**Call Me Maybe: Eavesdropping Encrypted LTE Calls With REVOLTE**

**Summary**

Authors in the paper propose a technique called ReVoLTE that can be used to eavesdrop and recover the contents of an encrypted VoLTE call. This attack exploits a concept called keystream reuse when two calls use the same keystream to encrypt the data during one active radio connection. By conducting a call within a short time window, the attacker is able to recover the initial keystream that can then be used to decrypt the contents of a recorded target call. The authors of the paper also demonstrate real-world evaluation of this approach and find that two out of three operators on whom the attack was conducted were vulnerable. Paper is ended with short and long-term countermeasures that can be used to prevent this type of attack.

**Strengths**

* The ReVoLTE attack described in the paper is feasible over commercial networks and practical evaluation is conducted unlike the previous attack vectors such as Raza and Lu [36] which had only theoretical assessment.
* The impact and severity of the attack are high considering VoLTE is used widely around the world and experiments conducted by the authors show that 89% of the binary representation of the recorded call was decrypted successfully and 12 of the 15 sampled eNodeB are prone to REVOLTE across wide geographical locations.
* The authors also provide detailed potential mitigations that can be deployed by the providers and also discuss how users can protect themselves. This is very relevant in this paper considering the wide usage of VoLTE by people all around the world.

**Weaknesses**

* This attack requires knowledge of the victim’s phone number and current position. Hardware worth $7000 might also be necessary while sniffing radio layer transmission. Although this is not a significant deterrent for sophisticated attackers, however, this might reduce the scope and practicality for a normal attacker.
* For a targeted attack, the adversary has to know whether the victim is currently on a call or not. Authors suggest some stepping-stone attacks but don't necessarily test whether those attacks and ReVoLTE work well together or not.
* To provide complete decryption of the call, the keystream call must be at least as long as the target call so that it provides a sufficient number of bits, or only part of the call can be decrypted.