Call Me Maybe: Eavesdropping Encrypted LTE Calls With ReVoLTE

12.08.2020 USENIX Security Conference

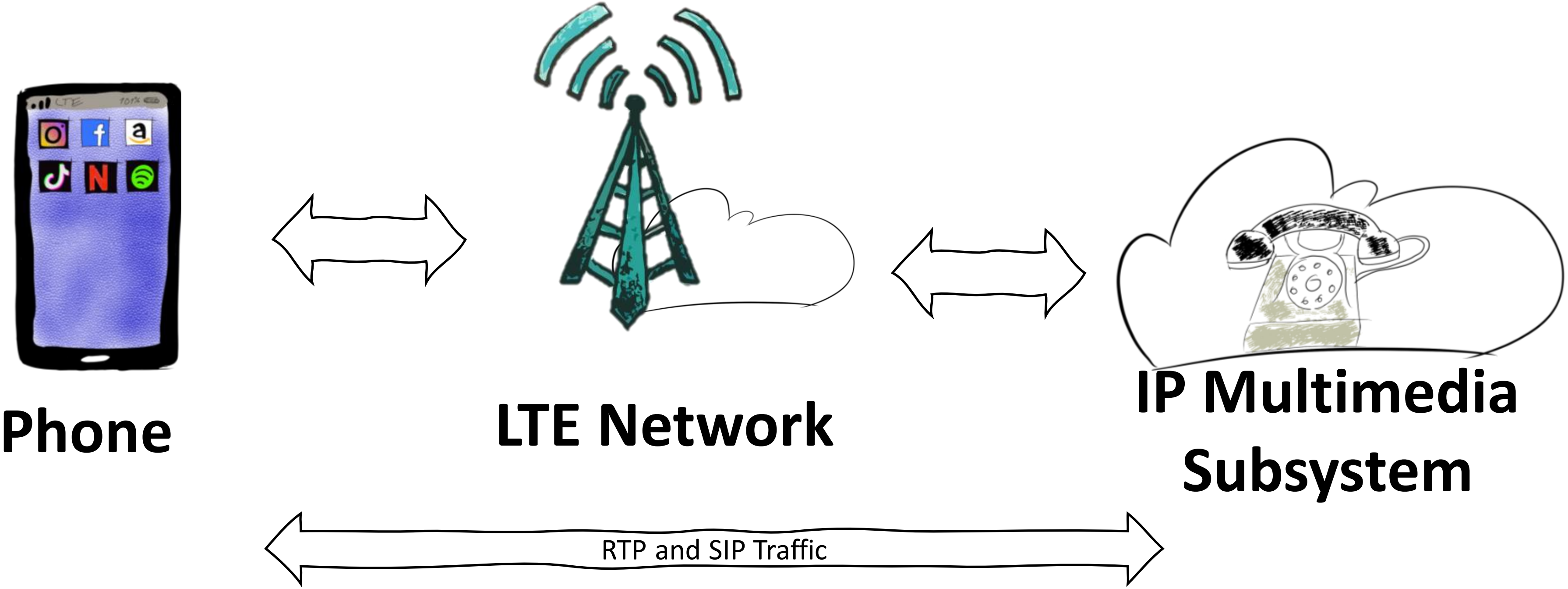
David Rupprecht, Katharina Kohls, Thorsten Holz, Christina Pöpper

Motivation

Are **VoLTE** calls **secure** against **eavesdropping?**

https://gsacom.com/paper/gsa-announces-253-operators-investing-volte/

VoLTE Basics



Phone

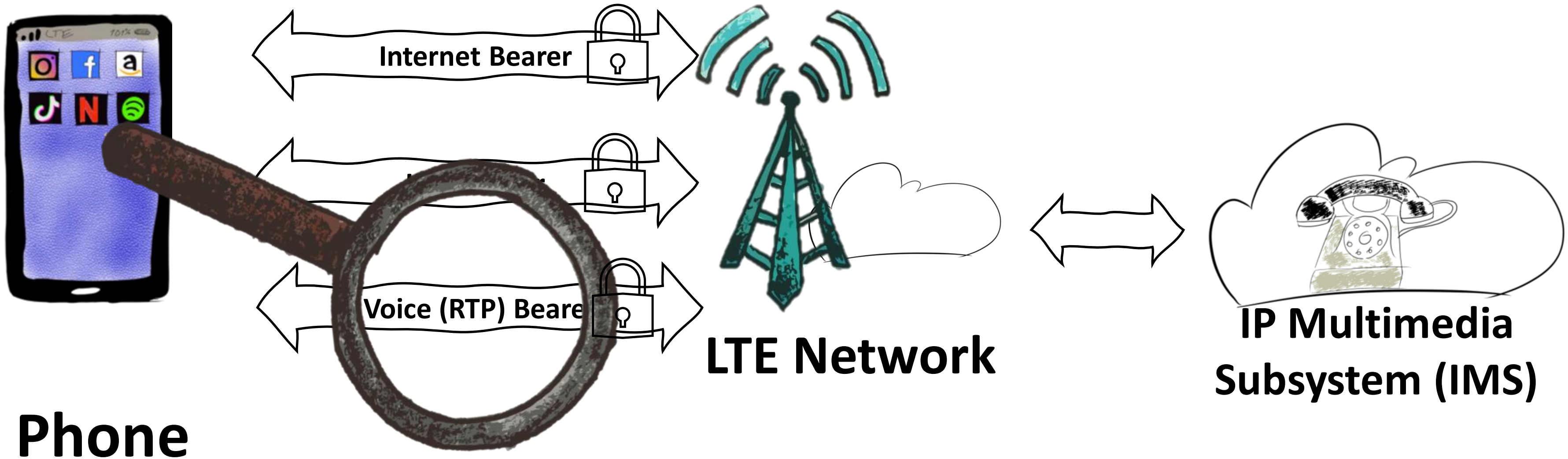
LTE Network

IP Multimedia Subsystem

RTP and SIP Traffic

Real-Time Transport Protocol (RTP)
Session Initiation Protocol (SIP)

Radio Bearers for VoLTE



Internet Bearer

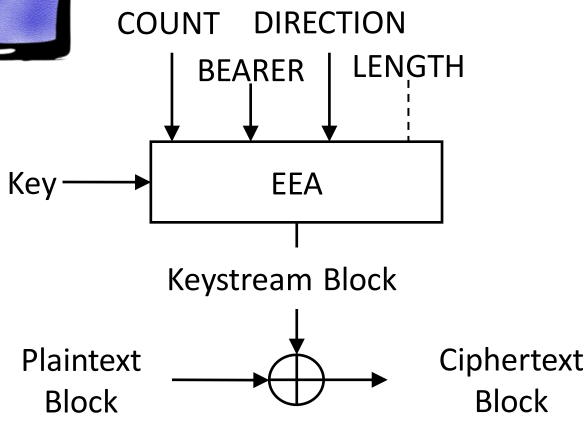
Voice (RTP) Beare

LTE Network

IP Multimedia Subsystem (IMS)

Phone

Stream Cipher



- **Key**: For VoLTE data user traffic key (k_up)
- **Count**: Sequence number of packets
- **Bearer**: The bearer identity depends on the used bearer
- **Direction**: Uplink or Downlink
- **Length**: Length of the keystream block

Same input generates the **same** keystream!

Keystream Reuse

$$(\text{Plaintext A} \oplus \text{Keystream}) \oplus (\text{Plaintext B} \oplus \text{Keystream}) = (\text{Plaintext A} \oplus \text{Plaintext B})$$

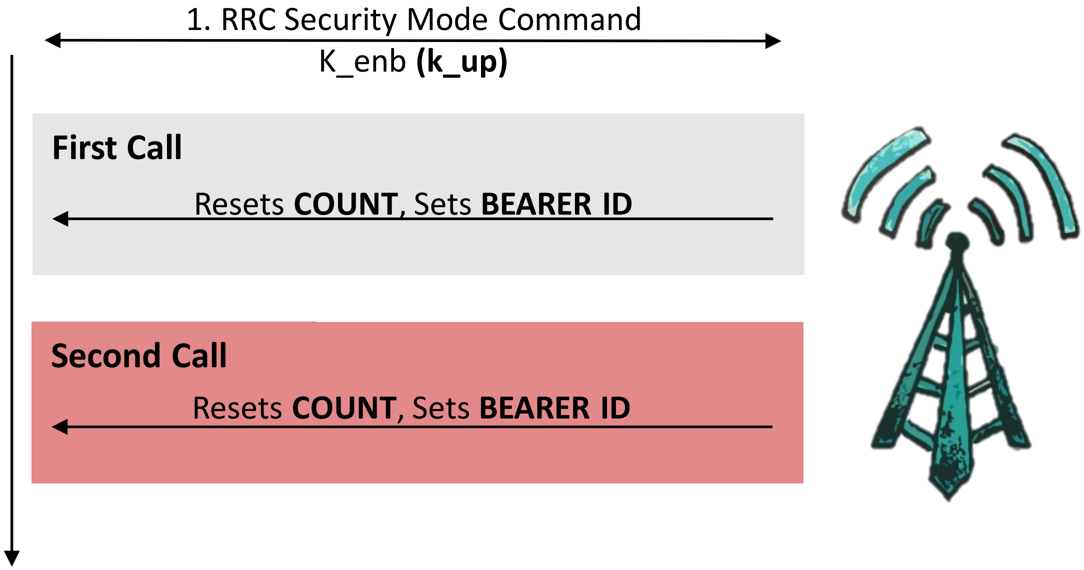
$$(\text{Plaintext A} \oplus \text{Plaintext B}) \oplus \text{Plaintext B} = \text{Plaintext A}$$

Keystream Reuse allows **Decryption**!

ReVoLTE: Reusing Encrypted VoLTE traffic to eavesdrop calls.

Attack Vector: Keystream Reuse in VoLTE Setting

Is the **BEARER ID** increased?



1. RRC Security Mode Command

K_enb **(k_up)**

First Call

Resets **COUNT**, Sets **BEARER ID**

Second Call

Resets **COUNT**, Sets **BEARER ID**

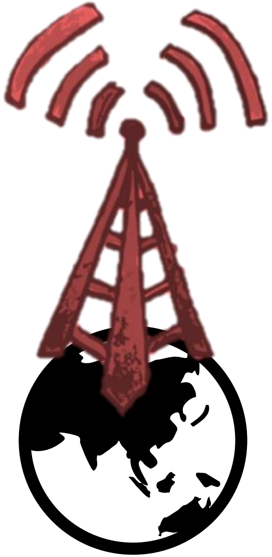
Muhammad Taqi Raza and Songwu Lu. **On Key Reinstallation Attacks over 4G/5G LTE Networks: Feasibility and Negative Impact.** Nov. 2018

https://www.researchgate.net/publication/328927054_On_Key_Reinstallation_Attacks_over_4G5G_LTE_Networks_Feasibility_and_Negative_Impact

Vulnerable eNodeBs

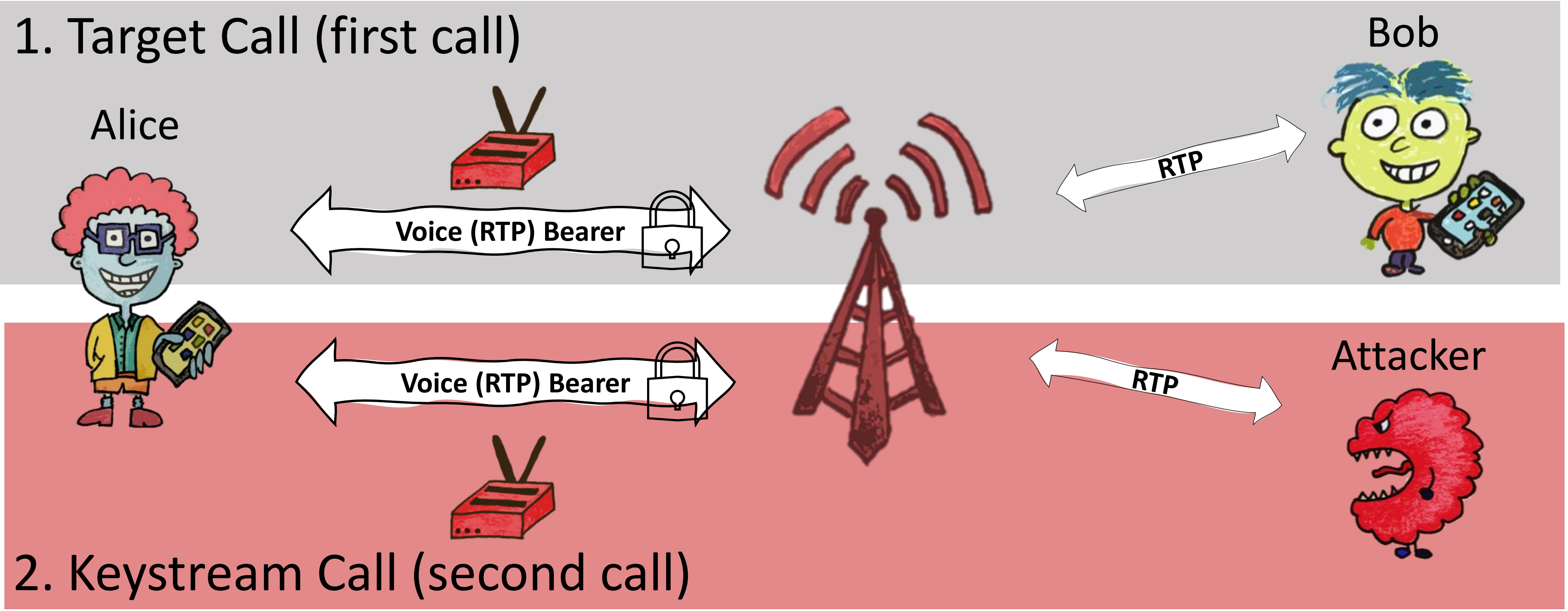
3 / 15 eNodeBs increase the bearer ID

12 / 15 **eNodeBs reuse the same keystream**



Thanks to Nils Fürste, Bedran Karakoc, and Seokbin Yun for performing the testing.

ReVoLTE Attack Concept



Real-World Demonstration

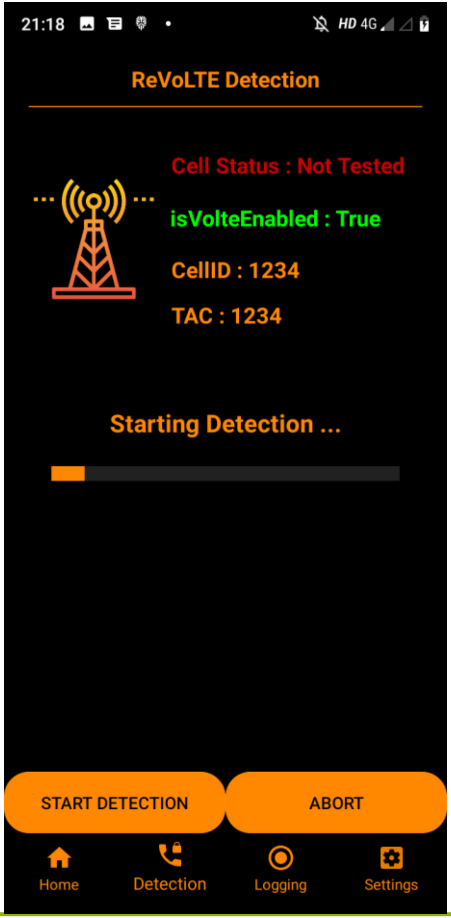
Results

- Implementation flaw
- Specification is ambiguous (few sentences about keystream reuse)
- Responsible disclosure via the GSMA CVD program: CVD-2019-0030
- Specification:
  - Test cases are now included
  - Ambiguity of the specification is resolved
- Deployment:
  - Affected vendors have patched the vulnerability
  - Affected providers have deployed the patches

https://www.gsma.com/security/gsma-coordinated-vulnerability-disclosure-programme/

Test your Network!

www.revolte-attack.net



ReVoLTE Detection

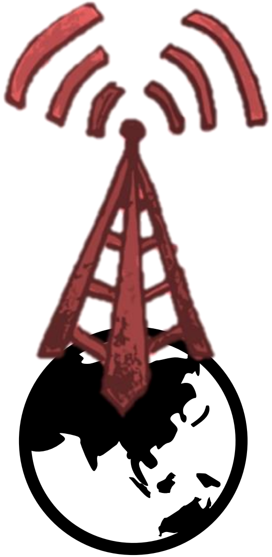
Cell Status : Not Tested

isVolteEnabled : True

CellID : 1234

TAC : 1234

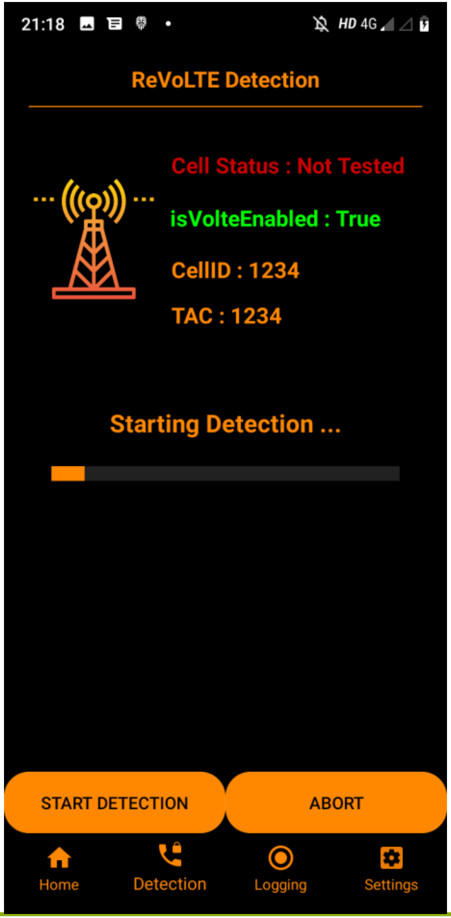
Starting Detection ...



Thank you!

www.revolte-attack.net

David Rupprecht
Ruhr University Bochum
david.rupprecht@rub.de


21:18 HD 4G

ReVoLTE Detection

Cell Status : Not Tested

isVolteEnabled : True

CellID : 1234

TAC : 1234

Starting Detection ...