# CYBER SECURITY DOCUMENTATION

**Applies to Ambu® aBox™ 2 and aView™ 2 Advance using software 2.4**

Ambu

# Contents Page

# 1. Introduction

This document is meant to offer an overview of the security features in Ambu® aBox 2™ and aView 2 Advance with software 2.4. From here on used interchangeably with *displaying and processing units*. This document is intended for personnel with cybersecurity experience, service technicians or IT personnel.
The Ambu MDS2 document rendition contains 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 2.4.

# 2. Executive Summary

The product is meant to be used in a private/local adjacent network, the Ambu *displaying and processing unit* network is client-oriented, and does not currently offer any hosted network services (other than ICMP response). The *displaying and processing unit*'s 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 and SMB 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.

For users who wish to harden the security for DICOM, then DICOM-TLS is offered and supported on the device.

# 3. Security in brief

## 3.1. Process

Ambu develops threat intelligence by developing and maintaining a cybersecurity risk analysis and maintaining a vulnerability management program.
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 provided by DICOM Worklist prior to a procedure, or filled in manually by the operator after the procedure during export.
Patient data lifetime does not outlive the images/videos.

**Network Layer Protocols**

Ambu *displaying and processing unit* supports ethernet (Intel controller) and WiFi (Qualcomm).

- DICOM, SCU (Client). C-FIND and C-STORE.
- SMBv3, 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.
- Cybersecurity documentation is based on NIST Framework, MDCG and FDA pre-market guidance.
- ISO 12052:2017(en) Health Informatics - Digital imaging and communication in medicine (DICOM) including workflow and data management (DICOM PS3.1).

# 5. Device Configuration

This chapters goes into details with some of the configurations.

## 5.1. Operating System

The operating system is based on a custom configured Linux kernel 6.6.23, and is built using the buildsystem "Yocto". The application is built on the QT framework and is running on top of EGLFS.

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 partition checksum, along with the EXT4 partition used for deploying the entire system (single static update). This means that the device does not support application, firmware or system upgrade individually, but only accepts the full system together, hardening it for unintended 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 to be included. The method of opt-in, provides very few unused features, which has not intentionally been ported or included.

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. Communication, and HID. The latter is used for triggering picture or video capture.

Keyboard input is sanitized and delays between password attempts has been added, to harden against 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 has 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 still 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 6.6.23
4. Intel igb driver.
5. MAC layer: Intel I211 802 Controller.

### 5.3.2. Wi-Fi 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. Wi-Fi channel

The device supports the following Wi-Fi security protocols:

- WPA
- WPA2
- WPA2 Enterprise
- WPA3
- WPA3 Enterprise

The following authentication protocols are supported:

- EAP-TLS
- EAP-PEAPv0
  - MSCHAPv2
  - EAP-MSCHAPv2
  - TLS
  - EAP-TLS
- EAP-TTLS
  - MSCHAPv2
  - EAP-MSCHAPv2
  - EAP-TLS
  - MSCHAP
  - CHAP
  - PAP

### 5.3.3. Application layer

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

If the user wishes to harden the security of the standard DICOM DIMSE-C protocol, then DICOM-TLS per PS3.1 chapter 14 is implemented. The device has a functionality to accept in self-signed certificates for a local-trust-store either from a server endpoint (device only accepts X.509 files on endpoint) or through an USB mass storage device.

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 displaying and processing units.

## 6.1. Pentest

The device have been black-box pentested by Improsec A/S. according to NIST guideline reference: SP 800-115. As the pentest has a confidential tag, it would be exposed in this report. (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 patinet 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 on a triweekly basis monitors the SBOM components for vulnerabilities. The search is uses the NIST NVD database. The outcome is followed up on a quarterly software maintenance meeting documented with minute of meeting.

## 6.4. Data Closure and Flow

The device does not accept any incoming data flow, the netfilter firewall have been configured to drop all traffic other than system established connections and ICMP packets.

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
- Patient data if imported by DICOM Worklist
- Audit log
- SMB configuration
- DICOM/PACS configuration

### 6.4.2. Data-in-use

- Real-time videos
- Video replay
- Configuration
- Video and image capturing
- Patient data during export (if populated by operator or imported from DICOM Worklist)

### 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
- Possible secure DICOM communication using DICOM-TLS
- HTTPS supported upgrade packages Endoscopic video/images in transit to SMB server.

Only the HTTPS system for updating requires an edge-router for internet uplink, DICOM and SMB communication is recommended in an internal network with modality segmentation. To facilitate operators to use DICOM-TLS the Ambu Monitor features a PKI system for importing self-signed X.509 certificates to promote a trust on the device for the PACS/VNA server.

## 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 support remote login, using SSH or other 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 on aBox 2 and ATA-lock the disk on aView 2 Advance.

## 6.8. Disk encryption

The aBox 2 offers full-disk encryption, which are locked/unlocked by the BIOS and controlled by chip-integrated MCU with the SSDs. The process is TCG OPAL 2.0 compliant, key provided by BIOS, using AES256.
The full disk is decrypted on boot-up from BIOS signal by the integrated chip MCU on the SSD, and then encrypted by boot-down.
The aView 2 Advance features an ATA-lock which is controlled by the BIOS.

## 6.9. 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 access).

### 6.9.1. Default Accounts and Authorization

There are two default accounts, the service technician and the admin account. They have unique permissions, which cannot be reproduced 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.

### 6.9.2. 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.

## 6.10. Removable Media

The device supports USB mass storage devices.
If the device's disk is removed it is ATA-locked (and full disk encrypted on aBox 2), which requires the per device unique BIOS password to unlock/decrypt the disk.

## 6.11. Keys On the System

The device has 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.

## 6.12. Data Deletion

Data deletion must be performed by the operator, using the data deletion protocol as seen in the Instructions for Use.

## 6.13. Event Logging

Access to the device is logged, and export of data is logged. Capturing images or videos are logged.
The device contains a dedicated audit log, which contains logs of actions related to procedures, authentication, user profiles and archival.

## 6.14. 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.

### 6.15. Over The Air, (OTA)

Updating can also be performed by using an internet uplink. 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. The architecture is not fully detailed in this document, due to security. The principle is a multi-step connection, which has defense-at-depth both in the protocol and on the device and Ambu OTA server.

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

The TLS connection is hardened to use TLS 1.2 and 1.3, using only DHE/ECDHE key exchange with RSA/ECDSA authentication, AES126/256 encryption and SHA256/384 HMAC integrity.

## 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
2750 Ballerup
Denmark
T +45 72 25 20 00
ambu.com

PUB-002018 – V01 – 2024/10.