Paper: 5G SUCI-Catchers: Still catching them all?

Summary:

This paper discusses the extent to which 5G standards fix the issue of tracking users dealt with by previous network generations and keeps the privacy promise made by it. This is done by demonstrating a proof-of-concept 5G SUCI catcher attack in a standalone 5G network to confirm the presence of multiple subscribers and explore the practical limits of the attack's scalability. This is built upon the shortcomings of the Authentication and Key Agreement (AKA) procedure and helps link encrypted SUCIs to the encrypted identities between sessions. The authors evaluate the SUPI-SUCI concealment and find that an active Machine-in-the-Middle (MitM) can verify the presence of an individual. They also enhance the SUCI-Catcher attack to track multiple users, demonstrating the ability to check for the presence of more than 500 Persons of Interest (PoI) within 60 seconds in a lab setting. The paper also discusses the attack's implications for users and possible mitigation strategies and hopes that their findings will enable operators to deploy SUCI encryption effectively and drive further security efforts within the 3GPP.

Strengths:

1. The SUCI attack uses one major flaw of the current 5G standard: it doesn’t rely on the failure cause, rather it detects the UE’s presence based on the message type (reject or accept). This means that even if the failure cause and message type could be hidden, the attacker would observe whether the connection establishment proceeds or not, this linkability can’t be circumvented currently.
2. The reset stage allows an attacker to repeat the SUCI probe step and search for multiple attackers. This helps to circumvent the limitation of only being able to search for a maximum of 2 people of interest.
3. The strength of the SUCI-Catcher attack is its scalability for small groups of targets, as it can quickly verify if the unknown person is among a group of 10 persons of interest.

Weakness:

1. The sim cards tested were based on 3 commercial operators, these are pretty low compared to the numerous providers available in the market. This doesn’t present a very strong claim made by USIM speed. Moreover, the attack is set up in a lab setting using Oneplus 8 user equipment. It would have been useful to have used at least 5-6 5G-supported devices to draw more convincing experimental results.
2. This attack remains feasible only as long as the linakbility and generation of fresh authentication tokens are feasible in the new standard.
3. Since the attacker can send multiple authentication requests and it’s not guaranteed that one request is enough for the attack to be successful, the UE can use some anomalous protocol behavior detection to limit/ delay or not respond to the request altogether, this limits the scalability of the attack.