Ben-Gurion University of the Negev **אוניברסיטת בן-גוריון בנגב**
Industrial Engineering and Management **המחלקה להנדסת תעשיה וניהול**

Project No.	**Project Title**	
2021 -01-253	Vulnerabilities and Security analysis of Speech Emotion Recognition (SER) systems	
Academic Advisor	**Co-Advisor**	
Dr. Nir Nissim		
Team Members		
Itzik Gurowiec		
itzikgu@post.bgu.ac.il		

Abstract

Speech emotion recognition (SER) system is a system that leverages sound waves information produced by humans to detect the concealed emotions in each utterance of the speaking human. In the last decade, many SER systems were implemented in a variety of applications and domains, including entertainment systems (e.g. Siri, the Apple virtual assistant), education, cyber-security systems etc. Over the last 20 years, researchers have focused their effort in developing SER systems that are more accurate, with richer functionalities, with a wide range of emotions that can be detected by the system, using variety of learning methods (from classic machine learning algorithms to Deep learning algorithms). However, exploring, and enhancing the security of SER systems has not been studied enough. SER systems both have access to a huge amount of personal data that is acquired by the system and take part in important decision-making processes. In this paper, our main contribution is a comprehensive exploration and analysis of the potential attacks aimed at SER systems. To do so, we have created the entire eco-systems describing the data flow between each component and player of a SER system, and explored the vulnerabilities of it, which might be exploited to attack and compromise the system. We present ten potential attacks that can be performed on a SER system, and the defense methods that can be used to prevent such attacks. We have found that the best available defense mechanism covers only 30% of the attacks, while 70% of the attacks and vulnerabilities of SER systems remain almost completely exposed. Moreover, 30% of the potential attacks has no relevant defense mechanism. Prior of doing so, and in order to better understand the potential attacks and the SER eco-systems, we present the main principles of SER system, from the process of collecting the sound waves themselves, to the process of appropriate features extraction needed for training and evaluating the system. Furthermore, we present a taxonomy of the main SER studies performed, and their evolvement along the years. Finally, as a result of our study, we could provide several concrete directions for improving the security of SER-based systems, which can turn this domain to a more secured, allowing humans to preserve their privacy and to SER companies to meet the modern security policies.

Keywords: Emotion; SER; Cyber-attack; Security; Malware