Call Me Maybe: Eavesdropping Encrypted LTE Calls With ReVoLTE

8-10 minutes

David Rupprecht, Katharina Kohls, Thorsten Holz, and Christina Pöpper

Ruhr-Universität Bochum & New York University Abu Dhabi

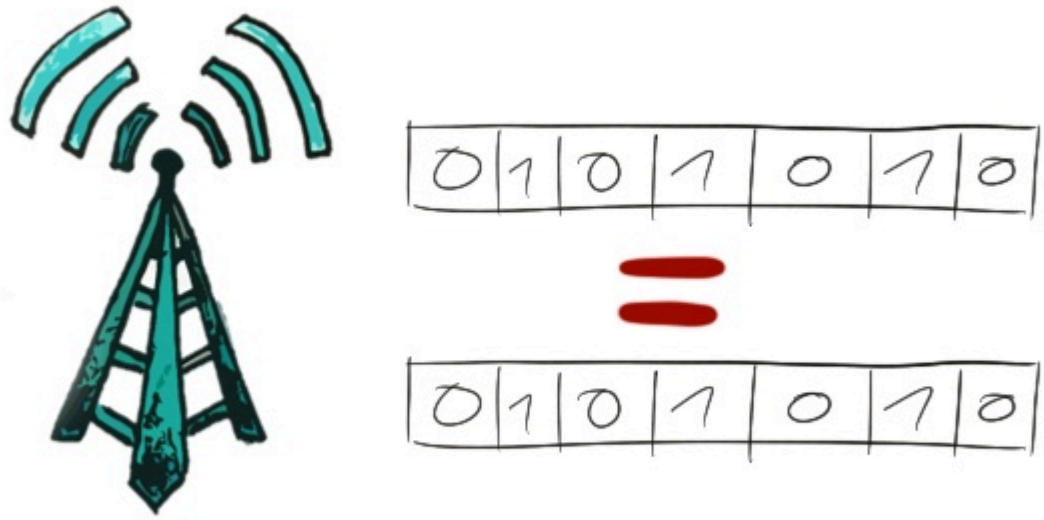
Introduction

Voice over LTE (VoLTE) is a packet-based telephony service seamlessly integrated into the Long Term Evolution (LTE) standard. By now all major telecommunication operators use VoLTE. To secure the phone calls, VoLTE encrypts the voice data between the phone and the network with a stream cipher. The stream cipher shall generate a unique keystream for each call to prevent the problem of keystream reuse.

We introduce ReVoLTE, an attack that exploits an LTE implementation flaw to recover the contents of an encrypted VoLTE call. This enables an adversary to eavesdrop on VoLTE phone calls. ReVoLTE makes use of a predictable keystream reuse. Eventually, the keystream reuse allows an adversary to decrypt a recorded call with minimal resources.

We provide an overview of the ReVoLTE attack, the implications, and demonstrate the feasibility of the ReVoLTE attack in a commercial network. Further, we publish an App that allows tech savvy people to track networks down that are still vulnerable. Our work will appear at the 29th USENIX Security Symposium (2020) and all details are available in a pre-print version of the paper.

ReVoLTE Attack



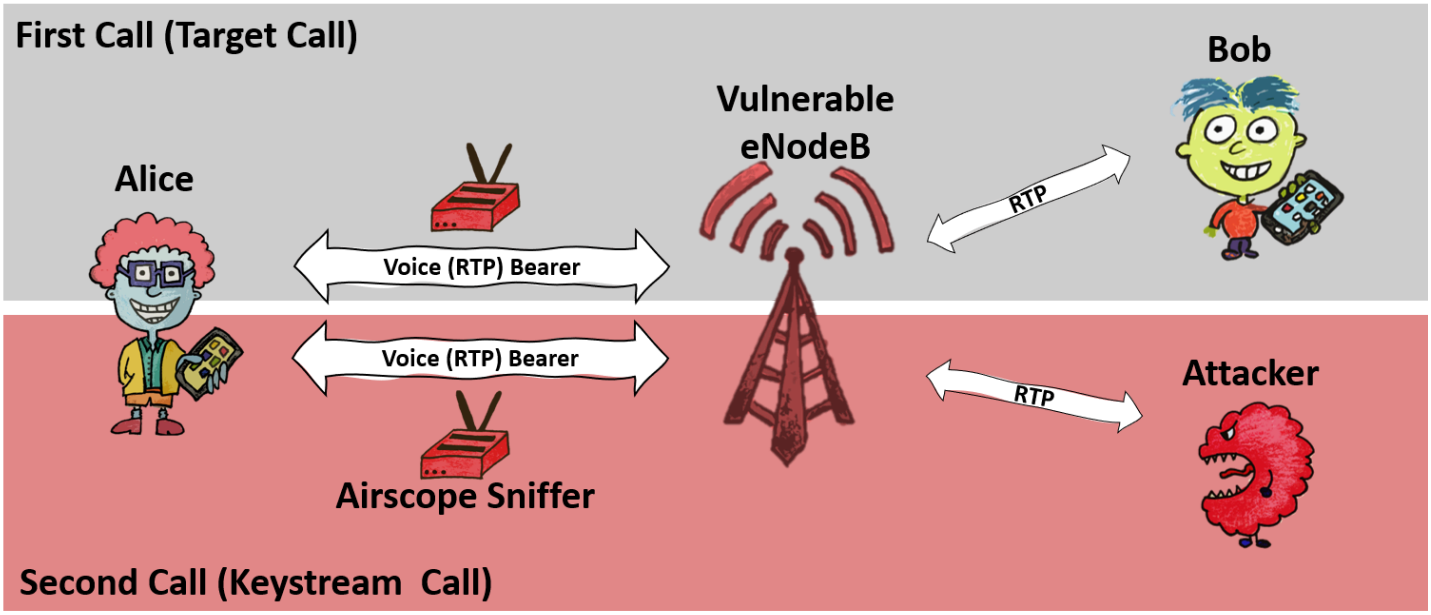
What does ReVoLTE exploit?

The ReVoLTE attacks exploit the reuse of the same keystream for two subsequent calls within one radio connection. This weakness is caused by an implementation flaw of the base station (eNodeB). In order to determine how widespread the security gap was, we tested a number of randomly selected radio cells mainly across Germany but also other countries. The security gap affected 12 out of 15 base stations.

How does the ReVoLTE attack work?

The ReVoLTE attack aims to eavesdrop the call between Alice and Bob. We will name this call the target or first call. To perform the attack, the attacker sniffs the encrypted radio traffic of Alice within the cell of a vulnerable base station. Shortly after the first call ends, the attacker calls Alice and engages her in a conversation. We name this second call, or keystream call. For this call, the attacker sniffs the encrypted radio traffic of Alice and records the unencrypted sound (known plaintext).

For decrypting the target call, the attacker must now compute the following: First, the attacker xors the known plaintext (recorded at the attacker's phone) with the ciphertext of the keystream call. Thus, the attacker computes the keystream of the keystream call. Due to the vulnerable base station, this keystream is the same as for the target (first) call. In a second step, the attacker decrypts the first call by xoring the keystream with the first call's ciphertext. It is important to note that the attacker has to engage the victim in a longer conversation. The longer he/she talked to the victim, the more content of the previous communication he/she can decrypt. For example, if the attacker and victim spoke for five minutes, the attacker could later decode five minutes of the previous conversation.



Are my phone calls still vulnerable to eavesdropping via ReVoLTE?

To mitigate the threat of eavesdropping, we have informed providers about the attack vector through the GSMA Coordinated Vulnerability Disclosure Programme process at the beginning of December 2019. The GSMA requested vendors to provide patches for affected base stations. By the time of publication, those vendors should have provided patches, and providers are requested to install and configure them securely. A re-test indicates that the German operators have managed to install the patches. However, we need to consider a large number of providers worldwide and their large deployments. It is thus crucial to raise awareness about the vulnerability. In case you want to know if your network is vulnerable or not, you can test it with our App.

Demonstration

To demonstrate the practical feasibility of the ReVoLTE attack, we have implemented an end-to-end version of the attack within a commercial network (which was vulnerable) and commercial phones. We use the downlink analyzer Airscope by Software Radio System to sniff the encrypted traffic. Further, we use three Android-based phones which are controlled via ADB and SCAT to obtain the known plaintext at the attacker's phone. For a demonstration of these steps, please refer to the video below.

Mobile Sentinel App

21:18 HD 4G

ReVoLTE Detection

Cell Status : Not Tested

isVolteEnabled : True

CellID : 1234

TAC : 1234

Starting Detection ...

START DETECTION

ABORT

Home Detection Logging Settings

Is it possible to detect if the base station is vulnerable to ReVoLTE?

Yes, we (mainly Bedran) have developed an App that allows to detect whether a base station is vulnerable to the ReVoLTE attack or not. The App requires a VoLTE capable Android phone with root access and a Qualcomm chipset. Please click here to visit the Github page regarding the Mobile Sentinel App.

Technical Paper

Abstract

Voice over LTE (VoLTE) is a packet-based telephony service seamlessly integrated into the Long Term Evolution (LTE) standard and deployed by most telecommunication providers in practice. Due to this widespread use, successful attacks against VoLTE can affect a large number of users worldwide. In this work, we introduce ReVoLTE, an attack that exploits an LTE implementation flaw to recover the contents of an encrypted VoLTE call, hence enabling an adversary to eavesdrop on phone calls. ReVoLTE makes use of a predictable keystream reuse on the radio layer that allows an adversary to decrypt a recorded call with minimal resources. Through a series of preliminary as well as real-world experiments, we successfully demonstrate the feasibility of ReVoLTE and analyze various factors that critically influence our attack in commercial networks. For mitigating the ReVoLTE attack, we propose and discuss short- and long-term countermeasures deployable by providers and equipment vendors.

Press Coverage

- ReVoLTE attack can decrypt 4G (LTE) calls to eavesdrop on conversations [1]
- ReVoLTE an attack that allows to intercept calls encrypted in LTE [2]
- REVOLTE ATTACK [3]
- ReVoLTE Attack Allows Hackers to Listen in on Mobile Calls [4]
- ReVoLTE Attack Allows Eavesdropping of Encrypted 4G (LTE) Calls [5]
- ReVoLTE Attack Encrypted Voice Calls Interception [6]