Mobile Data Charging: New Attacks and Countermeasures

Krishna Sindhuja Kalusani

USC ID: T25568677

Abstract: The most popular invention of technology era is mobile phone and the wireless internet services on mobile devices is becoming more and more useful. This is achieved by 3G/4G network deployment. The latest network operators uses the charging method which is billed depending on the traffic volume while accessing data service i.e. the user pays only for the data he used. The accounting scheme is basically built on standards – that define the architecture and mechanism and operators' policy practice – where operators specify their own charging policies. To communicate with a host on the Internet, the mobile device needs to first create a bearer service connection with the cellular network, which is further connected with the wired Internet. Once the connection is established, data packets are delivered. The connection has to traverse gateway-like devices (Serving GPRS support node & Gateway GPRS support node) in the cellular network core. These gateways then perform accounting operations by recording the data volume of those packets that traverse them, until the connection is completed. The main components of the architecture are Terrestrial Radio Access Network (RAN) and Core Network (CN). The SGSN handles the data packets that is acquired on the channel established by network and GGSN acts as a router between the device and the external wired internet.

Contributions: The main contributions of the paper are:

- ➔ Reporting the first ever security analysis on 3G/4G networks and identifying its loopholes
- ➔ The identified loopholes are exploited using two attacks a) toll-free-data-attack and b) Stealth spam attack undermining the charging system. Real experiments were conducted on operational networks to validate the feasibility and simplicity of the attacks and their potential damage
- ➔ In the toll free data attack enable the attacker to access any data service for free if only one particular data service is actually free for him. Whereas in Stealth spam attack incurs charges for very large amount of data that the user is not accounted for or unaware of.

➔ The root cause for the existence of these loopholes are discussed and effective solutions are proposed to eliminate them.

Weakness:

➔ I feel the major drawback of these mitigation strategies on the attacks is the scalability. Due to the increased usage of the mobile devices and internet on the device, the security design proposed may not be sufficient. It has to analyse each and every connection request and monitor and control data charging which would become a tedious job in process.

➔ This implies that the differentiated charging policy has to secure itself. The user has be to be careful.

➔ The IP push model used for the packet switching in the present day networks is not completely ready for the metered charging.