

Secure SMS

Two-Minute Briefing



Mobile SMS spam is a problem in transition. Some types of spam suck revenue from operators. All types of spam annoy phone users. Complaints about spam are rising quickly, with major implications for operators' revenues and their relationships with phone users.

Some 28% of consumers blame their operator for SMS spam no matter where it comes from and 44% would consider changing operators if spam continued to be a problem.

Mass unpaid bulk messaging using spoof and fake techniques defrauds operators of revenue. Because the senders of the spam know they cannot be identified, they are free to deploy the full range of their criminal ingenuity at high cost to innocent phone users. Further, because their action has no cost implications for them, spammers are much more likely to defraud a network into acting as a distribution hub for spam to other networks, multiplying damage and causing tension between operators. Finally, phone users can find themselves billed for messages – sometimes hundreds – that they did not send. Operator support centres become inundated with complaints from phone users.

Spamming in the mobile world only works as a business model if the spammers can somehow by-pass the charging mechanism and send thousands or even millions of messages for free. In order to do so, spammers need to do two things: gain access to a mobile network messaging centre via the back door, and hide their true identity.

The Telsis approach is to make it impossible for fraudsters to send spam for free and impossible for them to send messages whose origins cannot be traced. With their business case undermined and their real identity exposed, spammers have no incentive to continue.

SpooF

SpooF attacks rely on spammers manipulating sending addresses so that inbound messages appear to come from genuine roaming phone users. Networks are defrauded of revenue and subscribers are annoyed by spam.

The Telsis solution acts as a gatekeeper to the network, receiving all inbound off-net messages. As each message arrives, the system makes a number of real-time checks including determining the accurate location of the apparent sender. If real and apparent location differ, the message is determined to be fraudulent. Operators can configure the system to flag spooF messages in order to establish patterns of attack, or simply delete them.

Fake

Fake attacks rely on spammers using completely fictional sending addresses and sending spam to targets on a list of illegally cached or harvested HLR queries. Again, the operator is unable to collect a terminating fee and its customers are annoyed by spam.

The first step in preventing fake attacks is to shut off the harvesting of subscriber routing information. The Telsis solution uses one-time randomly generated time-limited keys to prove the identity of the originator and to tie the delivery of each message to within 30 seconds of its corresponding HLR query. Messages delivered 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 destined for home subscribers that have not been processed by the Telsis solution.

Telsis solutions shut the door on spooF and fake spam once and for all – and require no on-going maintenance.

Call us on UK +44 (0) 1489 76 00 00 | sales@telsis.com

