

SMS SPAMMING TECHNIQUES

Introduction

SPAMmers use a variety of techniques to spread SPAM through SMS. Some of these techniques exploit the flaws in the specifications of current computer networks and electronic communication systems, and others find workarounds about existing ICT security measures.

This article presents a brief about techniques adapted by SPAMmers to spread different types of SMS SPAM.

SMS SPAM CHARACTERISTICS

The architecture of Public Land Mobile Network (PLMN) places the SMSC at a vantage point through which all messages for a given PLMN transit. This provides a unique opportunity to leverage the similarity of transitory traffic at the SMSC to run SPAM filtering algorithm on the SMSC. An effective anti-SPAM solution should be implemented on the vantage point in order to ensure that the SPAM is eliminated from the mobile network as soon as possible to save the time and effort needed to deliver the message.

The ability to SPAM in an SMS area tends to be limited for several reasons. First, SMS messages are not delivered in real-time, giving a time window to collect and identify SPAM by mobile operators. Third, in the SMS network architecture, the SMSC is a vantage point for aggregation of all SPAM messages. Hence, there is no advantage to SPAMming from multiple sources.

For the reasons mentioned above, we can see that there are some basic requirements that any anti-SPAM solution should provide. Even when using similar technologies as used with email SPAM, there are some modifications required on the algorithms in order for it to operate effectively with SMS SPAM.

BASIC REQUIREMENTS FOR ANTI-SPAM SOLUTIONS

Requirement 1: For text based messages, the technique identifying SPAM messages should be based on the degree of similarity of short messages rather than the content (keywords) of an individual message. The textual and keyword based information available is insufficient to classify messages as SPAM. The SPAM could be just 15-characters string trying to dupe a user to return a call to the SPAM originator, tricking him into calling a premium-rate number. Hence, filter algorithms for mobile SPAM must not depend on keywords or textual information but should rely upon the degree of similarity of the SPAM message being circulated in the PLMN.

Requirement 2: The technique used for SPAM classification should be robust to minor modifications to the subsequent messages transiting the public land mobile network. SPAMmers are constantly adapting to new techniques being developed for SPAM filtering. SPAMmers would aim for minor alterations which without loss of meaning of the text message. For example the SPAMmers may aim to substitute certain characters in short messages with similar alpha numeric or other characters (e.g. 'o' could be replaced by 0 and vice versa).

Requirement 3: The technique should also support image recognition to recognize SPAM messages embedded within images.

Requirement 4: The technique for SPAM clustering and classification should generate an extremely low rate of false positives. Mobile messaging is used to support important services such as credit card alerts and bill payments. For this filtering scheme to be successfully incorporated for online SPAM filtering in mobile networks, it is essential

that it should not put user at the risk of accidental deletion or delay of important messages.