016-20180609-07 06 August 2018 G Brecher; R Solomon

CathexisVision 2018 Cyber Security Overview

Contents

1 Introduction

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 of information being assessed and the possibility of data being manipulated and offers some suggestions for increasing the security in areas of the systems that Cathexis cannot control, such as peripheral and third-party equipment.

2 Cathexis Security

This chapter outlines the various security measures taken by Cathexis.

a. Communication between CathexisVision components

i. Passwords are never stored as plain text and instead are hashed using SHA512 (from CathexisVision 2017).
ii. Login credentials are negotiated using RSA1024,
iii. Sensitive communication channels are encrypted using AES128/CBC,
iv. HMAC is used for integrity verification.
v. Public Key Infrastructure (PKI) is managed internally by Cathexis for added security
vi. This applies to:
    1. Cathexis “Recording Servers” to Cathexis “Clients,”
    2. Cathexis “Recording Servers” to other Cathexis “Recording Servers,”
    3. Cathexis “Recording Servers” to Cathexis “Video Wall,”
    4. Cathexis “Recording Servers” to Cathexis “alarm Management Gateway.”

b. Archiving of Data

i. When archiving video data, the integrity of the videos is secured using dual RSA1024 keys (for signing) and optional encryption is performed using AES128 block encryption with a randomised IV per block and a user generated pass-phrase.
ii. There is also an optional “watermarking” feature.
iii. The video footage and metadata can only be played via a proprietary Cathexis Archive video Player.

c. 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:

a. Camera Configuration

i. http: hyper text protocol,
ii. encrypted ssl/tls,
iii. supported by CURL (client-side URL transfer library).

b. Camera Control

i. RTSP – real time streaming protocol.

c. Video Streaming

i. RTP – Real time transport protocol.

4 I.T. Considerations

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

a. 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:

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

b. 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.