
</tr>
<tr>
<td>CVD-2018</td>
<td>0014</td>
<td>Syed Raffiul Hussain</td>
<td>Purdue University</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><a href="https://relentless-warrior.github.io">https://relentless-warrior.github.io</a></td>
</tr>
<tr>
<td>CVD-2018</td>
<td>0014</td>
<td>Ninghui Li</td>
<td>Purdue University</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><a href="https://www%E4%BF%A1%E6%81%AF%E6%8A%80%E6%9C%AF,ninghui">https://www信息技术,ninghui</a></td>
</tr>
</tbody>
</table>
Towards srsUE Protocol Conformance Testing

• Motivation
  • Conformance to 3GPP specifications
  • Interoperability
  • Regression testing
  • Extend current in-house testing

• Challenges
  • Very dynamic code base
  • Only interested in L2/L3 testing (full UE is out of scope here)
  • Integration into CI is a must
Typical Test Systems Don’t Fit

- Too big and expensive
- No protocol-only testing
Eclipse Titan

- Complete, full-featured TTCN-3 toolset developed by and widely used within Ericsson
- Released under Eclipse Public License (EPL) 1.0 in 2014
- Command line tools for compiling, executing and analysing functional and performance tests (generates native C++ code for GCC)
- Built-in codec generators for ASN.1 BER, JSON, XML, RAW
- GUI plugin for Eclipse with Executer and LogViewer
- Many testports also available under EPL 1.0 (e.g. TCP/UDP, telnet, SCTP, PCAP, SIP)
- 1.6 MLoC C++, 3kLoC in Java
Solution: Port 3GPP UE Testsuite to srsLTE/Titan

Goals:
- Develop SW to use 3GPP tests to test higher protocol layers of srsUE
- Full Jenkins/CI integration to execute with every pull-request

Steps:
1. Declare testports (TTCN3 to SS to DUT)
2. Implement codecs (e.g. ASN1 BER to PER converter, decorate type definitions for RAW codec)
3. Implement external function (e.g. security)
The NAS Codec Dilemma

- Titan (\(\leq 6.3\)) incapable of decoding NAS PDUs (from ETSI test suites)
- RAW codec cannot generate unpacker for mandatory fields in, e.g., ATTACH_REQUEST, with format LV (length and value but no type)

```plaintext
type record ESM_MessageContainer {
  IEI8_Type iei optional, /* present in case of TLV; omit in case of LV */
  INT16b iel,
  octetstring esmPdu optional /* ESM PDU without NAS security header; */
} with {
  encode "RAW"
  variant (iel) "LENGTHTO(esmPdu)";
};
```

- Ericsson provided internal EPS-NAS Definitions as 1st solution (now FOSS)
- Dilemma: Use those new types or make code generator work
- SRS filed bug, sketched possible solution and provided working hack
- Ericsson provided fix for RAW codec with new FORCEOMIT keyword
Current State

- Basic SS and TTCN3 DUT under AGPLv3 in srsLTE 19.09
  - Unmodified srsUE upper layers
  - RRC test model finished
  - MAC/RLC/PDCP work-in-progress
  - 5GNR EN-DC Inter RAT work-in-progress
- TTCN3 tester/testports, protocol codecs, security helpers, 3GPP testsuite patch for Titan not FOSS
- Full Jenkins/Github integration
Sources and Further Reading

- https://www.netdevconf.org/2.2/session.html?welte-ttcn3-talk
- http://www.ttcn-3.org/
- “Assessing Compliance of 5G Device Implementations To 3GPP Standards” by Olivier Genoud, ETSI (https://docbox.etsi.org/Workshop/2018/201812_ETSI_OAI/WORKSHOP/SESSION03/ETSI_GENOUID.PDF)
- https://www.3gpp.org/ftp/tsg_ran/WG5_Test_ex-T1/TTCN/Deliveries/TTCN3/
Thanks!
Backup slides
EUTRAN Test System Architecture

Figure 4.1.1-1: Architecture of system simulator

Source: TS 36.523 v8.6.0
srsLTE Testing (1)

- Static code analysis (SA)
  - Using Coverity and cppcheck
- Unit tests (UT)
  - Executed periodically in AWS Jenkins (i.e. make test)
  - Mostly PHY layer, and partly common (e.g. RLC)
  - Very limited for UE upper layers, (almost) non for eNB/EPC
  - Valgrind checks and address sanitizer runs (ctest memcheck)
srsLTE Testing (2)

- RF Conformance (TS 36.521)
- Protocol Conformance (TS 36.523)
  - 3GPP has defined entire conformance test architecture and conformance test cases based on TTCN3
- Pre-IOT Testing
  - RF continuous-integration (RF-CI)
  - Customer
- Interoperability Testing (IOT)
  - Carried out manually in the field in a live network