Yealink

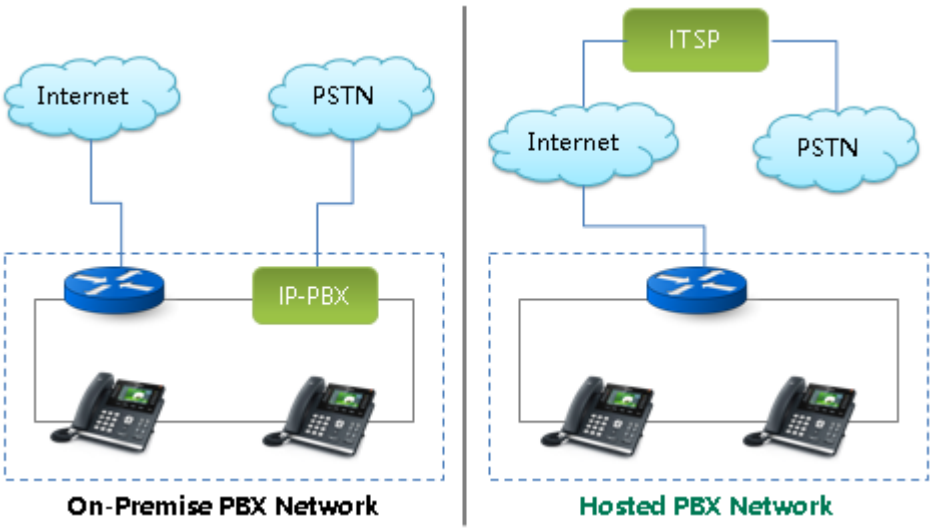
Phone Security Solution

White Paper

Dec. 2018

IP Phones in Network Topology

IP phone is also a network device, so security is very important, especially when you are using a Hosted PBX Network.

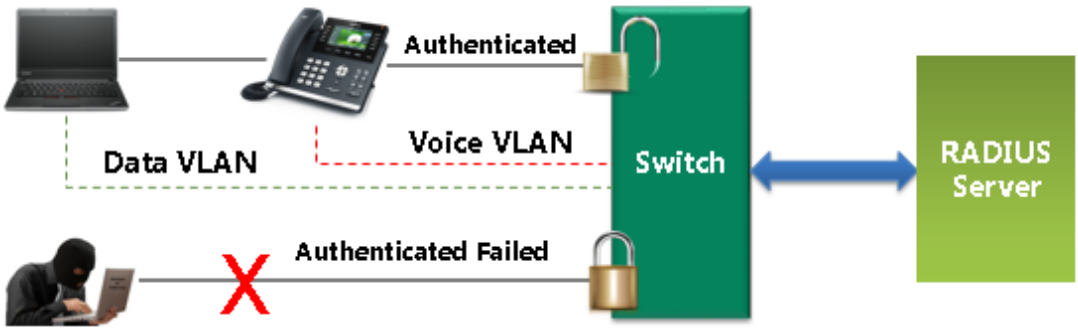


Security Challenges

Solution Overview

Network Access Security

802.1x



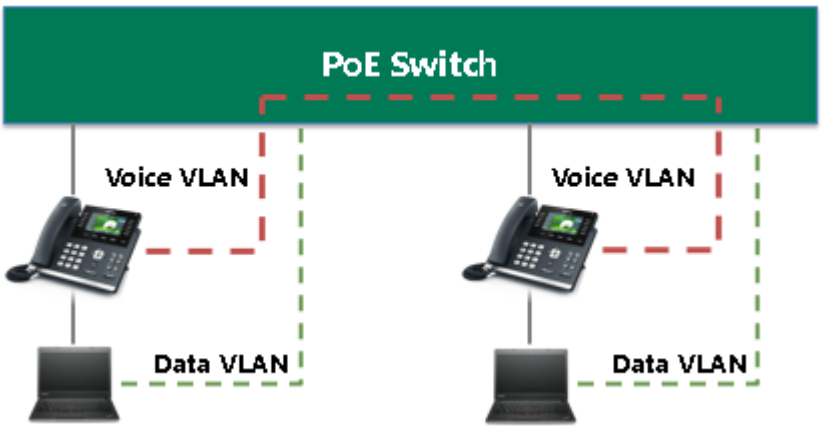
- 802.1X can permit or deny network connectivity.
- Multiple EAP methods supported, such as MD5, TLS and so on.
- Multi-Domain Authentication (MDA) mode supported.
- EAP Logoff mechanism
- Disable PC port

Yealink IP phones support the following protocols for 802.1X authentication:

- EAP-MD5
- EAP-TLS (requires Device and CA certificates, requires no password)

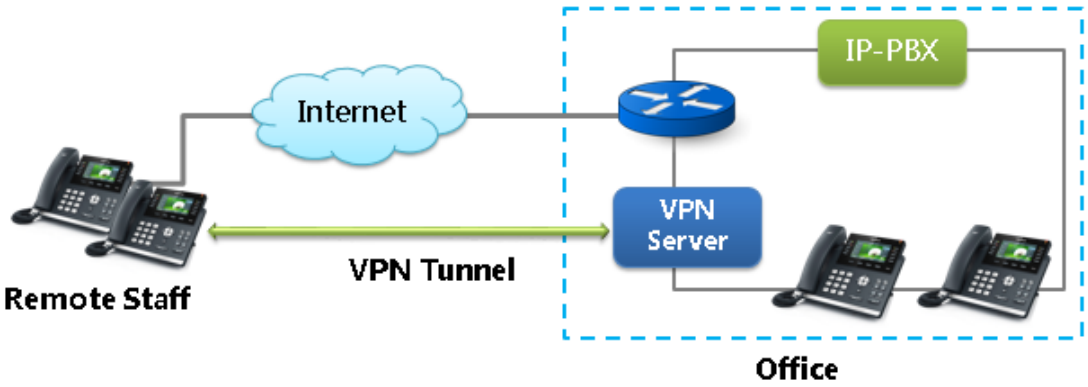
- EAP-PEAP/MSCHAPv2 (requires CA certificates)
- EAP-TTLS/EAP-MSCHAPv2 (requires CA certificates)
- EAP-PEAP/GTC (requires CA certificates)
- EAP-TTLS/EAP-GTC (requires CA certificates)
- EAP-FAST (supports EAP In-Band provisioning, requires CA certificates if the provisioning method is Authenticated Provisioning)

VLAN



- Manually assign VLAN ID or Automatically configure the VLAN ID through LLDP/LDAP or DHCP.
- Voice VLAN can guarantee the bandwidth for voice.
- Network Storm Prevention
- Configuration of IP phones Protection

OpenVPN

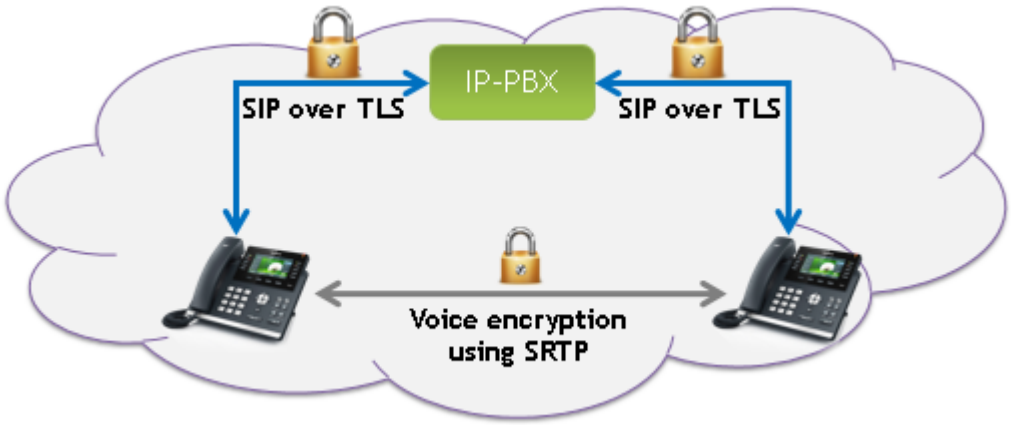


- Built-in OpenVPN client in the phone

- Remote staff can easily register their IP phones to the company IP-PBX with high security.

Session Security

TLS



- SIP over TLS
- 74 built-in trusted certificates.
- You can upload 10 custom trusted certificates at most
- Authenticate the caller and callee
- Encrypting the SIP messages
- TLS transport for Syslog
- LDAPs and LDAP TLS Start

The IP phones support TLS version 1.0, 1.1 and 1.2 and the following cipher suites:

ECDHE-RSA-AES256-GCM-SHA384

ECDHE-ECDSA-AES256-GCM-SHA384

ECDHE-RSA-AES256-SHA384

ECDHE-ECDSA-AES256-SHA384s

ECDHE-RSA-AES256-SHA

ECDHE-ECDSA-AES256-SHA

ECDHE-RSA-AES128-GCM-SHA256

ECDHE-ECDSA-AES128-GCM-SHA256

ECDHE-RSA-AES128-SHA256

ECDHE-ECDSA-AES128-SHA256

ECDHE-RSA-AES128-SHA

ECDHE-ECDSA-AES128-SHA

ECDHE-RSA-RC4-SHA

ECDHE-ECDSA-RC4-SHA

ECDHE-RSA-DES-CBC3-SHA

ECDHE-ECDSA-DES-CBC3-SHA

DHE-DSS-AES256-GCM-SHA384

DHE-RSA-AES256-GCM-SHA384

DHE-RSA-AES256-SHA256

DHE-DSS-AES256-SHA256

DHE-RSA-AES256-SHA

DHE-DSS-AES256-SHA

DHE-DSS-AES128-GCM-SHA256

DHE-RSA-AES128-GCM-SHA256

DHE-RSA-AES128-SHA256

DHE-DSS-AES128-SHA256

DHE-RSA-AES128-SHA

DHE-DSS-AES128-SHA

DHE-RSA-SEED-SHA

DHE-DSS-SEED-SHA

ECDH-RSA-AES256-GCM-SHA384

ECDH-ECDSA-AES256-GCM-SHA384

ECDH-RSA-AES256-SHA384

ECDH-ECDSA-AES256-SHA384

ECDH-RSA-AES256-SHA

ECDH-ECDSA-AES256-SHA

ECDH-RSA-AES128-GCM-SHA256

ECDH-ECDSA-AES128-GCM-SHA256

ECDH-RSA-AES128-SHA256

ECDH-ECDSA-AES128-SHA256

ECDH-RSA-AES128-SHA

ECDH-ECDSA-AES128-SHA

ECDH-RSA-RC4-SHA

ECDH-ECDSA-RC4-SHA

ECDH-RSA-DES-CBC3-SHA

ECDH-ECDSA-DES-CBC3-SHA

AES256-GCM-SHA384

AES256-SHA256

AES256-SHA

AES128-GCM-SHA256

AES128-SHA256

AES128-SHA

SEED-SHA

RC4-SHA

RC4-MD5

EDH-RSA-DES-CBC3-SHA

EDH-DSS-DES-CBC3-SHA

EDH-RSA-DES-CBC-SHA

EDH-DSS-DES-CBC-SHA256

DES-CBC3-SHA

DES-CBC-SHA

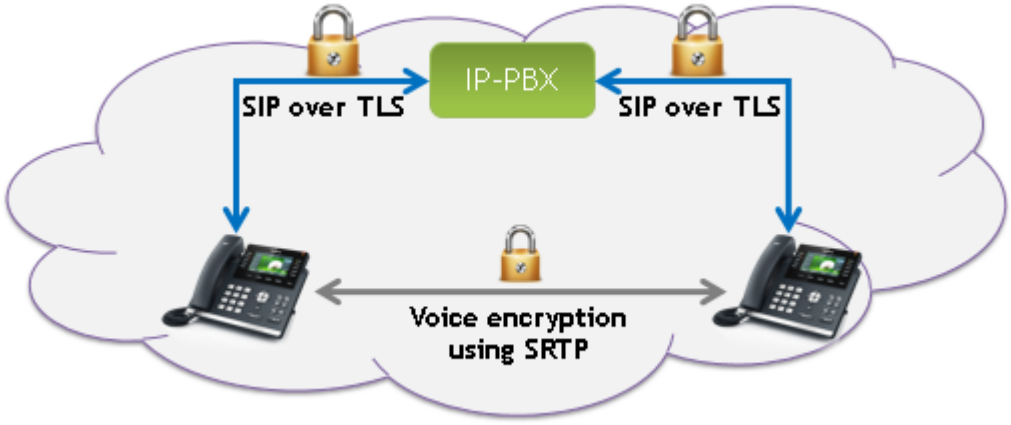
EXP-EDH-RSA-DES-CBC-SHA

EXP-EDH-DSS-DES-CBC-SHA

EXP-DES-CBC-SHA

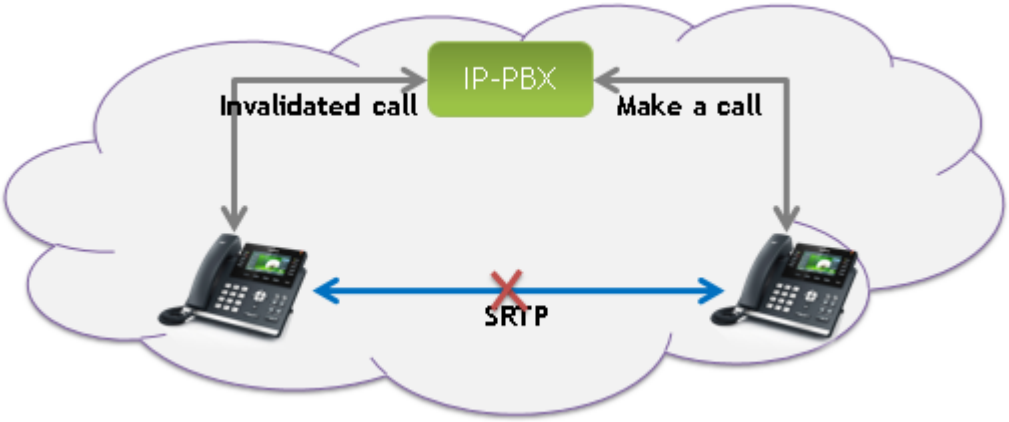
EXP-RC4-MD5

SRTP



- 128-bit AES encryption for SRTP
- Encrypting the media stream

Incoming Network Signaling Validation

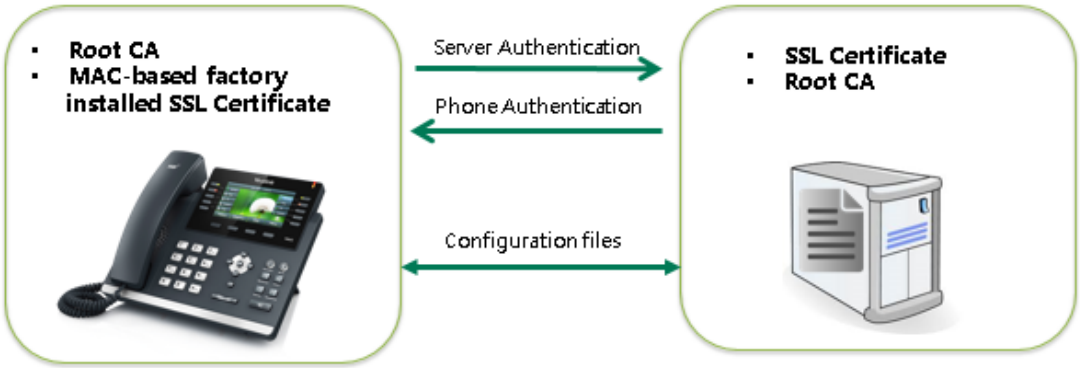


The IP phones support the following three optional levels of security for validating incoming network signaling:

- Source IP address validation: ensure the request is received from an IP address of a server belonging to the set of target SIP servers.
- Digest authentication: challenge requests with digest authentication using the local credentials for the associated registered account.
- Accept SIP trust server only: enables the IP phones to only accept the SIP message from your SIP server and outbound proxy server.

Provisioning Security

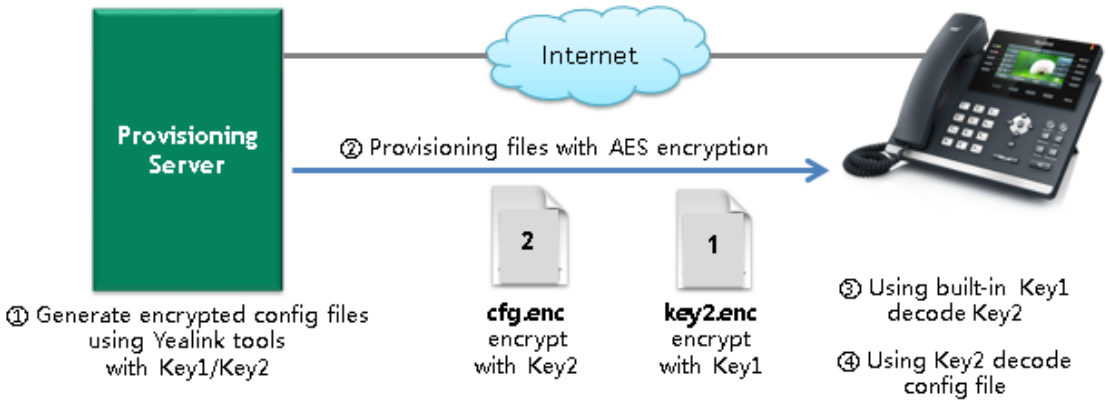
HTTPS Provisioning



- Mutual TLS authentication in provisioning process.
- Factory installed MAC-based certificate
- Factory installed Mainstream Root CA list.

- Custom Root CA and SSL certificate available

Encrypting Configuration Files



- Encrypting Configuration Files
- Encryption tool with built-in AES key
- Unique Built-in AES key in the phone
- Encrypting Contact Files

Devices Security

Security Slot

By fastening one end of a universal security cable to a desk or table and the other end to the security slot available on phones, you can prevent your phone from being removed.

USB Port Lock

The following features are not available when you disable the USB port:

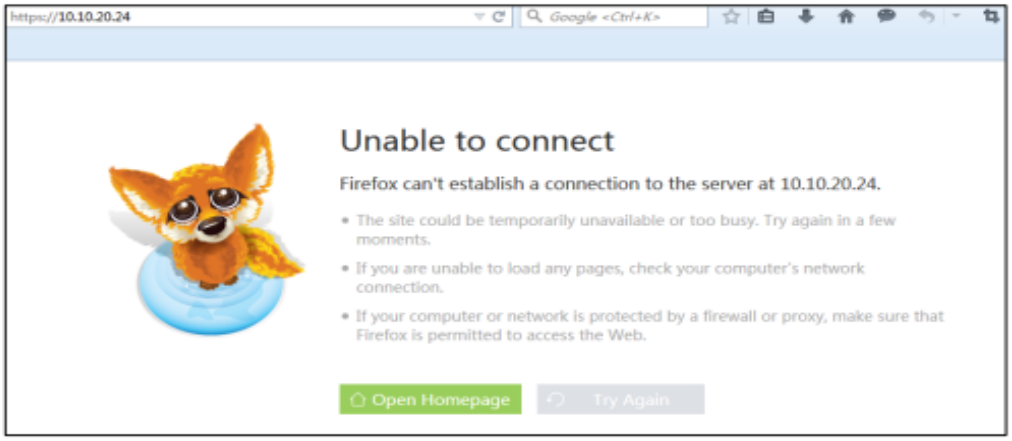
- USB Flash Drive for Wallpaper Picture
- USB Flash Drive for Screensaver Picture
- USB Wi-Fi
- USB Bluetooth
- USB Recording

Firmware

Check the firmware integrity when the firmware is used, installed and upgraded.

Application Security

HTTPS Web Server Type



- The IP phones will automatically log out if you have not performed any actions via web user interface.
- This can be disabled when it is not needed or when it poses a security threat
- Three times wrong password input will be forbidden to access in three minutes.

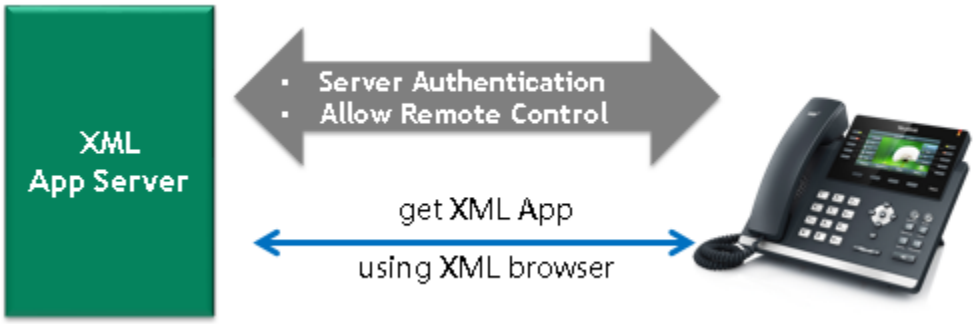
Phone Lock

- Users can lock their phones, and prevent unauthorized access to dialing/call log/contacts/menu.
- Three phone lock modes: All keys/Menu key/Function keys
- Trigger modes: Auto-lock/Manually lock
- Up to 15 digits PIN Protection
- Emergency numbers are always authorized.

CTI

- Only trusted server/PC can control the phone via Action URI/URL.
- Trusted IP list for Action URI/URL
- "Allow Remote Control" through users themselves

XML



- Only trusted server can control the phone via XML browser.
- Trusted server list for XML browser
- "Allow Remote Control" through users themselves

Access Level of Web/Phone

The Hosted PBX system administrator can restrict the user access permission using user access level feature. Yealink IP phones support access levels of admin, var and user.

Security Vulnerabilities

Wi-Fi

The IP phones support WPA-PSK, WPA2-PSK (recommended) or WPA2-EAP method. We fix vulnerabilities in WPA2 discovered before October 17, 2017.

- CVE-2017-13077: Reinstallation of the pairwise encryption key (PTK-TK) in the 4-way handshake.
- CVE-2017-13078: Reinstallation of the group key (GTK) in the 4-way handshake.
- CVE-2017-13079: Reinstallation of the integrity group key (IGTK) in the 4-way handshake.
- CVE-2017-13080: Reinstallation of the group key (GTK) in the group key handshake.
- CVE-2017-13081: Reinstallation of the integrity group key (IGTK) in the group key handshake.
- CVE-2017-13082: Accepting a retransmitted Fast BSS Transition (FT) Reassociation Request and reinstalling the pairwise encryption key (PTK-TK) while processing it.
- CVE-2017-13084: Reinstallation of the STK key in the PeerKey handshake.
- CVE-2017-13086: reinstallation of the Tunneled Direct-Link Setup (TDLS) PeerKey (TPK) key in the TDLS handshake.
- CVE-2017-13087: reinstallation of the group key (GTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame.
- CVE-2017-13088: reinstallation of the integrity group key (IGTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame.

Bluetooth

The phone provides pairing, binding, device authentication, link encryption and message integrity validation. We fix vulnerabilities discovered before September 13, 2017.

Linux

We use the Linux kernel version 4.9.75, which fix vulnerabilities discovered before January 05, 2018.