Submission to Reducing Scams code review by the Communication Alliance

Background of the author

I worked for 43 years in the Telco industry, in IT and fixed Network areas, most recently on NBN related projects. I did not work formally in Mobiles but the introduction of IP packet switched networks for mobile and fixed line, has resulted in analogous core architectures. I have been retired for 5 years so some assumptions maybe dated.

1. Document Scope

The scope of this proposal is limited to mobiles **SMS scam messages only**.

2. Issues

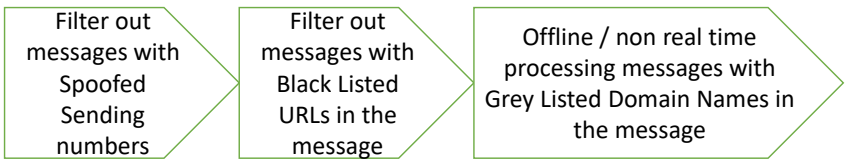
Australian mobile phone users are being bombarded with scam SMS messages. For the mobile users that fall for the scam this can be financially devastating, for the rest of us this can be more than annoying. Often the messages arrive during the night causing loss of sleep, which can be significant to elderly, sick, etc.

These messages typically take the following structure, of at least some of the following components:

I. If a Sending number is provided then, it is typically a spoofed Australian Mobile Number, dynamically (changing between messages) or static.
II. A sender "tag" in the message, (often meaningless, e.g. "linkt:", or sometimes a falsely represented organisation name, e.g. ANZ).
III. A call to action is stated: parcel not delivered due to lack of info, a large payment to be taken from your bank account, etc
IV. A URL to invoke for the receiver to provide information. (The URL of course points to a scammers web site).
    a. The domains for these websites are diverse, but at least in some case the Top Level Domains (TLDs) are notorious for allowing scammers to register domains. The Domain registration is often very cheap, and unvetted, allowing transitory use of the domain name. The Domain registrar is similarly opaque, and isolated from international scrutiny.
    b. So that some TLDs are an immediate red flag.

3. Proposal to address the issue.

Proposed filtering of scam SMS messages



a. Detection of Sending number spoofing:

i. The amount of processing SMS messages detailed below could be drastically reduced by the detection of scam SMSs by first detecting if the sending mobile number is valid, and blocking the message if it is not.
ii. The proposed method is a check along the lines of the following:
    1. Is the number in a number range released by ACMA to the Australian Mobile Network providers? (Block the message if not)
    2. Is the number in one of the following statuses with an Australian Mobile Network provider: Active, SIM issued? (Block if not). This would include blocking messages with suspended service numbers.
    3. The implementation of this check is envisaged by database look ups by the SMSC.
    4. The maintenance of issued number ranges in such a database would be by ACMA.
    5. The maintenance of Active, SIM issued services, would be by the Australian Mobile Network providers. This is analogous to the current maintenance of fixed line Voice services, in the INPD by fixed line Network Service providers for use by the Emergency Services.
    6. This would require all legitimate messages are from a real active mobile service. So there maybe some impacts to operations of current organisations.

b. Detection of scammer URL embedded in the message

The big ask of this proposal is that all solution options call for Deep Packet Inspection (DPI) of at least a subset of all SMS messages that possess a set of attributes indicating a potential Scam SMS.

It is assumed that the message inspection would occur at the Short Message Service Center (SMSC), as all SMS traffic, regardless of SMS over IMS, (SMS encapsulated in a SIP message), SMS using SMPP, SMTP, or HTTP would all traverse the SMSC.

It is appreciated that this would involve additional processing overhead at the SMSC, however the following points are made to mitigate the impact:

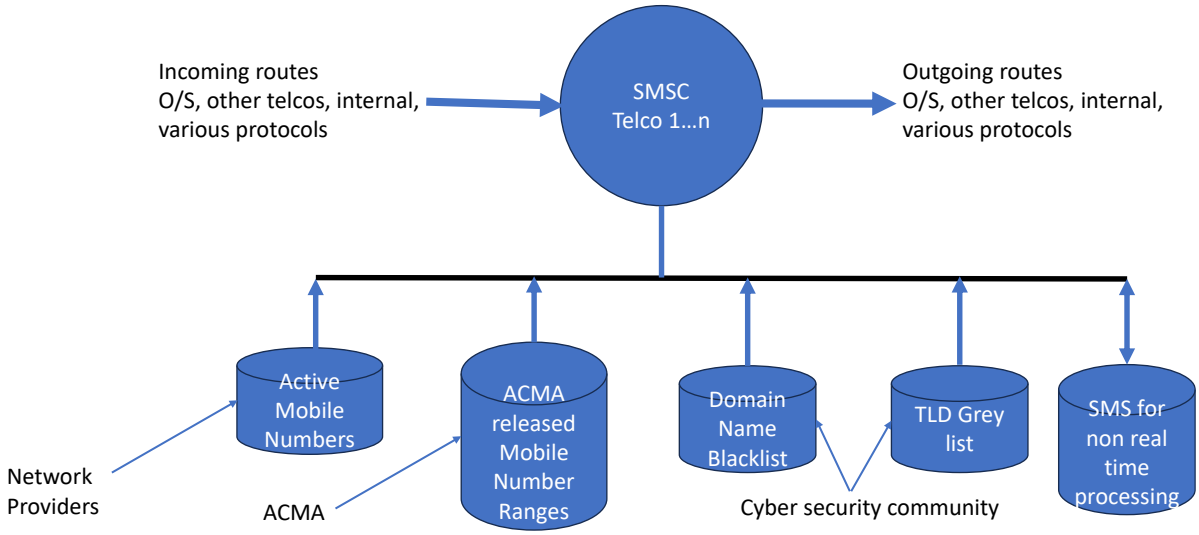
- The scam SMS packets are very small, less than 200 characters.
- The parsing algorithm to identify and extract a domain name from the message should be relatively simple and involve relatively light weight processing.
- The majority of the scam messages seem to be sent during times of light SMS traffic, so the SMSC could shed DPI during times of high traffic, yet still capture the majority of scam messages, especially during the small hours of the morning.
- The SMSC already has message storage capability to support store and forward capability this may need to be augmented due to slightly increased message latency due to DPI and processing.

Notional inspection and processing of each message, requiring DPI:

1. Determine if the message is coming from overseas or is nation.
    a. By route marking?, sender IP address?
2. If from O/S then perform the following processing.

   a. (Note if sufficient justification then Australian mainland originated SMSs could also be processed of course)
3. Parse the message to extract the URL (if it contains one).
4. If a URL is present then:
5. Check for the Domain Name on the Domain Name Black list
6. If it is on the Domain Name black list then block the message
7. Check for the TLD on the TLD grey list
8. If on the TLD grey list then write the message to storage for not real time, more heuristic like processing, e.g. to check if the message contains a "call to action" and if so, then block the message, else pass the message on. (The call to action check might just be a simple string search for phrases like: "not delivered", "your account", "free".)
   a. An alternative to message blocking based on TLD would be to pass the message to the receiving mobile with a warning message inserted such as "Warning: Message is suspected scam".

Notional logical architecture



(Due to message volumes, and desire to minimise latency, physical implementation, is envisaged to be co located storage repositories).

4. Notes:

1. The Domain Name black list could be added to by a cyber security community. Possibly consisting of: vetted volunteers, online security officers of the federal and state governments, private organisation online security staff. A qualification / registration process to bring users on would be required.
2. A similar process is envisaged for the TLD grey list.
3. To provide some ROI on development and operating costs, Network Providers could offer SMS scam blocking, as outlined above, as a subscription service. (E.g. I would be willing to subscribe to such a service, to get a good night's sleep!).
4. Whilst the overseas Domain Name registrars are beyond the control of the Australian Government, one notorious Domain Name registrar source for scammers is not. That

being for Cocos Islands, an Aust territory, a “Verisign subsidiary company, eNIC, which promotes it for international registration as "the next .com"”. This arrangement seems incongruent to the cybersecurity objectives of Australia.

Mike Rampant