Journal of Information Security and Applications, vol.101, pp.104554, September, 2026.

Analysis of the security and privacy of smart personal assistants with real and synthetic voices

C. Palacios Castrillo; R. Palacios Hielscher; R. Gesteira Miñarro; A. Chávez-Macías; G. López López

Abstract-

Smart Personal Assistants (SPA) can be trained with the owner's voice, and its voice features act as a biometric access password. The aim of this work was to analyze what information different personal assistants reveal without verifying the owner's voice, and what real risks exist in impersonating the owner's voice. To do this, a test protocol was defined, including commands for demanding generic information, personal information, and more sensitive requests such as making calls or purchases. To deceive the personal assistants, tests were carried out with various synthetic voices, including generative AI systems to create voice models based on the user registered in the assistants, hence allowing commands to be synthetically generated with the person's voice features. This study worked with Apple HomePod, Amazon Alexa, and Google Home assistants, which are the main devices on the market. It was possible to verify what type of information each system communicates without performing user validation and how accurate was the voice verification algorithm (activation command) depending on the synthetic voices used. We proposed a Synthetic Speech Detection system as a secondary security layer to identify whether a voice mimicking a target individual was synthetically generated. To evaluate this, a preliminary study on the fidelity of modern synthetic voices was conducted through subjective listening tests. The results indicate that human participants attained only a marginal performance above the 50% stochastic baseline, confirming the high perceptual transparency of current models and the inherent difficulty of the detection task.

Index Terms- Privacy; Generative AI; Voice cloning; Smart personal assistant; Cybersecurity; DeepFake voices

Citation:

Palacios-Castrillo, C.; Palacios, R.; Gesteira-Miñarro, R.; Chávez-Macías, A.; López, G. "Analysis of the security and privacy of smart personal assistants with real and synthetic voices", Journal of Information Security and Applications, vol.101, pp.104554, September, 2026.