SecurityGen

Telecom Security. Transcending Generations.

Threat Intelligence Report:

Insecure money transfer mobile network service

Table of contents

01. Executive Summary

Many network operators and banks offer the option to transfer money between mobile subscribers or bank clients. Typically, this can be accomplished through SMS or USSD, which are particularly popular in regions where older or "button-style" phones are prevalent. These devices lack the capability for mobile banking or other more advanced options, making **SMS and USSD** ideal technologies as they are universally supported by any phone.

However, every year we are contacted by mobile operators from different regions, experiencing a rise in fraud incidents associated with these technologies. Upon conducting a thorough investigation into these incidents, we usually discover that the root cause is quite similar - in most cases, it was the disabling of encryption on 2G radio networks. In this report, we aim to explain the negative impact of such configurations on the network and the subsequent opportunity created for fraudsters of various kinds.

02. Technical Details

2.1 Description

We have investigated several fraud cases, when someone was able to transfer money on behalf of a victim subscriber. During this investigation we found out that due to different reasons, **MNOs were not using encryption on the radio in GSM network.**

There were different reasons for this behavior by the MNOs. In some instances, operators were switching off as many features as possible to decrease network performance drop, and offload pretty old telco equipment. In other cases, encryption was disabled under the assumption that since many basic phones lack encryption support, it was unnecessary to implement encryption across the entire network.

However, **switching off encryption also results in switching off authentication on the radio interface.** And with this any malefactor can connect to the network pretending to be another subscriber just using different IMSI or TMSI. Attackers often indiscriminately target any available identity, utilizing brute force tactics to gain unauthorized access.

2.2 Attack Vector

The attack was executed through a typical subscriber connection to the 2G radio network, which lacked encryption due to deactivation by the network. Due to absence of authentication in such case, the attacker was able to substitute permanent or temporary identity of other subscriber and was able to send SMS and USSD on behalf of the victims (subscribers). This exploitation leads to abuse of money transfer services, representing the simplest method for malefactors to capitalize on such attacks.

2.3 Affected Systems/Technology

2G Radio

03. Impact Analysis

3.1 Threat Severity

Lack of encryption and authentication on 2G radio, enables malefactor to passively listen, actively execute spoofing of other subscriber activity, fully compromising subscriber connection and leading to following threads:

- Unauthorized access to the network
- Fraud
- DoS
- Impersonation
- Interception
- MiTM attack

3.2 CVSS

Threat: Fraud

CVSS Score: 8.8

CVSS Vector: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

04. Mitigation

We strongly advise turning on the encryption on the radio network. Even weak A5/1 is better than no encryption at all, as it introduces authentication, , making it significantly more challenging for malefactor to execute such attacks. However, it is highly recommended to use A5/3 which offers much higher security.