

1. Record Nr.	UNINA9910760295803321
Autore	Sun Kun
Titolo	Secure Voice Processing Systems against Malicious Voice Attacks // by Kun Sun, Shu Wang
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2024
ISBN	9783031447488 3031447484
Edizione	[1st ed. 2024.]
Descrizione fisica	1 online resource (122 pages)
Collana	SpringerBriefs in Computer Science, , 2191-5776
Altri autori (Persone)	WangShu
Disciplina	005.8 323.448
Soggetti	Data protection - Law and legislation Biometric identification Privacy Biometrics
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	1 Introduction -- 1.1 Overview -- 1.2 Background -- 1.2.1 Audio Signal Processing -- 1.2.2 Voice Processing Systems -- 1.2.3 Attacks on Speaker Verification Systems -- 1.2.4 Attacks on Speech Recognition Systems -- 1.3 Book Structure -- References . . -- 2 Modulated Audio Replay Attack and Dual-Domain Defense -- 2.1 Introduction -- 2.2 Modulated Replay Attacks -- 2.2.1 Impacts of Replay Components -- 2.2.2 Attack Overview -- 2.2.3 Modulation Processor -- 2.2.4 Inverse Filter Estimation -- 2.2.5 Spectrum Processing -- 2.3 Countermeasure: Dual-domain Detection -- 2.3.1 Defense Overview -- 2.3.2 Time-domain Defense -- 2.3.3 Frequency-domain Defense -- 2.3.4 Security Analysis -- 2.4 Evaluation -- -- 2.4.1 Experiment Setup -- -- 2.4.2 Effectiveness of Modulated Replay Attacks -- 2.4.3 Effectiveness of Dual-Domain Detection -- 2.4.4 Robustness of Dual-Domain Detection -- 2.4.5 Overhead of Dual-Domain Detection -- 2.5 Conclusion -- -- Appendix 2.A: Mathematical Proof of Ringing Artifacts in Modulated Replay Audio -- -- Appendix 2.B: Parameters in Detection Methods -- Appendix 2.C: Inverse Filter Implementation -- Appendix 2.D: Classifiers in Time-

Domain Defense -- References -- 3 Secure Voice Processing Systems for Driverless Vehicles -- 3.1 Introduction -- 3.2 Threat Model and Assumptions -- 3.3 System Design -- 3.3.1 System Overview -- 3.3.2 Detecting Multiple Speakers -- 3.3.3 Identifying Human Voice -- 3.3.4 Identifying Driver's Voice -- 3.4 Experimental Results -- 3.4.1 Accuracy on Detecting Multiple Speakers -- 3.4.2 Accuracy on Detecting Human Voice -- 3.4.3 Accuracy on Detecting Driver's Voice -- 3.4.4 System Robustness -- 3.4.5 Performance Overhead -- 3.5 Discussions -- 3.6 Conclusion -- References -- 4 Acoustic Compensation System against Adversarial Voice Recognition -- 4.1 Introduction -- 4.2 Threat Model -- 4.2.1 Spectrum Reduction Attack -- 4.2.2 Threat Hypothesis -- 4.3 System Design -- 4.3.1 Overview -- 4.3.2 Spectrum Compensation Module -- 4.3.3 Noise Addition Module -- 4.3.4 Adaptation Module -- 4.4 Evaluations -- 4.4.1 Experiment Setup -- 4.4.2 ACE Evaluation -- 4.4.3 Spectrum Compensation Module Evaluation -- 4.4.4 Noise Addition Module Evaluation -- 4.4.5 Adaptation Module Evaluation -- 4.4.6 Overhead -- 4.5 Residual Error Analysis -- 4.5.1 Types of ASR Inference Errors -- 4.5.2 Error Composition Analysis -- 4.6 Discussions -- 4.6.1 Multipath Effect and Audio Quality Improvement -- 4.6.2 Usability -- 4.6.3 Countering Attack Variants -- 4.6.4 Limitations -- 4.7 Conclusion -- Appendix 4.A: Echo Module -- Appendix 4.B: ACE Performance tested with CMU Sphinx -- Appendix 4.C: ACE Performance against Attack Variants -- References -- 5 Conclusion and Future Work -- 5.1 Conclusion -- 5.2 Future Work -- References.

Sommario/riassunto

This book provides readers with the basic understanding regarding the threats to the voice processing systems, the state-of-the-art defense methods as well as the current research results on securing voice processing systems. It also introduces three mechanisms to secure the voice processing systems against malicious voice attacks under different scenarios, by utilizing time-domain signal waves, frequency-domain spectrum features and acoustic physical attributes. First, the authors uncover the modulated replay attack, which uses an inverse filter to compensate for the spectrum distortion caused by the replay attacks to bypass the existing spectrum-based defenses. The authors also provide an effective defense method that utilizes both the time-domain artifacts and frequency-domain distortion to detect the modulated replay attacks. Second, the book introduces a secure automatic speech recognition system for driverless car to defeat adversarial voice command attacks launched from car loudspeakers, smartphones and passengers. Third, it provides an acoustic compensation system design to reduce the effects from the spectrum reduction attacks, by the audio spectrum compensation and acoustic propagation principle. Finally, the authors conclude with their research effort on defeating the malicious voice attacks and provide insights into more secure voice processing systems. This book is intended for security researchers, computer scientists and electrical engineers who are interested in the research areas of biometrics, speech signal processing, IoT security and audio security. Advanced-level students who are studying these topics will benefit from this book as well.