DECT Phone Security White Paper

This document applies to models: W90, W80, W70.

Overview

With the rapid development of the mobile internet, enterprise communication terminal devices are widely used in different scenarios. In the process of providing convenience to enterprises, security threats from multiple dimensions, such as hardware, system, application, and network, are becoming increasingly severe. The demands of end users for data security and privacy protection are becoming more and more prominent.

This white paper takes the protection of user privacy data as its core. Through enterprise security management, OWASP application security standards, and Android best security practices as software development guidelines, product security forms a systematic security protection system, continuously providing security guarantees for Yealink's end users.

Yealink complies with the provisions of the General Data Protection Regulation (GDPR), which is known as the world's strictest privacy and security law; Yealink devices comply with current EU data protection regulations and have completed an independent GDPR compliance assessment, reflecting industry-leading levels of data protection and privacy.

Yealink passed the GB/T 22080-2016/ISO/IEC 27001:2013 security system certification in July 2022. ISO/IEC 27001 is an international standard widely accepted as the best practice for security. The certification establishes a secure implementation process for products and means that the company continues investing in and optimizing security management and product security design.

This article introduces the products ' security technology and features to help users and security practitioners understand the security architecture and security solutions of Yealink products clearly. The article is mainly divided into the following sections: hardware interface security, system security, network security, transmission security, data security, encryption, user privacy, and product release process.

Hardware Interface Security

Debugging Interface

- By default, the UART serial port, ADB, Telnet and other debugging interfaces are disabled when the device is released from the factory. It is prohibited to enable related functions in any way externally to prevent unnecessary debugging interfaces from being exposed externally and causing data risks.

Secure Boot

The device supports secure boot, and the system verifies the device's integrity using a signed public key during the boot process. All boot programs (bootloader, kernel, partition integrity) are verified for integrity at any stage of the boot process. The system can start up normally when the security check is passed; otherwise, it cannot. The purpose is to prevent unauthorized programs from being loaded and run, and to prevent access to device control by entering the Shell interface by modifying the boot parameters.

Secure Boot enhances security by including the following:

- 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

Disk Encryption

The process of encrypting all user data on the device using a secure key (which is also encrypted) and storing it. 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.

Firmware Security

The firmware data is encrypted with high-strength encryption algorithm, and the firmware cannot be cracked or tampered with.

The firmware installation process has a security check, and incorrect firmware and tampered firmware will be identified and not allowed to be installed.

DECT Subscription Security

By default, Subscription functionality is disabled in Base. If users need to register a new handset with the Base, they need to enable the "Start Register Handset" feature either through the Base or by logging in to the web interface as an administrator. The default timeout for registration is set to 90 seconds, after which it will be automatically disabled.

During the registration and pairing process, handsets require strict identity authentication. Yealink DECT devices currently offer two authentication methods: 1. Using a 4-digit PIN code: Handsets need to enter a 4-digit PIN code during the registration process with the Base. If the entered PIN code is incorrect, the authentication will not be successful. The default PIN code for Yealink is 0000. It is highly recommended for the security administrator to change the PIN code promptly. Registration can also be done using the unique identifier IPUI of the handset. In this method, the IPUI value (a 10-digit random character) of the handset is pre-configured in the Base. Authentication and successful registration can only occur if the IPUI value of the handset matches the one stored in the Base. Refer to the configuration guide in the Yealink Admin Guide for specific usage.

DECT Authentication Security

After the PIN code verification is completed in DECT, every time the connection is restarted or reconnected after a disconnection, an authentication algorithm (DSAA) is used with an AES-64 bit key to establish a secure connection, ensuring that the two main security keys of the handset and the base are the same. Each handset and base have a unique primary key, and the primary keys are not shared between different devices.

The DECT security key verification process is as follows:

1. The DECT base station sends a random number to the handset to check if it is registered.
2. The DECT handset calculates the registration request using the key and the random number provided by the base station, and sends the calculated result back to the base station.
3. The base station also performs the same calculation using the algorithm and saves the result locally.
4. The base station compares the locally calculated result with the result returned by the handset. If they are identical, the base station allows the connection to be established.

DECT Data Encryption

In the DECT system, Yealink devices utilize the DECT standard encryption algorithm DSC to encrypt the bidirectional media stream (RTP) during the call process, preventing unauthorized users from eavesdropping. This encryption method is enabled by default, and during each call, the encryption main key is updated according to the protocol standard to prevent attackers from attempting to obtain the encryption key of the media data through brute force attacks.

DECT Frequency Band security

Yealink products strictly adhere to the RF frequency band allocations defined by various countries and regions for wireless communication. During the shipping process, Yealink products are preconfigured with the corresponding RF frequency bands of the destination countries. Yealink wireless devices comply with the standards of different countries for frequency band usage, which further enhances their resistance to interference.

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

Network Security

802.1X

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

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

- EAP-FAST

OpenVPN

The device supports the OpenVPN feature, and in a public network environment, the device can establish point-to-point secure data communication through the network tunnel created by OpenVPN. 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. For specific instructions on using OpenVPN, please refer to the configuration guide in the Yealink Admin Guide.

Transmission Security

Media Encryption (SRTP)

When a device establishes a session with another encrypted device, the media data is optionally transmitted using AES-128 Secure Real-Time Transport Protocol (SRTP) with a key length that supports configuration of AES-256 bits; the key is dynamically generated at the time of call creation and is unique.

Transport Layer Security (TLS)

All data transmitted over the Internet network, such as the connection between mobile devices and servers, can use a secure transmission channel to ensure data security. Data integrity verification is performed during the download process to ensure that information is not 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, communication using TLS1.0 and TLS1.1 is not allowed. At the same time, to be compatible with a wide range of servers, it is allowed to negotiate as TLS1.1 when acting as a client. Users can disable the TLS1.1 protocol to improve device security performance by configuring it, and the specific usage method can refer to the configuration guide of the Yealink Admin Guide.

Data Security

Data Storage

- The business data involved in the device is directly stored on the device, and only end users and administrators have relevant reading and access permissions.

- 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. Refer to the configuration guide in the Yealink Admin Guide for specific usage.
- When the device transmits private data in the network, it is encrypted by RSA and transmitted over the network. The private data is anonymized in the input box and will not be displayed in plaintext on the front end. If the number of incorrect attempts reaches 3 times during the brute force cracking process, the account will be locked to prevent attackers from brute force cracking the device. During the configuration backup process, the device will automatically clear password-related configurations to avoid the loss of the user's private data.

Data Deletion

When the device is restored to factory settings, all business data on the application will be deleted to ensure user data security.

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. User users only have ordinary operation permissions. The device supports administrators to customize different permissions for ordinary users. Refer to the configuration guide in the Yealink Admin Guide for specific usage.

Encryption

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.

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. Administrators can set the algorithm list for security-conscious users to increase the security level; please refer to the Yealink Admin Guide configuration guide for specific usage.

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

Log Collection

The device is not configured with a remote log collection service when it leaves the factory. If you need to configure a remote log service, please refer to the configuration guide in the Yealink Admin Guide. The device removes privacy data related to user authentication in the logs. If the user's device malfunctions and needs to be diagnosed, the user needs to cooperate and authorize the diagnosis file exported locally from the device for fault analysis. Unauthorized users cannot actively obtain the current device's diagnostic information.

Configuration Backup

The password-related configuration will be removed by default when exporting user configuration backup. The configuration file will be encrypted using the AES256 encryption algorithm inside the device and then exported as a config.bin file through the web page. This file needs to be decrypted by a dedicated security decryption tool before it can be decompressed, which can effectively protect user privacy.

Device Management

When you are an enterprise user, you need to use the Yealink Device Management Cloud Service (YMCS) to configure and manage devices (the relevant service is not enabled by default), and you need to report the following information to the server: (the specific information reported by the device to YMCS can also refer to: Yealink Management Cloud Service Security White Paper)

- Device information (MAC, device type, SN, IP)
- Device diagnostic log
- The data reported by the device includes: mainly personal information and confidential usage data, including configuration files (usernames, passwords, associated accounts), resource files, log files, screenshots, etc.
- Device software update.
- Obtain call quality statistics via RTCP_XR, following the protocol standard of RFC 3611

If users have any questions about the reported content, they can contact the enterprise administrator and Yealink technical support personnel.

Declaration:

The main purpose of the YMCS (Yealink Device Management Cloud Service) is to process information.

- Provide device management cloud services.
- Diagnose technical issues.
- Problem analysis to improve the technical performance of service.

- Respond to customer technical support requests.

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 function	Request method
https://rpscloud.yealink.com	Yealink redirection service address for automatic deployment. Devices will access this address after the factory reset, which will be closed after the successful deployment.	Active request
cn.pool.ntp.org pool.ntp.org	NTP's sever address, power-up and periodic queries.	Active request
https://dm.yealink.com	The address of the ROM package for checking and upgrading. It is turned off by default and needs to be enabled by the user.	Active detection
http://www.yealink.com	Web static address. When clicking it, users will be directed to Yealink's official website.	Passive request
http://support.yealink.com/	static Web address. When clicking it, users will be directed to Yealink technical support website.	Passive request

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

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.

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.

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 emergency response is mainly divided into four stages: problem collection, vulnerability assessment, vulnerability repair, and tracking resolution.

- Problem Collection: Collect relevant logs and information based on reported security incidents and assign dedicated personnel to track and handle them.
- Problem Analysis: Priority is given to determining vulnerability risks based on the problem. During the processing stage, temporary solutions will be provided first to avoid the problem from expanding.
- Vulnerability Fix: Analyze the root cause of the problem based on its occurrence, trace the reasons for the defects in the design and solve the vulnerability problem in a timely manner from the root cause.
- 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 (https://support.yealink.com) to learn about firmware downloads, product documentation, and frequently asked questions. For better service, we recommend that you use the Yealink ticket system (https://ticket.yealink.com) to submit technical issues.

Disclaimer

Declaration:

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. For more information about Yealink Room series devices, please visit Yealink's official website. For more security information, please visit Yealink Security Center.