

Autenticidad en los vídeos de seguridad para uso forense



Autor: Dr. Bob Banerjee, Product Marketing Manager

¿Qué es la autenticación de vídeo?

La autenticación de vídeo es el proceso de preservar la integridad del vídeo original para que sea admisible su presentación en la corte, es decir, que es considerada prueba suficiente para demostrar que el vídeo es original y no ha sido alterado en ninguna forma. La autenticación protege a las personas contra actos maliciosos o cambios accidentales.

La autenticación de vídeo en sistemas analógicos

En un sistema analógico puro, el vídeo se transmite desde una cámara, típicamente sobre cable coaxial a un receptor, que generalmente es una videogradora VCR y/o a través de un switcher, conmutador o matriz analógica a un monitor analógico. Vale la pena mencionar que es posible interceptar la señal del vídeo analógico, y sustituirla con una fuente falsa, y esto es casi imposible de detectar.

Sin embargo, asumamos que el vídeo entrante que fue grabado es auténtico (no sustituido). Una vez que el vídeo es transferido a una cinta es sencillo editar el vídeo y crear uno nuevo, por otro lado sería prácticamente imposible de detectar el cambio. Para minimizar este riesgo, se utiliza el concepto de “Cadena de Custodia” que asegura que la cinta se encuentra en todo momento bajo la supervisión continua y documentada por partes consideradas de confianza.

Esto obviamente asume que las partes son realmente confiables. La Cadena de Custodia se basa en la noción de seguridad y supone que no existe interés de alterar el vídeo por parte de estas personas, pero eso no significa que no lo puedan hacer.

Autenticidad en la Era Digital

La autenticidad en la Era Digital está basada en los principios de la criptografía, este es porque el vídeo es dato, no una señal analógica – una cadena de ceros y unos, que hace mucho más fácil detectar los cambios. Al utilizar algunos principios de la criptografía, eliminamos la posibilidad de que incluso las partes de confianza alteren el vídeo, aunque quisieran.

La utilización del término “casi eliminado” es intencional. La criptografía, remitiéndonos al Imperio Romano de Julio César, se encontraba basada en la confianza entre personas y la misión era y continúa siendo la minimización del número de personas en las que se debe confiar. El número ideal es 1.

Puntos de Vulnerabilidad

Transmisión de vídeo IP

Empalmar el cable coaxial y robar una copia del vídeo o sustituirlo con un vídeo falso como suele ocurrir en las películas de acción, es mucho más difícil en las redes IP, ya que las redes en general poseen una gran cantidad de opciones para proteger la integridad de los datos transportados, tanto en la capa física como en la de transporte.

Es importante señalar que mientras las medidas típicas de Seguridad Standard ya mencionadas se encuentren en funcionamiento para la red, no existirá ninguna diferencia entre un vídeo de 10 segundos, un e-mail confidencial, alguien revisando su cuenta bancaria o una compra online.

Asimismo, existe la posibilidad de confirmar la integridad de los datos, las redes IP pueden determinar la identidad del que emite la información y eliminar así la posibilidad de sustitución. Por lo tanto, una grabadora es capaz de grabar solamente cámaras IP conocidas y provenientes de codificadores con direcciones MAC confirmadas.

Bosch Sistemas de Seguridad incluye un CRC (Chequeo de Redundancia Cíclica) en los paquetes de información a medida que son transmitidos a través de la red. Si el CRC no se ajusta a lo enviado previamente, se define la información como corrupta. No existe indicación de cuan alterada se encuentra, ni si fue accidental o intencional, pero determina que es corrupta – no es la original y no puede ser presentada como prueba en la corte.



Exportación de vídeo IP

Para hacer uso de las grabaciones de vídeo de un sistema es necesario exportar el vídeo a otra computadora o medio de almacenamiento. El Reproductor de Archivos Bosch “Archive Player” se utiliza para extraer partes de vídeos ya grabados y almacenarlos en por ejemplo un disco. Se debe tener en cuenta que como el clip de vídeo se guarda como un simple dato, puede ser alterado. Una simple clave para proteger la integridad de este fragmento de vídeo es inadecuada, aunque es una buena primera medida de defensa.

Las firmas digitales son las utilizadas para detectar si el clip fue alterado.

Conceptualmente las firmas digitales son muy fáciles de comprender y a la vez extremadamente difíciles de descifrar o craquear. Típicamente una firma digital es un número muy largo, cuyo valor está influenciado por cada bit de datos del extracto o clip de vídeo. La firma es también reproducible, por cualquiera, lo que significa que el receptor puede recibir fragmento de vídeo, regenerar una firma digital del mismo y compararla con la firma entregada en el fragmento de vídeo

enviado en un primer momento. Si éstas son iguales todo se encuentra en orden, en caso de que esto no ocurra se puede concluir que el vídeo ha sido alterado. No tenemos idea de cuanto ha sido alterado – pueden ser un par bits, segundos o el vídeo completo. Sin embargo, sabemos que ha sido alterado y es inadmisibile para su presentación en la corte. Este sistema detectará si un cuadro del vídeo fue eliminado, o incluso si un píxel de un cuadro cambió.

El Reproductor de Archivos de Bosch “Archive Player” utiliza MD5 (Mensaje Cifrado de algoritmo 5) para generar las firmas digitales. Esta función de encriptación criptográfica “hash” mediante un algoritmo matemático, de 128 bits fue adoptada alrededor del mundo como un estándar de Internet (RFC 1321) ya que es rápida, confiable y no requiere ninguna clave secreta o llaves. Sólo confirma que se recibió exactamente lo que se había enviado anteriormente.

Aquí se puede ver una muestra de una firma de 128 bits – evoca el ADN de una huella digital:

```
010001001011010001110100011001110010101101001110001010101010000110001011010010101101001101000101111000101010010110101001010
```

La firma es siempre de la misma longitud sin importar el largo del clip de vídeo o el contenido del mismo y se altera por completo al cambiar una mínima parte. Por ejemplo, consideremos el MD5 de este texto corto en inglés (representado por un número hexadecimal de 32 dígitos y así permitir una lectura más sencilla en lugar de un número binario).

MD5 ("The quick brown fox jumps over the lazy dog") = 9e107d9d372bb6826bd81d3542a419d6

MD5 ("The quick brown fox jumps over the lazy dog.") = e4d909c290d0fb1ca068ffaddf22cbd0

Claramente obtenemos 2 firmas completamente diferentes al alterar una pequeña parte de la información, un simple ".", y esto ocurrirá aunque sólo se haya modificado un píxel en un cuadro del vídeo.

Resumen

Con las VCRs protegiendo la integridad del vídeo grabado, todo recaía exclusivamente en la confianza hacia las personas que tomaran contacto con los vídeos obtenidos. Asimismo, se asumía que el vídeo proveniente del cable coaxial (i) procedía de la cámara correcta (y no de una maliciosamente sustituida) y (ii) que no estaba siendo enmascarada en su camino a la VCR.

Con el vídeo IP, existe una combinación de mecanismos lógicos y físicos que provee niveles de seguridad de datos mucho más altos. Las redes IP poseen la encriptación incorporada, y pueden eliminar cualquier cámara que no aparezca en la lista de “direcciones MAC confirmadas”. Bosch aplica chequeos CRC a las tramas de red para confirmar que se recibió exactamente lo que se había enviado anteriormente y utiliza contraseñas para restringir el acceso de los usuarios al vídeo en vivo y grabado, el cual típicamente varía según un horario y nivel de acceso para incrementar la seguridad. Mas allá de esto Bosch añade la firma digital como función de encriptación criptográfica MD5 128 bits desde la misma cámara remota que genera la señal original hasta los vídeos exportados, esta marca de agua alerta si cualquier vídeo ha sido modificado en lo más mínimo.

Abril 2009

