White paper

Video Data Security

Prepared by:

Dan Berg, Sr. Sales Engineer, On-Net Surveillance Systems, Inc.

Date: February 5, 2018

Table of Contents

Introduction

In applications where video plays a critical role as evidence, it is paramount that the video data is transmitted, stored and exported securely. OnSSI's Ocularis video management system provides a series of security mechanisms that enable users to maintain full end-to- end security and integrity of video data.

Target audience and purpose

The primary audience for this white paper is surveillance system architects/designers and surveillance project consultants, as well as security officers, companies, organizations and law enforcement bodies with surveillance projects/installations where video and evidence handling is critical.

The purpose of this white paper is to give a general overview of how video is transmitted from the camera and stored securely in the Ocularis Recording Server databases, as well as how exported recordings are secured in the Ocularis Client and Viewer when used as evidence.

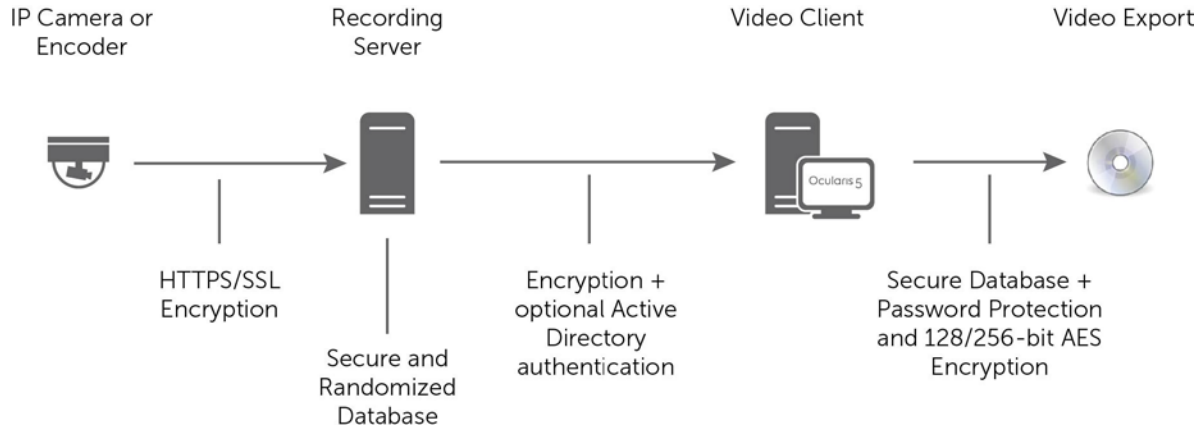
This white paper should enable the reader to understand how recordings are secured from transmission from the camera to viewing exported recordings as evidence, as well as how to implement and use the extended security in the most optimal way.

The reader is assumed to have a general understanding of Ocularis and IP video management solutions in general.

Video data flow

In a digital video surveillance system, the typical flow of data can be broken down into these steps:

1. Video is captured by the camera
2. Video data is streamed over the network to the Recording Server
3. Video data is stored by the Recording Server
4. Live and recorded video is streamed to the video client
5. Recorded video is exported by the client



Ocularis employs several methods to ensure the integrity of video data in each of these steps.

1. Video captured by camera

Risk: Cameras may be disconnected, stolen or simply fail.

Ocularis will automatically detect if the camera is not responding or stops streaming video to the system. Once the system detects this it triggers a "communication error" event which can be used to trigger alarms or rules notifying system administrators and operators via email, SNMP monitoring and on-screen alerts.

Users should also be aware that video recorded on the cameras SD card for Edge Recording support (as described in section 3) may be vulnerable if the camera is stolen.

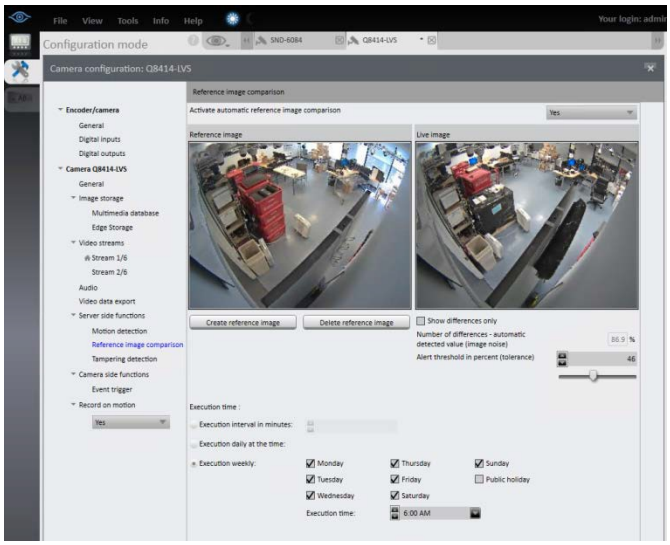
In the event a camera fails or becomes disconnected, any historical video data already stored on the Recording Server may be played back. It is not necessary to replace the camera first in order to play back video.

Risk: Cameras may be tampered with by turning it or by covering the lens.

Ocularis includes server-based tampering detection. Many cameras also include tampering events of different kinds, such as tampering, video loss, and temperature. These events can be received by the Ocularis system and used to trigger alarms or rules notifying operators and system administrators of the issue.

Risk: Cameras can become unfocused, move over time or become obscured by dirt or other obstructions.

Ocularis includes a scene change detection which compares a reference image to the current view. This can detect changes in the scene such as obstructions, slow movement of the camera (such as occurs if the mount is not properly tightened) or accumulation of dirt and debris that may not be noticeable to operators over time. This scene change detection ensures proper recording of video evidence by cameras that may not be frequently monitored.



Scene change detection in the Ocularis Recorder.

2. Video is streamed over the network to the Recording Server

Risk: The network may be compromised giving unauthorized persons access to tapping into the transmitted video or accessing the cameras directly.

To protect against potential hacking of passwords and commands communicated between the cameras and the Recording Server, Ocularis supports modern TLS 1.2 encryption protocols with cameras and encoders that support this feature. (For devices that do not support TLS 1.2, SSL 3.0 may be used but is not recommended as SSL 3.0 is no longer secure.)

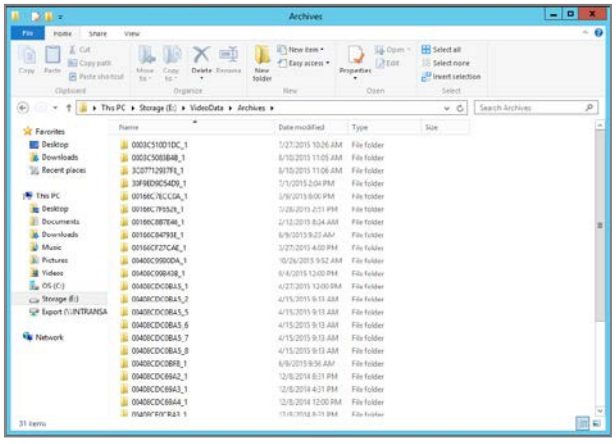
In addition to encrypting the video stream from the camera, the Ocularis architecture allows users to place cameras on a completely separate subnet from client workstations. This prevents direct access to the cameras from the general network further enhancing the security of the system.

3. Video stored in the Recording Server database

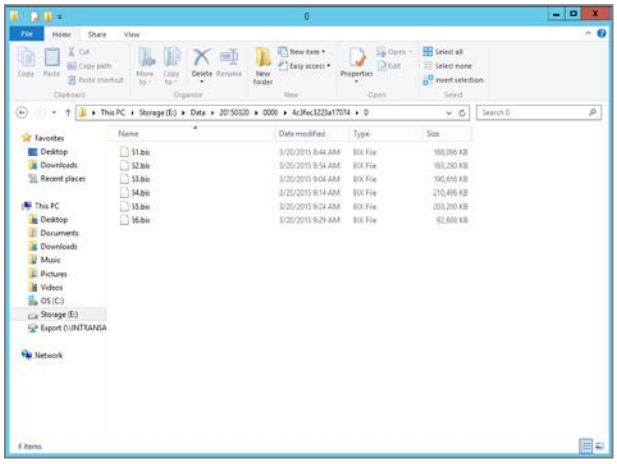
Risk: Video recordings stored on the server may be tampered with

Ocularis does not provide any tools or options for the system's client operators to access or manipulate the content or the authenticity of the recorded video. However, to prevent video tampering and provide for detection of such actions by persons that may have access rights to the actual recording server, Ocularis employs several prevention and detection methods:

- Ocularis utilizes a proprietary video database specifically designed to increase video recording speed and performance over standard databases, but more importantly to handle video security and authentication.
- Video data stored in the database can only be read by the Ocularis Recording Server software.
- Video data from all cameras and encoders is randomized in the database so that a person with access to the server will not be able to identify and possibly delete specific sequences for specific cameras.



Data stored in a typical VMS – organized by the MAC address of the camera allowing unauthorized persons to identify specific camera sequences.



Randomized data stored in Ocularis with no identifying camera information.

Risk: The Recording Server may be turned off or fail.

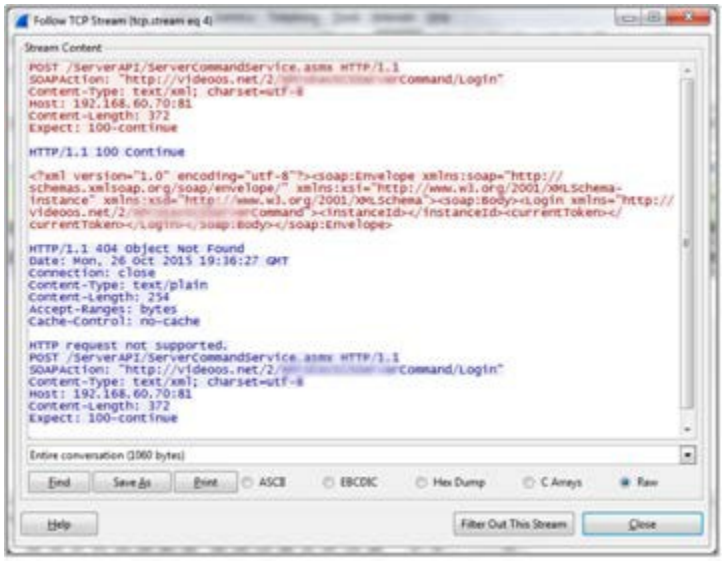
Ocularis Enterprise and Ultimate support Recording Server failover, which is a process in which the camera streams are redirected to an alternate Recording Server in the event the primary Recording Server is unavailable. If the primary Recording Server stops responding, due to failure or being turned off, for example for maintenance, the Failover Recording Server take over the task of recording the video.

In addition to Recording Server Failover, Ocularis Ultimate also supports Edge Storage on select devices. Edge Storage offers the function to record video in the camera itself and let the Recording Server retrieve these recordings after a network failure, effectively ensuring video recording even for periods with no connection to the camera.

4. Live or recorded video is sent over a network to a client

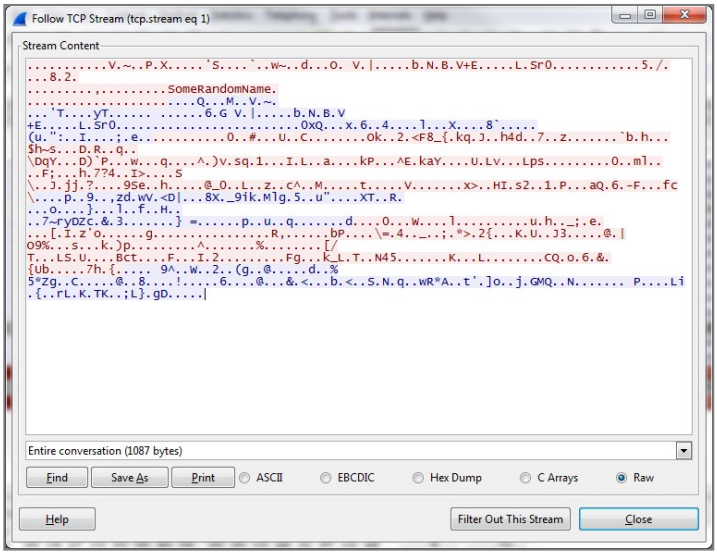
Risk: The network may be compromised giving unauthorized persons access to communication between the Recording Server and the Client.

In Ocularis, all communication between clients and the Recording Server is secured using 128-bit AES encryption. Ocularis also utilizes a proprietary video streaming protocol that cannot be accessed using commonly available media players. Only the Ocularis Client is able to decode the video stream from the server.



Typical unencrypted communication between VMS Recorder and Client.

Data captured using the free Wireshark packet analyzer application.



Encrypted communicationbetween Ocularis Recorder and Ocularis Client.

Data captured using the free Wireshark packet analyzer application.

5. Live or recorded video viewed by unauthorized persons

Risk: The video surveillance system may be hacked by unauthorized persons to obtain login credentials to view live or recorded video and to export.

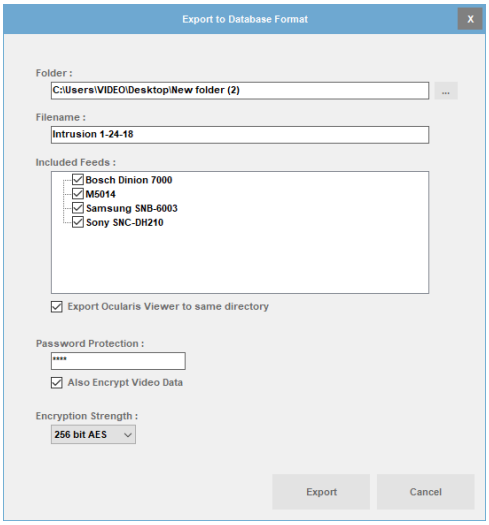
Video streamed from the recording server – both and live and recorded – is only viewable by the Ocularis Clients (including web and mobile). Ocularis offers centrally controlled security settings that set when and which cameras can be viewed live, played back and exported by the user. Permissions can be set at a group level and also for each individual user. All client operators' actions are logged by Ocularis with color-coded query results for easy identification of system usage.

To secure client access to the system, Ocularis recommends using secure Windows Active Directory® (AD) for authentication. When using Active Directory for authentication, OnSSI recommends that all users have their own separate account as this will make it easier to investigate in the Ocularis audit log who logged in, viewed live or recoded video or who exported video from the system.

Additionally, multiple administrator-level accounts may be configured within Ocularis so that changes made to the system can be tracked by individual administrator-level user. As with user-level accounts, administrator-level accounts may also use Active Directory for authentication.

Risk: The exported video may be viewed and copied by unauthorized persons.

To prevent unauthorized persons from viewing or copying exported video, Ocularis Client supports password protection and database encryption using 128 or 256 bit AES encryption on the exported video database.



Password protection and encryption options when exporting video from Ocularis Client.

Risk: The exported video may be tampered with removing critical sequences of the recorded video or be modified to give another impression of the recorded evidence.

Video exported in the proprietary Ocularis database format utilizes many of the same prevention and detection methods to prevent tampering and alteration as are employed on the Ocularis Recording Server:

- A proprietary video database specifically designed to handle video security and authentication
- Video data can only be viewed using the Ocularis Client or stand-alone Ocularis Viewer

Benefits and summary

In combination with proper network and IT security policies and procedures, Ocularis enables users to deploy video surveillance solutions with full end-to-end security. With the new encryption and signing features in Ocularis and Ocularis Client, it is possible to keep streamed and recorded video secure and prove the integrity of it all the way from the original stream from the camera to the point it is exported and then viewed.

About OnSSI

On-Net Surveillance Systems, Inc. (OnSSI) was founded in 2002 with the goal of developing comprehensive and intelligent IP video surveillance management software. OnSSI's Ocularis IP security and surveillance VMS platform increases security, reduces operational costs, and helps organizations move closer to prevention. Ocularis delivers open architecture, flexibility, and scalability for a range of applications including education, gaming, government, healthcare, manufacturing, public safety, transportation, and utilities. OnSSI is headquartered in Pearl River, New York and has representation in over 100 countries. With its acquisition of Germany-based VMS company, SeeTec GmbH and the launch of Ocularis 5, OnSSI continues to drive global expansion and technological innovations.

OnSSI HQ, Pearl River, NY (845) 732-7900

Info@OnSSI.com www.OnSSI.com