WH6X Security White Paper

This document is applicable to models: WH62, WH63, WH66, WH67, WH62 Portable, and WH63 Portable.

Overview

With the rapid development of the Internet, DECT wireless technology has been widely used in different fields. While being widely used, enterprises also attach increasing importance to security requirements. Yealink provides users with high-quality business DECT headsets in the field of mixed offices, not only focusing on high-quality audio experience, but also paying attention to the risks brought by DECT in security. Yealink provides reliable headset products for end-users and enterprise users by practicing the best security practices in the DECT industry.

Yealink passed the GB/T 22080-2016/ISO/IEC 27001:2013 safety system certification in July 2022. ISO/IEC 27001 is an international standard for safety best practices accepted by a wide range of users, and the system certification establishes a safety implementation process for the product and means that the company is Continuous investment and optimizing.

The article explains the working principle of DECT security and the security level of DECT to help users and security practitioners understand the security architecture and security solutions of Yealink DECT headset products. The article is mainly divided into the following sections: DECT working principle, DECT secure transmission, and DECT security management.

DECT Working Principle

DECT is a wireless communication technology standard that uses the 1.9G wireless frequency band for short-range communication. By following DECT security best practices, the risk of attackers obtaining access to DECT signals for eavesdropping and access control is minimal. DECT needs to perform the following security verification steps during the connection establishment process.

- Pairing: Establish a communication key between the Base and the headphones
- Authentication: Verify the identity through the key of both parties in communication. If the verification fails, communication cannot be established
- Encryption: Wireless data is encrypted during communication.

DECT Security Transmission

The DECT headset series uses a physical pairing method for security. The encryption scheme used between the base and the headset uses AES-128-bit encryption, which employs advanced encryption algorithms and complex encryption keys, meeting the industry's mainstream security standards.

Pairing Security

The Base and the primary headset must be paired through physical contact. The communication during this process is done using a unique Yealink mode, and it is difficult for outsiders to obtain the critical component information of the pairing process.
Base and earphones can be paired through physical contact or by pairing Base and earphones simultaneously to enter pairing mode. The entire

pairing process requires confirmation from the main earphone. If the main earphone is not confirmed within 10 seconds, it automatically disconnects and exits pairing mode.

Authentication Security

After the physical pairing is completed, DECT will confirm the key during the start of the connection. Communication can only proceed if the key authentication is successful. Each time the connection is restarted or reconnected after disconnection, an identity authentication algorithm is required to establish a secure connection using the AES-128 bit key to ensure that the two primary security keys of the headset and Base are the same. The primary key between each headset and Base is unique, and the keys are not shared between different devices.

The security measures of DECT that check the key include the following process:

- The DECT Base detects whether the headset has been registered by sending a random number.

- The DECT handle calculates the registration request and the random number given by Base through the key and returns the calculated result to Base.

- Base also uses the same algorithm to obtain a calculation result and save it locally in Base.

- The headsets send the calculated sound response back to the Base.

- Base compares the returned results of the local and handle. If the two results are consistent, Base allows the connection to be established.

Data Encryption

During the call, the wireless signal between the Base and the headset is encrypted using the AES 128 encryption algorithm for control signaling and bidirectional data flow (RTP) to prevent unauthorized users from illegally controlling and eavesdropping. This encryption method is enabled by default, and the primary encryption key is updated every 60 seconds according to the protocol standard during each call to prevent attackers from attempting to obtain the encryption key for media data through brute force cracking.

Frequency Band Security

In using wireless frequency bands, Yealink products strictly abide by the division of RF frequency bands in various countries and regions and preset the RF frequency bands of the corresponding countries during the shipment process. Frequent bands conform to the standard specifications of different countries and can further improve the anti-interference performance of Yealink wireless devices.

Frequency Band	National Version
1880 – 1900 MHz	Europe
1786 – 1792 MHz	Korea
1893 – 1906 MHz	Japan
1910 – 1920 MHz	Brazil
1920 – 1930 MHz	USA
1900 - 1910MHz	Thailand

Risk Analysis and Assessment

- **Eavesdropping**

Attack method: Third-party access through Bluetooth to listen to calls or use interception of wireless signals to parse out the data stream.

Risks: High security, pairing needs to be actively triggered, requires physical connection to get the key Low feasibility.

- **Third Access Control**

  Attack Method: Crack Bluetooth's identity and encrypted information through low-security authentication.

  Risk: High security, Yealink uses Bluetooth version 5.0 or later and completely removes insecure authentication methods.

- **Man-in-the-middle attack**

  Attack method: Control the device by message interception, tampering and forwarding to other devices.

  Risk: High security, the attacker needs to be close to the attack target in order to implement, beyond the wireless range cannot be implemented. Actually, this type of attack is a low likelihood of implementation.

Security Management

Code Security Standards

Key Management: The core key management adopts a dedicated strategy. Based on the principle of least privilege so ordinary engineers cannot access and obtain the key.

Code management: Yealink has strict coding security requirements inside, and every code update will review the code and perform reliability verification. Device-related code libraries have strict permission management mechanisms and requirements. It is strictly forbidden to upload to public or semi-public services such as Github, Gitee and other public code bases without permission to prevent source code leakage.

Security Environment: Yealink's security team and IT department regularly perform static and dynamic vulnerability scans and penetration tests for both production and internal network environments to ensure that software development, firmware packaging, and device production take place in a secure network environment.

Security Emergency Response

Security has always been a priority for Yealink. Industry security technology is constantly iterating, and Yealink invests high resources every year to upgrade Yealink security level to ensure that the security level matches the current security technology. If you find a possible security issue during the use of Yealink products, you can contact us in Yealink's Security Center or submit your issue through the Ticket system. We will respond and handle the issue in a timely manner.

Security emergency response is divided into four phases: issue collection, vulnerability analysis, vulnerability repair, and tracking and resolution.

- **Issue collection**: Based on the feedback of security incidents, collect relevant logs and information, and arrange for dedicated personnel to follow up and deal with them.
- **Vulnerability analysis**: Give priority to judging the risk of vulnerabilities based on the problem, and give priority to providing temporary solutions during the processing phase to avoid the expansion of the impact of the problem.
- **Vulnerability repair**: analyze the root cause of the problem, trace the cause of the defects in the design, and solve the vulnerability problem from the root cause in a timely manner.

- **Tracking and resolution**: Check whether all product lines have the same problem, and collect the problems to Yealink's vulnerability database for regular checking.

Technical support can visit Yealink Support for firmware downloads, product documentation, FAQ, and more. For better service, we recommend that you use the Yealink Ticket system to submit technical questions.

Disclaimer

Declaration

This white paper is for informational purposes only and does not grant any legal rights to any intellectual property in any Yealink product. You may copy and use the contents of this document for your internal use for reference purposes.

Yealink makes no express, implied or statutory warranties with respect to the information in this white paper. For more information about Yealink's BH7X series of headsets you can visit Yealink's official website and for more security related information you can visit Yealink SECURITY & COMPLIANCE.