Analysis of UE-initiated Signaling Storms and Their Impact on 5G Network Security

Signaling storm is a specific type of DDoS attack, which emerges from frequent small-scale signaling activities of a group of compromised UE. Typically, signaling messages are exchanged between UE and the network for establishing communication sessions and managing network resources. However, signaling attacks abuse regular procedures to generate high number of signaling messages within a short period. The generation of excessive signaling load increases the network congestion and consumes resources. In 5G, UEs must send a request to initiate themselves and establish the communication with the 5G core. These initial registration request messages contain UE related information about identity, location and capabilities. The recent research internship focused on signaling storms has revealed that an initial registration request flood can generate significant signaling load and stress the network core. In the scope of mentioned internship, a simulation environment was created using UERANSIM and open5GS to investigate the impact of repetitive initial registration requests from a botnet comprising hundreds of UEs on control plane resources. The master thesis involves a comprehensive research study based on this initial observation to identify other signaling attack scenarios initiated by UEs, that abuse regular UE signaling for registration processes, inter-slice handovers and mobility handovers. Furthermore, assessing the impact of these scenarios and exploring possible detection methodologies are crucial for the intended study.

Motivation: 5G networks are designed to be used for three types of connected services: Enhanced Mobile Broadband (eMBB), Ultra Reliable Low Latency Communications (URLLC) and Massive Machine Type Communications (mMTC). Higher throughput, reliable connections and low latency capabilities of 5G networks should meet uninterrupted and robust data exchange requirements of users. Both the industry and individual users heavily rely on seamless connectivity. However, numerous studies have shown that 5G networks are vulnerable to signaling threats and DDoS attacks, which are becoming more severe due to the growing number of mobile and IoT devices. Such attacks can increase latency and impact service availability. The majority of literature on this topic examines potential 5G threats including signal storms and their effect on users. Even some detection and prevention techniques have been proposed. Although these studies provide valuable information about signaling storms, it has not been particularly investigated how control plane resources can be exploited by flooding UE initiated and 5G protocol specific requests. The research gap regarding concrete statements to reproduce signaling attacks is the main motivation of this study.

Objectives and Research Question: This work will focus on UE initiated DDoS attacks targeting control plane resources of 5G networks and it will question if these attacks can have a severe impact on practical 5G test setup. Therefore, signaling procedures particularly the ones involving NAS and NGAP protocols, will be explored to identify scenarios for UE initiated signaling attacks. The characteristics of the identified scenarios will be derived by theoretical analysis. The remaining objectives are reproducing these scenarios conducting experiments with appropriate simulation tools, evaluating the impact of these attacks on the network and user experience and investigating detection solutions for signaling storms.

Challenges: The identified scenarios should be demonstrated and analyzed to study the research question, which poses two main challenges. Designing a simulation environment for realistic attack reproduction is elaborate, which requires determining the most suitable solution to simulate UE, gNB and 5GC among existing solutions. The simulation environment cannot completely replace the real 5G network and there will be some restrictions. Therefore, the second challenge is to design
experiments in a way that allows the derivation of general statements about 5G security threats from observations made during the experiments.

Contribution: This thesis will address the signaling attacks on the control plane of 5G networks by identifying concrete signaling scenarios to generate excessive packet floods, analyzing them, and demonstrating them to assess their impact on the network. The simulation environment will allow reproducing various attacks to derive characteristics of the attacks, which are required for detection by distinguishing between good and malicious communication patterns. Overall, this work will contribute to the improvement of network security.

**Advisors**

Oliver Zeidler, Maximilian Stephan
Tim Niehoff (IPOQUE)