RADIX SECURITY

SEcurity Assurance Library (SEAL) 5G

SEcurity Assurance Library (SEAL) 5G

5G network technology and its security pose a major challenge due to their complexity. Certification plans increase the pressure on vendors, test facilities, operators, and integrators.

Radix SEAL 5G allows for testing vulnerabilities and simulating attacks in a 5G core network. It includes the 3GPP testing standard, making it suitable for the product evaluation schemes GSMA NESAS and BSI NESAS-CCS-GI. The tool offers fast testing cycles and an easy-to-use command line interface. It can be integrated into an existing test environment (CI/CD) for rapid development.

Main Advantages

- **User-Friendly and Actionable**: An intuitive command line tool designed for users without extensive security expertise. This reduces the complexity and challenges of 5G Security to a level that is understandable and makes the results actionable.
- **Automation**: The testing process is significantly shortened due to high levels of automation. This allows for more frequent testing in the laboratory and current network operation, enabling quick adjustments to be made. On average, a complete test run for critical 5G components takes less than 10 minutes.
- **Compliance**: Ensures security compliance with industry standards such as GSMA NESAS and BSI NESAS-CCS-GI.
- **Integration options**: We hereby implement the usual industry use cases.
    - CLI: Can be used as a stand-alone command line tool.
    - CI/CD pipeline: Can be integrated into a CI/CD pipeline for continuous testing.
    - Kubernetes: Can be used for regular scanning in a Kubernetes cluster.

Use Cases

Currently, we see the following areas of application for Radix SEAL to test the vulnerabilities of your network.

- **Vendors:** You are required by your customer or legal requirements to meet the latest security standards. Radix SEAL can be easily integrated into your development pipeline to continuously check security of your products. You always know if your products meet the latest security standards, and if not, you get an actionable report for your development team.
- **Certification and test facilities:** You would like to offer test services for NESAS and NESAS-CCS-GI schemes. However, the 3GPP specification and test cases are complex to implement. Radix SEAL is designed to be easy to use, even without a 5G security background, and it simplifies the artefact generation, enabling you to offer NESAS and NESAS-CCS-GI certification.
- **MNOs:** You want or need to verify the security measures in your operational network, but the complexity of your network makes it impossible to do this manually. Radix SEAL is able to automatically test the virtualised network environment and generate actionable reports for your team and potential security auditors.
- **Integrators:** You are deploying a campus network for a customer and you are questioning if the network is secure, e.g. if the connection is encrypted over the air. Radix SEAL is designed to verify the security implementation of the network. This gives the customer the assurance that 5G is secure to use.

General Features

The test suite supports the following general features:

- User guide providing clear descriptions of test cases and sequence diagrams. It's designed to help you understand the test cases, regardless of your level of familiarity with 5G and security.
- Configuration through a straightforward TOML file.
- A command line interface with autocompletion, ensuring an easy-to-use experience in production.
- Reporting: We support different report formats:
    - JUnit: which allows seamless integration with existing test management frameworks.
    - JSON: which allows the integration into a web application
    - Colorized table view: which allows an overview in the command line
- Enhanced reporting that supports the automatic report generation for certification (NESAS and NESAS-CCS-GI) including:
    - More detailed reasons in machine-readable report files
    - Contains values that influence the verdict
    - Can be used by testers to verify verdict if the verdict is correct
    - It gives more information as to why a specific verdict was given
- Detailed logging in both log files and standard output.
    - separate log files for each check
    - Configurable log levels for in-depth packet analysis.
    - Detailed tracing in pcap files, allowing artifact evaluation via Wireshark.
- Connectivity:
    - SOCKS5 connectivity that enables you access to network functions (NFs) only available through a jump host, e.g., circumventing the demilitarised zone.
- Support of different test case versions and derivations:
    - The challenge is that different network products support different releases in 3GPP and need to be certified accordingly. In addition, these 3GPP test cases have also been refined by local authorities. For example, the BSI (Federal Office for Information Security (Germany)) refines certain test cases in the document called AIS-N2.
    - We implemented a test case version and tracking system, to execute the test cases variant
    - Internal test case versioning:
        - Major: breaking changes, e.g. different test flow than before
        - Minor: non-breaking feature additions, e.g. more verbose output
        - Patch: fixes to restore intended behavior

- Exit codes for easy integration into a CI/CD pipeline.

Supported Network Function

For each network function, we support the network functions and test cases. A full list of test cases can be found in the Appendix.

NRF

- Basic NRF SCAS Tests based on TS 33.518
- Additionally, several new test cases allow mapping of the 5G core network infrastructure.
    - Allowed PLMN list, allowedNFType, ...

AMF Tests

- Basic AMF SCAS tests based on TS 33.512.
- An additional AMF security test allows for testing the correct behavior of the AMF when faced with an attacker UE. This includes, for example:
    - Emergency bearer establishment circumvention
    - Invalid security capabilities in NSA deployment
    - Authentication circumvention via the use of unordered protocol procedures.

UDM Tests

- Basic UDM SCAS Tests based on TS 33.514
- Additional test cases:
    - A) Aim to extract the private keys for the SUPI encryption
    - B) Aim to manipulate the authentication state in the UDM of a UE.

General Tests (TS 33.117)

These test cases need to be applied to each network function if they are applicable, i.e. if they support the interface accordingly.

- Test cases based as described in 4.2.2.2.3 Authorization of NF Service Access

Requirements and Interfaces for Testing

The tool has the following requirements for testing:

- Testing the AMF requires exposure of the NGAP interface.
- For all other network functions, the exposed interface of the SBA needs to be available.
- If the core network uses OAuth and TLS, we need to be able to generate a certificate accordingly.

- Furthermore, we need to know one IMSI of a subscriber in the database and the corresponding permanent key.
- Additionally, we need to know the public key (Profile-A and Profile-B) of the SUCI Encryption feature.

Roadmap

We plan to release monthly updates and aim to include the following features in our roadmap. The roadmap is subject to change based on customer requirements.

Planned features for Q2/2024

- Split network config / global settings from run config for easier configuration
    - Allow using multiple network components of the same type (e.g. multiple AMFs)
- Improve usability of configuration formats
- Check connectivity before and during runs

Planned features for Q3/2024

- SMF test cases (3GPP TS33.515)
- AUSF test cases (3GPP TS33.516)
- Additional NRF test cases for OAuth2.0 (Additional to TS33.518)

Planned features for Q4/2024

- UPF test cases (3GPP TS33.513)
- UDR test cases
- SEPP test cases (3GPP TS33.517)
- Automatable general test cases (33.117)

Included Test Cases

AMF tests (3GPP TS33.512):

* TC_5G_GUTI_ALLOCATION_AMF_A (version 0.7.1)
* TC_5G_GUTI_ALLOCATION_AMF_B (version 0.7.1)
* TC_5G_GUTI_ALLOCATION_AMF_C (version 0.7.1)
* TC_AMF_REDIRECTION_5GS_EPS (version 0.7.1)
* TC_BIDDING_DOWN_XN_AMF (version 0.7.1)
* TC_NAS_INT_SELECTION_USE_AMF (version 0.7.1)
* TC_NAS_NULL_INT_AMF_A (version 0.7.1)
* TC_NAS_NULL_INT_AMF_B (version 0.7.1)
* TC_NAS_REPLAY_AMF (version 0.7.1)
* TC_RES_STAR_VERIFICATION_FAILURE_A (version 0.5.2)
* TC_RES_STAR_VERIFICATION_FAILURE_B (version 0.6.0)
* TC_SYNC_FAIL_SEAF_AMF_A (version 0.7.1)
* TC_UE_SEC_CAP_HANDLING_AMF_A (version 0.5.1)
* TC_UE_SEC_CAP_HANDLING_AMF_B (version 0.5.1)
* TC_UE_SEC_CAP_HANDLING_AMF_C (version 0.5.1)
* TC_UE_SEC_CAP_HANDLING_AMF_D (version 0.5.1)
* TC_UE_SEC_CAP_HANDLING_AMF_E (version 0.5.1)
* TC_UE_SEC_CAPS_AS_CONTEXT_SETUP (version 0.7.1)

NRF tests (3GPP TS33.518)::

* TC_DISC_AUTH_SLICE_NRF (version 0.8.0)
* AS_DISC_AUTHORIZATION_SLICE_NRF_CR (version 0.2.0)
* AS_DISC_AUTHORIZATION_ALLOWED_PARAMETER_A (version 0.1.0)
* AS_DISC_AUTHORIZATION_ALLOWED_PARAMETER_B (version 0.1.0)
* AS_DISC_AUTHORIZATION_ALLOWED_PARAMETER_C (version 0.1.0)

* AS_DISC_AUTHORIZATION_ALLOWED_PARAMETER_D (version 0.1.0)

* AS_DISC_AUTHORIZATION_ALLOWED_PARAMETER_E (version 0.1.0)

* AS_DISC_AUTHORIZATION_ALLOWED_PARAMETER_F (version 0.1.0)

UDM tests (3GPP TS33.514):

* TC_AUTH_STATUS_STORE_UDM (version 0.4.0)

* TC_DE_CONCEAL_SUPI_FROM_SUCI_UDM_NULL_SCHEME (version 0.5.0)

* TC_DE_CONCEAL_SUPI_FROM_SUCI_UDM_PROFILE_A (version 0.5.0)

* TC_DE_CONCEAL_SUPI_FROM_SUCI_UDM_PROFILE_B (version 0.5.0)

* TC_SUCI_PROFILE_B_REJECT_INVALID_PUBKEY (version 0.4.0)

* TC_SUCI_PROFILE_B_REJECT_NO_COMPRESSION (version 0.5.0)

* TC_SYNC_FAILURE_HANDLING (version 0.3.0)

* TC_UP_SECURITY_ENFORCEMENT_CONFIG (version 0.4.0)

* TC_UP_SECURITY_POLICY_CONFIG (version 0.3.0)

* TC_VERIFY_AUTH_SYNC_FAIL_MSG_UDM (version 0.3.0)

General tests (3GPP TS33.117):

* TC_AUTHORIZATION_TOKEN_VERIFICATION_FAILURE_ONE_PLMN_1 (version 0.4.0)

* TC_AUTHORIZATION_TOKEN_VERIFICATION_FAILURE_ONE_PLMN_2 (version 0.4.0)

* TC_AUTHORIZATION_TOKEN_VERIFICATION_FAILURE_ONE_PLMN_3 (version 0.4.0)

* TC_AUTHORIZATION_TOKEN_VERIFICATION_FAILURE_ONE_PLMN_4 (version 0.4.0)

* TC_AUTHORIZATION_TOKEN_VERIFICATION_FAILURE_ONE_PLMN_5 (version 0.5.0)

* TC_AUTHORIZATION_TOKEN_VERIFICATION_FAILURE_ONE_PLMN_6 (version 0.4.0)

* TC_AUTHORIZATION_TOKEN_VERIFICATION_FAILURE_ONE_PLMN_7 (version 0.4.0)

* TC_AUTHORIZATION_TOKEN_VERIFICATION_FAILURE_ONE_PLMN_8 (version 0.4.0)