

IP Storage Technologies for Physical Security

Date Published: 24 Nov 2009

By George C Paul

With various security sub systems the storage requirements would seem to be very high for a physical security system. However, among the various security sub systems only the video surveillance system would require significant storage space, when compared to the other systems. The output from the other security systems such as access control, intrusion systems, and fire & safety systems would be typically textual data carrying status and control information. With the video surveillance system depending upon the resolution of the camera, the frame rate, and the total number of cameras, the storage requirements can range from a few gigabytes to terabytes per system.

Prior to the advent of IP-based communication the storage systems for video surveillance was not overly complicated. The storage system would involve a tape recorder or a digital video recorder (DVR). In the tape-based system, once the tape was full it was replaced by another tape. After the stipulated number of days required for backup, the tapes were overwritten using new video footage from the surveillance camera. Similarly, the DVR used to record till it was full and then overwrite when there was no more space. These were basic storage units that were built for the video surveillance system. These surveillance systems used a separate communication network and did not share resources with the computer network.

The advent of IP-based physical security system shifted the focus from tape and DVR to IP-based storage systems such as network video recorders (NVR), network attached storage (NAS), and storage area network (SAN). These IP-based storage systems were developed for IT systems and hence had developed technologies that were used to backup, retrieve, archive, and protect enterprise level data. With the shift of video surveillance systems from serial to IP-based communication networks these technologies became available to the security managers to maintain their storage systems. Besides, in situations where the storage resources are shared with the enterprise system, the security managers need to be aware of certain storage technologies that are used to maintain those systems. A few of the major storage technologies that are currently being used to maintain and operate current generation storage systems are discussed below.

Data Deduplication

Data deduplication is one of those IP-based storage technologies that is gaining traction in storage management, as it directly affects the amount of storage space available. In enterprise storage there might be situations where the same set of data would be stored multiple times by multiple users across the enterprises network. This uses up valuable space if the data stored are large in

size such as a video file. Data deduplication is a technology that prevents this by deleting duplicates or copies of the same data set. The additional instances of the data would be deleted, keeping the indexing of those files. All these indexes of the duplicate files will point to the same data location, thereby reducing the space required for storage. This makes it easier to reduce the costs of storage, data protection, backup, and retrieval. There are various types of data deduplication methods and they all use hash calculations to return a value for each file that is compared with existing files to remove duplicate files.

Data deduplication would be useful in distributed video surveillance systems, where the same video feed is stored in different locations. There would be the source location and then there would be the central location, where select video is analyzed. There might also be secondary locations for both forensic and training purposes where the video data might have been copied. When all these data are backed up or archived, data deduplication automates the process and maximizes the capacity utilization.

Virtualization

Storage virtualization is a technology that separates the physical storage hardware from the logical representation of that storage space in a computer network. Prior to virtualization if there is 100 GB disk drive, the computer or the server to which the storage unit is attached can show a maximum of only 100 GB or less if there are more than one logical drive. Hence, the logical size of the storage drive is limited by the storage space on the physical disc drive. Virtualization overcomes this by combining all the physical storage units or disk drives available into one large logical drive. This also makes it possible to locate all the storage units in one physical location and provide logical drives to the users connected over the IP network. This is usually used in SAN-based systems, where the data on the logical drive are mapped to its physical location and can be independent of the location of the computer or server on which the user is working. This allows the IT manager to allocate additional storage space to the users and applications in real time without the delay in physically adding a new disk drive. If the entire storage system is running low on space, the IT managers can add additional storage racks and the system will automatically balance the load on existing disk drives to take advantage of the new disk space. All these operations would be performed without affecting the productivity of the users that are logged on at that time.

Virtualization would significantly improve the ease of maintaining a large video surveillance system. Systems that are continuously growing such as a city, road network, or rail network system would benefit the most. As the number of video channels increases, the storage space required can be increased in steps for the entire system without being concerned about mapping the space to the individual channels. The system would then balance the newer storage racks to maintain equal availability of storage space over the entire system.

Thin Provisioning

Thin provisioning is a technology that is used along with storage virtualization to increase the capacity utilization of the storage system. In systems where virtualization has not been implemented, the storage is provided based on the

expected requirements by the user. Hence, if there are ten users and on an average the space requirement is 10 GB, the total storage even at the beginning of the installation would be 100 GB. However, not all of them might use the entire 10 GB of space. Some may require 2 GB, some may use around 10 GB and a few may require more than 10 GB of space. Thus, the users that use only around 2 GB will have 8 GB of storage space that is not being used and for the few who use more than 10 GB will require an additional 10 GB disk drive for their requirement. Hence the capacity utilization of these systems is brought down due to this irregular distribution of storage space. This is also known as fat provisioning. In thin provisioning, a beginning storage of the minimum requirements by the users is provided and as and when more storage space is required, the IT manager allocates the additional space, thereby distributing the storage to achieve almost 100 percent capacity utilization.

Just as virtualization helps improve data management, thin provisioning also helps the storage manager to make the best use of all the existing storage space. Even if there is a combination of cameras with different resolution, frame rate, and on-screen activity the system use nearly 100 percent of the capacity by distributing the available storage space in real time.

Cloud Storage Solutions

Cloud storage is a form of storage virtualization technology, where the physical storage location is not even within the same office building. The storage can be maintained by the same company in an offsite location connected through the Internet or it can be outsourced to a third party data center. The SAN would be maintained in these offsite data centers, connected to the user servers over the Internet. The user provides the fee for whatever storage they use and does not have to worry about maintaining the hardware. Besides, as the data are accessed through the Internet the same data set can be accessed from anywhere through a Web-based interface. The only two concerns would be reliability in accessing the data and the security of the data being stored offsite. These can be mitigated by faster Internet connections and encryption technologies. At present, most of the enterprise level cloud storage is used for backup and disaster recovery. These data sets are not used on a daily basis and hence, are encrypted and stored in the cloud. In case of an emergency the data sets are retrieved and reinstalled to the operational SAN.

Encryption

Encryption is a second level of data security to prevent the data being accessed by unauthorized users. The first level of security would be logical security systems that use passwords, smart cards, and biometrics to provide access to the data. However, if the hacker gets access to the physical hard drive, he can directly copy the data by running third-party applications that extract the data stored on the hard drives. Encryption is a technology that prevents this by encoding the data being stored on the hard disks. Even if the hacker gets access to the physical hard drive, without the decryption keys the data retrieved would be encoded and would like gibberish. Hence, this is an important technology in securing data, especially over the cloud.

Solid State Storage

The technologies seen till now were mostly on the software level. The underlying hardware still uses the magnetic disk drives that were used in DVR for individual storage units, albeit with greater density and retrieval speeds. There is a new form of storage system that uses solid state or integrated circuits that do not have any moving part within them. Unlike magnetic drives that require the disks to spin at thousands of revolutions per minute, solid state devices (SSDs) store and retrieve information from IC chips. Before the advent of nanometer silicon manufacturing process, solid state devices were only able to store data in the kilobyte range. This was not feasible for data storage applications. However, with nanometer silicon manufacturing, the SSDs were able to store data in the gigabyte range in a small form factor. As it has no moving parts it used less power and had much lower wear and tear. In addition, the storage and retrieval speed was comparable to random access memories (RAM) in computers, which was significantly higher than magnetic disks. The only restraining factor with SSDs is the price when compared to an equal sized magnetic disk drive. However, prices are coming down and at present, the SSDs are used for storage of data that are used frequently and on a daily basis, with magnetic disks used for backup and optical disks or tape drives used for archival.

Spin Down and Self-healing Data Storage

Not all of the disk drives would be in use all the time. The power required for running and cooling these disk drives is immense. Hence, the spin down technology was introduced to reduce the operating costs of these storage systems. The storage management application automatically switches off the disk drives that are not in use and puts them on a mode similar to hibernate on the PCs. This is called spinning down the disk drives and is being implemented by most of the storage solution providers as part of their green initiative to conserve and improve energy efficiency.

One of the other problems with disk storage systems is the inherent nature of disk drives to sustain radial and spiral scratches due to continuous operation. This cannot be prevented, as the mechanical contact between the magnetic disks and the reader head is susceptible to this type of damage. These scratches lead to data corruption, which in most cases would lead to data loss. Only in some cases can the corrupted data be retrieved and in most cases it would lead to a complete loss of data. The self healing data storage system locates such scratches at the beginning stages and transfers the affected and adjacent data to a safer location to prevent data loss.

Most of the technologies mentioned above can be used for stand-alone physical security storage systems. However, for systems that share the resources with enterprise IT systems, the adoption of these technologies would be based on the IT administrator. Apart from cloud computing, encryption, and SSDs, most of the technologies can even be adopted for stand-alone physical security storage systems and for providing immense savings in terms of both cost and time.

Detailed market and technology reports across biometrics, access control, video surveillance, perimeter security and other security solutions are available through Frost & Sullivan's online subscription. For details on access, please contact Isabelle Moeller at manager@biometricsinstitute.org