XSpam/XSpoof
Prevention and Mitigation

Prevention and mitigation of spam and spoofing/vishing attacks for carrier voice services

XSpam and XSpoof are XCarrier platform applications that detect telephone spam and telephone spoof activities from the public telephone network and proactively suppress them in line with certain rules.

Carrier switch infrastructures are monitored automatically and in real time by the XCarrier applications, which proactively protect a carrier's end customers from fraudulent telephone spam and spoofing activities.
Regulatory requirements are met with these modules.

Terms and Definitions

Telephone or Voice Spam

"Voice spam" or "telephone spam" are the terms used to describe unwanted telephone calls that callers often automate and route in large numbers to the public switched telephone network (PSTN), including unsolicited calls from call centers. There are regulatory requirements in place, especially in European countries, to prevent voice spam.

Telephone or Voice Spoofing/Vishing

Voice or telephone spoofing (also known as "voice phishing" – or "vishing" for short) is the intentional use of a false caller identity. Automated telephone calls are used in an attempt to deceive and mislead the callee and to obtain personal data and details, etc. from them, with a view to subsequently carrying out fraudulent actions with the data obtained.

Carrier Call AG
Rank 6A, 5108 Oberflachs, Switzerland
T +41 56 544 66 00, info@carriercall.com
www.carriercall.com

Identifying Spam and Spoofing

- Calls arriving on an operator's carrier switches are identified by the A-number (originating number) and are checked for format and plausibility, volume, origin and other specific parameters.
- Various reference lists with different priorities are used as a basis for specific actions for this purpose.
  - **Black**: list of numbers or ranges of numbers to be blocked ("A# to be blocked")
  - **White**: list of numbers or ranges of numbers to be routed ("good list")
  - **Gray**: list with unclear or temporary assignments ("unclear list ?#?")
  - Red, yellow, etc.: additional lists with customer-specific elements and assigned rules
- XSpam and XSpoof use internal operator sources to ensure negative number or trunk identification.

Incoming call data records (CDRs), for example, are analyzed by carrier switch(es) in real time and processed by an extremely wide variety of rules, logics and algorithms in fractions of a second.

- Newly discovered spam numbers are identified and appropriate rule actions are immediately applied to those telephone number(s) or trunks.
- Country-specific, additional, external sources of information are dynamically available depending on the area of application (country) and regulation. When available, they are connected electronically via API and integrated into the processing logics.
- Additional, manual entries can be made using the graphical user interface at any time, either as an additive or a complementary solution.

Operation and Interfaces

- XSpam and XSpoof are configured and operated using XCarrier's graphical user interface (GUI).
- The following common import file formats and data collection protocols are currently in use. The following list is not exhaustive.

Import Formats

- .xls
- .csv
- Json
- Xml
- Dblink
- …

Data Collection Protocols

ftp, sftp
http, https
SOAP
REST
…

Carrier Call AG
Rank 6A, 5108 Oberflachs, Switzerland
T +41 56 544 66 00, info@carriercall.com
www.carriercall.com

Automated Protection Actions

XSpam and XSpoof act based on preconfigured action plans and self-learning algorithms

- Defined, dynamic lists with registered numbers or ranges of numbers
- Alerts via SMS, email and push notifications
- Automatic opening of trouble tickets
- Automatic switch provisioning and list enrichment of numbers/trunks to be blocked
  - Blocked numbers are marked uniquely and with a time stamp so that they can be post-processed.
  - Black, gray or white lists – or any other list type – are enriched and kept up to date.

Customer Added Value

Compliance
Compliance with laws, regulations and promises made to regulatory authorities and customers.

Added Value for Carriers
Increase in carrier brand identity due to communicated and effective end customer protection: “Carrier fights and comes out on top.”

Added Value for Carriers end Customers

- Protection of private and business end customers from voice spamming and voice spoofing/vishing activities.
- Preventive and additive security shield for end customer data.

Carrier Call AG
Rank 6A, 5108 Oberflachs, Switzerland
T +41 56 544 66 00, info@carriercall.com
www.carriercall.com