Image authentication

Recorded video images help to catch criminals – everyone agrees on that. It is a visual tool for identifying perpetrators and as such it speeds up investigations into a crime tremendously. But what happens afterwards? More and more, images are presented to courts as evidence. When that happens, the judge or jury has to place their trust in those images and the prosecutor has to prove their authenticity. The Quadrox software has all the necessary tools available to provide that proof.

The issue of traceability to the source

When talking about image authentication, most people want proof that the images "didn't change", or "weren't tampered with". This level of proof is slightly misleading because it doesn't define which changes are allowable. All surveillance video is "changed" in some sense during the transmission from camera to court. Depending on the situation, it may be digitized, resized, clarified or compressed. During these transitions, some image quality is inevitably lost and important details might be lost along with it.

For all practical purposes, what is meant is that the images that are presented as evidence are the originally recorded ones (from the crime scene in question) and that they haven't been tampered with or haven't been exchanged for other images on their way to the courtroom. In other words, the whole issue comes down to the traceability of the video back to the recording system and ultimately to the camera.

In the past, this was guaranteed by restricting physical access to the re-cording equipment and by having the tapes or digital video physically transported to evidence storage by (implicitly trusted) law enforcement officials. Having your video storage or even your entire recording system confiscated by the police is very expensive.

Watermarking

A term that is often mentioned in connection with image security is watermarking. This is a technique that adds some invisible information to the image itself to trace it back to its source. The most common use of watermarking is to protect copyrights.

This technique has to be applied before the image is compressed since it works with the raw image data itself. Applying a watermark on the already compressed image that comes from the network camera would require recompression which always has a negative influence on quality. Therefore, it doesn't have applicability for Network Video Recorders.

Watermarking can be useful on the cameras themselves. With such an implementation, the first part of the video path between camera and recorder can also become completely traceable.

In most cases today, security is only accomplished by user authentication schemes and network security, which are less secure (because they only protect the transmission channel and not the image itself) but not as complex and costly.

The latest generation of networked systems promise a much easier and faster way of getting the video to the police by simply sending it over the internet. A public network like the internet is not exactly the safest means of transport, however, digital video can be digitally secured and the ability to trace the video back to its origin is now a reality. This technology is called digitally signing the video.

Digital signature

A digital signature is a cryptographically encoded text that contains information about the file that was signed and about the entity that created the signature. Because cryptography is used, it is impossible to forge a signature (i.e. to create a forged signature that looks like it was generated by the original entity). A digital signature can also be uniquely linked to the file that was signed. This means that for all practical purposes it is impossible for a third party to create a different video file (or change the real one) and then create a signature that proves that it is original.

In other words, if the authorities retrieve a video file and its signature, and if they trust (see section titled "Trust") the entity that signed it, it is mathematically proven that the file is original (by verifying the signature) and didn't change since it was signed (by verifying the hash value). In the case of surveillance video, we want to trace the video back to the recorder (or camera), so that should be the signing entity.

Trust

The signer is embodied in a certificate (a cryptographically protected text that contains the electronic key pair with which the owner of the certificate can sign digital documents or content). There are two forms of the certificate: one that contains the private key used to create the signature and one that contains only the public key used to verify it. The former needs to be protected, the latter trusted.

The certificate containing the public key is only valuable if it is trusted by the authorities. Digitally signing a movie only moves the trust issue from the movie to the certificate . The benefit is in the fact that the certificate is easier to protect than the movie, and it only needs to be "trusted" once; afterwards all movies that are signed by it can be sent over insecure networks or other transport means and can then be verified by using the trusted certificate1.

The only way that a third party can tamper with a movie is to obtain the certificate that contains the private key. In that case, they can create a new movie and sign it as if it was coming from the real recording device. Since the certificate is located only on the recorder, restricting physical and electronic access to the recorder remains as necessary as always. The recorder should be behind lock and key and it should be protected by a strong authentication mechanism. The Quadrox software contains such a strong authentication mechanism in its Microsoft Windows user management functionality.

Digital signature content

The digital signature generated by Quadrox software contains the following information.

- The filename of the signed movie and its hash. A hash is a mathematically calculated number that uniquely defines the original information. There are always several information strings that produce the same hash value, but it is infeasible to find a "second original" based only on the hash. If you change a single bit in the original information, the hash will be different. Popular hashes used by the Quadrox software are MD5 and SHA-1. Together, filename and hash value, indisputably link the signature to the movie file.

- The time at which the video was recorded and at which it was exported.

- The system user that created the movie export.

- The identifier and name of the recorder, which together with the certificate that was used proves that the movie file was originally recorded on that particular system.

- The name of the camera from which the movie originated.

Together, this is all the information that is needed to verify the authenticity of the movie. Decoding the message with the trusted certificate guarantees that the signature was assigned on the recording system to which it belongs. The file name and hash value extend this guarantee to the movie itself.

---

[1] Technically speaking, you trust a certificate if you believe that it contains the public key matching the private key that belongs to the signing entity.

[2] http://www.microsoft.com/technet/archive/security/topics/issues/fipseval.mspx?mfr=true

A certificate looses its "trust value" over time, because the longer it is in place, the higher chance it has of being compromised. It is recommended that certificates be renewed regularly and that the old certificate is allowed to expire. This should happen in very controlled circumstances to maintain the trust in the new certificate.

There is a possibility to further enhance trust by having the certificate itself issued by a certification authority (CA). CA's are trusted organizations (usually controlled by governments) that verify the certificate belongs to the entity that claims it.

Quadrox has based all these systems on open, standard technology to prevent any possibility of security holes or "back doors". All algorithms that are used are well-known and widely used cryptographic standards, like MD5, SHA-1 and RSA. They cannot be broken if the key is not known, not even by the people that implemented them. The certificate is standard (X.509, PKCS #12), as is the digital signature format (PKCS #7). In addition to the true signature standard that can be viewed by specialized publicly available viewers, we also provide the signature in a standard email format (S/MIME format), so that it can be viewed by common email clients like Outlook Express. Quadrox uses Microsoft's implementations of these formats and algorithms, which are validated and certified by the National Institute of Standards and Technology (NIST)2 .

This means that the authenticity of a Quadrox movie can always be verified by using standard, publicly available tools. Since the signature is separate from the movie itself, the latter can still be played in any media player because, again, we use a standard movie format and standard codecs. We also provide our own movie verification tool for your convenience. We decided to open the source for everyone to examine, so that there can be no doubt that the tool provides acceptable verification.

The video authentication process

In practice, all these certificates, movies and signatures come together in an authentication flow, which is graphically represented in the following picture.
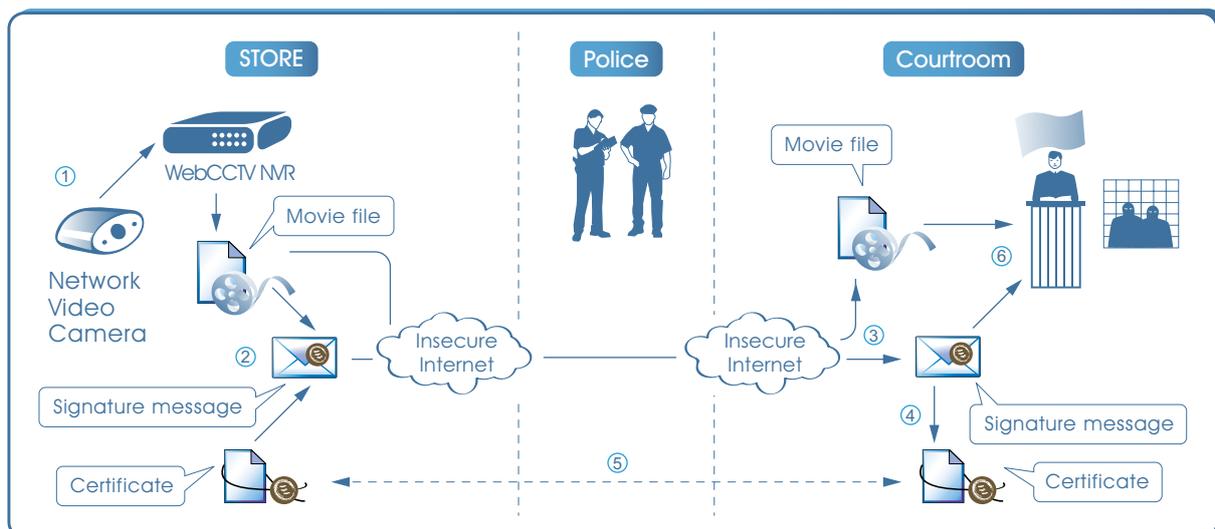
1.   Video from the camera is recorded in a standard ASF movie file.

2.   When a relevant piece of video is exported, information about that file (e.g. the timestamp, camera name, recorder information and the user who performed the export) is gathered in a signature message. This message is encrypted by the certificate, unique to each recorder, to form a digital signature.

3.   The movie file and the signature are transported to the courtroom. They don't necessarily have to travel together and the channel can be unsafe (e.g. they can be sent over the internet).

4.   From the signature, a copy of the certificate can be extracted. The certificate can also get to the courtroom in a different way (by exporting it from the recorder) or already be present because it was extracted from previous movies.

5.   This certificate should be trusted by the court. The court expresses this trust by explicitly adding it to the list of trusted root certificates. When doing this, the system will ask to manually verify the certificate, e.g. by comparing the thumbprint of the certificate to the thumbprint of the certificate that is present on the recorder. The latter should be retrieved by physically going to the recorder, it should be done by the authorities and a proven track record should be available. Trusting the certificate has to be done only once (not for every movie) and doesn't have to happen at the same time as the movie verification.

6.   The signature message can then be decoded. Because the certificate is trusted, we know that a) the information in the signature is correct (wasn't changed) and b) the signature was produced on the recorder from which the movie is claimed to have originated. If the signature was forged, the certificate will not decode it. Inside the signature, a hash value links the certificate uniquely to the movie file. By recalculating the hash in the courtroom, we can be sure that a) this signature belongs to this particular movie and b) the movie hasn't changed since the signature was created. If the movie is forged, the hash value will be different and the signature invalid.

Management summary

In order to use digitally stored surveillance video as evidence in court, it needs to be traceable to its source. Quadrox addresses this issue by eliminating costly physical confiscation of the recording media and replacing it by a standards-based digital signature. This way, trust in the video material can be maintained even if it is transported in an insecure way.

The movie is signed by the recorder via a certificate. Trusting the video then amounts to trusting the certificate. This should be ensured by securing physical and electronic access to the video recorder. It can also be electronically enhanced.

The use of standard technology and open-source tools ensures that no back-doors exist in the software to falsify the verification process.

About Quadrox:

Quadrox is a leading provider of digital video security solutions. Its standards-based WebCCTV™ product family provides an efficient and reliable infrastructure by which companies can distribute, update and manage video sources and content over corporate intranets, extranets and the Internet. Quadrox European offices are located in Belgium. Quadrox US offices are located in Henderson, Nevada.

For additional information, please, contact:

Svitlana Tanasiychuk

Quadrox NV, Duigemhofstraat 101, 3020 Herent, Belgium

Tel: +32 (016) 58 25 85

Fax: +32 (016) 58 25 86

E-mail: info@quadrox.be

Website: www.quadrox.com