:: Positive Technologies

First steps for mitigating Simjacker-related risks right now

WHAT STK IS

The SIM Application Toolkit (STK) is a relatively old technology that dates back to the pre-smartphone era. Mobile operators use it as a way to deliver information about their services to subscribers. On feature phones, the menu implemented via STK provided subscribers with an easy and convenient way to navigate their operator's additional services. Of course, each operator needed to customize SIM cards based on their set of services, language, and other parameters. In response, SIM card vendors devised a unified way to quickly get new batches of SIM cards to market while meeting operator needs.

Simply put, STK is a set of applications that run on the SIM card and interact with the mobile device.

These applications can:

- Display text on the screen of the device
- Initiate SMS messages, calls, USSD messages, and packet sessions
- Access the camera and speakers
- Engage in dialog with users ("Are you sure (Y/N)?")
- Get information from the outside via SMS or Cell Broadcast and save this information on the SIM card
- Provide additional menus to be displayed by the phone
- Modify the phone number of outgoing calls or forbid particular calls

SMS messages were chosen for making the STK menu interactive. From a technical standpoint, these SMS messages are defined by special parameters. A message contains not text, but rather a command to perform one of the actions from the above list.

Simply put, **STK is a set of applications** that run on the SIM card and interact with the mobile device.

There is nothing that subscribers can do about Simjacker. And now for the good news. Almost **any operator equipment has the capability to reduce the risk** of Simjacker exploitation.

SIMJACKER VULNERABILITY

In 2013, The Register published an article on vulnerabilities in SIM cards: theregister.co.uk/2013/09/23/white_hat_sim_hacker_disillusioned_and_dismayed_by_operator_response/. The cited research focused on the ability to infect a SIM card with an attacker-created malicious application via STK.

A year later in 2014, researchers at Positive Technologies discovered several ways of exploiting STK and gave talks on the topic at security conferences.[1] However, they concentrated on penetrating the software of a 4G dongle by using STK commands.

This year, nearly all IT-related media have reported on the ability to hack SIM cards on which S@T Browser is installed. A vulnerability, dubbed Simjacker, has been shown to be in wide use by hackers to surveil subscribers.

S@T Browser enables an attacker to run commands on SIM cards. With these commands, it is possible to learn the subscriber's location, send SMS messages to certain phone numbers (such as for fraud), initiate voice calls as the subscriber, open web browser pages, disable the SIM card, and obtain device internal identifiers.

WHAT TO DO ABOUT SIMJACKER

Unfortunately, there is nothing that subscribers can do about these attacks. The vast majority of mobile operators provide SIM cards with STK pre-installed. It is not possible to disable STK on the mobile device itself. Therefore, the job of security falls squarely with mobile operators.

And now for the good news. Almost any operator equipment that handles SMS traffic has the capability to reduce the risk of Simjacker exploitation.

This can be done by configuring certain parts of the MNO infrastructure to block SMS messages that have content coding characteristic of STK messages.

```
▲ TP-DCS: 246
      1111 .... = Coding Group Bits: Data coding/message class (15)
      .... 0... = Reserved: 0
      .... .1.. = Message coding: 8 bit data
      .... ..10 = Message Class: Class 2 (U)SIM specific message (0x2)
```

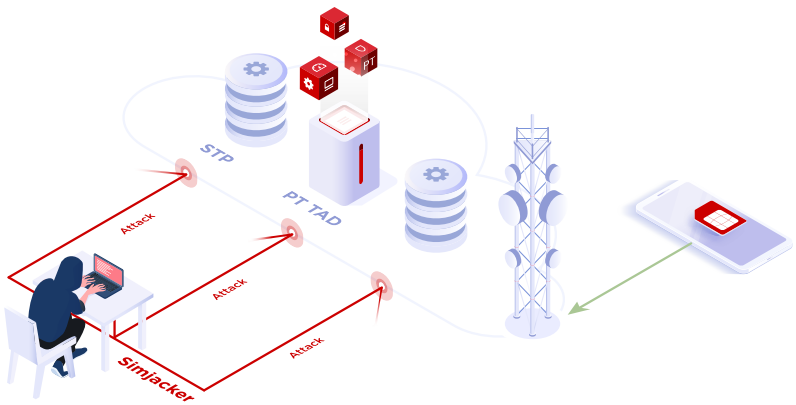
1 securityaffairs.co/wordpress/31663/hacking/hacking-4g-usb-modems.html

To stop Simjacker attacks, there are three groups of equipment that MNOs should configure properly:

1. SMS Centres (SMSCs) that handle outgoing SMS traffic from MNO subscribers. Subscribers can exchange SMS messages (regular text) with each other and with application servers. Messages with STK coding from home subscribers should be going only to the MNO platform—and definitely not to other subscribers.
2. SMSCs to which partner content providers are connected via SMPP and SS7. Content providers generally send text in the form of A2P SMS messages. Their traffic should not contain messages with STK coding.
3. SMS Home Routing hosts for incoming SMS traffic to home subscribers from external connections. There can be no doubts here. If an external host is sending SMS traffic with STK coding to home subscribers, this is clearly illegitimate activity that must be stopped.

Such configuration is a good first step for mitigating Simjacker-related risks.

However, attackers have ways of bypassing security that could be used to exploit Simjacker and other vulnerabilities. We offer MNOs the ability to block malicious requests at the network border with the help of signaling firewalls, which identify and block such messages from attackers. When the system detects an illegitimate STK request in an SMS message, it simply blocks the entire signaling message, leaving the subscriber secure.[2]



PT Telecom Attack Discovery (PT TAD) next-generation signaling firewall empowers mobile network carriers to secure networks that use Signalling System 7 and Diameter protocols

We urge mobile operators to regularly monitor the security of external connections. Regular monitoring shows operators whether someone is attacking their network and—if an attack is detected—they can take timely measures to protect subscribers.

You can take advantage of our Express Monitoring service right now to verify whether your network is vulnerable to Simjacker. See how hard (or easy) it would be for an attacker to pull it off.[3]

2 positive-tech.com/products/signalling-firewall/

3 positive-tech.com/services/express-monitoring/

positive-tech.com
contact@positive-tech.com

About Positive Technologies

Positive Technologies is a global cybersecurity company. Its flagship Telecom Cybersecurity Suite enables network operators to drive business performance while protecting their subscribers and services. By providing greater visibility into infrastructure vulnerabilities and securing customer services, Positive Technologies helps to strengthen loyalty, drive revenue with value-added security offerings, and protect emerging telecom technologies such as 5G and the IoT.