white paper

combating mobile crime public policy

abstract

Technical solutions to device theft and cloning help regulators and service providers to combat mobile crime but they're only part of the solution. To truly deter criminals and to avoid placing undue burdens on consumers, service providers and manufacturers, effective public policy must be developed. This paper explores recommendations for detecting and thwarting mobile device-related criminal activity around the globe.

introduction

The soaring popularity of mobile devices has brought with it an unwelcome rash of device theft, counterfeiting and cloning problems around the world. As these devices become more sophisticated and valuable, criminals have seized a lucrative new opportunity for illicit income.

Regulators and service providers have a fiduciary responsibility to protect their citizens from these threats and they have increasingly looked to technology providers to help solve the problems associated with device theft and cloning. The good news is that technical solutions and clear best practices have emerged. Using the triplet consisting of international mobile equipment identity (IMEI), international mobile subscriber identity (IMSI) and mobile subscriber ISDN number (MSISDN) to monitor and track suspicious activities and deviations in devices, regulators and service providers can proactively detect unwanted events and prevent them from recurring.

Despite growing sophistication of the technology solutions, a big part of effectively combating device theft and cloning has nothing to do with technology at all. The challenge is developing effective public policy that discourages abuse and avoids punishing innocent victims or placing undue cost burdens on service providers, manufacturers or other members of the ecosystem. There are literally dozens of critical policy decisions that regulators must make while deploying device registration solutions. There are simple ones such as how to push black, white, and grey list information to service providers (where black implies active blocking of the device in the network, white implies normal device operation and grey implies tracking and active monitoring of the device while allowing normal device operation), to much more complicated considerations, such as what to do about a copycat device that has been in use in the market for a few months.

This paper explores the policy issues associated with enforcing anti-theft and anti-cloning regulations and highlights some of the best practices for stopping mobile criminals in their tracks.

device theft: policy recommendations

On a high level, the rules for enforcing anti-theft regulations seem simple and straightforward. If a device is proven to be stolen, it should be blocked from further use in any national or international network. Once the simple blacklist function is decided, there are numerous policy decisions required on how to truly discourage device theft. costs of implementation and the risks of greater churn, number portability can promote growth in subscribers and revenue for service providers that deliver high quality, innovative marketing, service features and pricing models.

combating mobile crime public policy

In most markets, only 20-25% of stolen phones are actually reported to the police or service providers. That means the vast majority of stolen devices go undetected and, as a result, they never show up on any blacklist. Criminals know this, which is why handset theft has increased year-over-year in virtually every market that has implemented a simple blacklist scheme. In order to truly make an impact on device theft, a set of policies needs to be enacted that will actually deter criminal activity.

Amongst the policies that we recommend are:

- Whenever a triplet is changed, a national database should use analytics to determine if the device is likely stolen
- If a SIM card is removed from a phone and reappears in another device within a specified time window, it should be determined that the device is not likely stolen.
- If a registered IMEI is to be reassigned to another triplet, only the MSISDN owner should have the authority to authorize the reassignment.
- Devices that are detected as stolen should be turned in to authorities for disposal to prevent rebranding or export.
- A grandfather clause for stolen phones currently in circulation should not be permitted.
- When a device is suspected stolen and is detected to be in use within the country, a grace period of 24 hours should be granted during which the MSISDN holder can report a reassignment. After 24 hours, the greylisted device should be moved to the blacklist and blocked from registration.
- f a stolen device is recovered, the original MSISDN holder should be able to return it to the whitelist.

device cloning or IMEI rebranding: policy recommendations

A cloned or rebranded device is, in many cases, a stolen phone with the IMEI altered to avoid detection by the blacklist. In other words, today's stolen devices are often tomorrow's cloned devices. Effective policies to prevent cloning are absolutely necessary in order to reduce device theft and illegal importation.

The primary method of detecting cloned or re-badged IMEIs is to build a national database of triplets and compare them for duplication. A national device registry can compare the triplet data from every device in a country and determine in which cases the same IMEI appears in multiple simultaneous triplets. Any case where an IMEI is duplicated will indicate a cloned device. There may also be cases where IMEIs are of invalid length, invalid format or contain invalid numerical values. For example, leading digits 34, which are unassigned TAC ranges reserved for future use.

There is a great deal of debate on proper policies to determine if a cloned IMEI is valid or not. For example, if there are 100 devices detected with the same IMEI, how do the authorities determine which device is the true uncloned device? In practice, cloned IMEIs are typically badged in 1,000 lots, so in most cases none of the devices detected as cloned will be valid. A device registry system can use time stamps and historical data to determine if devices are likely the victim device and the triplet should be allowed to continue. Historically, these cases are fairly uncommon.

Once devices are determined to be cloned or duplicated, the following policies are recommended for consideration:

- In the initial implementation, most regulators prefer a grandfather clause for devices with invalid IMEIs. Since in most markets the numbers of these devices will be more than one million, the blanket disabling of all devices will cause significant disruption for service providers and subscribers. We recommend that either the subscribers be given a 30-day notice period, via SMS that they have a cloned device, to procure a new device, or the subscriber be allowed to pay a registration fee and continue to use the device as long as the triplet is unbroken. Any device with an invalid IMEI should follow the same process.

- In cases where the IMEI data does not match device description data, the device should be placed into the greylist and verified via SMS.
- Once the initial grandfathering is complete, any device that uses a duplicate IMEI should be blocked.
- An incentive program for users to turn in cloned devices to authorities should be put in place.

device number change: policy recommendations

In most cases, the triplet will be broken when the SIM card is removed. The other case of triplet modification is when the number is changed — either through the placement of a new SIM in the device or through number portability. Both cases should be allowed and even encouraged.

In the case of a multiple SIM user, the user should be able to register multiple SIMs associated with an IMEI and/or a device registry should automatically detect that the IMEI has multiple associated SIMs. In this case, changes to the triplet should be allowed and no action should be taken.

In cases where the number is ported, the IMSI will change but the telephone number and IMEI will stay the same. In many markets, the regulator requires a validation of the IMEI against a device registry before allowing a number port. So if the user requests a port of a number, the IMEI queries the blacklist and greylist to determine if the device is stolen or cloned. If it has, the number port is not allowed. In most cases this step is not necessary, as the device should have already been blocked.

other considerations

In addition to theft and cloning, other key issues facing regulators include counterfeiting, illegal importation, tax evasion and device misuse. All of these issues cause serious damage to mobile networks and government financial structures. In fact, there is an increasing body of evidence that suggests counterfeit or non-certified devices cause serious quality degradations in networks. For example, signal degradation and packet loss can increase by more than 75% in cases where large numbers of non-certified devices are present. This leads to reduced cell coverage and cell throughput, and an increase in capital and operational expenses for service providers, since additional cell sites are needed to make up for the degradation in device performance. [TSG Counterfeit Device Network Impact Study, presented by Qualcomm at the GSMA Terminal Steering Group (TSG), June 2012].

Policies to combat device counterfeiting and illegal importation should be considered, including:An incentive program

- Blocking any device that is determined to be a copy or counterfeit.
- Blocking devices that do not have valid TAC ranges or IMEI numbers.
- Checking device triplets against manufacturer lists and customs/import lists.
- Requiring all devices to undergo network emission and health checks by a certification authority.

Another area that must be considered is battery replacement. In many counterfeit and cloned devices, battery faults are common. Traditional handset manufacturers have strict quality controls for battery manufacturing and testing. Batteries that fail these tests are often recycled, meaning they end up being sold and used in uncertified devices. These batteries often leak, and in extreme cases, they can explode.

Unfortunately, there are no serial number or tracking systems for mobile device batteries. There is also no transmission path for reporting batteries. Unlike IMEI, which is transmitted in the registration message between the handset and the base station, battery identifiers do not exist. The most effective way to control for defective or harmful batteries is through import controls and public awareness campaigns.

conclusion

The theft of mobile devices, and related downstream problems such as cloning or rebranding of IMEIs, has become a major public health and welfare issue globally. In fact, in the Philippines, device theft was listed as the number-one complaint of consumers regarding their communications services — higher than price and service quality combined. Taking resolute action to prevent all forms of device-related crime must be a major priority for regulators and service providers. The combination of best practices in technology with strong public policy is a key lever for solving this critical problem.