



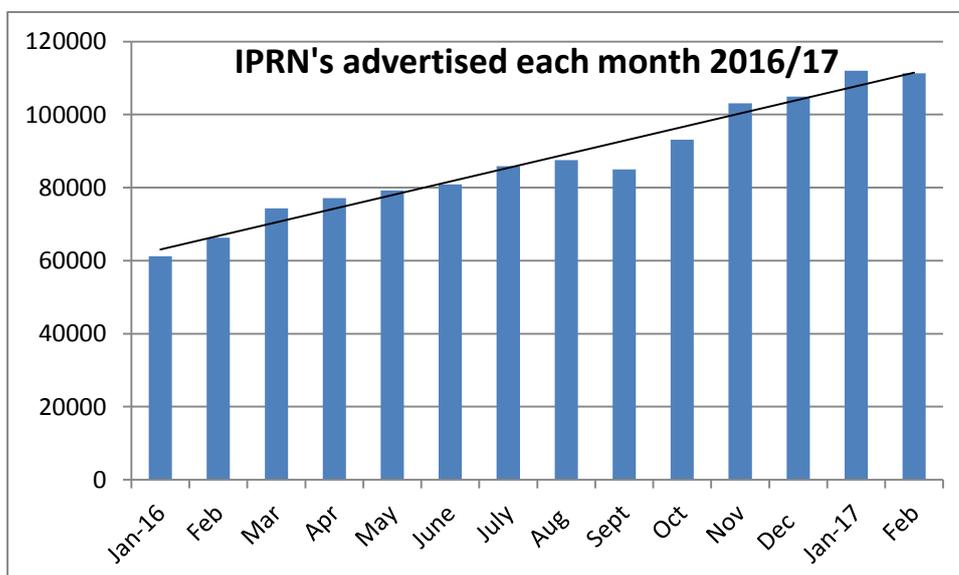
PRISM – FAQ

Q. What is PRISM and what can it do?

A. PRISM is a database of over 412,000 International Revenue Share test numbers (as at 6th Feb 2017), which are provided by IPRN resellers to test that a revenue share destination and number range can be called from a given location. These test numbers, if used correctly in a hotlist, are an extremely useful tool to alert CSP's of a pending or live IRSF attack.

Q. How are these IRS Test Numbers kept up to date?

A. New IPRN Resellers are being identified regularly, and existing number Resellers are updating and changing their numbers frequently, certainly on a 2-4 weekly basis. To ensure that PRISM numbers are current, the database was updated every 4 weeks to include any new numbers identified since the last update. However, due to the increase in new numbers being added to the IPRN's rate cards at odd times during each month, these monthly database updates have now been increased to twice per month. PRISM users are notified each time a new update is available so that this new version of PRISM can be downloaded. This notification also includes information on current high risk destinations for the month or any other information that is considered of interest to our PRISM users. New updates are now made available around the 7th and 21st day of each month. We can add anywhere between 15,000 and 25,000 new numbers to the database each month. The numbers advertised each month continues to increase. In January 2016, there were 60,000 IPRN's advertised that month. In January 2017, we identified 112,000 numbers advertised, an increase of 83%. The growth each month is reflected in the graph below;



Q. How do I use PRISM?

A. The PRISM database should be used as a hotlist on all called numbers from a Fraud Management System or through other network monitoring systems that are available, and also on all roaming traffic, (inbound and outbound). Once an alert is generated the originating device and subscriber should be investigated to determine if they are fraudulent and this may also lead to the identification of other fraudulent connections.

Q. Why would I utilise PRISM on inbound roaming traffic?

A. This is an opportunity to provide some added value to your roaming partners. IRSF losses through the use of a Simcard roaming in a visited network can increase at a rate of \$10,000 per hour. A visited network is required to provide a home network with details of roaming calls within 4 hours. Alerting your roaming partner of likely IRSF activity an hour or two before they receive NRTRDE files could help them avoid significant fraud losses. This is likely to be seen as a differentiator of service from other in Country networks, and could result in your organisation being considered a preferred roaming partner, consequently increasing your roaming revenues.

Q. I don't have an FMS. Can I still use PRISM?

A. Yes you can still use PRISM by integrating it into your manual or semi-automatic hotlist checking processes. Alternatively there are some low cost FMS offerings available which can automate this function for you. Obviously the key to maximising the value from using PRISM is the reaction time between the time any alert is generated and the time a fraudulent device is identified and taken down.

Q. How does PRISM differ from other commercial number databases on the market?

A. PRISM contains IRS test numbers that we know are currently being offered for use by IPRN Providers. If a number is in PRISM, then it is being advertised for use by an IPRN Provider. This includes the many ITU numbers that are allocated to operators and are then leased on to IPRN resellers, so may be used in IRSF attacks. It also includes unallocated, invalid and in some cases customer numbers which are hijacked (short-stopped) by organised fraud groups.

Q. How does PRISM differ from the GSMA hotlist number range database?

A. The GSMA hotlist number database is compiled using operator fraud reports of actual IRSF incidents and therefore relies on the goodwill of operators to share such information with the GSMA. It also relies on the GSMA publishing updates to these numbers and actively managing the database. PRISM is an actively managed database with updates, providing new IPR Test Numbers gained from analysing the content of new and known IPRN Reseller websites, every 2 weeks. Typical updates will contain any new numbers identified, plus

retain previous numbers not published by the IPRN Resellers during this period, as it has been found that often these numbers will re-appear, or have been traded with another Reseller. In this way the latest version of the PRISM database is always up to date with all known test numbers that may be used. Also, the GSMA Hotlist Number Database contains numbers that have been used to terminate fraud calls. PRISM contains test numbers, which will alert you to a likely IRSF attack, before fraud losses escalate. A recent review by an FMS provider whose customers were suffering regular IRSF attacks, and were relying on the GSMA Hot number range list to identify suspected IRSF calls, found that over 30% of the IRSF attacks they had suffered during this period could have been prevented had they been using PRISM.

Q. Can we just block the numbers in the PRISM database?

A. PRISM contains numbers that are being advertised as International Revenue Share test numbers. We do not recommend that these numbers are blocked, but rather used in a hotlist so you can be alerted to any activity on the network that could alert you to a potential IRSF attack. If you block these numbers, which are not typically used in the actual IRSF attack itself, then you will lose the intelligence that these numbers can provide as an early warning tool. Fraudsters often have access to more than one device and an early warning of a likely IRSF attack does provide the opportunity to investigate, and identify any other devices that should also be blocked. Some IPRN Resellers do also provide numbers for legitimate purposes, such as content services, Psychic lines etc. Blocking these numbers could prevent customers accessing a legitimate service, and revenue would be lost.

Q. I have heard that some PRISM users have occasionally located an assigned customer number within the database. How can that happen?

A. If a number is entered in the PRISM database, then it has been advertised by an IPRN Reseller on their rate card or test number schedule. Some IPRN Resellers are heavily involved in number misappropriation (number hijacking), and will often hijack a small operators complete number range during a period when they intend carrying out an IRSF attack. In this case, they will often publish assigned customer numbers which will only generate revenue for them during the period of the number hijack. This is another very good reason why PRISM numbers should not be blocked. In this case, a very quick investigation could reveal that the call is placed by a legitimate customer to the genuine user of the PRISM advertised number.

Q. Can PRISM numbers be uploaded directly to an Operators FMS as a hot list without any rejections?

A. Yes. Through initial testing, we found there were white characters and other formulas identified within some Resellers numbers that caused these numbers to be rejected from an FMS. Now all new numbers are subjected to a 'cleansing process' by engineers at FRSLABS

(responsible for maintaining the PRISM database) to ensure there are no longer any rejections.

Q. What does a typical IRS test call look like?

A. A typical test call will consist of very short calls (sometimes as short as 2 or 3 seconds) to these test numbers. If you have suffered an IRSF attack at any time, look through the fraud calling schedule, and the test calls will be obvious. These will generally be between 1 and 5 short calls to the same numbers followed by multiple calls to different numbers within the same ranges. If the called country is changed midway through the IRSF attack, you will generally see more short duration calls to that Country Code, again checking to ensure that this new Country can still be connected from the device being used. Occasionally, if the fraudster has an existing relationship with an IPRN Reseller, there may be no test calls.

Q. Other than IRSF what else can PRISM be used for?

A. Since PRISM contains a list of active IRS test numbers it can be used for a number of purposes other than detecting IRSF attacks. One example is using the PRISM database for Wangiri fraud detection. By replacing the last 2 digits of the IRS test numbers with wildcards we have a wildcard database consisting of over 7 million numbers. Monitoring calls from these numbers onto your network, especially where these numbers are dialling more than a certain number of unique domestic numbers, has been shown to be effective in detecting Wangiri fraud attacks. Similarly this also works as an outgoing hot list if a rule is set at say >5 calls to a specific PRISM range from different subscribers in xx minutes.

Q. Does it really work?

A. Yes. Our user experience has shown that PRISM does work. It is actively managed and updated on a fortnightly basis and while we don't claim that it contains every single IRS test number it does provide very effective protection. Existing PRISM users now regard this database as the key defensive tool in their IRSF detection strategy. Only one alert from a test number dialled is necessary to identify a possible IRSF attack. A recent analysis of calls made during an IRSF attack on a network which was not a PRISM customer found that from 18,000 calls to 745 unique numbers, 260 of these numbers were recorded in PRISM. Had this operator been using PRISM, 260 IRS Fraud Alerts could have been raised, although the fraud would have been detected, and shut down following the first alert. We have many similar examples to this one.

Q. Does PRISM only detect fraud on mobile networks?

A. No. If an IRSF test number that is in the PRISM database is called, it does not matter whether the device used to generate the call is a mobile, a PBX, VoIP or any other technology. If that called number is checked against the PRISM hotlist, then a fraud alert will be generated.

PRISM has been successful at identifying IRSF incidents on mobile, fixed and Voice over IP networks.

Q. What is the cost of a PRISM licence?

A. A single user (operator) PRISM licence is available at a cost of €5,900.00 per year. Multi operator (Group) licences are also available by negotiation.

Q. How do I get access to PRISM?

A. Email Colin Yates at colin@yatesfraudconsulting.com or Shankar Palaniandy at shankar.palaniandy@frslabs.com for more information (including an application form), or visit <http://www.yatesfraudconsulting.com> or <http://www.frslabs.com>.