Paper on Handling Menace of International Grey Traffic

White Paper 01 of 2012

PiRRC

In this paper discussion is only about the conventional international voice telephony requiring a license to bring in operate and not voice communication over applications like Skype, Google Talk etc.

1. Background

1.1 International incoming grey traffic (illegal or unlicensed international calls) is one of the regulatory and financial headaches both for Regulator and legal telecommunication operators in the Pacific. The grey traffic operators bypass the legally established telecom network in order to gain financial advantage by offering very low international incoming termination rate to international carriers and wrongfully deprive legitimate operators of lawful revenue. This problem is not unique to Pacific; rather it exists in every country where the international settlement rates are higher than the cost of termination of traffic or domestic termination rate. The difference between the cost of termination or domestic termination rate and settlement rate is the incentive for grey operators to bypass legal gateways, the more the difference, the more the incentive and consequently the more the grey traffic.

1.2 In addition to non-cost based settlement rates, recent advancements in technology, especially VoIP[1], has made it easier to terminate conventional voice traffic bypassing legal international gateways without a valid license.

2. Revenue loss to Government

2.1 Grey telephony in the Pacific is causing sizeable revenue loss to government exchequer and also shaking revenue streams of legal Access Service Providers (ASP), who have invested millions of dollars as license fees, deployment of infrastructure and on paying other government taxes/levies/charges.

2.2 Taking the example of Fiji, where wholesale tariff has been revised by Fiji Commerce Commission recently and fixed international termination at USD 0.22, whereas local termination rate for mobile is FJD 0.13[2]. Based on experience in other countries, the gap between local and international termination rate would increase already existing grey traffic in Fiji.

3. National Security Aspect

3.1 Grey market is also a threat to national security as the communication via illegal/unknown routes cannot be monitored / tapped by the security and counter intelligence agencies.

4. Trends & Challenges:

4.1 Experience shows that the *modus operandi* used by illegal grey operators includes arranging international traffic from various VoIP operators across the globe and terminating it on their own illegal VoIP gateways using broadband connections. This traffic is then distributed to the domestic destination numbers using GSM[3] SIMs[4], CDMA[5] RUIMs[6] and PSTN[7] connections.

---

1 Voice over Internet Protocol
[2] http://www.commcomm.gov.fj/docs/determination%20Fiji%20International
[3] Global System for Mobile Communications
[4] Subscriber Identity Module
[5] Code division multiple access
[6] Removable User Identity Module

4.2 Currently, governments, regulators and law enforcement agencies are facing two major challenges with regards to grey market telephony. Firstly, there is a need for them to acquire IP[8] bandwidth monitoring facility. Since most the illegal traffic is terminated using IP bandwidth, it is necessary to put IP backbone of the country under scrutiny. Once subject facility is in place, all IP communication whether legal or illegal would be under check. Second challenge relates to finding exact location of suspected SIMs and RUIMs. A large number of such SIMs/RUIM can be detected/reported by the ASP but it is not possible to locate them exactly beyond BTS site especially in congested areas.

5. Counter Measures

5.1 The measures to limit or arrest the grey market needs to be multi-dimensional; technical as well as regulatory. These measures should be taken at every level i.e. in addition to the Regulator; each ASP should safeguard its network from illegal termination or distribution of traffic. Only in this way, reduction in grey telephony is possible.

Technical Measures

5.2 Following are the technical measures including monitoring, detection, apprehension and elimination of illegal setups on IP backbone, fixed and cellular networks:

(a) IP Bandwidth Monitoring: Since most of the illegal traffic is terminated/originated using VoIP, it is very important to scrutinize IP backbone of the country. The possible solution can be a technical facility installed at international bandwidth links. The facility should analyze 100% IP traffic for voice content and classify it according to any desired criteria. It would then generate reports indicating the IP addresses suspected to be involved in illegal transportation of voice as per the criteria. These IP addresses along with details provided such as B telephone numbers are then used to locate illegal gateway exchanges for consequent necessary legal action. It can also generate noise in RTP (Real Time Transport Protocol) stream of those suspected IP addresses so that the conversations are not possible, resulting into degradation of the traffic of grey operators, thus pushing them out of business. The facility could also be used for generating CDRs[9] of international incoming traffic terminated using VoIP, which would be helpful in reconciliation with the reported traffic.

(b) Non-Passive Network Analysis Techniques: Illegal networks and routes can also be detected by carrying out non-passive or pro-active analysis of the telecom networks. In this technique, calls are automatically generated from abroad using different software systems which dial through calling cards. These calls are then terminated on non-published telephone numbers, whose CLI[10] and call tracing facility is also activated before call bombardment. Calls land on these numbers using legal as well as grey routes. CLI information of suspected numbers is displayed and routes can be traced back

[7] Public Switched Telephone Network
[8] Internet Protocol
[9] Call Detail Record
[10] Calling Line Identification

to detect illegal setups. This technique, also called real time bypass detection system, can be very effective without much hassle.

(c) Passive Network Analysis Techniques: In contrast to pro-active technique, this methodology is based on analysis of telecom networks and call data records after the calls have been made. It involves deployment of hardware/software at the node to be monitored or interconnect points. The solution collects the data records or signaling information as per given criteria and short lists the suspected numbers. This criterion can be based upon heavy callers, bulk connections and other calling trends. SS7[11] probes can also be used for analyzing signaling information.

(d) Using CLI as Detection Tool: CLI can be used as an effective tool to detect grey traffic termination. There is a possibility to forge CLI information or this information may not be available in some cases. However, by taking few steps, it can provide useful information regarding illegal numbers. Regulator can prohibit hiding or masking CLI by all ASP and gateway operators. Regulators can also allocate codes to International Gateway operators for inserting these while handing over international calls, if CLI information is absent.

(e) Using Fraud Management System (FMS) tools: Operators has a significant role to play in this as their vigilance can minimize the grey traffic. Operators while using FMSs tools can analysis all the on-net and off-net calls to search for unusual usage behavior patterns (like high number of out-going calls but no incoming calls) to effectively detect grey traffic and block phone numbers and/or the handsets (e.g., by barring IMEI[12] numbers) engaged in such activities.

Regulatory Measures

5.3 In addition to technical measures, regulatory measures are also necessary for arresting the menace of grey telephony. Rather regulatory measures are more effective then use of technical measures. Some of the possible regulatory measures include:

(a) Cost Based Settlement Rates: High financial arbitrage provided by non cost-based settlement rates is a major reason of grey telephony. International Telecommunication Union (ITU) recommendation D140 also recommends cost based settlement rates and reducing these on gradual basis in a time period of three to five years. Reducing the settlement rates lowers the financial incentive for grey operators resulting in reduction in grey telephony.

(b) Raids: Carrying out raids over illegal operators is also an effective deterrent measure but it is not the only method to reduce grey traffic, however, it does act as a catalyst in reducing such traffic. Coordination and help from law enforcing agencies is also required from carrying out raids. Success of raid depends on sound legal framework to tackle such hi-tech crimes and well-informed Judiciary about recent technological methods used for such bypassing.

[11] Signaling System No. 7
[12] International Mobile Equipment Identity

(c) Consumer Awareness: Creating consumer awareness is another measure which the regulators and governments can take to reduce suspicious activities. The general public could be made aware of the implications of illegal telecom business so that they may not unknowingly indulge in such activities and may inform the regulator, if they have knowledge of any such activity. Moreover, general public may be invited to report display of local numbers during international calls on advertised toll free numbers managed by the Regulators.

(d) Stake-holders Participation: Reduction / elimination of grey traffic is not only the job of the Regulators alone but all stakeholders must make due contributions. Every ASP operator, on its own level, can oversee its subscribers for their involvement in grey activities. For example, the ASP/ISP can examine network plan of its corporate clients for any vulnerable area before commencement of services. Moreover, the ISPs can keep a vigil over their static IP clients for transportation of voice on data bandwidth.

(e) Opening-up of International Gateway (IGW): One of the reasons of grey market is the restriction on number of IGW licensees. More competition in IGW would considerably reduce the size of the grey market as more IGWs will make all-out efforts to bring maximum traffic through legal means. Keeping existing ASP operators outside the domain of international telephony is not a wise decision as it added up the cost of incoming traffic. Only an ASP with IGW facility is better suited to bring the cost of settlement down to fight grey traffic.

6. Conclusion

Governments and regulators may consider adopting any or all technical and regulatory measures mentioned up to arrest the menace of grey traffic but it must be remembered if the high financial arbitrage between termination rate and settlement rates remains, grey traffic can be reduced but cannot be eliminated.