DECT Phone

Security White Paper

Yealink Network Technology CO., LTD.

White Paper

Nov. 2023

This document applies to models: DECT Phone W90, W80, W70B.

Overview

Yealink, a leading global provider of communication and collaboration solutions, is dedicated to ensuring the security of user information. We prioritize security and put users first, creating a safe environment for our global customers to utilize our products.

This white paper focuses on protecting user privacy data as its central theme. We have established a comprehensive security protection system by implementing enterprise security management, following OWASP application security standards, and adhering to Android's best security practices as software development guidelines. Through this system, we continuously provide security guarantees for our end users.

With over 20 years of security experience and in alignment with industry best practices, Yealink offers secure and reliable products and services to customers worldwide. We have obtained ISO 27001:2013 and SOC2 Type 2 certifications, demonstrating our commitment to safety. Additionally, we comply with GDPR and other relevant laws to ensure data privacy. For more detailed information, please visit the Yealink Trust Center at https://www.yealink.com/en/trust-center.

ISO/IEC 27001 is an internationally recognized standard for implementing safety best practices. Certification of our system signifies our dedication to product safety and ongoing investments in optimizing safety management and product design. The SOC (System and Organizational Controls) framework, developed by the American Institute of Certified Public Accountants (AICPA), is widely accepted as a comprehensive standard for internal control auditing. Our SOC2 Type 2 audit report verifies that Yealink has a stringent service control system encompassing security, availability, confidentiality, and privacy.

This demonstrates our capability to provide secure and stable products and services to our customers. This article aims to provide a clear understanding of Yealink's security architecture and solutions by introducing the security technologies and features of our products. It is divided into several sections: Hardware Interface Security, System Security, Network Security, Transmission Security, Meeting Security, Data Security, Encryption, User Privacy, and Product Release Process.

This document applies to the following model: DECT Phone W90, W80, W70B.

Hardware Interface Security

2.1 Debugging Interface

- Disable device debugging interface

The UART serial port, ADB, Telnet, and other device debugging interfaces are disabled at the factory to prevent unauthorized access and potential data risks.

2.2 Secure Boot

The device supports secure boot, and the system verifies the device's integrity using a signed public key during the boot process. At any stage of the boot process, all boot programs (bootloader, kernel, partition integrity) are required to undergo integrity verification. Only when they pass the security checks can the system be successfully booted; otherwise, it will fail to start. The purpose is to prevent devices from loading and running unauthorized programs, thereby avoiding the possibility of unauthorized programs gaining control over the device by modifying boot parameters or other means during startup, which could potentially grant access to the device's shell interface.

Secure Boot includes:

- Unable to flash non-Yealink official firmware.
- Unable to run non-Yealink official firmware.
- Any data tampering at any stage will cause the device to fail to start.

System Security

3.1 Flash Encryption

Yealink encrypts and stores all user data on the device using secure keys, with the keys themselves also undergoing encryption for enhanced security. After encryption, all data (user-created data) is stored in encrypted form in the device storage space after being stored on the disk.

Disk encryption uses the AES 256-bit advanced encryption standard algorithm. The 256-bit AES algorithm encrypts the master key (implemented through calls to the OpenSSL library). The storage of the master key will be protected according to security standards to prevent external access to related key information.

3.2 DECT Subscription Security

The base, by default, disables the Subscription feature. To register a new handset to the base, users must enable the 'Start Register Handset' function through the base or via the administrator account logged into the device's web interface. Additionally, it defaults to a 90-second timeout closure.

The handset undergoes strict identity verification during the registration process. Currently, Yealink's DECT devices offer two authentication methods:
1. 4-digit PIN code authentication: During the handset registration to the base, the handset needs to input a 4-digit PIN code. If the code is entered incorrectly, the authentication will not succeed. Yealink's default PIN code is 0000. It is recommended for security administrators to promptly change the PIN code.

2. Registering via the handset's unique identifier IPUI: This involves pre-configuring the IPUI value (a 10-digit random character) in the base for the handset. Authentication and usage are only possible when two values are identical.

3.3 DECT Authentication Security

After PIN code verification in DECT, each reboot or reconnect requires using the Digital Secure Authentication Algorithm (DSAA) with an AES-64 bit key to establish a secure connection, ensuring that both the handset and the Base share the same pair of security keys. The primary key between each handset and the Base is unique, and keys are not shared between different devices.

The process by which DECT security measures inspect keys includes the following steps:

1. The DECT Base sends a random number to the handset to verify if it's already registered.
2. The DECT handset calculates an authentication request by processing the random number received from the Base.
3. The Base also uses the same algorithm to perform the calculation.
4. The handset sends back the calculated result to the Base.
5. The Base compares the two calculated results, allowing handset connection establishment if the results match.

3.4 DECT Data Encryption

In the DECT system, Yealink devices utilize the DECT Standard Cipher (DSC) encryption algorithm to encrypt the bidirectional media streams (RTP) during calls, preventing unauthorized users from eavesdropping. This encryption is enabled by default. During each call, the encryption's primary key is updated according to protocol standards, preventing attackers from obtaining the encryption key for media data through brute-force attacks.

3.5 DECT Frequency Band Security.

In the utilization of wireless frequency bands, Yealink products strictly adhere to the RF frequency band allocations designated by various countries and regions. Yealink's products come pre-configured with the respective RF frequency bands for each country upon factory shipment. Adhering to various countries' standards and regulations regarding frequency band usage enhances the resistance to interference for Yealink wireless devices.

Frequency Bands	Country Versions

Frequency Bands	Country Versions
1880 – 1900 MHz	Europe
1786 – 1792 MHz	Korea
1893 – 1906 MHz	Japan
1910 – 1920 MHz	Brazil
1920 – 1930 MHz	USA
1900- 1910 MHz	ThaiLand

Network Security

4.1 802.1X

The device supports the 802.1x feature. User devices connected to the switch port need to be authenticated, and unauthorized users are prohibited from accessing the network. The device supports seven 802.1X modes:

- EAP-MD5
- EAP-TLS
- EAP-PEAP/MSCHAPv2
- EAP-TTLS/EAP-MSCHAPv2
- EAP-PEAP/GTC
- EAP-TTLS/EAP-GTC
- EAP-FAST

4.2 OpenVPN

The device supports the functionality of OpenVPN, allowing it to establish secure point-to-point data communication over a network tunnel created by OpenVPN in a public network environment. While users achieve secure data transmission through the VPN tunnel, it also supports application layer data encryption such as SRTP and HTTPS, implementing multi-layer encryption to protect data. You can refer to the Yealink Administrator Guide device usage guide for specific Open VPN usage.

Transmission Security

5.1 Media Encryption (SRTP)

When establishing a media session between two devices, media data transmission supports the Secure Real-time Transport Protocol (SRTP) with

AES-128 and AES-256 key lengths. The encryption keys are dynamically generated during the call setup process and possess uniqueness, ensuring the security of the media transmission.

5.2 Transport Layer Security (TLS)

All data transmitted over the Internet can be secured using secure transmission channels to ensure data integrity and confidentiality, thereby preventing information from being stolen or tampered with during the network transmission process between the device and the server. The terminal device supports the TLS1.3 function and is enabled by default. TLS1.3 improves performance and security compared to TLS1.2 (such as removing vulnerable and less-used algorithms). As a server, using TLS 1.0 and TLS 1.1 for communication is not allowed. However, to ensure compatibility with a wide range of servers when acting as a client, negotiation of TLS 1.1 is permitted. Users have the option to enhance device security performance by disabling the TLS 1.1 protocol through configuration. Specific instructions can be found in the Yealink Administrator Guide.

Data Security

6.1 Data Storage

- Data Storage

The device utilizes the AES256 encryption algorithm to encrypt stored data, ensuring the security of static data. Dynamically loaded data is stored directly in the system memory, preventing it from being subjected to static analysis.

The configuration data within the device is stored directly on the device, implementing strict access control policies that restrict access to authorized users or administrators only.

- Configuration file encryption

The device supports CFG configuration encryption. You can encrypt the original configuration file first, decrypt it automatically after deploying it to the device, and then update the configuration to the device. Yealink provides encryption tools for Windows, Linux, and other platforms to encrypt configuration files. The user sets the key. For specific usage instructions, please refer to the Yealink Administrator Guide or Device User Guide.

- Password Security

When the device transmits private data in the network, it is encrypted by RSA and transmitted over the network. Privacy data is anonymized in input fields and is not displayed in plain text on the front end. If the number of input errors reaches three, the account will be locked to prevent attackers from brute-forcing the device. During the backup configuration process, the device will automatically clear password-related configurations to prevent the leakage of sensitive data.

6.2 Data Deletion

The device will delete all business data on the applications when restored to the factory settings to ensure data security.

6.3 Access Control Security

The device has differentiated access control permissions by default settings: divided into User and Administrator, each with a different password. When accessing advanced settings on the phone, an administrator password is required. Regular users have basic operational privileges, but the device allows administrators to customize different levels of permissions for regular users. For detailed instructions, please consult the Yealink Administrator Guide or Device User Guide.

Encryption

7.1 Device Unique Certificate

Devices are pre-installed with a device certificate with a unique identifier issued by Yealink Root CA. The certificate uses the SHA256 signature algorithm with a key length of 2048. The security standard follows the protocol standard of RFC 2818.

7.2 Encryption Algorithm

During the TLS negotiation process, the device uses a high-security level encryption algorithm suite by default, disables anonymous and other insecure algorithm suites, ensuring the security of data transmitted over the network. For users with stringent security requirements, administrators can enhance the security level by configuring algorithm lists. For specific instructions, please consult the Yealink Administrator Guide or Device User Guide.

Algorithm List:

- TLS_AES_256_GCM_SHA384 (0x1302)
- TLS_CHACHA20_POLY1305_SHA256 (0x1303)
- TLS_AES_128_GCM_SHA256 (0x1301)
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
- TLS_DHE_DSS_WITH_AES_256_GCM_SHA384 (0x00a3)

- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x009f)
- TLS_ECDHE_ECDSA_WITH_AES_256_CCM_8 (0xc0af)
- TLS_ECDHE_ECDSA_WITH_AES_256_CCM (0xc0ad)
- TLS_DHE_RSA_WITH_AES_256_CCM_8 (0xc0a3)
- TLS_DHE_RSA_WITH_AES_256_CCM (0xc09f)
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
- TLS_DHE_DSS_WITH_AES_128_GCM_SHA256 (0x00a2)
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x009e)
- TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8 (0xc0ae)
- TLS_ECDHE_ECDSA_WITH_AES_128_CCM (0xc0ac)
- TLS_DHE_RSA_WITH_AES_128_CCM_8 (0xc0a2)
- TLS_DHE_RSA_WITH_AES_128_CCM (0xc09e)
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x006b)
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA256 (0x006a)
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x0067)
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA256 (0x0040)
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA (0x0038)
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)

- TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA (0x0032)
- TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
- TLS_RSA_WITH_AES_256_CCM_8 (0xc0a1)
- TLS_RSA_WITH_AES_256_CCM (0xc09d)
- TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
- TLS_RSA_WITH_AES_128_CCM_8 (0xc0a0)
- TLS_RSA_WITH_AES_128_CCM (0xc09c)
- TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)
- TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c)
- TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
- TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
- TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)

Privacy Security

8.1 Log Security

The device provides local logging and remote logging services for troubleshooting and security information event management. The content of the log output strictly follows the protocol standard of RFC 5424 and prohibits the printing of sensitive data, such as password information, encryption information, etc., in the log, diagnostic debugging information, and alarm information. You can choose the TLS transmission method for network transmission, which can effectively guarantee the confidentiality and integrity of the logs.

Suppose the device malfunctions and requires Yealink to provide service support. In that case, the product logs and diagnostic information require user authorization to access the relevant files, and unauthorized users cannot actively access the diagnostic information of the current device.

8.2 Configuration Backup

Password-related configuration is removed by default when exporting device configuration backups to avoid the risk of password leakage. The configuration file is encrypted using the AES256 encryption algorithm. This encryption algorithm is a strong symmetric encryption algorithm that provides a high degree of data protection.

The exported configuration file can optionally be saved in an encrypted binary format, such as config.bin instead of a plaintext text file. This security measure effectively protects user privacy and configuration information from unauthorized access and disclosure during backups.

8.3 Device Management

In the industry, IP phone device manufacturers typically provide Remote Provisioning Service (RPS) to address the challenges of large-scale and bulk device deployment. Yealink also offers optional RPS (Remote Provisioning Service) for its customers.

Yealink's RPS mechanism solely offers redirection services, updating the pre-deployed server address specified by the customer onto the device. After the update, the connection between RPS and the device is disconnected, during which no business processing occurs, and there is no data exchange.

Users can also choose Yealink's device management platform for bulk device management. Yealink provides device management platforms with two different deployment methods.

YDMP (Yealink Device Management Platform), customers can install Yealink DM software in their own data center. YMCS (Yealink Management Cloud Service), Yealink uses Microsoft Azure, which is widely recognized and trusted by enterprise users, to build DM services. YMCS is SOC2 Type 2 and GDPR certified and has independent data centers in the United States, Europe, and Australia to protect data security fully.

The core benefits of the Yealink Device Management service are as follows:

- Device status monitor
- Bulk device upgrades and management
- Remote diagnosis

8.4 Preconfigured Domain Name Information

When the device is restarted or when executing business, it is necessary to access the preset server address. The specific list is as follows:

Domain Name	Business Functionality	Request Method
rpscloud. yealink.com	The RPS automatic deployment feature (optional service) triggers a redirection request once during factory reset, closes upon successful deployment, and can be disabled if not required.	Enabled by default

Domain Name	Business Functionality	Request Method
pool.ntp.org time.windows.com	NTP's sever address, power-up, and periodic queries.	Enabled by default
www.yealink.com	Web page hyperlink address that provides quick access to the official Yealink web site.	Disabled by default, customers need to enable it manually
support.yealink.com	Web page hyperlink addresses that provide quick access to Support's Web site features.	

Note:

Some addresses may change during the software release process. The specific information should be based on the configuration of the device preset or deployed. If you have any questions, you can consult Yealink's technical support.

Security Management

9.1 Product Launch Process

Yealink follows a secure software development lifecycle (S-SDLC). During the coding phase, the security team conducts risk assessments of third-party libraries and tools used in the product to ensure that vulnerabilities introduced by the supply chain are avoided. They also conduct security reviews. Before the software version is released, it undergoes Alpha version, Beta version testing, and UAT testing. At each stage, the security team participates in penetration testing, attack surface analysis, and security scanning of software and hardware to ensure that the released product software meets the security standards for the software release.

Penetration testing includes but is not limited to the following:

- System security: secure boot, file encryption, compilation condition detection, etc.
- Web Testing: XSS Cross-Site Scripting Attack, File Upload Vulnerabilities, CSRF Cross-Site Request Forgery Attack, etc.
- Vulnerability scanning: Use multiple mainstream scanning tools in the industry to test firmware and deployed devices to ensure the security of the software.

9.2 Code Security Specification

Key Management: The core key management adopts a dedicated strategy, with the principle of least privilege, and ordinary engineers cannot access or obtain the keys.

Code Management: Yealink has strict coding security requirements internally. Each code update is reviewed and undergoes reliability verification. The device-related code library has strict permission management mechanisms and company red-line requirements. It is strictly prohibited to upload to public or semi-public services such as GitHub and Gitee without permission to prevent source code leakage.

Secure 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.

9.3 Security Emergency Response

Security has always been a focus of Yealink. As industry security technology iterates, Yealink invests heavily in resources yearly to improve Yealink's security level. At the same time, Yealink will find multiple well-known, authoritative third-party organizations for security verification every year to ensure that the security level matches the current security technology. If you find a possible security issue while using Yealink products, you can contact us in Yealink's security center or submit a ticket through the ticket system, and we will respond promptly and deal with relevant issues.

Security incident response typically consists of four main stages: vulnerability collection, vulnerability assessment, vulnerability remediation, and tracking resolution.

- Vulnerability Collection: Collect relevant logs and information based on reported security incidents and assign dedicated personnel to track and handle them.
- Vulnerability Analysis: Priority is given to determining vulnerability risks based on the problem. During the processing stage, temporary solutions will be provided first to prevent the problem from expanding.
- 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.

- Track and Resolve: Investigate whether all product lines have the same problem and follow up to resolve it. At the same time, collect the problem and regularly check it in Yealink's vulnerability database.

Technical support can access the Yealink Support website to learn about firmware downloads, product documentation, and frequently asked questions. For better service, we recommend that you use the Yealink ticket system to submit technical issues.

Disclaimer

10.1 Affirmation:

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

Yealink makes no express, implied, or statutory warranties regarding the information in this white paper. To learn more about the Yealink DECT Phone device, you can visit Yealink's official website. For additional security-related information, you can visit the Yealink Security Center.