SMS Fake Protection

Protect against SMS attacks to network subscribers from outside the network

Advanced measures to protect against SMS Spam and Malware

Telsis High Value Mobile Innovation

www.telsis.com

Telsis SMS Fake Protection | Prevents SMS Fake attacks, safeguarding the network from potential loss of subscriber confidence.

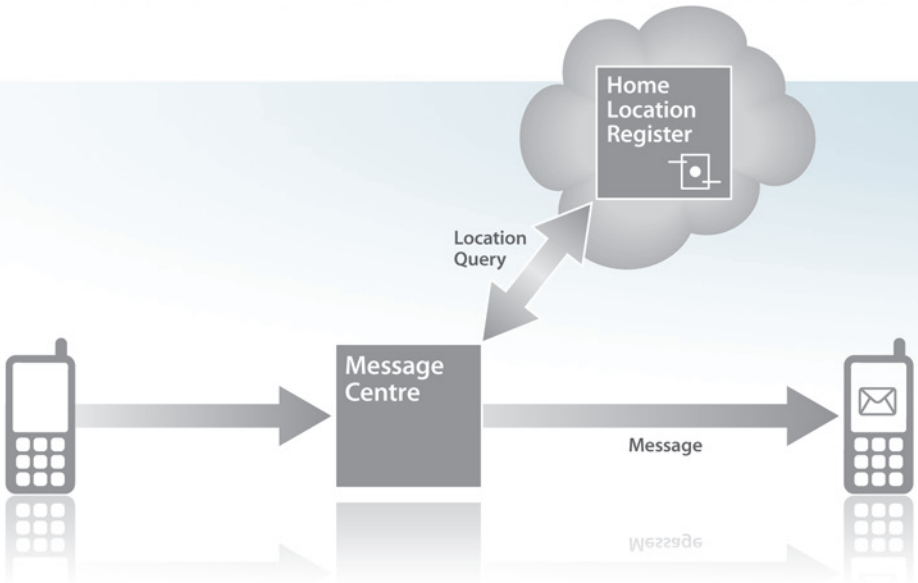
Whereas spammers can send millions of messages for nothing over the Internet, message sending in the mobile world conventionally has a cost. It is therefore appealing to the originator if they can somehow by-pass the charging mechanism and send thousands or even millions of messages for free. In order 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.

SMS Fake is a fraud in the mobile terminated (delivery) path. To understand how it works, let's examine how a genuine message is delivered. Normal SMS delivery takes place in two phases: a location query followed by message delivery to the handset.

~ In the first phase, the originating subscriber (A Party) message centre queries the recipient (B Party) Home Location Register (HLR) to determine the address of the Mobile Switching Centre (MSC) where the B Party is currently connected.

~ In the second phase, the message is sent direct by to the B Party phone from the A Party network



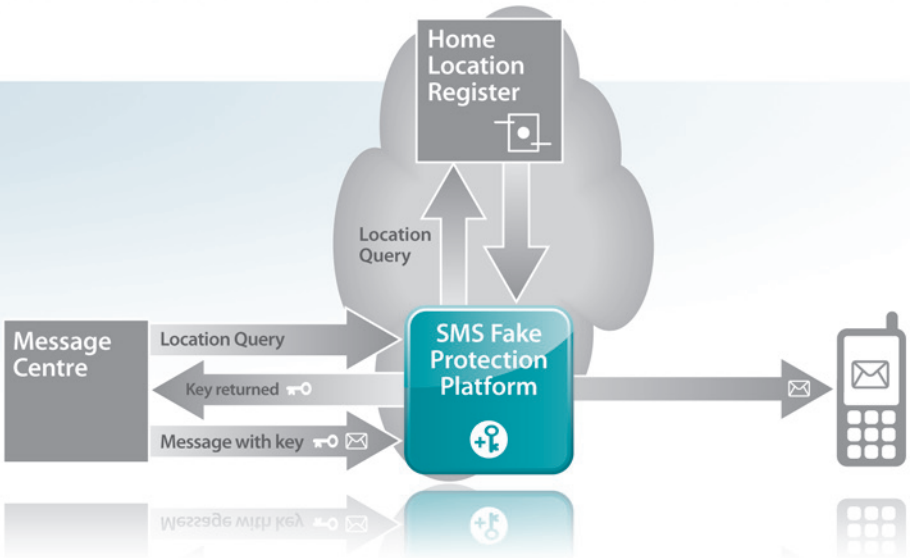
The GSM Association describes SMS Fake as detailed below:

> *"In this faking scenario, a fraudster with access to the SS7 network first sends a SRI-SM to the attacked network's HLR, looking for the location of one or more subscribers, which the HLR will return to them. This is the same as a normal signalling flow. However in the second part of the attack, the fraudster sends a message in the MT part of the message flow, but like SMS spoofing, the low-level signalling parameters of the MT message are manipulated so that it appears to be coming from a different A-party and/or network. In this scenario, the fraudster has faked the A-party's identity – in fact the A-party may not even exist – in order to send a message to a subscriber."*

In reality, in the first part of this scenario, the collection of handset locations (IMSI and VLR) is built up over time using standard (SRI_SM) queries and stored in a database for later use. The success of this approach relies on the fact that phone users tend be at the same place at the same time each day – typically work or home. Some time later, messages are sent using the collected subscriber data, using false originating network and A Party details.

Impact of SMS Fake

The victims of SMS Fake are the faked originating network and the subscribers who receive these messages. Because the originating address has been changed, the terminating network will bill the message to the faked originating network. As such, inconsistencies will be found during reconciliation of interconnect billing records, which can lead to billing disputes that have, in some cases, resulted in interconnects being shut off. SMS Fake messages are used as a method to deliver Spam or Malware, and as such will lead to customer dissatisfaction, brand damage and even churn.



Fake Protection

Telsis SMS Fake Protection prevents SMS Fake attacks, safeguarding the network from potential loss of subscriber confidence.

Telsis SMS Fake Protection works by adjusting the normal SMS delivery path so that off-net SMSCs no longer have direct access to subscriber information and are therefore unable to deliver messages directly to handsets.

Rather than having direct access, the SMSCs transparently interwork with the Telsis SMS Fake Protection system. Genuine messages are passed without any disruption to the message originator or destination handset, while deliveries of SMS Fake messages are blocked.

The first step in preventing SMS Fake attacks is to shut off the collection of subscriber routing information. Rather than responding to HLR queries with real subscriber information, the Telsis SMS Fake Protection system responds with time-limited information encoded with a one time key to hide the subscriber's delivery address and location. Attempts to deliver messages without the one-time key and outside of the time limit are rejected.

The second step is to configure the network to filter any messages that are destined for home subscribers but have not been processed by the solution.

The door on SMS Fake fraud is shut.

Actions

Due to the unique way in which SMS messages are delivered, it is not possible to simply monitor SMS Fake messages and allow those messages to be delivered. The two stage message delivery sequence means that any SMS Fake messages will automatically be blocked. The system raises an alert to indicate when SMS Fake messages are being blocked.

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

Home Routing

SMS Home Routing is a hot topic at the moment. It was developed by Telsis in 2001 and solves some problems that are unique to SMS. Before the days of Home Routing, if a subscriber from another network sent you a message while you were roaming, that message would not pass through your home network at all. Your operator would have no opportunity add value to the messages that you receive and would not be able to protect you from malicious OTA content or spam. Also, every time someone sent you a message, your privacy was threatened because the sending operator could tell which country you were in and whether your phone was on.

With Home Routing, now in service with a number of operators, messages can be delivered via the recipient's home network, allowing the provision of a range of advanced services for the benefit of the recipient. Home Routing is a pre-requisite for protection against SMS Fake and Mobile Malware threats that are carried using SMS.

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