

STC ROBOCALL Mitigation Capabilities

ROBOCALL Description:

Auto-Dialers - Robocalling (Machine Behavior) generates large number of calls and use prerecorded messages.

Business Implication

Subscriber inconvenience & potential SCAM. Robocalls are usually coupled with CLI spoofing to make subscriber believe that the calls are being made from their bank, credit card company, hospital, a government organization like tax department etc and the calling party manipulate subscribers to pass personal information which can lead to subscription fraud or direct monetary loss to subscriber.

STC ROBOCALL Detection Methodology:

Features are generated for Calling number related to UNR, call duration spreads, successful/failed call ratios, called number patterns, disconnecting party etc and then these features are evaluated against already trained ML models to classify the cases into robocalling or not. These would be subject to lighter actions like Spam/Scam likely display on CLI or something on those lines if such an action is available.

Covered Scenarios:

1. Caller is calling too many unique numbers (UNR is high) and most of calls are low duration or not being picked.
2. Caller is doing too many hyper short calls (for example: calls_of_duration <= 10s) to many numbers and calling too many unique numbers and not picking lot of received calls
3. Caller is doing <n> calls per hour and percentage of same duration calls among them is more than <m> %.

Data Feeds:

1. SS7 (ISUP International, CAP International, ISUP National (Domestic Off-net), CAP National - off-net and BICC National (Domestic On-net))
2. Add-on (Number range DB and STC subscribers CRM).

Protocol Involved:

1. **SS7**
 - a. ISUP
 - b. BICC
 - c. CAP
2. **SIP**
 - a. SIP traffic capture

Data retention period:

15 to 30 days

Robocalls Monitoring:

Systems reports/alerts are used to act when there is potential or confirmed ROBOCALL cases in coordination with all related teams during working hours (Sunday to Thursday).