CathexisVision 2020 Cyber Security Overview

Contents

1 Introduction[1]

Cathexis has been developing and supplying video management solutions to the global market for more than 20 years. Security involved in both access to data and the data integrity has always been a high priority considering the secure environment in which the Cathexis products have been used.

In recent times, the term “Cyber Security” has become a hot topic in the physical security systems space and is something that Cathexis takes very seriously.

This document outlines the measure employed to reduce the risk possibility 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.

[1] While Cathexis has made every effort to ensure the accuracy of this document, there is no guarantee of accuracy, neither explicit, nor implied. Specifications are subject to change without notice.

2 Cathexis Security

This chapter outlines the various security measures taken by Cathexis.

2.1 Communication between CathexisVision Components

CathexisVision shall ensure secure communications between its components, including:

i. Recording servers to clients,
ii. Recording servers to other recording servers,
iii. Recording servers to Video Walls,
iv. Recording servers to Alarm Management Gateways.

Secure communication between the above components shall be ensured by:

i. 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),
    d. All (all connections encrypted, including high volume video links).
ii. Passwords are never stored as plain text and instead are hashed using SHA512 (from CathexisVision 2017).
iii. Login credentials are negotiated using Diffie-Hellmann key exchange and signed with an RSA private key (supports 1024 and 2048 RSA keys).
iv. Encryption on network channels is performed using AES128/GCM with unique cipher keys negotiated per connection.
v. HMAC is used for integrity verification.
vi. Public Key Infrastructure (PKI) is managed internally by Cathexis for added security.

2.2 Archiving of Data

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

2.3 Protection of Personal Information (POPI)

In order to assist in ensuring that video footage does not get into the public domain, we have added the ability to:

i. Archive video that can only be played back under password control.
ii. Overlay a watermark on the video to depict the source of the information (e.g. user info).

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

i. HTTP: hypertext protocol,
ii. Encrypted ssl/tls,
iii. Supported by CURL (client-side URL transfer library).

3.2 Camera Control

i. RTSP – real time streaming protocol.
ii. HTTPS encrypted camera connection control (where supported by the manufacturer).

3.3 Video Streaming

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

4 I.T. Considerations

This section covers security considerations around the I.T 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:

i. Firewalls,
ii. Intelligent Network Switches,
iii. Managed Networks,
iv. Control “physical” access to the network.

4.2 Operating System lock-down

In order to attack software, access must be gained through the operating system on the system 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:

i. 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,
ii. Disabling “root” access to the OS,
iii. Ensuring strong password levels,
iv. Adding anti-virus and anti-malware software, which is continuously updated,
v. Restricted internet access.

5 Conclusion

For further information consult the CathexisVision website (www.cathexisvideo.com) or contact support@cat.co.za.