Experimental Evaluation of xApp-related Vulnerabilities in the O-RAN's RAN Intelligent Controller Implementation

In previous mobile network generations, Radio Access Networks (RAN) have been treated as a proprietary, closed network segment that is specific to every operator. To accelerate development and innovation, new initiatives such as the O-RAN ALLIANCE were born, aiming to split the RAN into different components and standardize the open interfaces that connect them.

Fundamentally, O-RAN leverages the concept of Software Defined RAN (SD-RAN) by decoupling the RAN data plane from the control plane and introducing several new RAN-controlling components. One of the central components is the near real-time RAN Intelligent Controller (nearRT-RIC), which manages the RAN (network slices, handovers, etc). The nearRT-RIC is designed to allow both the use of traditional, rule-based policies and Machine Learning or data-driven ones to optimize the RAN operation. The logic of these policies is encapsulated in applications called xApps that run on the nearRT-RIC platform and can read and modify different parameters of the RAN.

While providing opportunities for efficient resource management, the nearRT-RIC is also a prospective target for attackers, because of its control power over the RAN. Specifically, an attack vector is a malicious xApp that can interfere with other legitimate xApps running on the nearRT-RIC.

NearRT-RIC implementations are still in their infancy and suffer from bugs and security vulnerabilities. These vulnerabilities are also prevalent in open-source implementations such as O-RAN Software Community’s (OSC) RIC [1], where malicious xApps may disrupt the nearRT-RIC operation. The H Release of the OSC nearRT-RIC suffers from two major vulnerabilities that can compromise the operation of the RIC and crash it [2]. Additionally, a crafted packet sent by an xApp can crash memcpy and implicitly the whole OSC nearRT-RIC [3]. Such vulnerabilities significantly hinder the wide-scale adoption and deployment of O-RAN.

Objectives

The goal of this student thesis is to reproduce the attacks discussed in [2] and [3] for the newer OSC nearRT-RIC I Release. Additionally, after reproducing the existing attacks and understanding the OSC RIC Platform, the student is expected to explore new attack attempts with the same goal of disrupting OSC nearRT-RIC. Special focus will be put on the critical components of the system, such as the Subscription Manager and Subscription Procedures, Routing Message Router, other xApps, and O1/A1/E2 Terminations.
https://docs.o-ran-sc.org/en/latest/projects.html#near-realtime-ran-intelligent-controller-ric,


https://www.trendmicro.com/en us/research/23/l/the-current-state-of-open-ran-security.html,

Prerequisites
- Experience with Docker and Kubernetes
- Linux Knowledge
- C/C++ Knowledge is a plus

Contact
- Razvan-Mihai Ursu (razvan.ursu@tum.de)
- Dominik Brunke (Dominik.Brunke@ZITiS.bund.de)

Advisors
Razvan-Mihai Ursu