СЕКЦИЯ «ЗАЩИТА ИНФОРМАЦИИ»

RESEARCH ON SOFTWARE MODULE FOR PROTECTION OF INFORMATION FROM A LEAKAGE VIA ACOUSTIC CHANNELS

Dai Junyi [1]

[1] *Belarusian State University of Informatics and Radio Electronics*
Minsk, Republic of Belarus

O.B. Zelmansky – PhD, associate professor

Annotation. Aiming at the problem of information leakage in acoustic channels, a software module is designed and studied. This module can effectively reduce the risk of leakage and ensure information security in multiple scenarios, which has important practical value.

Keywords. acoustic channels, sound leakage prevention, software module, information security.

Introduction

With the rapid development of information technology, smart devices are widely popularized, which brings convenience to people, but also increasingly serious information security issues 1. . Acoustic channels, as a potential channel for information leakage, have gradually attracted attention2. . The built-in microphones of smart devices are often in a "monitoring" state, making it very easy for voice information to be stolen through the acoustic channel, which in turn leads to the risk of privacy leakage. In places such as government, military, and scientific research institutions that have extremely high requirements for information confidentiality, information security is of great importance, and once leaked, it will cause serious consequences. Therefore, in order to effectively respond to these information security threats, it is crucial to design a software module to prevent information leakage in acoustic channels, which has extremely important practical significance for protecting personal privacy, corporate trade secrets, and national information security.

To achieve this goal, the following tasks were determined:

– Investigate existing technologies and risks: Study the current acoustic channel information leakage related technologies, analyze their principles and application scenarios, accurately identify information leakage risk points, and provide a basis for software design.

– Build software module architecture: Design the overall architecture of the software module, integrate voice cloning, acoustic interference control and user management functions, and ensure that the architecture is stable.

– Develop core functional modules: Implement audio management and voice cloning core modules, ensure audio security management and high-quality voice cloning, and improve information protection capabilities.

– Test and optimize software performance: Test the software in multiple scenarios, evaluate the anti-leakage effect and performance, optimize according to the test results, and enhance the practicality and stability of the software.

Research on acoustic channel information leakage

1. Acoustic channels and monitoring technology

Acoustic channels use sound waves to transmit information and are widely used in underwater communications, medical, industrial, and consumer electronics 3 . . With the development of technology, monitoring technology has been evolving from traditional microphone-based monitoring methods to advanced technologies such as laser microphones and vibration sensors, as well as non-invasive monitoring technologies such as gyro microphones and visual microphones, which pose a serious threat to privacy 4 . .

Different monitoring technologies have their own characteristics. Laser microphones can collect sound from a long distance, but are greatly affected by the monitoring surface and environmental factors; vibration sensors can achieve non-line-of-sight monitoring, but the clarity of audio collected in noisy environments is limited; acoustic sensors are restricted by the environment and microphone quality. In addition, the reliability of existing countermeasures against monitoring technology needs to be improved.

2. Information leakage risk and protection strategy

Smart device microphones can easily obtain sensitive information of users when collecting environmental sounds, and malware may also secretly transmit this information through acoustic channels 5 . . In the communication system, if there is a security vulnerability in the transmission of sound signals, attackers can capture and restore the signals and steal important information. Information leakage will cause serious harm to individuals, enterprises and national security 6 . .

To deal with these risks, acoustic information protection strategies are divided into active protection and passive protection. Active protection technologies such as active noise interference, acoustic encryption, dynamic acoustic barriers, and real-time acoustic monitoring and alarm systems block the risk of information leakage by intervening in the propagation of acoustic signals in real time, but they have problems such as low energy efficiency, real-time bottlenecks, high-frequency attenuation, and sensor interference 7 . .

Passive protection technologies include acoustic stealth technology, physical isolation, environmental noise protection, and acoustic signal confusion 8 . . These technologies reduce risks by designing security measures, but they also face limitations such as poor low-frequency performance, large space occupation, environmental dependence, and signal distortion.

Software module design and implementation

1. System design goals and requirements analysis

1.1 Protection scenarios and problem definition

For open office environments, the software module mainly guards against two risks: one is voice feature leakage, that is, attackers use voice cloning technology to forge user voice features to interfere with the voice recognition system; the other is voice content leakage, that is, attackers use cloned voices to play meaningless texts, reducing the recognition accuracy of the voice-to-text system.

1.2 Core functional requirements

The software module has the function of user voice cloning, and voice training is realized through the Fineshare API. The input is a clear recording uploaded by the user with a sampling rate of more than 1 minute and 16kHz (supports MP3 format, no more than 50MB). The API automatically completes voice feature extraction and cloning model training (about 3 minutes), and outputs cloned audio files (MP3 format).

In terms of acoustic interference control, it provides basic environmental noise (such as rain, cafe background sound, white noise) and supports volume adjustment; preset meaningless text templates, and use cloned timbre to play text randomly in real time.

The user management system covers basic functions such as registration/login, playing public and private audio library audio, managing private audio, and cloning personal voice.

2. Software module architecture design

2.1 Overall architecture design

The software module adopts a three-layer architecture, including the front-end interaction layer, the back-end service layer, and the third-party API layer. The front-end interaction layer is responsible for page structure display and dynamic content rendering, including page templates such as login and registration, which are implemented through the Jinja2 template engine. CSS is responsible for page style layout, and JavaScript implements client interaction logic, including modules such as audio playback control and voice cloning management.

The back-end service layer is based on the Flask application, processes front-end HTTP requests, and implements business logic and data access management. The routing layer is responsible for processing user authentication, audio files, user information, voice cloning and other related requests. The storage layer uses SQLite database to store user information and system configuration, and the file system stores audio files, which are divided into public audio library, private audio library and cloned voice library.

The third-party API layer provides voice cloning function, processes voice sample conversion and returns cloned voice files. Each layer interacts through a clear interface to realize functions such as user operation processing, data transmission and storage, and voice cloning.

2.2 Database Design

The system uses SQLite database and implements data persistence through SQLAlchemy ORM framework. Database design follows the principle of normalization to ensure data integrity and consistency. The user model defines the user data structure, including fields such as user ID, user name, password, email, administrator ID, password reset token and expiration time.

Database configuration is implemented by creating database engine, session and declaring base classes. The data access layer encapsulates database session management and CRUD operations, including functions such as obtaining database session, creating users, and querying users by username. The database security mechanism includes password encryption storage and transaction management to ensure user password security and atomicity of data operations.

3. Core module implementation

3.1 Audio management module

The audio management module is responsible for the storage, playback and management of audio files. It adopts a hierarchical design to isolate and manage public noise libraries and private voice libraries. Set the file storage directory and allowed file extensions, and limit the uploaded file size to 16MB. Get the list of audio files from the specified directory through the function implementation, and provide an interface for obtaining the public audio playlist in the web application.

Playback control is implemented through the PlaybackManager class of JavaScript, which supports loop playback and random playback modes. File upload processing is implemented in the routing of the Flask application, checking the user login status, whether the file exists, whether the file type is legal, and saving the file to the user-specific directory to ensure the security and standardization of file upload.

3.2 Voice cloning module

The voice cloning module provides users with voice cloning functions through recording and API integration. The recording interface is implemented using the VoiceCloneManager class of JavaScript to obtain the audio stream of the user's media device for recording. Manage sample text and provide multiple preset texts for user recording. Process voice file upload in the Flask application, create a user-specific directory to save files, and handle file name conflicts

Conclusion

This study designed and implemented a software module based on Web application, which can effectively reduce the risk of information leakage in the acoustic channel, ensure information security in a variety of scenarios, and has good practicality and flexibility. In the future, the module will continue to be optimized to further improve its performance and security to better cope with the ever-changing information security challenges.

List of sources used:

1．Gaouzi, Z., & Chougdali, K. (2022). Impact of security and privacy risks on the adoption of IoT: A state of the art. Information Security Journal, 29(2), 115-130.

2．Oleynikov, A., Bilotserkivet, O., & Shirokyi, O. (2023). Modeling the Acoustic Channel of Voice Information Leakage. Cybersecurity & Privacy Journal, 18(3), 250-266.

3．Pan, C., Liu, S., Qing, X., & Qiao, G. (2023). Feature extraction and classification of deep-sea mobile underwater acoustic channels. Marine Science Journal, 14(2), 85-99.

4．Cunningham, C. F., Hopps, A. M., Losee, W., Sandberg, R., Allred, D., & Neilsen, T. (2023). Frequency Characterization of Laser Microphones. Journal of Acoustical Science, 45(3), 210-225.

5．Duan, L., Zhang, K., Cheng, B., & Ren, B. (2021). Privacy Threats of Acoustic Covert Communication among Smart Mobile Devices. Cybersecurity Journal, 12(4), 678-693.

6．Prytys, V., Krymchak, L., & Havlovska, N. (2020). Leakage of Information as a Key Problem of Economic Security. Cyber Risk Journal, 19(5), 421-438.

7．Lai, S. K. (2019). Real-time prediction of noise signals for active control based on Bayesian forecasting and time series analysis. Acoustics and Noise Control Research, 37(1), 55-72.

8．Feng, X., Yan, L., & Chun, W. (2021). Review on vibration isolation technology. Journal of Physics: Conference Series, 1820(1), 012009.