CYBER SECURITY DOCUMENTATION

Ambu® aBox™ 2

Ambu

Contents Page

1. Introduction **3**

2. Executive Summary **3**

3. Security in brief **3**

3.1. Process 3

3.2. On device 3

4. Standards and Certification **4**

5. Device Configuration **4**

5.1. Operating System 4

5.1.1. Device support 4

5.2. Video and Imaging Pipeline 4

5.3. Network Stacks 4

5.3.1. Ethernet stack 5

5.3.2. WIFI stack 5

5.3.2.1. WIFI channel 5

5.3.3. Application layer 5

6. Security **5**

6.1. Pentest 5

6.2. Information Security 5

6.3. Vulnerability Management & Scanning 5

6.4. Data Closure and Flow 5

6.4.1. Data-at-rest 6

6.4.2. Data-in-use 6

6.4.3. Data-in-motion/Data-in-transit 6

6.5. Production Environment 6

6.6. Login Security 6

6.7. Access Control 6

6.8. Account Management 6

6.8.1. Default Accounts and Authorization 6

6.8.2. Admin Recovery 6

6.9. Removable Media 6

6.10. Keys On the System 7

6.11. Data Deletion 7

6.12. Event Logging 7

6.13. Update Deployment 7

6.14. Over The Air, (OTA) 7

7. Appendices **7**

7.1. Appendix #1 Development Process 7

1. Introduction
This document is meant to offer an overview of the security features in Ambu® aBox 2™. This document is intended for personnel with cybersecurity experience, service technicians or IT personnel.
The Ambu MDS2 document rendition holds more detailed information and can also be considered for security evaulation of the Ambu Product(s).
The document aims to be version agnostic for maintainability, and reducing errors. The updated software versions can be found in the SBOM. If there's disparity between the two, the SBOM should be considered the primary source of information.

The validity of this document is for Ambu software version 2.1.

2. Executive Summary
The product is meant to be used in a private/local adjacent network, the Ambu aBox 2 network is client-oriented, and does not currenly offer any hosted network servies (other than ICMP response). The Ambu aBox 2 only remote network feature, is it's over-the-air (OTA) feature, which allows the device to download an update package via an internet uplink, this feature is opt-in and default disabled on the device. The device is a visualization device, which takes images and videos through the Ambu single-use endoscopes, the device uses a custom made Linux operating system built on the principle of least-requirements, the Linux system base is built on an opt-in principle, in which features beyond basic functionality must be actively included.

The device functions such as updating, configuring and exporting, must be started by the operator, requiring roled-based authentication (password) for access.

The device supports, HTTPS for OTA and DICOM for image/video distribution.

Patient data is either filled out when exporting images/video after a procedure, or provided by a DICOM worklist service prior to a procedure start.

3. Security in brief
3.1. Process
Ambu develops threat ingelligence by developing a cybersecurity risk analysis, performing open-source threat ingelligence and maintaing a vulnerability management program, to monitor security development.
Cybersecurity requirements and validation tests confirm port, network-services and input hardening.

3.2. On device
Application Layer
Network services are client only and network transmissions are protected by a firewall that only opens ephemeral ports to create outgoing connections.
The application is jailed on the device, inputs are sanitized and user management in the GUI is isolated from the OS, users profiled used for the application is restricted empty users.
The application uses the QT framework to profile indirection to the underlying Linux system.

OS Layer
The Linux operating system is custom made, and is designed to be closed down.
User management is deferred to the operating system.
Uses the standard Linux network stack for ethernet and WiFi.

Information Security
Patient data is proviced by DICOM Worklist prior to a procedure, or filled in manuallyby the operator after the procedure during export.
Patient data lifetime does not outlive the images/videos.

Network Layer Protocols
aBox 2 supports ethernet (Intel controller) and WiFi (Qualcomm).
- DICOM, SCU (Client). C-FIND and C-STORE.
- HTTPS, TLS 1.2, OAuth session, upgrade utility.
- ICMP, device adressibility.
- DHCP, DNS and ARP.

See chapter 5.3 Network stacks for WiFi and ethernet stacks.

4. Standards and Certification

- The QMS (Quality Management System) is ISO 13485 certified and the development process is ISO 62304 compliant.
- The cybersecurity risk analysis have been performed following AAMI TIR 57:2016, EN ISO 14971:2019 and EN 62304:2006 + AMD1:2015.
- The analysis was also inspired by and have partially followed AAMI UL 2900-1:2017 and AAMI UL 2900-2-1:2017.
- The vulnerability management program uses MITRE att&ck and evaluation uses MITRE d3fend.
- Cybersecurity documentation is based on NIST Framework, MDCG and FDA pre-market guidance.

5. Device Configuration

This chapters goes into details with some of the configurations.

5.1. Operating System

The operating system is a Linux Kernel 4.19.130 custom distro, it made by the buildsystem "Yocto" which works by providing a set of source files that is build up a custom distro around the Linux kernel. The graphical engine EGLFS, uses the QT framework and the Linux to maintain windowing services for the touch interface. EGLFS is naive rendered on the screen, the underlying Linux system is locked out and does not log into the pseudo terminal (which is disabled for physical access). Every user input is sanitized, the underlying real-time rendering engine is GStreamer.

The updating functionality is provided by RAUC (Pengutronix), which uses openssl for authenticating a signed X.509 certificate on the upgrade packages. The X.509 uses sha256 signature algorithm from an assymetric RSA 2048 key pair. The signed package contains a manifest detailing the cryptographical hashed parition checksum, along with the EXT4 partition used for deploying the entire system (single static update), this means that the device does not use application, firmware or system upgrade individually, but only accepts the entire system together, hardening it for un-intended changes/modifications in the field.

The design consideration for OS is least-requirements, meaning that the Yocto build system start from a lightweight bare-metal embedded system, and every addition is actively choosen by Ambu innovation to be included. This sort of opt-in means few un-used features, which have not been intentionally ported.

The operating system uses PAM for access control, and uses the Netfilter firewall for network access control. Barebox is used for bootloading and the BIOS is password protected to protect boot-order.

The system runs on system V, but does offer non-serviced systemd features where applicable.

5.1.1. Device support

The device only supports certain USB classes, such as Mass Storage Class (MSC,08h) for USB 2 and 3. Audio, communication, HID or custom classes are not supported.

To protect the integrity of the OS keyboard have been disabled for OS access, to avoid brute-force attacks.

5.2. Video and Imaging Pipeline

The videos are recorded in MPEG-4 using H.264 encoding.
The GStreamer open-source project is used to record the real-time video, and uses video 4 linux (v4l) as a device handler.
The device have a FPGA which serves a live-view image, this is made separate from the CPU handled rendering, and therefore if anything happens a safety mode stil render the live-view.
Further discussion into the video and image support have been excluded from this document, and can be found in the safety documentation.

5.3. Network Stacks

The device supports two active stacks, an Ethernet and WIFI stack. The device implicit supports ARP and DHCP/UDP stacks.

5.3.1. Ethernet stack

1. User-space, QT dbus interface.
2. Socket layer offered on interface to kernel.
3. Kernel space: Linux TCP/IP & UDP/IP kernel support 4.19.130.
4. Intel igb driver.
5. MAC layer: Intel I211 802 Controller.

5.3.2. WIFI stack

1. User-space, QT application for scan & selection.
2. User-space, QT WPA-supplicant interface.
3. User-space, WPA-supplicant for socket negotiation.
4. Kernel-space: Linux 80211cfg & 80211mac.
5. Qualcomm ath10k driver.
6. MAC layer: Qualcomm QCA6174 80211 Controller.

5.3.2.1. WIFI channel

Ambu WIFI supports WPA1 and WPA2, but not 802.1X enterprise.

5.3.3. Application layer

Both stacks are used for exporting using DICOM. DICOM uses the DIMSE-C protocol.

Per market assessment, there's a very low adoptation rate of the DICOM 3 chapter 14 TLS security feature, and therefore its have been assessed by Ambu that it's not ready for market deployment. Due to the nature of the old standard being used, if it is to be supported, its security level is considered acceptable from a risk-oriented assessment.

Ambu does recommend not to use remote DICOM server with internet uplink, but rely on network isolation and segmentation.

6. Security

This chapter goes into further details about some of the security features on the Ambu aBox 2 product.

6.1. Pentest

The device have been black-box pentested by Improsec A/S. As the pentest has a confidential tag, it would be exposed in this report, contact Ambu about the pentest. (No critical or major deficiencies was found)

6.2. Information Security

From information security there are two modes. In one mode; DICOM Modality worklist is used, allowing a patient to be selected from a worklist prior to starting the procedure coupling paitnet association to the current procedure. In the other mode, the operator of the device, can choose to export the procedure data via DICOM to a PACS/VNA server. During the export the operator can fill out patient data, these will not be persisted on device, but will be embedded within the DICOM package that is transmitted, the data is deleted after export.

The operator can also export images/videos to USB in DICOM format or the images/
videos in a basic encoding format.

6.3. Vulnerability Management & Scanning

Ambu runs an internal vulnerability management program, which uses manual inspection of different database (for instance NVD) to assess new vulnerabilities on the devices, these informations are consilidated and documented quaterly in a cybersecurity maintenance meeting.

The device is internally scanned by an Yocto service (CVE-check).
The device is port and network scanned by network and vulnerability assessment tools.

6.4. Data Closure and Flow

The device does not accept any incoming data flow, the netfilter firewall have been installed to only allow associated/ estasblished TCP-states.

The device is meant to be defined under the closure of the local hospital infrastructure network, due to the nature of the DIMSE-C DICOM protocol, the security is primary upheld by the hospital infrastructure. Without broad adoptation, Ambu can only secure the device end-point, and does not control end-to-end transmissions.

Below is a list of data definitions on the device. The handling of images/videos from at-rest to in-motion is done by DICOMConnect, developed by SoftGate (see DICOM conformance statement for more information).

6.4.1. Data-at-rest
- Images and videos
- Network configuration
- Device configuration

6.4.2. Data-in-use
- Real-time videos
- Video replay
- Configuration
- Video and image capturing
- Patient data during export

6.4.3. Data-in-motion/Data-in-transit
- DICOM Association (transmission negotiation)
- DICOM C-STORE packages containing DCM dataformat with image/video and meta-data
- DICOM C-FIND during worklist acquisition and update (request and response)
- Possible patient data, dependent on operator fill-in during export
- HTTPS supported upgrade packages

6.5. Production Environment
Ambu production is isolated from Ambu development.
Production in Ambu is maintained by BriteMed, which are ISO 27001 certified and is audited by Ambu QA regarding security.

6.6. Login Security
The device differentiates between OS login and Application layer.
Both are maintained by the PAM (Pluggable Authentication Module) in Linux and their pass keys are stored in the shadow using cryptographical hashes.

The usage of the application layer is restricted, and does not have disk allocation, nor terminal/shell association, used for UID association and password management, this de-coupling means that application layer users cannot be used to compromise the OS, and offers isolation for user-management to the application layer.

6.7. Access Control
The application layer is isolated from the OS layer access, by a jailed QT application.
The device does not use remote login, so no SSH or otherwise direct OS user access.
The device does not feature multiple-users and does not allow for IT/or-others to log into the OS layer.
The device does not allow for physical console/terminal login.
Access to the device is protected by a password login, and is only done on Ambu secure facilities.
The boot is protected by a per-device password generated in production and placed in BIOS.
The BIOS password is used to full-disk encrypt the disk.

6.8. Account Management
Accounts generated for the application layer are maintained by PAM, but does not provide home directories or bash-shells, and are purely made for the uid and gid they provide, used to validate operating in the application layer, and limit ressource access for different elevated user accounts (role-based authorization for acess).

6.8.1. Default Accounts and Authorization
There are two default accounts, the service technician and the admin account. They have unique permissions, which cannot be re-produced by creating new users, runtime user management is restricted to advanced users or basic users.
The application layer segments access control is based on the role-base authorization.

6.8.2. Admin Recovery
To help customers recover lost admin passwords, Ambu will provide a service in which a customer can contact Ambu and receive a per-device per-day unique shared key to recover the admin account.

6.9. Removable Media
The device supports USB mass storage devices.
The device can have the disk removed, by the MCU on the disk have been keyloaded with the production BIOS password, and without the right BIOS to disk, the disk will not unlock the MBR.

6.10. Keys On the System
The device have a RSA2048 public key used to authenticate update bundles for the device. The device also contains key(s) used for the OTA service, to uniquely identify the device by the cloud service.

6.11. Data Deletion
Data deletion must curnret be performed by the operator.

6.12. Event Logging
Access to the device is logged, and export/DICOM is logged. images/videos are logged.
The device does not contain a dedicated audit log, and the information must be derived from the general logging.

6.13. Update Deployment
The update bundle performs a single statically assigned update of the entire device stack.
The bundle will mount a new rootfs, install, validate and promote the new rootfs as current.
The bundle will update the firmware through shell-scripts.
The bundle is initially authenticate by an appended X.509 signed certificate, the validation precedes execution of the binary files before expanded.

6.14. Over The Air, (OTA)
Updating can also be performed by using an internet uplink. This feature is default disabled, and must be opt-in enabled. The connection uses an HTTPS, account authentication & role-based authorization, along with cryptograhic key exchange (in addition to the TLS key exchange), the integrity is maintained by a timed OAuth 2 token. Due to security, in the architecture is not fully detailed in this document, but the principle is a multi-step connection, which have defense-at-depth both the in protocol and on device/cloud.

The OTA is inteded for an evolving healthcare market, which in time will need rapid software deployment, especially for security features.

7. Appendices
7.1. Appendix #1 Development Process
The development process is controlled by IEC 62304.
A cybersecurity risk has been performed on the system, based on TIR-59.
Cybersecurity documentation is based on NIST Framework, MDCG and FDA premarket guidance.

Ambu

Ambu A/S
Baltorpbakken 13
DK-2750 Ballerup
Denmark
T +45 72 25 20 00
ambu.com

PUB-001444 – V01 – 2022/03. TCC 11256