Indian Computer Emergency Response Team
Ministry of Electronics and Information Technology
Government of India

सत्यमेव जयते

CERT-In Advisory CIAD-2016-0087

Securing SIM cards

Original Issue Date: December 27, 2016

Description

Subscriber Identity Module or Subscriber Identification Module (SIM) is an integrated circuit that is designed to securely store the international mobile subscriber identity (IMSI) number and its related key, which are used to identify and authenticate subscribers during mobile communication. "SIM cards" are transferable between different mobile devices. A SIM card contains its unique serial number, international mobile subscriber identity (IMSI) number, security authentication and ciphering information, temporary information related to the local network, a list of the services the user has access to, and two passwords: a personal identification number (PIN) for ordinary use, and a personal unblocking code (PUK) for PIN unlocking.

Attacks on SIM cards and their countermeasures

The primary threat to SIM card is the possibility of cloning. Cloning means reading the contents of a SIM card and writing them into the memory of another SIM card. The opportunity to clone SIM cards could be used for malicious activities. Having received short-term access to the victim's SIM card, an adversary could clone it and thus compromise the legitimate SIM card. If a cloned SIM card is active during the time when the legitimate subscriber is registered in the mobile network, the latter would get its connection cut off and still remain totally unaware of it. In that case, all inbound calls and messages will be directed to the adversary, and they, in turn, would be able to make calls, send messages and browse the Internet on the victim's behalf.

Cryptographic attacks on encryption keys are also possible which can compromise the security of SIM.

The possible countermeasures for SIM based attacks are given below.

- Set up a pin for accessing your phone. This is the first line of defense against people trying to break into your phone to obtain information. However, this won't stop someone from taking a SIM out of a stolen phone. A pin for your SIM will usually consist of two pins for you to set up and enter correctly; There is also the PUK/PUC (PIN Unblocking Key/Code) that will disable a SIM if a pin is entered incorrectly (amount of incorrect tries varies).
- Keep your PIN and PUK code in a safe place.
- If you get a missed call from another country code number or any absurd number such as number starting from #, never call back to such number.
- Never hand over your SIM in physical form to unknown person.
- Never give your personal information through SMS or any other form to any unknown person.
- If you get a call from telecom company, regarding your personal information, do not reveal your personal information.
- Use back-up SIM cards. In case if you lose your SIM card, you can have a backup with all of your information on it.
- Consider encrypting your web browsing, SMS, voice calls, and if possible your synced accounts.

References

https://blog.kaspersky.com/sim-card-history-clone-wars/11091/
http://www.zdnet.com/article/des-encryption-leaves-sim-cards-vulnerable-to-exploitation/
http://www.sim-only.co.uk/sim-cards/how-to-keep-your-sim-card-secure/
http://www.pandasecurity.com/mediacenter/mobile-security/how-to-protect-your-sim-card-key-whatsapp/

Disclaimer

Contact Information

Email: info@cert-in.org.in
Phone: +91-11-24368572

Postal address

Indian Computer Emergency Response Team (CERT-In)
Ministry of Electronics and Information Technology
Government of India
Electronics Niketan
6, CGO Complex, Lodhi Road,
New Delhi - 110 003
India