Paper: AdaptOver: Adaptive Overshadowing Attacks in Cellular Networks

Summary:

This paper presents a new type of attack system called AdaptOver, designed to perform man-in-the-middle attacks on cellular networks, like LTE and 5G-NSA. This system allows an attacker to decode, overshadow, and inject arbitrary messages between the mobile device and the core network, without the need for a fake base station. Leveraging overshadowing, AdaptOver can cause a persistent denial-of-service attack or a privacy leak by triggering a user's mobile device to transmit its persistent identifier (IMSI) in plain text. It can overshadow both downlink and uplink messages on the radio link at any point in time and on any communication layer of LTE. It can also launch stealthy and persistent DoS attacks or privacy leakage by making the UE broadcast its IMSI in plain text. It can attack all UEs in a cell in parallel or selectively based on their TMSI. These attacks can be launched against all users within a cell or specifically target a victim based on their phone number. The effectiveness of AdaptOver is demonstrated on live operational LTE and 5G-NSA networks, using a software-defined radio and a low-cost amplification setup. The ability of AdaptOver to launch an attack on a victim more than 3.8km away from the attacker is proven by empirical results in the paper. The authors suggest that a paradigm shift is needed in designing security mechanisms to address the new threat posed by systems like AdaptOver as existing countermeasures against attacks on cellular networks, which are mainly focused on detecting fake base stations, are no longer sufficient. Overall, the paper highlights the need for more robust security mechanisms to protect against man-in-the-middle attacks on cellular networks, which can have significant impacts on privacy and availability.

Strengths:

1. The AdaptOver attack system executes higher-layer protocol attacks which gives it the ability to modify ongoing procedures between UE and the core network in real time. It debunks the belief of the requirement of a fake base system to achieve this scenario and hence presents a novel attack.
2. The layout of the attack in terms of assumptions made gives a strong explanation of the conditions taken into consideration. It shows the attacker’s capability without having access to cryptographic material, user equipment, or cellular network infrastructure. The equipment required is commercial off-the-shelf hardware hence attack costs aren’t high.
3. The IMSI Extractor method is able to circumvent the security mode the UE enters. This attack system is able to link both previous and future passive connection observations that have TMSI and persistent IMSI since the UE retries the original re-attachment procedure and circumvents this issue.

Weakness:

1. In the uplink DoS attack, the attacker needs to find an IMSI that will trigger an Attach Reject with a cause value corresponding to a persistent DoS which can be achieved through brute-forcing the IMSI space, but this can be time-consuming and resource-intensive.
2. The AdaptOver attack takes into consideration that an attacker is using just one set of equipment, the evaluation of attack in presence of multiple attacker equipment isn’t discussed by the paper, would this addition result in longer DoS attacks? More efficiency? More coverage of area/ cells? These questions remain unclear.
3. The paper discusses potential countermeasures that baseband manufacturers and operators could implement to mitigate the proposed DoS attacks. It does not provide an in-depth analysis of the effectiveness of these countermeasures or state the effectiveness or impact of other possible defenses they mention.