SMS Spoof Protection

Protect the network and subscribers against SMS attacks

Advanced measures to protect against SMS Spam and Malware

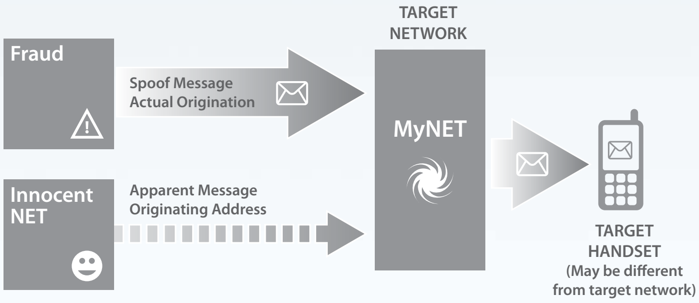
Telsis High Value Mobile Innovation

www.telsis.com

Telsis SMS Spoof Protection | Prevents SMS Spoof attacks, safeguarding the network from potential loss of revenue and loss of confidence in the brand.

Whereas spammers can send millions of messages for nothing over the Internet, message sending in the mobile world conventionally has a cost. It is therefore appealing to the originator if they can somehow by-pass the charging mechanism and send thousands or even millions of messages for free. In order to do so the fraudster needs to do two things: gain access to a mobile network messaging centre via the back door, and hide their true identity.

The back door for most frauds of this type is SS7, the signalling protocol that commonly interconnects GSM operators. When SS7 signalling protocols were introduced, security was not deemed an issue due to the restricted access originally proposed. However, with the proliferation of worldwide communications it is relatively easy, particularly in some countries, for non-operators to gain access to the SS7 network and send SMS messages using 'spoofed' or 'faked' origination details.



The GSM Association describes SMS Spoof as detailed below:

"This type of SMS fraud exploits the lack of authentication on the mobile originated leg of the message transfer. Remember that a SMS submitted by an A-party will always go to that subscriber's SMSC – even if he is roaming abroad - i.e. the SMS does not go to a SMSC in any other country but his own. So in this case the roaming A-party's SMS will be sent from his handset, be received by the radio network of whatever country he is in, and will be sent via intermediate SS7 nodes until it eventually gets to the A-party's SMSC, from the international facing connection of the SMSC.

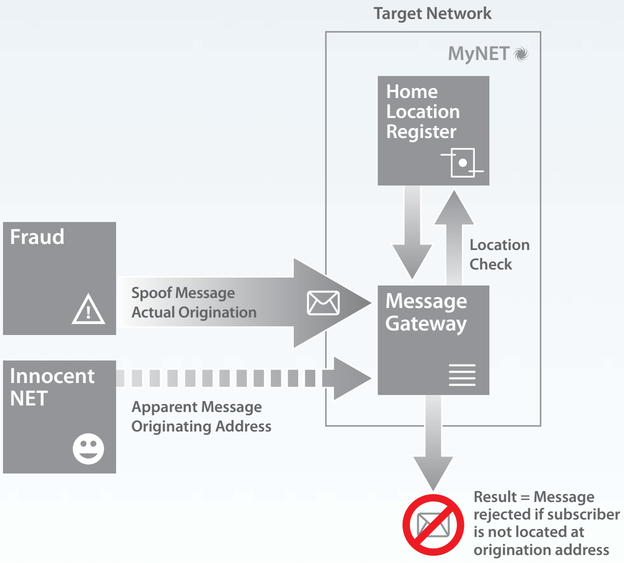
"Fraudsters can exploit this assumption of trust by submitting MO messages from anywhere in the world, but by pretending that the A-party is roaming. In fact the A-party is probably not roaming, nor is it even sending this message, but his identity and potentially his location is being spoofed – something else is using his identity in sending a message. As the SMSC normally trusts the information that it is given, it will accept the message, and attempt to deliver it to its eventual destination. The fraudsters manage to trick the SMSC by modifying the low-level signalling parameters of the MO message, and due to the assumption of trust in SS7, these parameters are not normally challenged and are accepted at face value. Thus the message is accepted by the SMSC and at this point could be sent legitimately to any part of the world."

Impact of SMS Spoof

The impact of SMS Spoof is:

~ The legitimate user of the originating number will be wrongly billed for sending the message
~ The home network may be charged a termination fee for delivering a message off-net
~ Damage to the targeted subscribers who receive the spam or malicious messages
~ The 'apparent' originating network (Innocent NET) will be accused of generating these messages

The first point can be resolved by the user calling customer support and insisting that they were not roaming at that time; however, this action results in additional pressure on customer service resources and can contribute to customer churn and brand damage.


Target Network
MyNET
Home Location Register
Location Check
Fraud
Spoof Message Actual Origination
Message Gateway
Innocent NET
Apparent Message Originating Address
Result = Message rejected if subscriber is not located at origination address

Telsis SMS Spoof Protection prevents SMS Spoof attacks, safeguarding the network from potential loss of revenue and loss of confidence in the brand.

Spoof Protection

Since the integrity of all networks cannot be assumed to be as good as that of the home network, it is not safe to assume that messages received from other networks are genuine.

In order to verify that off-net MO messages are genuine, the Telsis SMS Spoof Protection system performs a number of real-time checks on each message as it arrives, including a query to the network's Home Location Register (HLR) to verify that the messages 'apparent' origination is where the handset is actually connected.

If the message originates from somewhere other than the handset it attached, it can be assumed that the origination address is false, and the message is an SMS Spoof. Some networks run SMS Proxies for MO messages that perform security checking and result in the messages appearing to come from a different location. Telsis SMS Spoof Protection provides the ability to define SMS Proxies and bypass any additional spoof fraud checks.

Once a message has passed the SMS Spoof check, it is then forwarded to one of the network's SMSCs for delivery, using a loadsharing algorithm.

On-Net Spoof Protection

In order to send an on-net message, the handset must be attached to an on-net MSC. In order to attach to such an MSC, the handset must first authenticate itself with the home network.

If the integrity of the network cannot be guaranteed, then On-Net Spoof checking may also be necessary.

Actions

When SMS Spoof is detected, one of three actions may be carried out, as shown below:

Monitor

In Monitor Mode, messages are delivered as normal, however an alert is raised to indicate that there is a potential SMS Spoof attack. The operator cannot view these messages, but can decide whether to Groom or Block messages from this SMSC.

Groom

In Groom Mode, rather than being delivered, messages are groomed to a Service Provider account for further analysis and an alert is raised to indicate that there is a potential SMS Spoof attack. The operator can then choose to discard or deliver these messages.

Block

In Block Mode, any potential SMS Spoof message is silently discarded, and an alert is raised to indicate that there is a potential SMS Flood attack in progress.

The operator can switch between modes of operation, depending on the prevailing network conditions.

Telsis SMS Spoof Protection, together with SMS Fake Protection, SMS Malware Protection and SMS Flood Protection can provide a safety net around the network, protecting both subscribers and brand reputation.

Contact: sales@telsis.com

www.telsis.com

UK	Germany	España	Italia	Middle East	Singapore	Australia
T: +44 (0) 1489 76 00 00	T: +49 (0) 6151 827 850	T: +34 91 532 72 10	T: +39 02 655 1644	T: +971 4 361 6179	T: +65 6224 5585	T: +61 (0) 2 9978 5300
F: +44 (0) 1489 76 00 76	F: +49 (0) 6151 827 8521	F: +34 91 532 96 40	F: +39 02 657 5302	F: +971 4 439 3554	F: +65 6224 7356	F: +61 (0) 2 9978 5333

Telsis High Value Mobile Innovation