Future Generation Computer Systems, vol.144, pp.12-23, July, 2023.

Analysis of security and data control in smart personal assistants from the user's perspective

C. Valero Amores; J. Pérez Sánchez; S. Solera Cotanilla; M. Vega Barbas; G. Suárez de Tangil; M. Álvarez-Campana Fernández-Corredor; G. López López

Abstract-

Advances in the fields of the Internet of Things, Speech Recognition and Artificial Intelligence have facilitated the development of Smart Personal Assistants. As a result, Smart Personal Assistants currently allow requesting a wide range of tasks naturally and intuitively through voice interaction. Their wide popularity, together with the high technological complexity of their environments, have made them an attractive target from a security point of view. Recent works have shown some of the security and privacy issues they stand upon. In this work, we propose a methodology to carry out a systematic security analysis of Smart Personal Assistants using a comprehensive set of tests designed to measure issues around the installation, the interaction, key functionality, and overall Security and Privacy controls. We apply this methodology to analyse security and data control in predominant commercial Smart Personal Assistants (SPA), including Apple HomePod, Google Home and Nest, Amazon Echo (Show and Dot), and Facebook Portal. The main findings of our research are: (i) SPA are not resilient to voice replay attacks; (ii) their skills activation mechanisms can be significantly improved to be more reliable in multi-user households; (iii) the users’ control to restrict the collection and access of Personally Identifiable Information can be also improved; (iv) they lack configurations adapted to minors, which should be included to make them more appropriate for a segment of users who interact more and more with them and have especially high regulatory requirements regarding security and data protection. Among the many hot research topics within this area, we find voice authentication and authorization especially interesting since they may push the usability of Smart Personal Assistants further, as long as they are robust enough from the security perspective.

Index Terms- Cybersecurity; Data control; Internet of things; Minors; Smart personal assistants; Testing methodology

Access to the Journal website

Citation:
Valero, C.; Pérez, J.; Solera-Cotanilla, S.; Vega-Barbas, M.; Suárez, G.; Álvarez-Campana, M.; López, G. "Analysis of security and data control in smart personal assistants from the user's perspective", Future Generation Computer Systems, vol.144, pp.12-23, July, 2023.