Survey of Security Issues with Virtual Assistant Technology

Chirag Liladhar Nehete[1] and Prof. Divakar Jha[2]

Student, Department of MCA[1]
Mentor, Department of MCA[2]
Late Bhausaheb Hiray S S Trust's Hiray Institute of Computer Application, Mumbai, India

Abstract: *Today, virtual voice-assistants are used for manifold purposes. Besides their promising potential, many users are concerned about their privacy and what happens to the data recorded by the voice assistant. Relating the well-known privacy utility trade-off, we found out that not the price of a voice assistant is the most important factor for its acceptance, but privacy. Nevertheless, the acceptance of voice assistance and the decision to use a voice assistant always depends on a combination of different factors, of which privacy seems to be most important.*

Keywords: Virtual Private Voice Assistants, Security Risks, Privacy, Threat, Vulnerabilities

REFERENCES

[1]. "Amazon Alexa virtual assistant bug fixed after cybersecurity firm discovered vulnerabilities." https://www.8newsnow.com/news/localnews/amazon-alexa-virtual-assistant-security-bug-fixed-aftercybersecurity-firm-discovered-vulnerabilities/ [Online; last accessed 5-Nov-2020]

[2]. N. Zhang, X. Mi, X. F, X. Wang, Y. Tian, and F. Qian, "Dangerous Skills: Understanding and Mitigating Security Risks of Voice-Controlled Third-Party Functions on Virtual Personal Assistant Systems," 2019 IEEE Symposium on Security and Privacy.

[3]. H. Hyunji Chung, Michaela Iorga and Jeffrey Voas. NIST, Sangjin Lee, Korea University, "Alexa, Can I Trust You?", The IEEE Computer Society 2017

[4]. Cook, J. Amazon employees listen in to thousands of customer Alexa recordings. 2019. Available online: https://www.telegraph.co.uk/technology/2019/04/11/amazon-employees-listen-thousands-customer-alexa-recordings/ (accessed on 25 March 2020).

[5]. Chung, H.; Park, J.; Lee, S. Digital forensic approaches for Amazon Alexa ecosystem. Digit. Investig. 2017, 22, S15–S25. [CrossRef]

[6]. Siebra, C.; Correia, W.; Penha, M.; Macedo, J.; Quintino, J.; Anjos, M.; Florentin, F.; da Silva, F.Q.B.; Santos, A.L.M. Virtual assistants for mobile interaction: A review from the accessibility perspective. In Proceedings of the 30th Australian Conference on Computer-Human Interaction, Melbourne, Australia, 4–7 December 2018; pp. 568–571.

[7]. Amazon Alexa Integrated with IoT Ecosystem Service. Available online: https://www.faststreamtech.com/blog/amazon-alexaintegrated-with-iot-ecosystem-service/ (accessed on 22 February 2021).

[8]. Dikla Barda, Roman Zaikin, Yaara Shriki, "Keeping the gate locked on your IoT devices: Vulnerabilities found on Amazon's Alexa." https://research.checkpoint.com/2020/amazons-alexa-hacked/ [Online;last accessed 1-December-2020].

[9]. Carlini, N., Mishra, P., Vaidya, T., Zhang, Y., Sherr, M., Shields, C., Wagner, D., Zhou, W.: "Hidden Voice Commands." In: Proceedings of the 25th USENIX Security Symposium (2016)

[10]. "Amazon 2017 About Alexa Voice Profiles", https://www.amazon.com/gp/help/customer/display.html?nodeId=202199440. [Online; last accessed 8-November-2020].

[11]. JIDE S. EDU, JOSE M. SUCH, GUILLERMO SUAREZ-TANGIL,"Smart Home Personal Assistants: A Security and Privacy Review ACMComputer. Survey.", Vol. 1, No. 1, Article. Publication date: August 2020

[12]. Deepak Kumar, Riccardo Paccagnella, Paul Murley, Eric Hennenfent, Joshua Mason, Adam Bates, and Michael Bailey.2018. "Skill Squatting Attacks on Amazon Alexa". In 27th USENIX Security Symposium