xintec

iGENUITY™

Anti-Smishing **Solution**

The focus is on monitoring subscriber behaviour to identify potentially harmful patterns

Smishing - A definition

Smishing is the SMS (Short Message Service) equivalent of phishing, which involves sending fraudulent emails to trick recipients into revealing personal information or clicking on malicious links. In Smishing, scammers send high volumes of text messages to a wide array of recipients to entice them to take actions that compromise their personal data.

Key Differences from Phishing

One major distinction is that regulations often prevent the direct examination of SMS content. As a result, mobile operators cannot block specific SMS messages containing URLs or links based solely on their content.

The Challenge of SMS Spam

Many spam SMS messages are generated by automated systems. Detecting unusual patterns in SMS traffic is crucial, as SIM cards used for smishing can send thousands of messages to unsuspecting recipients.

The Cost to the Operator

The misuse of retail SIM cards for high-volume SMS messaging can lead to significant financial costs for mobile operators. For instance, when legitimate businesses use retail plans instead of appropriate business accounts, they may breach terms and conditions, potentially leading to lost revenue opportunities and increased operational costs for the mobile operator.

About iGenuity – The Solution

The Xintec iGenuity tool is designed to combat SMS fraud by analysing SIM card behaviour and identifying suspicious activities. It monitors multiple data points, such as

- Volume of messages: the number of messages sent and received by a SIM
- Receiver profile: analysing the diversity of B-numbers
- Sender profile: analysing CRM information on the SIM owner. Is the SIM anonymous?
- Comparison between volumes of sent and volumes of received SMS
- Velocity of sending SMS: is it humanly possible in a given timeframe
- Analysis of roaming and domestic traffic taken together

By correlating this data, iGenuity can quickly detect anomalies indicative of potential smishing attempts, whether in local or international contexts.

Features and Benefits of iGenuity:

- Automated Detection: the system performs real-time or near-real-time analysis to quickly identify and block fraudulent SIM cards
- Customisable Parameters: users can adjust settings to align with specific subscriber behaviours, enhancing detection accuracy
- Reduced False Positives: by analysing patterns thoroughly, the system minimises the chances of mistakenly identifying legitimate user behaviour as fraudulent
- Regulatory Compliance: the tool supports adherence to both local and international laws regarding SMS messaging
- Support for Law Enforcement: iGenuity aids in tracking and prosecuting fraudsters, contributing to broader efforts to combat mobile-related fraud
- Avoiding potential revenue loss caused by fraudulent SIMs abusing the T&Cs of the operator

Conclusion

iGenuity streamlines the process of identifying and mitigating SMS fraud, protecting consumers and ensuring compliance with legal standards. Its automated analysis allows fraud analysts to focus on deeper investigations, ultimately enhancing the overall security of their mobile network.

Smishing detection capabilities can be enhanced by cross-operator detection, where the country's regulatory frameworks allow it. This involves monitoring messages from other operators, not just internally, and analysing patterns in the incoming messages based on diversity of B numbers (receivers) and the low diversity of A numbers (senders).