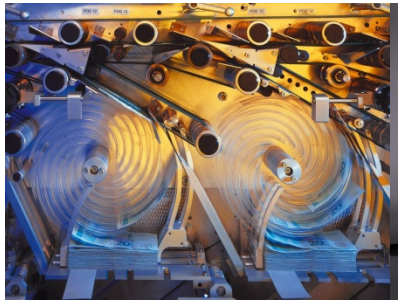
Development and Industrial Application of Multi-Domain Security Testing Technologies

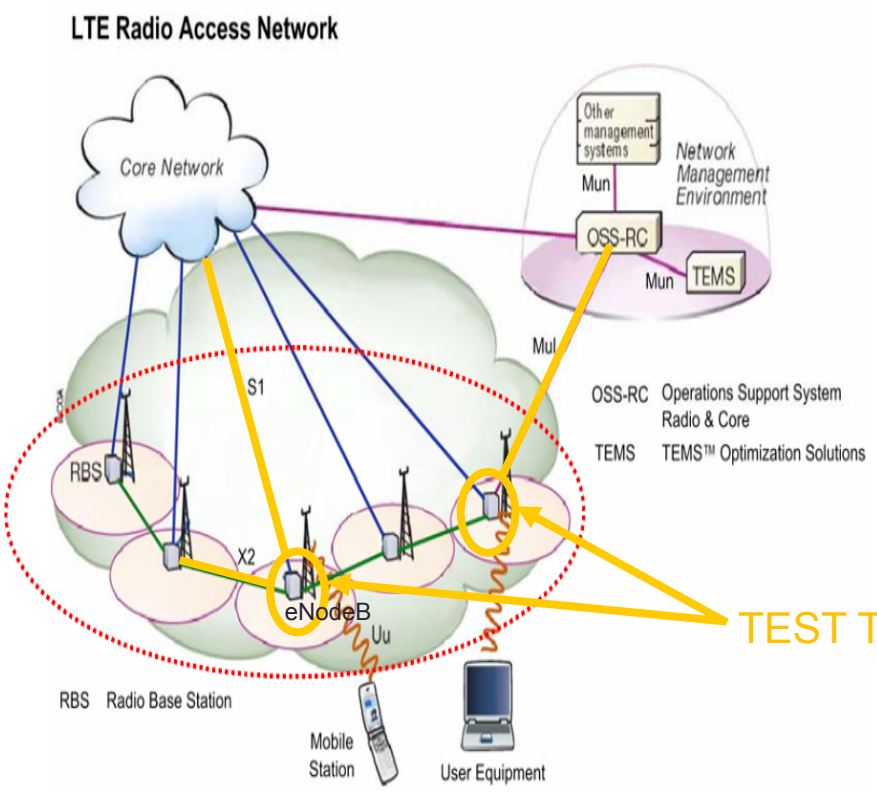
Case Study Experience Sheet
Telecom Case Study from Ericsson




ITEA 2
INFORMATION TECHNOLOGY FOR EUROPEAN ADVANCEMENT

Telecom Case Ericsson

Case study characterization



Telecommunications network (LTE, 4G) with all-IP network and smart terminals will introduce new threat scenarios triggered from radio network side. The main test target initially were radio base stations but during the project different types of network nodes were tested.

Telecom Case Ericsson
Case study characterization

- Security challenges
  - **More sophisticated end-terminals:** The possibility to use smart terminals as attack devices as it is closer to PC than pure phone.
  - **End-user device becomes target:** All IP-addressing makes end-user device an attractive target.
  - **Risk factor for attacks from radio side higher:** Limited tools and knowledge available, but increased interest from hackers due to all IP and smart terminals becoming main stream.
  - **No open-source or commercial tools available off-the-shelf for testing certain parts of radio protocols:** Proactively find ways to run security testing on radio side and find vulnerabilities early enough.

Telecom Case Ericsson

Testing approach: risk-driven fuzz testing

- Combine risk driven methodologies with fuzz testing
  - Derive initial set up test cases from security-oriented risk analysis
  - Take traffic capture of the valid, real traffic for the target test protocol and node
  - Analyze the capture and plan for actual test cases based on the capture and risk analysis
  - Generate test cases with generic fuzzer framework using valid traffic as input
  - Send **invalid sequences** to the target
  - Observe and validate results, report found vulnerabilities to the product organization to further evaluation and resolution
  - Re-test when vulnerabilities corrected

Telecom Case Ericsson
Results

- **Focus on vulnerabilities on new protocol layers**
  - No open source or commercial tools existed earlier
- **Some vulnerabilities also found**
  - protocol message faults, handover instabilities and even target crashes
  - errors visible in log files, but no major impact on node robustness
- **Metrics**
  - Measurable results for the tests were to gain understanding of the security posture for specific protocol

Telecom Case Ericsson
Exploitation

- **Generic fuzzer developed has been proved of value in**
  - test case selection
  - Addressing specific needs in radio layer testing with narrow test scope, but still getting good results
  - Testing vendor specific extensions
- **Saved time and resources due to**
  - The ability to take traffic capture of real traffic
  - Use that as input to restrict number of test cases that will actually be run
  - Faster verification of found vulnerabilities after fixing them
- **Confidence that security posture of new protocol layers can actually be tested with reasonable effort**

Telecom Case Ericsson
Summary

- **Improvement gains according to DIAMONDS STIP:**