Attack configuration Engine for 5G networks

Zujany Salazar[0000−1111−2222−3333], Huu Nghia Nguyen[0000−1111−2222−3333], Wissam Mallouli[0000−1111−2222−3333], Ana R. Cavalli, and Edgardo Montes de Oca[0000−1111−2222−3333]

Montimage, France
firstname.lastname@montimage.com

Abstract. The evolution of 5G mobile networks towards a service-based architecture (SBA) comes with the emergence of numerous new testing challenges and objectives. Regarding security testing, 5G issues have been the subject of numerous studies. Standardization organisms list collections of threats and vulnerabilities, also investigated by academia and industrial researchers. However, there is no specific tool on the market that allows easy 5G security testing to verify if its components are protected against reported security issues. In this paper, we propose AcE which is an attack configuration engine conceived in the context of H2020 SANCUS project dealing with 5G network security.

Keywords: 5G · Traffic Engineering · Attack Injection · Fuzz Testing.

1 AcE: Attack configuration Engine for 5G networks

1.1 Context: SANCUS project

Security, Trust and Reliability are crucial issues in mobile 5G networks from both hardware and software perspectives [2]. These issues are of significant importance when considering implementations over distributed environments, i.e., corporate Cloud environment over massively virtualized infrastructures as envisioned in the 5G service provision paradigm. The SANCUS[1] solution intends providing a modular framework integrating different engines in order to enable next-generation 5G system networks to perform automated and intelligent analysis of their firmware images at massive scale, as well as the validation of applications and services. SANCUS also proposes a proactive risk assessment of network applications and services by means of maximising the overall system resilience in terms of security, privacy and reliability.

1.2 Attack configuration Engine

The proposed AcE engine in SANCUS delivers inclusive solution for modelling and emulating network container services and applications, along with network-wide attacks, forensic investigations, and tests that require a safe environment

[1] H2020 SANCUS project was started on September 1st, 2020 and lasts 3 years. More details can be found in: https://www.sancus-project.eu/

without the risk of proprietary data loss or adverse impact upon existing networks. It also simulates the main attacks identified by the ENISA [3]. The strength of this engine is that it will allow testing not only large-scale network infrastructures, but also emulating the end-users (IoT, routers, hotspots). One of the main components of this tool is 5Greplay solution designed by Montimage.

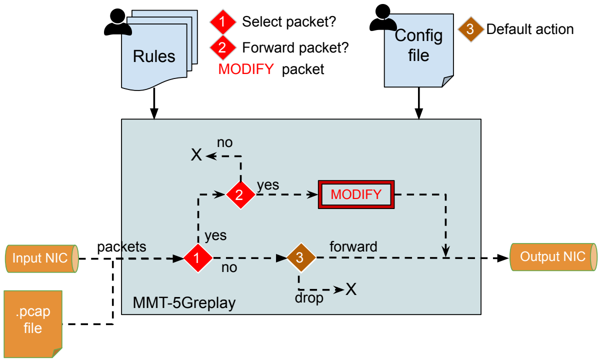

Fig. 1. 5Greplay main architecture

5Greplay[2] is an open-source 5G fuzzer that allows forwarding 5G network packets from one network interface card (NIC) to another with or without modification. It can be considered as a one-way bridge between the input NIC and the output one. It can also take as input pre-captured 5G packets that are saved in a PCAP-format file. Its behavior is controlled by user defined rules and completed by a configuration file. The user defined rules allow explicitly indicating which packets can be passed through the bridge and how a packet is to be modified in the bridge. The configuration file allows specifying the default actions to be applied on the packets that are not managed by the rules, i.e., if they should be forwarded or not. Thanks to its ability to create a variety of 5G network traffic scenarios, 5Greplay enables the implementation of cyberattacks, such as those identified by ENISA [3], as well as the security test cases proposed by the 3GPP [1]. 5Greplay's global architecture is depicted in Figure 1.

References

1. T. 3rd Generation Partnership Project (3GPP). 3gpp ts 33.117 – catalogue of general security assurance requirements, 2020.
2. I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov. Overview of 5g security challenges and solutions. *IEEE Communications Standards Magazine*, 2(1):36–43, 2018.
3. ENISA. Enisa threat landscape for 5g networks, Feb 2021.

[2] http://5greplay.org/