Subex Telecom Fraud Alerts

February 2010

Soft SIM- new variant of roaming fraud

A previous fraud alert for the month of October 2009 spoke about Skuku which is an international bypass product, using international VOIP routing to a sim-box located in the home network (for more information visit www.skuku.com). Recently a new variant of roaming fraud has emerged through a 'reverse-Skuku' type approach. In this type of fraud SIMs are purchased in bulk (typically through subscription fraud) and placed in a soft-SIM rack. These soft SIMs are then immediately connected to radio equipment in foreign countries and used to perpetrate roaming frauds, often just minutes after the SIMs are purchased. Soft SIMs can also be switched to other roaming networks almost instantaneously to effectively SIM-swap in different countries. Soft SIMs may appear much like cloned SIMs (i.e. very fast moving), but would also differ in that there would never be overlapping calls associated.

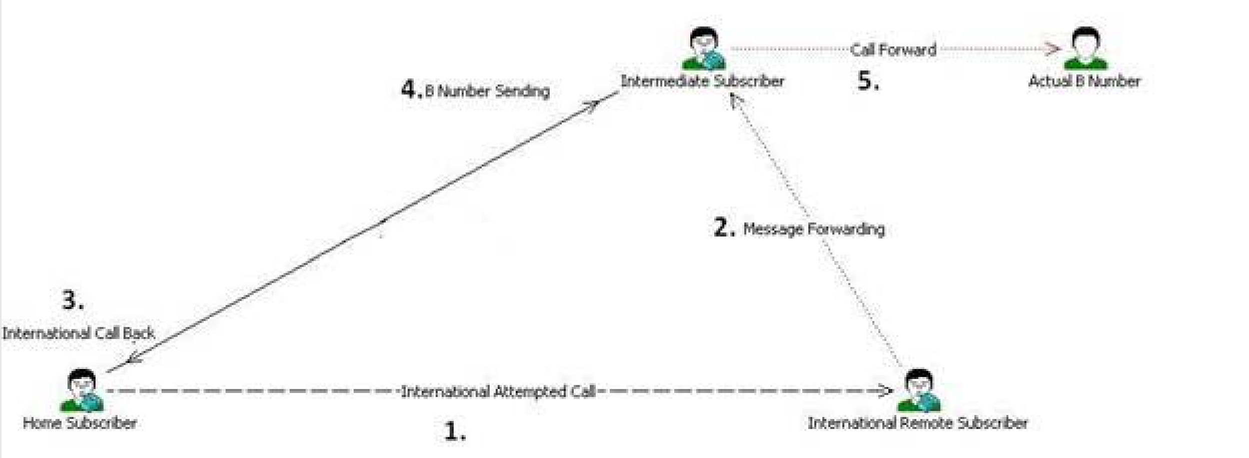
Caller ID (CLI) spoofing

Recently some interesting side effects of CLI spoofing have been noticed. It is important to note that there is a marked difference between the 'network CLI' (used to route calls and bill customers) and the 'presented CLI'. In particular, the network CLI is difficult to manipulate, whilst the presented CLI is relatively easy to attack and spoofing of presented CLI has been common-place for some time e.g. to commit Wangiri-type fraud. Two issues related to spoofing of presented CLI were reported. These were:

- 3rd party content/service providers generated bills on the wrong CLI. 3rd party content/ service providers bill on presented CLI and as spoofing manipulates the presented CLI, they end up billing the wrong CLI.
- A caller using spoofed CLI accessed mailbox of voicemail systems as they sometimes use presented CLI to verify the identity of the caller

Bypass Frauds using Call Back

Bypass Frauds using call back is a scenario whereby the subscriber makes an attempted call and the called party is induced to return the call. These types of Call-Backs being considered as Fraud depend on the legislation where the operator is located and whether call-back operation is being run as a service offering and not as a normal personal call back which cannot be considered as Fraud. In this case the billable network usage is low or zero for the initial inbound call. This type of fraud can result in heavy losses and subscriber dissatisfaction. A recently discovered complex fraud scenario using call-backs is depicted in below diagram. In the below scenario the call-back has an IVR response "Enter your pin Number" and that's how the B-Number sending process is initiated (step4).



Sequence of actions in complex Call-Back Fraud

The team observed that an intermediate subscriber (as shown in the Figure above) was involved in the fraud and could not be barred directly from the network. Hence, a decision was taken to block calls to all international numbers observed in the associated call records.