Sanchar Nigam Executives' Association, Kerala

SNEA Bhavan, Dharmalayam Road, Trivandrum – 695001

Circle President	Circle Secretary	Circle Treasurer
George Varghese DE Tripunithura, ENK 9447162900 (M) gvsnea@gmail.com	T.Santhosh Kumar SDE Vizhinjam, TVM 9446072525 (M) cssneakerala@gmail.com	G.Premkumar SDE Karyavattom, TVM 9447102277 (M) premkumarg92@gmail.com

No. SNEA/KRL/CGM/2015-16/24   Dated 4-5-2016

To

The Chief General Manager Telecom,
BSNL, Kerala Circle,
Thiruvananthapuram.

Respected Sir,

Sub: PBX Hacking and **International Revenue Share Fraud-** reg.

Recently it has come to the notice that fraudulent ISD calls are made from land phones particularly from EPBX with ISDN PRI connections resulting in huge bills of the order of tens of Lakhs of Rupees. On analysis this showed the features of a typical IRSF activity.

IRSF **(International Revenue Share Fraud)** is an artificial inflation of traffic terminating to international revenue share providers. The top ten countries where such fraudulent calls most often terminates are, in descending order: Cuba, Somalia, Bosnia and Herzegovina, Estonia, Latvia, Guinea, Serbia, Sierra Leone, United Kingdom and Lithuania. There are so many other countries also in Africa, Latin America and some small Island nations with very low traffic and high tariff.

Today, communication fraud is perpetrated from remote distances by highly skilled, technologically sophisticated criminals who have little fear of being detected, let alone apprehended or prosecuted. Their modus operandi is as follows.

1. They acquire international Premium Rate numbers that enables them to revenue share from the terminating operator. All calls made to these numbers generate a significant profit for the criminal.
2. They trick people into calling the number like missed calls call back (***Wangiri*** calls) or use a hacked PBX to dial it themselves.

Wangiri (literally, "One (ring) and cut") is a phone fraud that originated in Japan. The scam involves a computer dialling a large number of mobile phone numbers at random. The numbers appear as missed calls on the recipients' phones. Believing a legitimate call was cut off, or simply curious, users are enticed to call back. The numbers are either premium rate, or contain advertising messages. Some time back this type of fraud is prevalent in BSNL and it is curtailed by deactivating the default ISD facility from prepaid mobile connections.

Criminals hack PBX systems by illegally breaching the security of a PBX system to gain access to the trunk lines to generate as many calls as possible to expensive overseas Premium Rate telephone numbers of which the criminal collects upto 90% of this revenue. They target telecom operators that promptly pay the ILD charges. The originating customer and the operator is the sole loser in this fraud as the intermediate carriers and operators get their share promptly due to multilateral agreements.

PBX hacking is done by many methods. Nowadays PBX functionality is realised using IP technologies instead of dedicated EPABXs. A PC is configured as PBX server using open source software such as FreePBX, Asterisk etc. or proprietary software and the ISDN PRA is terminated to an interface card in the PC. The internal extensions are extended using the same LAN wiring used for data and internet and the phone equipment may be Softphone or the PC itself connected to the LAN. This IP PBXs poses an easy target for PBX hacking if proper security measures are not implemented as these PCs are also connected to the internet for other instant messaging and VOIP applications also.

As per reports at **http://arstechnica.com/tech-policy/2011/11/how-filipino-phreakers-turned-pbx-systems-into-cash-machines-for-terrorists/** some International terrorist organizations also turn to PBX hacking and IRSF to collect money for their operations.

BSNL incur heavy losses due to such frauds in many ways as the customers refuse to pay such huge bills.

1. Loss of revenue to BSNL. ISDN PRI is a very lucrative competitive business.
2. Loss of a high net worth customer. The irritated customer may terminate other services also.
3. Loss of BSNL goodwill and credibility.
4. Prolonged litigation with the customer.
5. Loss towards service Tax even though the bills are not paid.
6. Loss to the country's exchequer towards ILD charges to international carriers in foreign currency.

To curtail these illegal activities and loss of revenue the following suggestions are made for consideration.

1. All ISDN PRA customers should be sensitized about such frauds to implement sufficient security measures.
2. ISD dynamic barring to be provided to all PRI connections with administrative keyword and customers should be instructed to keep the ISD locked while not in use.
3. Exchange Expensive Call Monitoring (EECM) alarms in MSC to be made as critical alarm and displayed in TTY as other critical alarms so that Xge in charge will be able to ascertain the genuineness of the call and necessary action if any, can be taken at least during working hours.
4. At present the EECM is not a critical alarm and it is just displayed in ROP along with numerous other reports which may run to thousands of pages for a single day's activities. Instruction may be issued to check ROP daily for EECM by the Xge in charges.

5. CDR records are pulled by mediation software of CDR billing system periodically as and when an AMA file is written into the MSC and Fraud Management system (FMS) is an inherent component of CDR project. Usage data (i.e. CDRs) and usage pattern resulting from any such activities is analyzed by FMS and input data is matched against defined rule conditions and associated thresholds. Any deviation to defined values / rules will generate alarms for the further investigations. As per the requirement user can define any number of rules / thresholds. Necessary rules / thresholds should be defined to identify IRSF fraudulent activities. Such fraud Ticket alerts should be escalated to xge incharge and higher ups including TRA personal by SMS and email from CDR system. At present the alert facility for exceeding the unbilled amount beyond the normal monthly charges is sent to TRA personal through mail and that is also a delayed / deferred process without meeting the desired result required since these activities should be stopped within few hours. It is also observed that these fraud activities are mainly managed during holidays and most of the exchanges are unmanned during holidays. If the alert is through SMS effective action can be taken on noticing the alerts. Necessary provision may be made for SMS alert either through CDR system or through NMS in case of EECM alarms.

   Necessary provision in CDR/ NMS may be incorporated for implementation of the above system
6. Subscriber also should be alerted by SMS and email and the ISD facility maybe temporarily withdrawn automatically if the threshold exceeds some high value. After ascertaining the genuineness of the calls from the subscriber the ISD facility can be restored.
7. These fraud case may be referred to other external agencies like TRAI, Intelligence and security agencies and Enforcement Directorate to detect the real as the culprits may be operating from foreign soil and the calls are spanning many international links.
8. The payment towards Service Tax and ILD charges may be deferred and disputed as it is the result of a fraud. Prompt payments further encourage the fraudsters.
9. An effective monitoring mechanism should be implemented in ILD TAXs to monitor calls to such fraudulent destinations in rapid succession. Call screening and filtering may be employed.
10. Many commercial Fraud Management Systems (FMS) available may be made use to prevent such activities..

Thanking you,

Yours Sincerely

(T.Santhosh Kumar)
Circle Secretary,SNEA,
Kerala Circle.