

CHRIS VAN HOLLEN  
MARYLAND

SH-110 HART SENATE OFFICE  
BUILDING WASHINGTON DC 20510  
OFFICE (202) 224-4654  
FAX (202) 228-0629

APPROPRIATIONS  
BANKING, HOUSING, AND URBAN AFFAIRS  
BUDGET  
FOREIGN RELATIONS

# United States Senate

September 28, 2021

The Hon. Gina Raimondo  
Secretary, U.S. Department of Commerce  
401 Constitution Ave NW  
Washington, DC 20230

Dear Secretary Raimondo,

The Telecommunications Industry Association recently made us aware of the attached supply chain security analysis of the Yealink T54W IP Business Phone and Device Management Platform conducted by ChainSec, Inc. which raises serious concerns about the security of audio-visual equipment produced and sold into the U.S. by Chinese firms such as Yealink.

We would appreciate if you could respond to us in writing as to whether you are aware of the security concerns raised by this report, and if the report's findings are credible, the actions you believe should be taken by the Department in response to such potential security breaches.

We thank you for your attention to this important matter.

Sincerely,



---

Chris Van Hollen  
United States Senator

Enclosure

## STATE OFFICES

ROCKVILLE OFFICE  
111 ROCKVILLE PIKE  
SUITE 960  
ROCKVILLE, MD 20850  
PHONE (301) 545-1500  
FAX (301) 545-1512

ANNAPOLIS OFFICE  
60 WEST STREET  
SUITE 107  
ANNAPOLIS, MD 21401  
PHONE (410) 263-1325

CAMBRIDGE OFFICE  
204 CEDAR STREET  
SUITE 200C  
CAMBRIDGE, MD 21613

BALTIMORE OFFICE  
1900 NORTH HOWARD STREET  
SUITE 100  
BALTIMORE, MD 21218  
PHONE (667) 212-4610  
FAX (667) 212-4618

HAGERSTOWN OFFICE  
32 WEST WASHINGTON STREET  
SUITE 203  
HAGERSTOWN, MD 21750  
PHONE (301) 797-2826

LARGO OFFICE  
1101 MERCANTILE LANE  
SUITE 210  
LARGO, MD 20774  
PHONE (301) 322-6560

# Supply Chain Security Analysis of The Yealink T54W IP Business Phone and Yealink's Device Management Platform (YDMP)



July, 2021



## Table of Contents

Chain Security Background .....	3
Executive Summary .....	5
Methodology .....	11
Analysis and Conclusions .....	13
Detailed Findings.....	19
Appendix A: Yealink SIP-T54W Parts Review.....	41
Appendix B: Yealink SIP-T54W Parts Suppliers Review .....	45
Appendix C: Yealink Agreements and Policies .....	46
Appendix D: Trusted Certificate Authorities .....	47
Appendix E: Default Configurations .....	48
Appendix G: Yealink Management Portal .....	53



## Chain Security Background

Chain Security is a Reston, Virginia based consulting engineering firm that is engaged in two related areas:

1. Securing the supply chains of commercial high technology companies.
2. Compliance of companies that are regulated by the Defense Counter - Intelligence Security Agency (DCSA) or the Committee on Foreign Investment in the United States (CFIUS).

Our consulting practice is informed by the unique combination of skills and backgrounds of our team. Chain Security's leadership includes members who have deep commercial product development and delivery experience in Silicon Valley. It also includes team members who have recent and deep experience in U.S. Government security practices and policies.

We bring extensive government security experience from organizations such as CFIUS DOD, DHS, the Federal Communications Commission (FCC) and the FBI. This includes team members with recent experience at DHS's Cybersecurity and Infrastructure Security Agency (CISA).

Most of our CFIUS and DCSA related work is focused on the development and implementation of mitigations for our clients. Chain Security personnel are also engaged in the area of CFIUS investigation of foreign technology companies.

Our CEO serves on the board of directors of Marvell Technologies' Government Solutions subsidiary. In that capacity he serves as an outside director and Chairman of the Government Security Committee of the board.

Examples of diverse project areas to which we have applied our security expertise includes:

Semiconductor design, materials, manufacturing, packaging and test  
Electronic auto parts  
Enterprise software  
Embedded Linux systems  
Commercial servers and PCs  
Mobile wireless networks and management systems



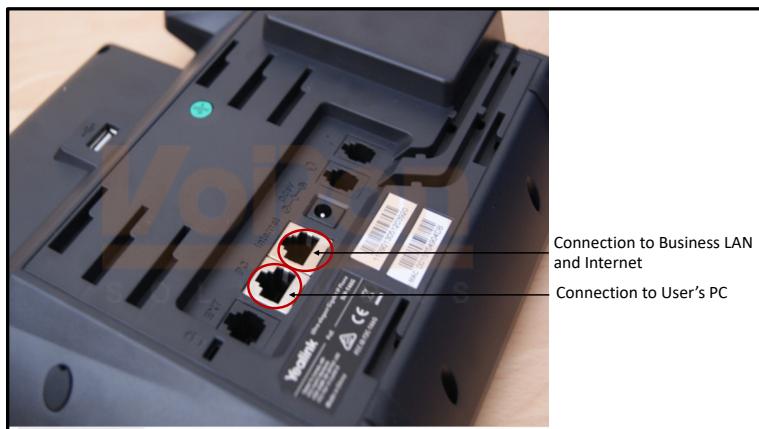
Enterprise-grade firewalls  
Security of military robotics  
Biometric identification and verification systems  
Systems for creation of official U.S. Federal Government IDs  
Fiber optic networks  
Ordnance materials engineering and manufacturing for electronic triggers in weapons systems  
Design of an electronically isolated academic research laboratory for the discovery of vulnerabilities in consumer, commercial and medical IoT systems.



## Executive Summary

Chain Security conducted an analysis of the Yealink company and its Model SIP-T54W Prime Business Phone (T54W). Chain Security believes that the T54W is representative of Yealink's overall business VoIP telephone product line.

The T54W is a business desk phone that has 2 Ethernet ports. One of the Ethernet ports provides the interface to the business local area network. The other Ethernet port connects a business laptop or PC.



When the T54W has a user's business laptop or PC connected to it, the T54W provides added functionality of acting as a network switch for the device. In this mode, all connected PC or laptop traffic flows through the network switch which is in the T54W. This is typical functionality for a business VoIP telephone.



We categorize our findings into 3 broad categories:

- a. Findings that represent common practice and which do not pose any heightened threat or vulnerability to a customer
- b. Findings that represent common industry practices of manufacturers of similar products, but which create a heightened opportunity for threat actors because of Yealink's ties to government of the PRC and the requirement that it operate under the laws of the PRC
- c. Findings that represent practices that are not common industry practices of manufacturers of similar products, and generally create heightened device or network vulnerabilities

This categorization of individual findings is contained within the [Detailed Findings](#) section of this report.

This report addresses the following topics:

- An analysis of the interaction between Yealink's Device Management Platform<sup>1</sup> (YDMP) and the T54W
- Security of operations of the T54W on a U.S. public business VoIP service
- Security testing of the software/firmware on the T54W
- A summary analysis of the major semiconductors contained within the T54W
- A threat assessment of Yealink based on its sources of public financial support in the PRC, personnel in technical leadership positions and historical associations with foreign technical talent recruitment programs in China such as the Thousand Talents Program

Four units of the T54W were tested. Chain Security conducted tests of the T54W on a public VoIP network in the United States. The T54W was also connected to Yealink's Device Management Platform, and the behaviors of the YDMP were observed.

---

<sup>1</sup> <https://ymcs.yealink.com/>

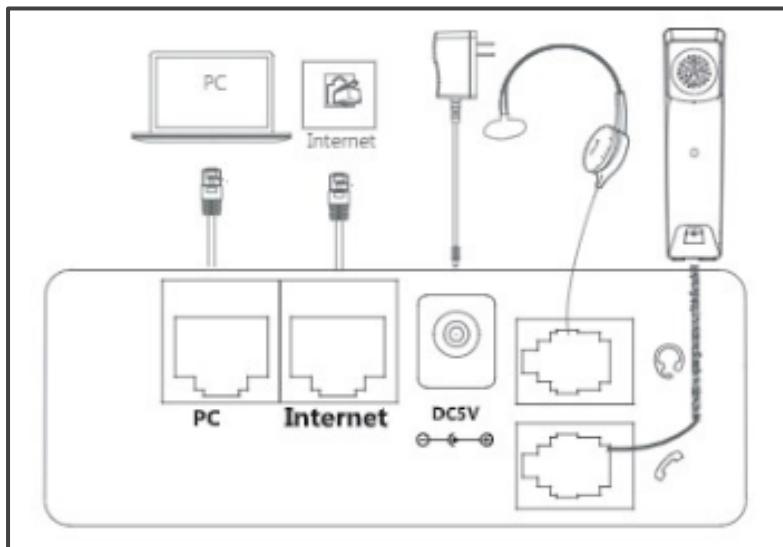


Lab bench security testing of the T54W software/firmware was conducted. A hardware teardown of one phone was performed in order to create a list of major parts and to understand the origin of the parts, and if any of the parts had underlying vulnerabilities.

This report and its appendices contain details of the analysis performed and the full set of conclusions with the reasons for those conclusions.

Below is a summary of the major findings:

1. *The Yealink Device Management Platform (YDMP) is a source of significant vulnerability and threat to any VoIP systems operator or company that relies upon it:*
  - a. Users' information and behavior can be surveilled from the YDMP – including communications of a PC that is attached to the T54W where the phone is also acting as an Ethernet switch.



- b. The T54W delivers users' call detail records to the YDMP when it is registered with that platform.
  - c. A Yealink administrative user in China can initiate a call recording from the portal, store the recording in the T54W and then upload it to the YDMP.
  - d. The YDMP Service Agreement requires users to accept the laws of the PRC and arbitration of disputes in Xiamen province and a related



set of service terms allows the active monitoring of users when required by the “national interest” (this means the national interest of China).

2. *The T54W exhibits poor security behavior when installed in its default configuration on a standard VoIP network:*

- a. Every time the phone reboots or once per day, a data exchange occurs where the T54W sends an encrypted message to a remote server (that is hosted Alibaba’s AliCloud service) and receives an encrypted message in response. This exchange is repeated twice more (for a total of 3 exchanges), each time showing the same byte counts for sent and received messages.

This is done without informing the owner of the phone and the phone persists in attempts to continue this behavior even after it has been administratively prohibited.

- b. The T54W is highly susceptible to unauthorized remote access, from which a device or general network attack can be initiated. The T54W comes preconfigured to accept digital certificates from 187 certificate authorities for remote access. One of the certificate authorities is in China and has been blocked by Google for irresponsibly facilitating Man-In-The-Middle- (MITM) attacks on web traffic.

3. *The Yealink IP phone, as designed and as the firmware is implemented, provides the ability for a malicious 3rd party, with access to the phone’s network, to conduct a Man-In-The-Middle (MITM) attack on the customer phone/network with plausible deniability on the part of Yealink.*

- a. An unauthorized and malicious third party could deliver a software/firmware load containing an attack to the phone relatively easily. This results from the fact that the T54W does not require digital signatures for new software to be loaded.



- b. Chain Security was successful in conducting a denial of service (DoS) attack on the T54W. Therefore, the T54W is susceptible to successful DoS attacks.
- 4. Major components in the T54W are of Chinese or Taiwanese origin. The main microprocessor seems to be an Application Specific Integrated Circuit (ASIC) from Rockchip, a Chinese national champion. The Rockchip processor is likely based on a commercial Arm design. Lack of public information about the Rockchip ASIC suggests that there are likely vulnerabilities present that are undocumented, and are therefore not in public databases such as NIST's NVD. The table below summarizes the major components and their origins<sup>2</sup>.

Function	Manufacturer	Model Number	Nationality	Location of Fabrication
Main Processor	Rockchip	YL2018G	PRC	Unknown
Network Interface	Dongguan Mentech	G4811CG	PRC	Unknown
Network Switch	Qualcomm	QCA8334-AL3C	USA	Taiwan
Flash Memory	Winbond	25N01GVZEIG	Taiwan	Taiwan
Display MCU	Holtek	HT66F004	Taiwan	Taiwan

- 5. Yealink has both historic and current deep ties to the Chinese State:
  - a. Xiamen City and Party Committee (市委市政府) gave direct financing (直接金融渠道) to Yealink.
  - b. Yang Gui, a current engineering executive at Yealink is an *Expert Committee Member of the China Ministry of Science and Technology (MOST)*.
  - c. Due to GUI's role in MOST, Yealink should be considered a high-risk company for the illicit transfer of knowhow and technology from

---

<sup>2</sup> For the PRC components we assume, but could not verify, that fabrication, testing and packaging are done in China. For the Taiwan components, there are strong indications, but no verification, that testing and packaging are done in Taiwan or the PRC as well.



countries outside China, the recruitment of foreign experts and the inducement of foreign experts to violate non-disclosure agreements<sup>3</sup>.

- d. Yealink was a management company of record in China's Thousand Talents Program (TTP).

---

<sup>3</sup> Threats to the U.S. Research Enterprise: China's Talent Recruitment Plans, STAFF REPORT - PERMANENT SUBCOMMITTEE ON INVESTIGATIONS, November 18, 2019



## Methodology

The dimensions of analysis that were used include:

- a. Behavior and interaction of the Yealink Device Management Platform with the Yealink device
- b. Security of the device during normal operations on a commercial U.S. VoIP network
- c. Security of Yealink's software/firmware in the device<sup>4</sup>
- d. Underlying hardware technology
- e. Government support

Chain Security obtained 5 T54W devices from a U.S. commercial distributor of Yealink business IP phones

The phones were then assigned to the following tasks:

- 2 phones were connected to a live commercial VoIP service platform and its behavior observed over a period of 2 weeks. Representative data was collected.
- 1 of the phones that was connected to the commercial VoIP service platform was also managed by the YDMP.
- The phone that was managed by the YDMP was observed with a typical user PC attached to the phone using the Phone's built in Ethernet switch, and the phone was also observed while no PC was attached to it.
- 1 phone was used to investigate its vulnerabilities by an examination of its software.
- 1 phone was torn down in order to photograph, identify and catalog its intelligent components<sup>4</sup>.

---

<sup>4</sup> Chain Security defines an intelligent component as “ (a) any hardware processor, or software or firmware executable on any microprocessor, (b) the microprocessor itself, (c) any semiconductor device that has processing ability (d) any device that has internal memory, (e) any component or device that performs a communication function, and (f) any hardware, firmware or software (including operating



- 1 phone was retained as a spare.

In addition, using open-source information, Chain Security has assembled information about Yealink, its links to the government of the People's Republic of China (PRC) and the Thousand Talents Program.

---

systems) integrated into or installed on an any component in (a)-(e). For example, a low-cost ARM processor in a printer or an Ethernet controller is an intelligent component, as is the firmware that executes on such a processor.”.



## Analysis and Conclusions

The conclusions are derived from the information provided in the tables in the Detailed Findings section of this report.

### An analysis of the behavior if Yealink's Device Management Platform (YDMP)<sup>5</sup>

The YDMP is a source of significant vulnerability and threat to any VoIP systems operator or company that relies upon it due to the following behaviors and characteristics of the platform:

1. The YDMP service agreement requires users to accept the laws of the PRC and arbitration of disputes in Xiamen province. In addition, the agreement's privacy policy does not include any references to international data protections such as GDPR.
2. The YDMP collects and retains the WAN IP of the U.S. device and its private network IP creating useful attack data that is stored on a server controlled by persons within the jurisdiction of the PRC.
3. A Yealink employee in China, acting as a YDMP administrative user, can initiate a packet capture for traffic on the Ethernet and WAN switches in the phone. This means corporate users' information and behavior can be surveilled.
4. The T54W delivers users call detail records to the YDMP when it is registered with that platform.
5. A Yealink employee in China, acting as a YDMP administrative user, can initiate a call recording from the portal, store the recording in the T54W and then upload it to the YDMP.

---

<sup>5</sup> Administrative login page: <https://ymcs.yealink.com/>



## Security of operations of the T54W (default configuration) on a U.S. public business VoIP service

1. During normal operations the Yealink phone communicates with a server located in Chinese controlled AliCloud infrastructure, without the permission of the owner/user or notice that it performs this activity of the phone.
2. Yealink's IP phone has the potential to be used to conduct network surveillance of the customer's IP network because the phone's default configuration does not require voice and data transmission on separate VLANs, unless the customer has already set up its router to manage separate VLANs for its IP phones. However, separate VLANs can be custom configured by the VoIP service provider as part of their installation processes—in a variety of ways.
3. Default login credentials make the Yealink phone susceptible to attack. The Yealink phone uses common login credentials, known by most security/pen testing assessment tools: admin/admin. The phone does not force the administrator to create a new login or password when the phone is initially configured, though it does show a fairly low-key reminder to do so, as can be seen in various configuration screenshots in **Appendix E**.
4. The Yealink phone is made vulnerable because it comes pre-configured to accept credentials for connection and access to the device from 187 “trusted” digital certificate authorities (CAs). The specific vulnerability is that use of any of these certificates provides trusted access to the administrative interface of the T54W.  
It requires knowledgeable action on the part of the user company's administrator to edit the list of trusted certificate providers to remove any that are undesirable.
5. The Yealink phone provides no option of protecting the administrator login with multifactor authentication nor any protection from brute force credential stuffing attacks by locking the account after a number of unsuccessful attempts.



## Security testing of the software/firmware on the T54W

1. The Yealink IP phone, as designed and as the firmware is implemented, provides the ability for a malicious 3<sup>rd</sup> party, with access to the phone's network, to conduct a MITM attack on the customer phone/network with plausible deniability on the part of Yealink.

This is due to the fact that the phone does not validate digital signatures prior to installing a new version of software, which is not consistent with industry standard practice, nor is the firmware encrypted using reasonably strong cryptography ( e.g. AES) to protect any device from a false load of firmware (fake firmware). Yealink does not implement common industry practices to protect their device from attackers. This provides both opportunity to a knowledgeable threat actor, and plausible deniability to Yealink.

Therefore, any attacker familiar with the T54W's software structure and update protocol could send and install arbitrary software on any phone to which it obtains a network address.

2. The T54W does not require new firmware loads to contain a digital signature. Without digital signature and version check security measures in place, the firmware image on the device can be overwritten, using any means available including remotely, with a custom image, as long as the structure of the file matches what the on-board firmware loading Executable and Linkable Format (ELF) is expecting in the validation phase.
3. A threat actor unconstrained by copyright restrictions and with knowledge of the Yealink firmware (obtained by decryption, decompilation, reverse engineering techniques or PRC state authorities) that contains the specific Linux kernel in the Yealink phone could use that knowledge to tailor an attack against the phone by exploiting the fact that the Yealink phone does not validate digital signatures prior to installing new software.

The latest version of Yealink phone firmware uses the Linux 4.9.75 Kernel. This is a relatively old Linux kernel which was superseded by



release 4.14 in the last quarter of 2017. The current release is 5.13<sup>6</sup> (recently released) but the long-term support version is 5.10. Releases from 4.14 to 5.10 contain many security upgrades<sup>7</sup>. We compare this to U.S. based Texas Instruments (TI). TI is current in its OMAP system on a chip (SoC) processors to Linux 5.10<sup>8</sup>

4. The firmware in the phone systems is exploitable, with persistent access to run both user-space and kernel level code. The only protections observed is custom encryption schemes applied to the block filesystem headers.

A threat actor can create a custom designed firmware package that contains an attack. The threat actor can then exploit the processor on the T54W to either export the attack to other T54W's on the customer's network, export the attack across the Internet or implement the attack from the T54W itself.

5. The T54W is susceptible to a denial-of-service attack which was successfully executed against the operating device in the lab by attacking its web based administrative interface.

<sup>6</sup> Linux kernel release history: [https://en.wikipedia.org/wiki/Linux\\_kernel\\_version\\_history](https://en.wikipedia.org/wiki/Linux_kernel_version_history). Both 4.9 and 4.14 are old versions but designated as long-term support.

<sup>7</sup> List from NIST of the 1353 Linux kernel 4.14.x vulnerabilities, of which we believe 13 or 14 may apply to IP phones. A well-funded state actor could find those vulnerabilities and use them to craft attacks.

<sup>8</sup> <https://git.ti.com/cgit/rpmmsg/remoteproc/>



## Analysis of the supply chain for the hardware contained within the T54W

1. The main processor in the phone Rockchip (model number YL2018G) appears to be a custom Application Specific Integrated Circuit (ASIC) developed by Rockchip for Yealink. Rockchip is a national champion of the PRC for China based design of semiconductors. Vulnerabilities for ASICs do not get regularly reported in public vulnerability databases such as NIST's NVD data base<sup>9</sup>.
2. Open-source information indicates that other Rockchip products have had vulnerabilities identified, both introduced by Rockchip at an individual product level as well inherent in the ARM IP licensed by Rockchip. In the case of vulnerabilities from Arm IP, these vulnerabilities are common across many Arm licensees.

## Threat assessment of the Yealink Company

This is based on Yealink's sources of Government financial support in the PRC, personnel in technical leadership positions and historical associations with foreign technical talent recruitment programs in China such as the Thousand Talents Program.

1. Yealink has obtained financial assistance from industrial programs that are sponsored by the government of the PRC.
2. Yealink has obtained PRC government assistance in recruiting technical talent from Silicon Valley.

At least 1 current Senior technical staff member at Yealink has strong historic ties to PRC Government programs.

These programs are both responsible for recruiting foreign technical talent to relocate to the PRC. The U.S. Government has assessed one of the programs to, *"include provisions that violate U.S. standards for research integrity, place Thousand Talents Program members in"*

---

<sup>9</sup> <https://nvd.nist.gov/>



*compromising legal and ethical positions, and undermine fundamental U.S. scientific norms of transparency, reciprocity, and integrity”<sup>10</sup>.*

This Yealink engineering executive is an Expert Committee Member of the China Ministry of Science and Technology.

---

<sup>10</sup> *Threats to the U.S. Research Enterprise: China’s Talent Recruitment Plans, STAFF REPORT - PERMANENT SUBCOMMITTEE ON INVESTIGATIONS*, November 18, 2019.



## Detailed Findings

The following tables includes Chain Security's findings based on our investigation.

The tables are organized first by overall threat category as follows:

First by Threat category meaning (in order):

- Findings that represent common practice which don't pose any heightened threat or vulnerability to a customer
- Findings that represent common practices but which create a heightened threat or vulnerability because of Yealink's ties to government of the PRC and the requirement that it operate under the laws of the PRC
- Findings that represent practices that are not industry standard

Then, within each of those tables, the findings are organized by these categories (in order):

- Device Management Platform
- T54W Behavior Under Default Settings
- T54W Software/Firmware Evaluation
- T54W Hardware Evaluation
- Company Evaluation



<b>Category 1 – Findings that Represent Common Practices Which Don’t Pose any Heightened Threat or Vulnerability to a Customer</b>			
	<b>Observation</b>	<b>Discussion</b>	<b>Conclusion</b>
<b>Device Management Platform</b>			
1.	None		
<b>T54W Behavior Under Default Settings</b>			
2.	The VLAN configuration (see screenshot in <b>Appendix E</b> ) is disabled by default.	It appears that the enabled option will try to pull the proper VLAN ID from the DHCP server automatically if VLANs are being used and are setup in a DHCP server.	This is a reasonable default configuration.
3.	<p>Packet capture observations:</p> <p>Common protocols appeared normal in packet length and protocol conversation/flow. No anomalies were apparent.</p> <p>IP address allocation was standard via DHCP, nothing outside of expected behavior.</p> <p>LLDP and CDP were enabled by default.</p>	<p>LLDP and CDP being enabled is often seen in VoIP devices to enable routing and discovery by other networking devices/vendors.</p> <p>However, these protocols have inherent weaknesses and vulnerabilities. Traffic associated with these protocols should have enhanced logging and auditing in place and the administrator should at least be prompted to do so.</p>	Except for the logging refinement, this behavior conforms to industry standard practice.
<b>T54W Software/Firmware Evaluation</b>			
4.	None		
<b>T54W Hardware Evaluation</b>			



**Category 1 – Findings that Represent Common Practices Which Don’t Pose any Heightened Threat or Vulnerability to a Customer**

	<b>Observation</b>	<b>Discussion</b>	<b>Conclusion</b>
5.	<p>Chain Security also undertook a selective survey of the intelligent components suppliers to Yealink. Please refer to <b>Appendix B</b> for selected highlights.</p> <p>All of the suppliers are public companies. The Taiwanese companies all follow a standardized template for disclosure, which includes information about presence in, dependencies on and influences by China.</p> <p>Both Taiwanese companies disclosed these, to some extent, in their annual report.</p> <p>Qualcomm’s situation vis-à-vis China is complicated and beyond the scope of this SOW to fully observe and discuss. In lieu of being able to identify where the Ethernet switch was made, we take it at face value that it was somewhere in Taiwan due to the markings.</p>	<p>Both Winbond and Holtek are clearly highly dependent on China for their financial health, based on their disclosures about sale to “Asia”, which likely means “China”. It’s 93% for Winbond and 79% for Holtek.</p> <p>In addition, there appears to be high dependence on a small number of customers. For example, for Holtek, 4 customers account for 75% of sales.</p> <p>Both companies indicate no dependencies on China for raw materials and also indicate that their China presence are for sales and tech support. However, Winbond appears to have at least a process integration and testing facility in China.</p> <p>Packaging and test locations were not available.</p>	<p>Direct linkages between the Taiwanese companies and China are concentrated in sales and support organizations.</p> <p>There are indications of indirect linkages that may go beyond sales and support into production and testing activities.</p> <p>Both Taiwanese companies are highly dependent on sales in China.</p> <p>We assess the Taiwanese companies to be “moderate risk” to US customers, particularly USG and critical infrastructure customers.</p>
<b>Company Evaluation</b>			
6.	None		



**Category 2 – Findings that Represent Common Practices but Which Create a Heightened Threat or Vulnerability to a Customer Because of Yealink's Ties to the PRC and its Operating Under the Laws of the PRC**

	<b>Observation</b>	<b>Discussion</b>	<b>Conclusion</b>
<b>Device Management Platform</b>			
1.	<p>We successfully registered a phone to the Yealink management portal. We are still digesting the full extent of the management portal's capabilities. But we observed the following behavior (screenshots in Appendix G):</p> <ol style="list-style-type: none"> <li>1. The phone can be remotely provisioned. SIP Usernames and passwords must be entered.</li> <li>2. We were able to update the configuration and reboot the phone without user knowledge, as well as push new firmware to the phone.</li> <li>3. The management portal collects a lot of information about the phone. The portal knew the WAN IP and it also displayed its private network IP.</li> <li>4. We could initiate a packet capture on the management portal for traffic on the Ethernet and WAN switches in the phone.</li> <li>5. Call details and quality are pushed up to the management portal.</li> <li>6. Call recording appears to be initiated on the portal and then uploaded from the phone.</li> <li>7. Logs can be downloaded from the phone.</li> <li>8. Overall, there is a lot of communication between the phone and the management portal.</li> </ol> <p>Yealink provides a robust set of documentation and tutorials.</p>	<p>We do not know how information is stored on the Yealink backend and even if encrypted we suspect that it can be easily decrypted by Yealink.</p> <p>It appears that a lot of call detail record information (metadata) is collected and stored in the Yealink management portal backend, including call recordings.</p> <p>The logs provide details on the network traffic as well as other call detail metadata.</p> <p>We don't believe the actual media is being captured in the testing we performed as that is typically a point-to-point transmission. But with the phone susceptible to MITM attacks, software could be inserted to fork the media at the phone.</p>	<p>The overall management portal application is similar to that found in US-based cellular IoT management portals (e.g., Jasper Technologies, purchased by Cisco, which provides management portal applications to Tier 1 MNOs worldwide).</p> <p>However, the difference is the level of trust. While we cannot know for sure, we conclude that it is highly likely that Yealink is sharing information about its customers with the government of the PRC (indeed, under Chinese law, it would have an obligation to do so).</p> <p>At a minimum, this possibility ought to be of serious concern to any governmental agency (federal, state or local) as well as any company in one of the 16 critical infrastructure sectors considering a phone purchase.</p>



**Category 2 – Findings that Represent Common Practices but Which Create a Heightened Threat or Vulnerability to a Customer Because of Yealink's Ties to the PRC and its Operating Under the Laws of the PRC**

	<b>Observation</b>	<b>Discussion</b>	<b>Conclusion</b>
T54W Behavior Under Default Settings			
2.	<p>According to the document in <b>Appendix D</b> regarding certificates, it appears that the phone will engage in mutual TLS with servers presenting a certificate from any of 187 “trusted” certificate authorities (as of this version of software: 96.84.0.30).</p> <p>.</p>	<p>One of the “trusted” certificate authorities is a state-controlled entities for the PRC (two entries on list but the same entity):</p> <p>111. China Internet Network Information Center EV Certificates Root</p> <p>112. CNNIC ROOT</p> <p>This was on page 3 of a Google search:  <a href="https://techcrunch.com/2015/04/01/google-cnnic/">https://techcrunch.com/2015/04/01/google-cnnic/</a> indicating that Google banned it after a security breach.</p>	<p>All US customers, particularly USG and critical infrastructure customers, should erase all certificates and install one generated from a trusted source.</p> <p>In addition, all US customers should not use Yealink’s device platform.</p> <p>May be others after testing.</p>



**Category 2 – Findings that Represent Common Practices but Which Create a Heightened Threat or Vulnerability to a Customer Because of Yealink's Ties to the PRC and its Operating Under the Laws of the PRC**

	<b>Observation</b>	<b>Discussion</b>	<b>Conclusion</b>
3.	<p>When the phone was acting as an Ethernet switch for an attached device, we did not observe any pattern of traffic rerouting, either voice or data.</p> <p>In addition, we did not observe the phone attempting to search the network to which it was attached. For example, it appeared to stop its once a day “phone home” session and transmit any information to rps.yealink.com in a 24-hour period, unlike when it was in a stand-alone configuration.</p> <p>We observed the PC establishing mutual TLS sessions with a variety of Microsoft destination addresses.</p>	<p>We were concerned that the phone may be intercepting and/or re-routing traffic. That was not observed during our tests.</p> <p>The fact that we did not observe this behavior does not mean it doesn't exist. For example, it is possible that we just don't know the command to activate this behavior. Many management platforms have capabilities not exposed to their customers.</p> <p>In addition, we are concerned that the phone's behavior appeared to change with respect to the “phone home” feature once it was used as a network switch.</p> <p>Additional detailed investigation is required to determine the behavior of the “phone home” feature in the phone and operating configurations available.</p>	<p>The phone appears to function as a normal Ethernet switch with the current software load.</p> <p>We do not know why the “phone home” behavior changed. This could be an area for further study with an extended and structured test plan.</p>



**Category 2 – Findings that Represent Common Practices but Which Create a Heightened Threat or Vulnerability to a Customer Because of Yealink’s Ties to the PRC and its Operating Under the Laws of the PRC**

	<b>Observation</b>	<b>Discussion</b>	<b>Conclusion</b>																		
4.	<p>Port/Protocol Discovery (port scan) showed the following:</p> <table><tr><td>PORT</td><td>STATE</td><td>SERVICE</td></tr><tr><td>53/tcp</td><td><b>open</b></td><td>domain</td></tr><tr><td>80/tcp</td><td><b>open</b></td><td>http</td></tr><tr><td>443/tcp</td><td>open</td><td>https</td></tr><tr><td>5060/tcp</td><td><b>open</b></td><td>sip</td></tr><tr><td>5061/tcp</td><td>open</td><td>sip-tls</td></tr></table> <p>MAC Address: 80:5E:C0:84:C0:80 (Yealink(xiamen) Network Technology)</p>	PORT	STATE	SERVICE	53/tcp	<b>open</b>	domain	80/tcp	<b>open</b>	http	443/tcp	open	https	5060/tcp	<b>open</b>	sip	5061/tcp	open	sip-tls	<p>We recommend that manufacturers, by default, close ports 53, 80 and 5060 to ensure only secure communications are occurring.</p> <p>If the customer wishes to open them up then that is a custom configuration for them.</p>	<p>These default settings conform to industry standard practice—but we don't recommend it and it does not represent current best practices.</p>
PORT	STATE	SERVICE																			
53/tcp	<b>open</b>	domain																			
80/tcp	<b>open</b>	http																			
443/tcp	open	https																			
5060/tcp	<b>open</b>	sip																			
5061/tcp	open	sip-tls																			

## T54W Software/Firmware Evaluation



**Category 2 – Findings that Represent Common Practices but Which Create a Heightened Threat or Vulnerability to a Customer Because of Yealink's Ties to the PRC and its Operating Under the Laws of the PRC**

	<b>Observation</b>	<b>Discussion</b>	<b>Conclusion</b>
6.	<p>We observed at least one identified built-in vulnerability that can be triggered on the phone.</p> <p>During Dynamic Analysis (Penetration Testing), a basic vulnerability/exploit scanner was run against the listening ports.</p>	<p>The web server hosting the administration panel was exploited with a Denial-of-Service bug and crashed the service.</p>	<p>With high confidence, we believe that this represents an attack surface that can be exploited by a threat actor.</p>
7.	<p>In addition to the Linux kernel, we observed two other open-source modules by extracting strings from the root volume:</p> <p>LightHTTPD HostAPD</p>	<p>However, the inability to fully mount the root filesystem precludes the ability to obtain a full listing of all open-source modules used to build the Linux system.</p> <p>The two obtained suggest that there will be many open-source modules, as would be expected.</p>	<p>We cannot conclude with any certainty that the open-source modules in the phone are limited to what one would normally find in this kind of device.</p>
8.	<p>There were no indicators found showing that the phone is using anything other than the standard Linux kernel network stack.</p> <p>This is augmented by the 24-hour test (above) which captured all traffic from the phone and connected PC.</p>	<p>However, with the network options setup in the kernel, there is also no evidence showing that standard network traffic routing options within standard Linux builds are not available to a threat actor.</p>	<p>The phone is vulnerable with respect to re-routing of its traffic.</p>

T54W Hardware Evaluation



**Category 2 – Findings that Represent Common Practices but Which Create a Heightened Threat or Vulnerability to a Customer Because of Yealink's Ties to the PRC and its Operating Under the Laws of the PRC**

	<b>Observation</b>	<b>Discussion</b>	<b>Conclusion</b>
9.	<p>Please refer to <b>Appendix A</b> for selected details about the parts classified as "intelligent components".</p> <p>The main processor and NIC are sourced from Chinese suppliers (Rockchip YL2018G and Dongguan Mentrech G4811CG, respectively).</p> <p>Flash memory and the display MCU are sourced from Taiwanese suppliers (Winbond 25N01GVZEIG and Holtek HT66F004, respectively).</p> <p>The Ethernet switch is sourced from a US company (Qualcomm QCA8334-AL3C), which appears from the markings on the packaging to be manufactured in Taiwan.</p>	<p>There are only a few intelligent components in this phone, which was expected.</p> <p>Sourcing components from Chinese companies is not surprising as Yealink is a Chinese company.</p> <p>We would have expected all intelligent components to be sourced from Chinese companies.</p> <p>We note that the processor and NIC are also the most critical components with respect to vulnerabilities and attack surfaces, especially if the software enables those vulnerabilities.</p>	<p>In lieu of supply chain transparency, which is difficult to obtain in China, we assess the China-based parts and suppliers as "<b>high risk</b>" to US customers, particularly USG and critical infrastructure customers.</p> <p>We assess the Taiwan-based parts and suppliers as "<b>moderate risk</b>" given the dependencies those suppliers have on China overall.</p>
<b>Company Evaluation</b>			
10.	None		



### Category 3 – Findings that Represent Practices That are not Industry Standard

	Observation	Discussion	Conclusion
Device Management Platform			
1.	<p>The Yealink Device Management Cloud Service Agreement is embedded as a PDF in <b>Appendix C</b> and is also available at this link:</p> <p><a href="https://www.yealink.com/news_171.html">https://www.yealink.com/news_171.html</a></p> <p>Specific items of concern include:</p> <ul style="list-style-type: none"> <li>II.A: No real privacy and protection of PII (e.g., no references to GDPR)</li> <li>III.B.1: No reciprocal indemnification (one-sided)</li> <li>IV.B.2. 3. 6: No real privacy and protection of registration information</li> <li>IV.C: They can monitor use of the service</li> <li>IV.D: Public disclosure of use of service</li> <li>VIII.A: PRC governing law</li> <li>VIII.B: Mediation in Xiamen</li> </ul>	<p>While much of the agreement will appear to a US customer as standard boilerplate language, it is problematic in several areas, starting with the governing law being the PRC.</p> <p>Using PRC governing law, the language in the other clauses do not have the same meaning as would be the case with a different choice of governing law.</p> <p>The choice of PRC law is particularly of concern because the Agreement expressly states that Yealink is free to “actively monitor” users “if the national or public interest requires or [for] other legal requirements.”(part II.A.) Presumably this would happen at the direction of the government of the PRC.</p>	<p>Yealink’s Device Management Cloud Service Agreement does not conform to industry standard practice.</p> <p>All customers, not just the ones in focus for this SOW, should be concerned about this agreement, particularly the use of PRC governing law.</p> <p>The government of the PRC has different views, as compared to the government of the US, on what constitutes violations of the law sufficient to warrant Yealink turning over all information to the government of the PRC.</p>



### Category 3 – Findings that Represent Practices That are not Industry Standard

	<b>Observation</b>	<b>Discussion</b>	<b>Conclusion</b>
2.	<p>The Yealink Privacy Policy is embedded as a PDF in <b>Appendix C</b> and is also available at this link:</p> <p><a href="https://www.yealink.com/news_167.html">https://www.yealink.com/news_167.html</a></p> <p>Specific items of concern include:</p> <ul style="list-style-type: none"> <li>Section 2: Personal data collected</li> <li>Section 3: Use of personal data</li> <li>Section 5: Protection of personal data</li> <li>Section 6: Sharing of personal data</li> <li>Section 7: Even if you try to control your personal data, you may not be able to</li> </ul>	<p>This isn't really a privacy policy at all. It is a policy stating that Yealink has the right to share PII with anyone they want, including the government of the PRC. They also state explicitly that PII can be transferred and stored in other countries.</p> <p>The only prohibition they claim regarding data not collected is as follows:</p> <p>“We will never collect any personal data revealing your racial or ethnic origin, political opinions, religious or philosophical beliefs, and any other sensitive data defined by applicable data protection legislation.”</p>	<p>Yealink's Privacy Policy does not conform to industry standard practice.</p>



### Category 3 – Findings that Represent Practices That are not Industry Standard

	<b>Observation</b>	<b>Discussion</b>	<b>Conclusion</b>
3.	<p>The Yealink End User License Agreement (EULA) is embedded as a PDF in <b>Appendix C</b> and is also available at this link:</p> <p><a href="https://support.yealink.com/forward2Download?path=ZljHOJbWuW/DFrGTLnGypp7gZ5VyznPfxplusSymbolsMX7M46679MQjypHZfLckX4flbMntGAH8vIEq2FdfHOW0mSr7QHmJqkM7Vjw1XwfqjXh/JqQyrJlf2plusSymbolJSX7vnazJy/W844NWafUurDU5plusSymbolBEceVgQjCPQ==">https://support.yealink.com/forward2Download?path=ZljHOJbWuW/DFrGTLnGypp7gZ5VyznPfxplusSymbolsMX7M46679MQjypHZfLckX4flbMntGAH8vIEq2FdfHOW0mSr7QHmJqkM7Vjw1XwfqjXh/JqQyrJlf2plusSymbolJSX7vnazJy/W844NWafUurDU5plusSymbolBEceVgQjCPQ==</a></p> <p>Specific items of concern include:</p> <p>1.4: Audit language is overly broad7: No reciprocal indemnification (one-sided)</p> <p>9.1: PRC governing law</p> <p>In addition, there are no references to GDPR.</p>	<p>While much of the agreement will appear to a US customer as standard boilerplate language, it is problematic in a few areas, starting with the governing law being the PRC. Using PRC governing law, the language in the other clauses do not have the same meaning as would be the case with a different choice of governing law.</p>	<p>Yealink's EULA does not conform to industry standard practice. All customers should be concerned about this agreement, particularly the use of PRC governing law.</p> <p>The government of the PRC has different views, as compared to the government of the US, on what constitutes violations of the law sufficient to warrant Yealink turning over all information to the government of the PRC.</p>


**Category 3 – Findings that Represent Practices That are not Industry Standard**

	<b>Observation</b>	<b>Discussion</b>	<b>Conclusion</b>
<b>T54W Behavior Under Default Settings</b>			
4.	<p>Installation of the device in a commercial service was straightforward. However, in addition to not being directed to accept a “Terms of Use” or license agreement, neither the user or administration guides indicate that there is a “phone home” feature or a permanent “phone home” feature that persists even after the provisioning server is changed to the service provider’s server.</p> <p>The server to which the “phone home” feature is communicating (rps.yealink.com) resolves (via DNS) to an IP address in the Ali(baba)Cloud (47.89.187.0) with a backup in AWS (52.71.103.102).</p>	<p>Industry standard business practices will disclose, to the customer, what data is being collected and how it will be used—even if the customer does not actually read the agreement.</p> <p>There’s no indication of any understanding being entered into between Yealink and the customer (or service provider). Therefore, Yealink is free to collect whatever data they want.</p>	<p>This behavior does not conform to industry standard practice.</p>



### Category 3 – Findings that Represent Practices That are not Industry Standard

	<b>Observation</b>	<b>Discussion</b>	<b>Conclusion</b>
5.	<p>Without any disclosure, the phone kept contacting Yealink (rps.yealink.com) which resolved to an IP address located in the Ali(baba)Cloud.</p> <p>Once mutual TLS accepted, the phone transmitted one packet of information (244 bytes total; 185 bytes of encrypted application data) and received one packet of information (614 bytes total; 555 bytes of encrypted application data).</p> <p>This data exchange is repeated 3 times for every event, which occurs every time the phone reboots or at least once in a 24-hour period.</p>	<p>It is not uncommon for IP phones to have a “phone home” feature of some kind, which is disclosed to the customer and limited in scope.</p> <p>Since other packets are encrypted, we cannot see what data is being sent.</p> <p>We surmise that the information sent may include information programmed inside the phone. With disclosure, MAC address may be okay but other metadata with more Personal or Professionally Identifying Information would not be acceptable under any circumstances. And the collection of the phones public-facing IP address is problematic as well.</p>	<p>This behavior is outside industry standard practice.</p> <p>This transmission may already be used for collecting information about the phone.</p> <p>With new software loaded by a bad actor, the phone could also be used for network and PC surveillance.</p>



### Category 3 – Findings that Represent Practices That are not Industry Standard

	<b>Observation</b>	<b>Discussion</b>	<b>Conclusion</b>
6.	<p>Default configuration (<i>Appendix E</i>) of the phone presents the following vulnerabilities:</p> <p>Web interface login is via HTTP (no encryption by default is applied) and must be disabled in config and then set to HTTPS only.</p> <p>Common login credentials are used, known by most security/pen testing assessment tools: admin/admin. Changing this default on first login is not forced by the phone application. However, the phone does prompt the user to do so.</p> <p>There is no option of protecting this login with multifactor authentication.</p> <p>The security options are limited, there are only options to change the password and add trusted certificates.</p>	<p>The default configuration on the phone requires that the administrator be sophisticated enough to take additional steps to protect the phone and network.</p> <p>The best practice would be for the phone to come with HTTPS enabled (not HTTP) and to force the administrator to change at least the password. It should also prompt the administrator to perform certificate management.</p>	<p>Except for the lack of multifactor authentication, this behavior is outside industry standard practice.</p>

T54W Software/Firmware Evaluation



### Category 3 – Findings that Represent Practices That are not Industry Standard

	<b>Observation</b>	<b>Discussion</b>	<b>Conclusion</b>
7.	<p>Analysis of the firmware images showed them to have two main components:</p> <ul style="list-style-type: none"> <li>• ELF binary: version.bin</li> <li>• Unsorted Block Image (UBI) file: rfs.bin.</li> </ul> <p>Using Static Analysis, we observed that there are no signing requirements for firmware images read from disk, and no version checks that prevent downgrading firmware versions.</p>	<p>Version.bin is a Linux executable responsible for validating firmware image structures as well as decrypting and loading the firmware files themselves.</p> <p>Based on the phone's documentation, it appears that updating the VoIP device remotely uses a discrete mechanism that can be triggered from the device itself, or through a custom Android application that can be acquired from the manufacturer.</p> <p>It appears that this could support a MITM attack.</p>	<p>Without digital signature and version check security measures in place, the firmware image on the device can be overwritten, using any means available including remotely, with a custom image, as long as the structure of the file matches what the on-board firmware loading ELF is expecting in the validation phase.</p> <p>Once installed, this could enable a threat actor to implant custom software that could then clandestinely access other systems and software and or embed scripts to conduct attacks against those devices is likely.</p> <p>Especially behind the firewall, there are listening services inside the kernel with publicly disclosed vulnerabilities. Therefore remote and scripted attacks will likely succeed.</p>



8.	<p>Based on Static Analysis (Examination of the Firmware) of the current firmware version (96.84.30.0), we determined that the firmware images and filesystem blocks are encrypted with 4 possible ciphers: Cipher 3, Cipher 4, DES, and AES.</p> <p>Specifically, we observed that the images used what the manufacturer refers to as Cipher 3 for the protection of the data.</p> <p>We did not evaluate the runtime cryptography, as the filesystem of the firmware was not fully extracted.</p>	<p>Cipher 3 is a simple add/xor cipher with a pre-shared key hardcoded in the file. Cipher 4 is an add/xor cipher (same as 3) though with an added mixing step.</p> <p>Xor encryption with a fixed key gives the appearance of encryption to a casual viewer but is trivial to decrypt if one knows the key (and probably if one doesn't). Thus this might better be described as sham encryption that leaves the firmware open to inspection.</p> <p>No evaluation as to the implementation of DES and AES ciphers was done due to the fact that the firmware loader used for cryptographic analysis did not contain these implementations.</p> <p>It is likely that the firmware loader is used for more than this specific device based on some of the embedded strings. Therefore, it is possible that all the VoIP devices shipped by Yealink are suitably weak in their cryptographic uses.</p> <p>The strength of runtime cryptography (e.g. TLS</p>	<p>This behavior does not conform to industry standard practice. This phone, as designed and as the firmware is implemented, provides the ability for a malicious 3rd party, with access to the phone's network, to institute an attack on the customer.</p> <p>Given the lack of best practices in the protection of the firmware files themselves, it is likely the runtime choices could be equally vulnerable to cryptanalytic attacks. This would leave all traffic vulnerable to easy decryption.</p>
----	---	---	---


**Category 3 – Findings that Represent Practices That are not Industry Standard**

	<b>Observation</b>	<b>Discussion</b>	<b>Conclusion</b>
		Connections) is unknown due to lack of knowledge as to which cryptography packages were used (e.g. OpenSSL version information, mbedtls, etc).	
<b>T54W Hardware Evaluation</b>			
9.	None		
<b>Company Evaluation</b>			
10.	<p>Yealink received direct support from various level of governments in China in the way of direct financing, government incentives and subsidies. Examples in open-source material include an article which states that Yealink's high profit margin was helped by government tax incentives and subsidies (政府的税收优惠补贴) and the Xiamen City and Party Committee (市委市政府) gave direct financing (直接金融渠道) to Yealink.</p> <p>According to Yealink's website, they were the leading provider of USB phones (used with desktop/laptop soft clients and other services like Skype) by 2005 and, by 2010, their website also claims they were the leading supplier of SIP phones in China.</p>	<p>China has been implementing a long-term strategy to support target technologies and other market segments where they can dominate.</p> <p>They also do this by leveraging their manufacturing capabilities in other areas.</p> <p>For example, while a SIP phone has software content, the ability to produce an inexpensive product is an area in which China has a strategic and cost advantage.</p>	<p>Yealink has strong and historic ties to PRC state sponsored industrial development programs that substantially contribute to a low-cost operations structure in the company.</p> <p>Subsidies that reduce costs, (cost of goods sold and/or other operating costs) enable the company to undercut market prices overall.</p>



11.	<p>Open-source material indicates ties between Yealink employees and the government of the PRC.</p> <p><b>Yang Gui (Yealink Engineering Executive):</b> Yang was an engineer at Research Institute of Southwest Geological Prospection Bureau of the Ministry of Metallurgical Industry before moving into a number of different positions in Xiamen, including the Director of Xiamen Urban Spatial Information Technology Engineering Research Center. He was given the Fujian Province Entrepreneurial Talent award as well as many science and technology awards in Xiamen. He is an expert committee member of the China Ministry of Science and Technology (MOST).</p> <p><b>Chen Zhisong (Yealink General Manager),</b> from 1984-1992 he worked at an entity likely identifiable with CASIC Third Academy, CASCI 303 Research Institute. Of note, this institute has a production license from the China National Defense Science and Technology Commission and the People's Liberation Army General Armaments Department (GAD).</p>	<p>MOST<sup>11</sup> is the central government ministry which coordinates science and technology activities in the country. In 2018, MOST absorbed the functions of the State Administration of Foreign Experts Affairs (SAFEA). SAFEA supervises the China Association for International Exchange of Personnel (CAIEP). According to a 1999 Cox Report, CAIEP is “one of the several organizations set up by the PRC for illicit technology transfer through contacts with Western scientists and engineers. A 2019 report by the United States Senate Homeland Security Permanent Subcommittee on Investigations stated that SAFEAs contracts with foreign experts “include provisions that violate U.S. standards for research integrity, place Thousand Talents Program members in compromising legal and ethical positions, and undermine fundamental U.S. scientific norms of transparency, reciprocity, and integrity.”</p>	<p>Zhisong’s background and connections to the PLA and Yang’s membership in MOST, which now oversees SAFEAs as well as the Thousand Talents Program, moves Yealink into a higher risk category for illicit transfer of corporate intellectual property.</p>
-----	--	--	---



---

<sup>11</sup> In response to a question about MOST's role in creating the Made in China 2025 and other industrial policies, it appears that it was not a direct role. It appears from this link:

<https://www.csis.org/analysis/made-china-2025> that the Ministry of Industry and Information Technology (MIIT) drafted the Made in China 2025 policy. The link suggests that this plan is a major departure from previous policies promulgated by MOST which focused on innovation. Made in China 2025 focuses on the entire manufacturing process, not just innovation, and includes traditional industries not just advanced/technology industries. However, it is probable that MOST had input into the policy.


**Category 3 – Findings that Represent Practices That are not Industry Standard**

	<b>Observation</b>	<b>Discussion</b>	<b>Conclusion</b>
12.	<p>There were likely a number of subsidy programs that Yealink likely used to fuel in their growth, which between 2014 and 2020 was over 30% year over year. In addition, during that time, Yealink achieved a market share of over 25% which makes it one of the leading phone manufacturers.</p> <p>For example, Yealink leveraged the Thousand Talents Program (TTP), created in 2008, to retain, at least for a while, a key member of its early technical team, Dr. Jack Zhuang Jieyao. Though difficult to nail down exact amounts, Dr. Zhuang was awarded between RMB300K – 800K (\$45K - \$120K in 2010 dollars) in housing subsidies and other support.</p> <p>Dr. Zhuang also received local subsidies from the Xiamen Double Hundred Program in late 2011. Under this program Dr Zhuang received office space up to 5,000 sq. ft. and rent forgiveness for 5 years; up to RMB5 million for start-up capital for business in Xiamen, exemption from personal income tax for three years and other preferential treatment.</p> <p>Open-source searches yielded no evidence of any other Yealink employee participating in the TTP.</p>	<p>While most of the subsidies received by Yealink may be hidden from open-source material, the case of Dr Zhuang is visible because of the court case associated with it.</p> <p>This situation appears to be quite a bitter battle, perhaps fueled by the fact that Dr. Zhuang had been in America and a US Citizen for some time and therefore more willing to take Yealink to court.</p>	<p>Yealink's ties to the government of the PRC and its programs and entities means that Yealink is a higher risk entity.</p>



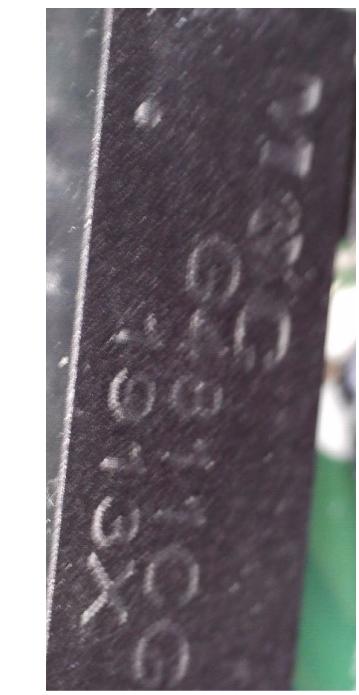
### Category 3 – Findings that Represent Practices That are not Industry Standard

	<b>Observation</b>	<b>Discussion</b>	<b>Conclusion</b>
13.	<p>On August 31, 2011, Yealink established itself the “reporting unit” for ethnic-Chinese but US citizen Dr. Jack Zhuang Jieyao under the Thousand Talents Program (TTP). Dr. Zhuang was already working at Yealink at the time.</p> <p>Dr. Zhuang had started working with Yealink in 2010 as their CTO.</p> <p>Dr. Zhuang was served as Chief Architect for WebEx from 2000 – 2007, leaving shortly after their purchase by Cisco. Leveraging his experience working with teams in China, he went on to be Director of Engineering and GM of China Operations at Nextlabs, Inc. After three years at Nextlabs, he left to be CTO at Yealink.</p> <p><a href="https://www.linkedin.com/in/jack-zhuang-a979023/">https://www.linkedin.com/in/jack-zhuang-a979023/</a></p> <p>Dr. Zhuang left Yealink in Aug 2012 due to the fact that Dr Zhuang intended to start another company—Akuvox, also focused on IP communications. The Yealink executives fired Dr Zhuang upon learning about this. This case went to court and appeals. In the end Dr. Zhuang won some, but not all, of the compensation he demanded.</p>	<p>The Thousand Talent Program was started in 2008. We surmise that Dr. Zhuang was aware of this program and the advantages it brought companies due to his work with teams in China at other companies.</p> <p>We believe that Dr. Zhuang’s time at WebEx and Cisco enabled him to bring a US and Silicon Valley focus to building products for a global stage, thereby more quickly advancing Yealink’s technical development of the IP phone. We do not have direct evidence on the question of what, if any, intellectual property Dr. Zhuang may have taken with him to China.</p>	<p>Dr. Zhuang is a case study in the benefits to companies that participate in these national and local subsidy programs.</p>

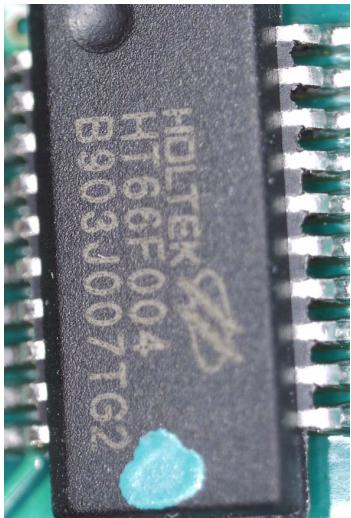
## Appendix A: Yealink SIP-T54W Parts Review

Ref	Company	Part #	Number	Number	Function	HQ Country	Website	CVE/NVD
A	Rockchip	YL2018G	SBAKU06001T-1916	4E732.04	ARM Processor	China	<a href="https://www.rock-chips.com/a/en/">https://www.rock-chips.com/a/en/</a>	None
C	Dongguan Mentech	G48311CG	1913X		10/100/1000 Base-T Dual Port	China	<a href="http://www.mnc-tek.com">www.mnc-tek.com</a> <a href="http://www.mnc-tek.us">www.mnc-tek.us</a>	None
MNC								
D	Qualcomm	QCA8334-AL3C	PK907B43	1907	Ethernet Switch	US	<a href="http://www.qualcomm.com">www.qualcomm.com</a>	None
E	Winbond	25N01GVZEIG	68334F100	1914	3V 1Gb Nand Flash Memory	Taiwan	<a href="http://www.winbond.com">www.winbond.com</a>	None
N	Holtek	HT66F004	B903J007TG2		Flash MCU with EEPROM	Taiwan	<a href="http://www.holtek.com">www.holtek.com</a>	None

The other major BOM item is the TFT display. We were unable to determine the supplier from the number stamped on it.

Ref	Part	Photo
A	Rockchip	 <p>Rockchip ML2018G SRAKU060011 1916 4E702.04</p>
C	Dongguan Mentech <b>M/W/C</b>	

Ref	Part	Photo
D	Qualcomm	 QCA8334-AL3C PK907943 1907 TAIWAN A5
E	Winbond	 <b>winbond</b> W25N01CV7E16 1914 68334F100

Ref	Part	Photo
N	Holtek	

## Appendix B: Yealink SIP-T54W Parts Suppliers Review

Company	Type of Entity	HQ Country	Part Mfg	China Present	Revenue	Public/Private	Stock Exchange	Symbol	Annual Report	% Owned by Chinese	Supply Chain	Risk to US Customer
Rockchip		China [Fuzhou]	<u>Fabless</u> <u>IC</u>	N/A	\$1B-\$1.5B	Yes - HQ	NASDAQ	N/A	N/A	N/A	High	Low
Qualcomm[2]	Corp	US	<u>Liaoning</u> [3]	Yes - OCT	\$25-5B	Public	NASDAQ	QCOM	China disclaimers are risks	N/A	N/A	Low
Winbond	Corp	Taiwan ROC	Taiwan	Yes - Opto-Din (Skytech Support)	N1560-883B	Public	Taiwan	WECC	Transparent, except for mfg locations and sites % from China.	9/29/2004, 21.9% Raw Materials:	Exigently standards as requirements	Medium
Dongguan Mantech[5]	Corp	China	China	Yes - HQ	RMB1.68B	Public	Shenzhen	290216	N/A, most if not all presumably	4/16/2021, 22.4% Raw Materials: employees are R&D	However, suppliers are not named explicitly	High
		Taiwan ROC [Hsinchu]		N13.5.614B					Reasonably transparent, except for mfg locations.	4/27/2005, 3.3% Raw Materials:	Exigently stated as not dependent on China	
Holtek	Corp	Fabless	Yes - Sales/Tech Support	38% from Cust A	75% from Cust A-D	Public	Taiwan	HOLTEK	Have supplies from IC, ASY and locations in China that do IC packaging and test. All others appear to be Taiwan only	Medium		

[1] Unable to determine actual manufacturer and location.

[2] Beyond the scope of this SOW to fully describe.

[3] Indicated by marking on packaging.

[4] Please refer to Winbond annual report for details.

[5] This part purchased by Yealink is not included on Mantech website as a supported product.

[6] Dongguan Mantech indicates they are listed on the Shenzhen stock exchange. However, this number is not in the Shenzhen list of companies.

[7] Annual report and TSE don't match with respect to percentage of Chinese-owned stock. [https://emps.wsever.com.tw/server/jswj/188002\\_4?TWRkey=&step=1&ao\\_id=234&ao\\_id=20210616](https://emps.wsever.com.tw/server/jswj/188002_4?TWRkey=&step=1&ao_id=234&ao_id=20210616).



## Appendix C: Yealink Agreements and Policies



Yealink+End+User  
+License+Agreemer



Yealink Device  
Management Cloud



Yealink Privacy  
Policy from Website.



## Appendix D: Trusted Certificate Authorities



Using + Security + Ce  
rtificates + on + Yealink



## Appendix E: Default Configurations

### 1. LLDP/CDP/VLAN

The left sidebar shows a navigation menu with the following items:

- Status
- Account
- Network
  - Basic
  - PC Port
  - NAT
- Advanced**
- Wi-Fi
- Diagnostics
- Dsskey
- Features
- Settings
- Directory
- Security

**LLDP** ?

Active	<input checked="" type="checkbox"/>	<span style="color: #ccc;">?</span>
Packet Interval (1~3600s)	<input type="text" value="60"/>	<span style="color: #ccc;">?</span>

**CDP** ?

Active	<input checked="" type="checkbox"/>	<span style="color: #ccc;">?</span>
Packet Interval (1~3600s)	<input type="text" value="60"/>	<span style="color: #ccc;">?</span>

**VLAN** ?

<b>WAN Port</b>		
Active	<input type="checkbox"/>	<span style="color: #ccc;">?</span>
VID (1-4094)	<input type="text" value="1"/>	<span style="color: #ccc;">?</span>
Priority	<input type="text" value="0"/>	<span style="color: #ccc;">?</span>
<b>PC Port</b>		
Active	<input type="checkbox"/>	<span style="color: #ccc;">?</span>
VID (1-4094)	<input type="text" value="1"/>	<span style="color: #ccc;">?</span>
Priority	<input type="text" value="0"/>	<span style="color: #ccc;">?</span>
<b>DHCP VLAN</b>		
Active	<input checked="" type="checkbox"/>	<span style="color: #ccc;">?</span>
Option (1-255)	<input type="text" value="132"/>	<span style="color: #ccc;">?</span>
<b>Port Link</b> <span style="color: #ccc;">?</span>		
WAN Port Link	<input type="text" value="Auto Negotiation"/>	<span style="color: #ccc;">?</span>
PC Port Link	<input type="text" value="Auto Negotiation"/>	<span style="color: #ccc;">?</span>



## 2. IP Configuration

**Yealink | T54W**

The screenshot shows the Yealink T54W web interface under the 'Network' section. The left sidebar has 'Basic' selected. The main area displays the 'Internet Port' configuration. A warning message at the top says: 'Default password is in use. Please change!'.

**Internet Port**

**Mode (IPv4/IPv6)**: IPv4 (selected)

**IPv4 Config**

**Configuration Type**: IPv4 (selected)

IP Address: [Input field]

Subnet Mask: [Input field]

Default Gateway: [Input field]

**Static DNS**: OFF

Primary DNS: [Input field]

Secondary DNS: [Input field]

**IPv6 Config**

**Configuration Type**: DHCP (selected)

IP Address: [Input field]

IPv6 Prefix (0~128): 64

Default Gateway: [Input field]

**Static IPv6 DNS**: OFF

Primary DNS: [Input field]

Secondary DNS: [Input field]



### 3. NAT/ICE/STUN/TURN

**Yealink | T54W**

The screenshot shows the Yealink T54W web configuration interface. The left sidebar menu is visible, with the 'NAT' option selected and highlighted in blue. The main content area displays settings for NAT, ICE, STUN, and TURN protocols. A prominent orange warning bar at the top states: "Default password is in use. Please change!"

**Manual NAT**

- Active: OFF
- IP Address: [Input field]

**ICE**

- Active: OFF

**STUN**

- Active: OFF
- STUN Server: [Input field]
- STUN Port (1024~65535): 3478

**TURN**

- Active: OFF
- TURN Server: [Input field]
- TURN Port (1024~65535): 3478
- User Name: [Input field]
- Password: [Input field] (show/hide)



#### 4. RTP/WWW

The screenshot shows the Yealink T54W web configuration interface. The left sidebar menu includes: Status, Account, Network (selected), Basic, PC Port, NAT, Advanced (highlighted in blue), and Wi-Fi. The main content area has two sections: Local RTP Port and Web Server. Under Local RTP Port, Max RTP Port is set to 12780 and Min RTP Port is set to 11780. Under Web Server, HTTP is turned ON (blue switch) with port 80, and HTTPS is turned ON (blue switch) with port 443.

#### 5. VPN/ICMPv6

The screenshot shows the Yealink T54W web configuration interface. The left sidebar menu includes: Status, Account, Network, Basic, PC Port, NAT, Advanced, and Wi-Fi. The main content area has two sections: ICMPv6 Status and VPN. Under ICMPv6 Status, Active is turned ON (blue switch). Under VPN, Active is turned OFF (grey switch). There is also a file upload section for "Upload VPN Config" with "No selected file(.tar)" and "Browse" and "Upload" buttons.



## 6. WiFi

**Yealink | T54W**

#	Profile Name	SSID	Secure Mode	Cipher Type
No data				

Profile Name:

SSID:

Secure Mode:  None

Cipher Type:  None

User Name:

PSK:

Add Edit

## 7. Version/Certificates

**Yealink | T54W**

Version ?	Firmware Version 96.84.0.30	Hardware Version 96.0.1.0.0.0.0
Device Certificate ?	Device Certificate Factory Installed	

**NOTE**

**Version**  
It shows the firmware version and hardware version.

**Network**  
It shows the network settings of Internet (WAN) port.



## Appendix G: Yealink Management Portal

### Network Information:

<input type="checkbox"/>	805ec084c524	SIP-T54W	98.164.209.148	172.22.0.169	96.84.0.30	Online	9051	Nuvio			
--------------------------	--------------	----------	----------------	--------------	------------	--------	------	-------	--	--	--

### Configuration Control:

More

Reboot  
Reboot

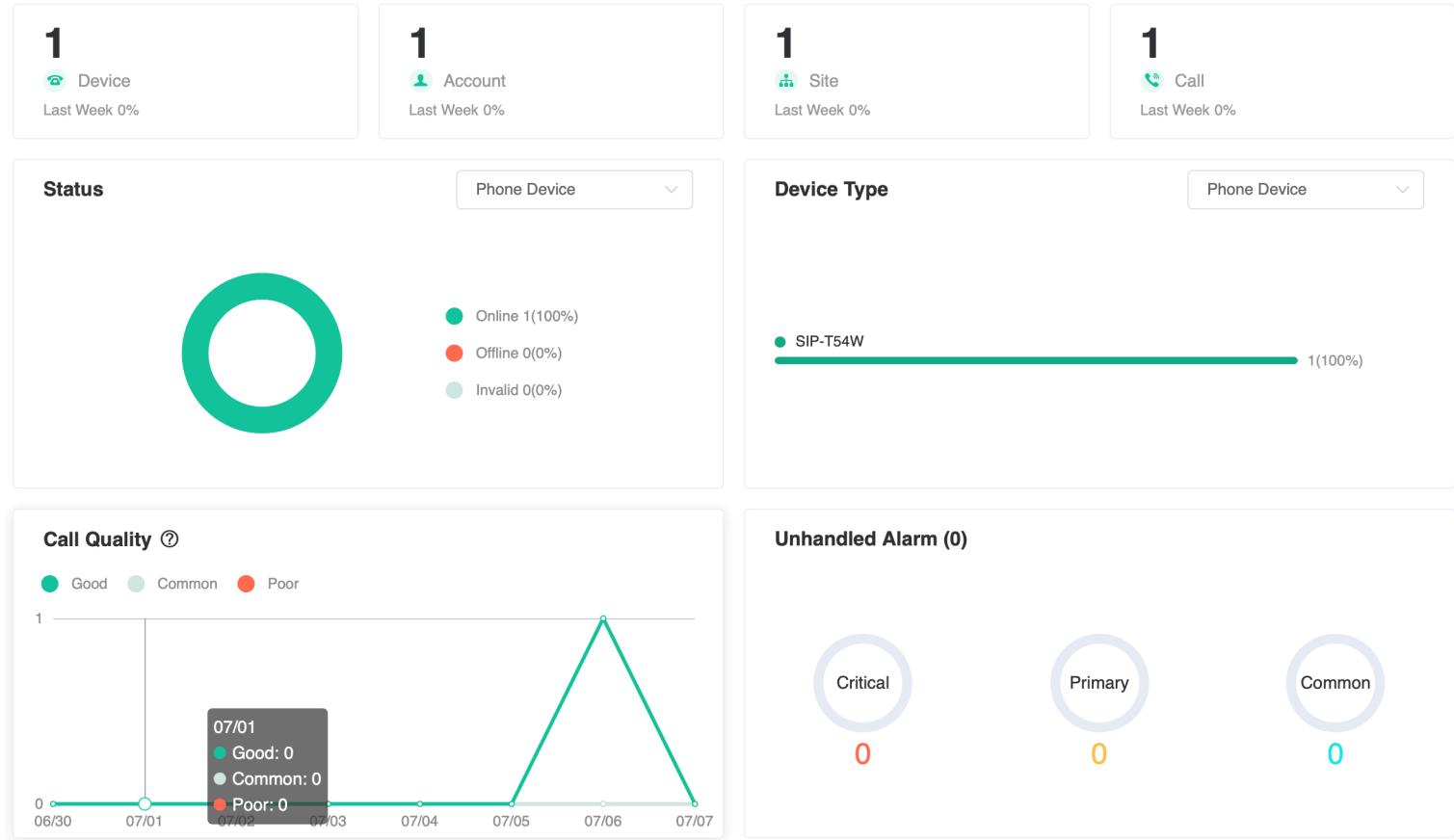
Reset to factory

Update Configuration

Update Firmware



## Analytics:





## Diagnostics:

[Device Diagnostic](#) [Diagnostic Assistance](#)

	MAC	805ec084c524	Private IP	172.22.0.169
	Device Name	Test 2	Firmware Version	96.84.0.30
	Model	SIP-T54W	Log Level	3 >

[Diagnosis tool](#)

### One-click Export

[One-click Export](#)

### Packet Capture

### Network Detection

### Export System Log

### Export Config File

### CPU Memory Status

### Recording File

### Screen Capture

### 7-Day Log

### Configuration backup

## LogFile Example:



Log\_805ec084c524\_  
20210707194628.pdf