validsoft

Securing the Chatbot

How Voice biometric technology is unleashing the full potential of Chatbots and Natural Language Processing

The inexorable rise of the voice-based Chatbot has the potential for far reaching impacts on the way we communicate with not only devices, but the organisations we deal with on a regular basis. Many people would have already issued a spoken command to their smart speaker at home, their smart phone voice assistant or even their car. These are all examples of AI-based Chatbots, with lesser or greater degrees of conversational ability.

Advances in Natural Language Processing (NLP) is extending both the sophistication and functionality of Chatbots, whilst enabling a greater range of use-cases. Within financial services, as an example, these include replacing human agents in contact centres, introducing chatbots within automated IVR systems to replace static menus and integrating conversational ability within web pages and mobile apps.

"Voice is now becoming the new human User Interface"

The first and most obvious impact of NLP chatbots, apart from cost savings and convenience, is they are changing the way we interact with these customer-facing channels. Whilst we have always conversed naturally with the contact centre agent, we have traditional pressed buttons on a phone keypad for IVR options and used a mouse, keypad or finger to type, click and tap on our screens and computers.

Voice is now becoming the new human User Interface when dealing with computers, not just humans. The impact of this is profound on how we authenticate users through Chatbots and how organisations can leverage their investment in Chatbots.

The limitations of NLP alone

Chatbots, including the aforementioned examples of smart speakers, smartphone assistants and automobiles, are designed to do one thing well; to understand *what* you're saying or asking. What they don't do, at all, is understand *who* is saying or asking. This may not be important if requesting a song to be played or asking a general knowledge question, but it is very important when a financial transaction is being requested or sensitive personal information is being sought, whether at home or via an organisation's website, app or contact centre.

"Chatbots must understand not only the *what*, but the *who*"

For Chatbots to realise their full potential of being truly autonomous assistants and transaction initiators, they must understand not only the *what*, but the *who*. Without strong authentication, Chatbots will not be able to handle any sensitive requests or authorise risk-bearing transactions. This has been a limitation already with banks in particular eager to deploy financial skills to Alexa and Google, but without the ability to identify the initiator the functionality cannot be deployed.

Frictionless no longer means weak

“Authentication is invisible, fast and continuous”

The rise of Chatbots, and the corresponding migration to voice as the User Interface, provides channels such as the web, apps and IVR with the ability to provide strong authentication in a totally frictionless approach that contact centres already have today.

Frictionless authentication has invariably meant weak authentication. By avoiding interaction with the user at all costs has meant authentication based on best guesses, risk analysis of devices rather than actual human identity or simply relying on the most minimalist approach to security.

This approach changes with Chatbots because ValidSoft incorporates the authentication into the conversation. No passwords or other proxy forms of identification, no reliance on unreliable device or browser fingerprinting, no need for behavioural biometrics which are now redundant with a voice UI and no need for myriad data sources. The authentication is invisible, fast, continuous and provides identity assurance of a human, not just that someone (anyone) is in possession of a device or supposedly secret information.

It takes one to know one

“Deepfakes will render existing impersonation attempts redundant”

2019 has seen the world’s first reported incident of a successful Deepfake fraud, one involving the loss of a substantial amount of money. Deepfakes are computer generated video or audio created by advanced machine learning techniques. The fraudster, presumably using a deepfake voice skin that enables a live conversation, fooled a UK CEO into believing he was speaking with his German counterpart.

Deepfake technology has the ability to render existing human impersonation attempts redundant, with its unprecedented levels of likeness and accuracy, undetectable to the human eye and ear.

However, what a computer creates a computer can also detect. ValidSoft’s advanced algorithms can not only authenticate humans, they can detect the difference between a human speaking and a deepfake speaking, regardless of how perfect sounding the synthetic impersonation or the fact a human could discriminate.

ValidSoft’s Deepake detection ensures Chatbot deployments will not be fallible to this emerging threat, whilst also providing detection against replay (recording) fraud attempts.

Learn More

ValidSoft is a leading voice biometrics software company with a long history of innovation in voice authentication and biometrics. Our technology is built using active, passive, and continuous voice-based authentication, guaranteeing that the speaker is who they are, always. Our solutions help to eliminate call fraud and identity theft. ValidSoft's EuroPriSe™ privacy seals ensure 100% compliance with EU GDPR and other leading Data Protection and Data Privacy laws like HIPAA, Digital Identity Guidelines, Vectors of Trust, Federal Identity Program Guidelines, etc. ValidSoft is consistently recognized by third-party analyst firms as a market leader. See how ValidSoft is powering the Future of Identity at www.validsoft.com

Contact ValidSoft

UK Office:
30 Moorgate
London EC2R 6JJ
United Kingdom

USA Office:
100 Pearl Street
Hartford, CT 06103
United States of America

Email
request@validsoft.com

Phone
+1(888) 392-0230

Confidentiality and Disclaimer

This document may contain references to information that has been obtained from sources believed to be reliable. ValidSoft does not guarantee the accuracy, completeness or adequacy of such information, and shall have no liability for errors, omissions or inadequacies. The recipient assumes sole responsibility for the interpretation and use of this material for its intended results. Predictions and forward-looking statements in this document reflect current expectations concerning future events and are subject to risks and uncertainties, many of which are beyond the control of ValidSoft. ValidSoft undertakes no obligations to update these statements as a result of new information. Opinions expressed in this document are subject to change without notice.