CathexisVision 2023

Cybersecurity Overview

Contents

1. Introduction 3
2. Cathexis Security 4
2.1 Communication between CathexisVision components 4
2.1.1 Carbon and CathexisVision Mobile App 4
2.1.2 Enterprise 4
2.2 Archiving of data 5
2.3 Protection of Personal Information 5
3. Peripheral Equipment 6
3.1 Camera configuration 6
3.2 Camera control 6
3.3 Video streaming 6
4. IT Considerations 7
4.1 Network Access 7
4.2 Operating System Lockdown 7
5. Conclusion 8

1. Introduction

Cathexis has been developing and supplying video management solutions to the global market for more than 20 years. We take cybersecurity seriously.

Cryptographic techniques are applied to ensure system integrity, secure communication and data protection.

This document outlines the measures employed to reduce the risk of information access and data manipulation, and offers some suggestions for increasing the security in areas of the systems that Cathexis cannot control, such as peripheral and third-party equipment.

USEFUL LINKS

*To view **tutorial videos** on CathexisVision setup, visit https://cathexisvideo.com/resources/videos*

*Find answers to Cathexis **Frequently Asked Questions**: https://cathexis.crisp.help/en/?1557129162258*

2. Cathexis Security

This section outlines the various security measures Cathexis takes.

2.1 Communication between CathexisVision components

CathexisVision shall ensure secure communications between its components, including:

1. Recording servers to clients
2. Recording servers to other recording servers
3. Recording servers to video walls
4. Recording servers to Alarm Management Gateways.

Secure communication between the above components shall be ensured by:

1. All external site connections support encryption of varying levels:
   a. Disabled,
   b. Minimal (only critical connections encrypted),
   c. Secure (the default option which encrypts all connections except those with high volume video (i.e., the bulk video data). All control, information, and metadata are encrypted.)
   d. All (all connections encrypted, including high volume video links).
2. Passwords are never stored as plain text. Instead, they are hashed using SHA512 (from CathexisVision 2017).
3. Login credentials are negotiated using Diffie-Hellmann key exchange and signed with an RSA private key (supports 1024 and 2048 RSA keys).
4. Encryption on network channels is performed using AES128/GCM with unique cipher keys negotiated per connection.
5. Hash-based Message Authentication (HMAC) is used for integrity verification.
6. Public Key Infrastructure (PKI) is managed internally by Cathexis for added security.

2.1.1 Carbon and CathexisVision Mobile App

All connections from a Carbon UI, and the new CathexisVision mobile app, use the same encryption and authentication technology as CathexisVision.

2.1.2 Enterprise

All connections into and out of the Enterprise are encrypted using the same mechanisms deployed in the CathexisVision suite. Unlike CathexisVision, the encryption cannot be disabled.

2.2 Archiving of data

1. The integrity of the recorded video is secured using dual RSA1024 keys (for signing),
2. Optional encryption is performed using AES128 block encryption with a randomised Initialisation Vector (IV) per block and a user generated pass-phrase.
3. Video can be watermarked to indicate the source of the information (i.e., user info).
4. The original video footage and metadata can only be played via a proprietary Cathexis Archive video Player.
5. Exported/archived video may be restricted to password-controlled playback.

2.3 Protection of Personal Information

To assist in ensuring that video footage does not get into the public domain, CathexisVision has the ability to:

- Archive video that can only be played back under password control.
- Overlay a watermark on the video to depict the source of the information (for example, user info).
- Add privacy zones to cameras in order to restrict areas viewed, thus protecting privacy.
- Restrict exported native archives from being exported to a media file (for example, MP4).
- Redact faces in archiving/exporting.

3. Peripheral Equipment

The variety of product and protocols to which CathexisVision connects determines the security of peripheral equipment (e.g., IP cameras). For this reason, Cathexis is working with technology partners and other industry players to increase the security of this interface.

In general, connection with IP cameras includes the following:

3.1 Camera configuration

- HTTP: hypertext protocol,
- Encrypted SSL/TLS (Secure Socket Layer/Transport Layer Security),
- Supported by CURL (Client-side URL transfer library).

3.2 Camera control

- RTSP – real time streaming protocol.
- HTTPS (Hyper Text Transfer Protocol Secure) encrypted camera connection control (where supported by the manufacturer).

3.3 Video streaming

- RTP – Real time transport protocol.
- Encrypted video streaming (where supported by the manufacturer).

4. IT Considerations

This section covers security considerations around the IT system beyond the control of Cathexis.

4.1 Network Access

The first step in any system is to ensure that access to the network is properly controlled. There are various techniques for this which are well documented and should be known and adopted by any competent networking company. These include:

- Firewalls,
- Intelligent Network Switches,
- Managed Networks,
- Control “physical” access to the network.

4.2 Operating System Lockdown

In order to attack software, access must be gained through the operating system of the hardware on which the software is running. It is therefore important to ensure that the OS is “locked down” to prevent unauthorised access. This can be done in several ways, including:

- Preventing the opening of unauthorised ports enabling use of items like ftp, telnet, email. If any communication needs to occur via these means, then one needs to ensure that security protocols like SSH/SFTP are utilised,
- Disabling “root” access to the OS,
- Ensuring strong password levels,
- Adding anti-virus and anti-malware software, which is continuously updated,
- Restricted internet access.

5. Conclusion

For more information, consult the Cathexis website (www.cathexisvideo.com) or contact support@cat.co.za

For guides on complying with privacy legislation in the use of video surveillance systems, consult:

- ***Cathexis Privacy Guide: Protection of Personal Information*** (POPIA)
- ***Cathexis Privacy Guide: General Data Protection Regulation*** (GDPR) (https://cathexisvideo.com/resources/cathexisvision-privacy-guide/).