UNIVERSIDAD NACIONAL AUTÓNOMA Đ MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN

Seguridad Multimedia:

Protección de la propiedad intelectual con técnicas criptográficas

TRABAJO ESCRITO BAJO LA MODALIDAD DE ALTO NIVEL ACADÉMICO QUE PARA OBTENER EL TÍTULO DE

INGENIERO EN COMPUTACIÓN

Presenta: Israel Andrade Canales

Asesor: José Luis Villarreal Benítez

MÉXICO **UNAM** **2008**

Agradecimientos

El siguiente escrito representa mi primera aportación de ideas y razonamientos que tienen como objetivo tomar la responsabilidad de fortalecer la cultura para crear un mejor país; responsabilidad que ha inculcado en mi la Universidad Nacional Autónoma de México.

Sin embargo, este esfuerzo se ha visto iluminado por mis padres Hilda Canales Guerreo y Javier Andrade Dircio; mis hermanos Ismael, Karina y Javier Andrade Canales; y mis amigos Ricardo, Luis, Adriana, Vanessa, Juan, Fabián, entre otros que no incluyo por que el margen de esta página es demasiado estrecho.

Por otra parte dedico un agradecimiento especial a Luis Ramírez Flores y a mi asesor José Luis Villarreal Benítez quienes durante la carrera motivaron mi gusto por el conocimiento y la verdad a través de la razón.

Finalmente, el presente escrito pretende servir para el trabajo de generaciones futuras.

Gracias.

IAC

Índice general

Prefacio

La ubicuidad de redes y computadoras, aunado a la alta penetración de herramientas para la producción de gráficos y audio, han favorecido un ambiente de comunicación multimedia y su integración en las Tecnologías de la Información y la Comunicación (TIC).

La tecnología multimedia sobre cómputo ubicuo traerá muchos beneficios en la Sociedad de la Información; principalmente implementando a través de ésta los cambios cualitativos, como la integración de diferentes áreas que a simple vista son totalmente diferentes, lo que permitirá generar nuevos paradigmas.

Sin embargo, aún se presenta mucha resistencia por los creadores y los usuarios ya que no se ha logrado un entorno de cómputo seguro. Esta incertidumbre sobre el mal uso y abuso de los contenidos, vulnera la protección intelectual y la certidumbre sobre la calidad de los contenidos.

Para lograrlo es necesario proteger a desarrolladores y usuarios. A desarrolladores dándoles la confianza de que sus trabajos no los podrán alterar, para cambiarles de nombre. A los usuarios dándoles la confianza de que los contenidos que están consultando son confiables.

Este problema es complejo y multifactorial, por lo que requiere –y de hecho se ha abordado- de soluciones de derecho, políticas, culturales y tecnológicas.

Las leyes que se han dado en nuestro país para proteger los derechos de autor, no han tenido los resultados esperados, un área como la tecnología es muy dinámica, cambia constantemente, por lo que si se toma el tiempo para discutir una ley, es probable que cuando se apruebe, sea obsoleta.

La cultura puede ayudar a que se respeten los derechos de autor, pero desafortunadamente en la actualidad no se cuenta con esa cultura, generar conciencia y cambiar las formas de pensar de la gente no es una tarea fácil.

La investigación y el desarrollo tecnológico, en cuanto a seguridad en imágenes y protección a los derechos de autor, han obtenido logros importantes. Las marcas de agua digitales y las técnicas criptográficas son un claro ejemplo, estas surgen precisamente como la solución para la protección de los derechos de autor en los archivos de datos multimedia, de esta forma se puede determinar quién es el autor, propietario, distribuidor autorizado, consumidor autorizado.

Hasta el momento han fallado todas; sin embargo, con una nueva perspectiva se pueden aprovechar algunas áreas, para poder atacar el problema de forma

conjunta. Para confrontar el problema se tienen que crear aplicaciones para proteger nuestros datos, pues con esta carencia nos encontramos desprotegidos ante cualquier ataque, pero estas aplicaciones deben diseñarse con un contexto cultural y legal. Por los inconvenientes anteriormente descritos se deben crear aplicaciones que confronten dichos problemas.

La tecnología y la cultura, son los puntos en los que se puede mejorar más rápidamente, siendo la tecnología un área en la que los cambios pueden ser más significativos. Esto se debe a su capacidad de cambio y su adaptabilidad en la sociedad informática y combinado con la cultura para crear una conciencia de protección y respeto a los derechos de autor, se potencian.

La apuesta está hecha en la tecnología y la cultura, por lo cual se desarrolló una aplicación que utiliza la tecnología para la protección de los derechos de autor en imágenes, a través de una estrategia multimedia que fomente el cambio cultural y sujeto a nuestras leyes (es importante que la tecnología preste sus servicios a las leyes, que le de herramientas para hacerla más eficaz y eficiente).

Por lo anterior la herramienta que se propone, realiza un primer acercamiento al utilizar técnicas criptográficas para implementar los servicios de autenticación de autores y contenidos; confidencialidad e integridad de los mismos; y el no repudio de derechos referentes a la propiedad intelectual establecidos por la ley federal del derecho de autor.

De esta manera se busca que las tecnologías de seguridad informática, como la criptografía, sirvan como herramienta para la aplicación de leyes y de esta manera generar una cultura que respete el uso adecuado de los contenidos multimedia y fomentar el desarrollo y el perfeccionamiento de más instrumentos que tengan la misma finalidad.

El resultante es un sistema que implementa políticas institucionales de seguridad y protección de imágenes. No se pretende hacer un estudio sobre cómo hacer inviolable una imagen, sino que el usuario destino sepa que fue alterada o vista por otra persona sin derechos de hacerlo; así como fomentar las buenas prácticas (tanto de respeto por la autoría de otros, como de previsión para protección de uno mismo) para alcanzar un cómputo seguro y confiable.

Capítulo I
Ambientes de cómputo seguro

La información siempre ha sido útil en nuestra sociedad debido a que este activo interviene en la toma de decisiones sobre las que posteriormente se toma algún tipo de acción. Sin embargo, el acceso, la divulgación y el manejo más democrático de la información que han facilitado los medios electrónicos en la actualidad le han dado valor agregado.

Esto se debe a que las tecnologías de la información y la comunicación (TIC) han facilitado el manejo de grandes cantidades de información en sus diferentes estados (creación, adquisición, almacenamiento, procesamiento y transmisión), propiciando que hoy en día la información se consuma principalmente en medios electrónicos, lo cual hace más versátil la información y más rentable a los medios.

Sin embargo, la información al ser más versátil y por ende más valiosa es un blanco de amenazas (robo, sabotaje, falsificación, etc.). Por otro lado, al ser más rentables los medios por su demanda, surgen tecnologías y diseños de baja calidad (mal diseño, errores de seguridad, etc.) que hacen vulnerable a la información.

Por lo que las virtudes de dichas tecnologías, paradójicamente también facilitan el abuso de la información dando lugar a problemas como el fraude electrónico, hostigamiento publicitario, robo de identidad, plagio y realización de copias ilegales de contenidos, entre otros.

Es por esto que surge la necesidad de trabajar en ambientes de cómputo confiable, los cuales son un conjunto de esquemas tecnológicos (ciencia e ingeniería) y sociales (leyes, educación) que reducen las amenazas a las tecnologías de la información (software, hardware y datos; y su interacción en redes, bases de datos, multimedia, etc.)

Para desarrollar ambientes de cómputo confiable es necesario conocer el problema de la seguridad en cómputo e identificar de qué manera son vulnerables las TIC; posteriormente conocer los mecanismos disponibles para la protección de la información en medios electrónicos.

Estos mecanismos no son exclusivamente de ciencia e ingeniería, también deben ser legales y sociales, porque el objetivo es reducir las posibilidades de que se comentan estos delitos. De esta manera, con leyes más claras y mejor definidas que pugnen dichos crímenes (**e-crime**), integrados con diseños,

implementaciones y metodologías de seguridad en el desarrollo de nuevas aplicaciones; y el desarrollo de una cultura de seguridad informática, se logra un ambiente de cómputo confiable.

Estos esquemas promoverán e incrementarán el impacto de estas tecnologías y el desarrollo de paradigmas del uso de la información que beneficiarán a la sociedad, por lo tanto, es elemental incorporar una cultura de seguridad informática en el desarrollo de esta nueva sociedad de la información.

El problema de la seguridad en las tecnologías de la información y la comunicación

Los recursos computacionales en los que se basan las TIC lo conforman básicamente tres componentes: hardware, software y datos. Por lo que para desarrollar ambientes de cómputo confiables es necesario distinguir qué tipo de vulnerabilidades, amenazas y ataques sufren estos componentes y de igual importancia, las personas que los utilizan.

En un sistema de cómputo, una **vulnerabilidad** es la debilidad de seguridad generada por una falla o deficiencia en el diseño, en la implementación y/o en su uso, que aumenta el riesgo de pérdidas o errores. De esta manera al conjunto de circunstancias o entidades que tienen la posibilidad de causar eventos de daño o pérdida de los recursos informáticos se les conoce como **amenazas.**

Las amenazas pueden manifestarse a través de eventos que explotan las vulnerabilidades del sistema de cómputo, los eventos que son realizados deliberadamente se llaman **ataques**.

Para entender la manera en que sucede esto es preciso clasificar la forma en que los ataques pueden comprometer un sistema de información. Los ataques se clasifican en cuatro subconjuntos según su manifestación: intercepción, interrupción, modificación y fabricación de los recursos informáticos (Fig. 1.1).

- Intercepción.- ocurre cuando un ente no autorizado ha obtenido acceso a un recurso.
- Interrupción.- se manifiesta cuando un recurso se torna no disponible o inutilizable.
- Modificación.- ocurre cuando una tercera parte no autorizada obtiene acceso a un activo y atenta su integridad.
- Fabricación.- ocurre cuando un atacante crea un activo espurio y lo hace pasar por genuino.

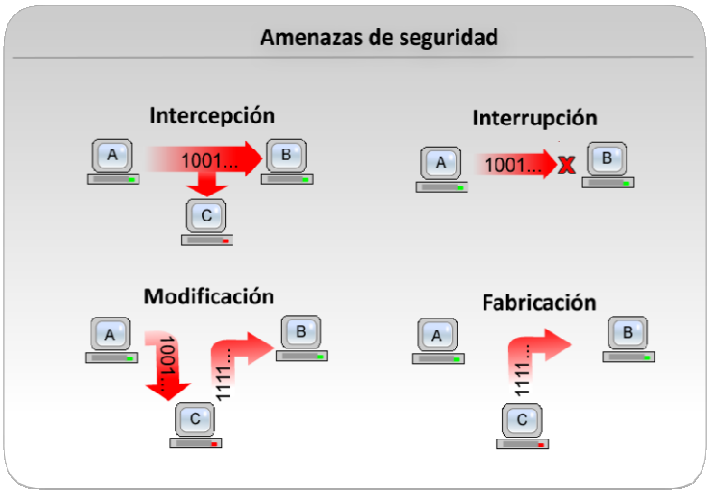

Figura 1.1 Amenazas de seguridad en cómputo.

Un ataque únicamente se puede realizar si posee de manera inherente un método, una oportunidad y un motivo. Siendo el método: las habilidades, el conocimiento y las herramientas para orquestar el ataque; la oportunidad: el tiempo y el acceso (vulnerabilidades) para completar el ataque; y el motivo: la razón para desempeñar el ataque en contra del sistema.

De tal suerte, si alguna de estas tres razones es denegada se puede evitar un ataque. Sin embargo el motivo y las habilidades del atacante difícilmente se pueden descartar, así que la tarea está en eliminar las oportunidades para que el ataque no se realice.

Por lo anterior, es preciso identificar qué tipo de vulnerabilidades generalmente dan acceso a los atacantes para comprometer los recursos informáticos.

Vulnerabilidades de hardware

El hardware es el conjunto de artefactos que conforman la parte física del sistema de cómputo, estos dispositivos se interconectan comúnmente a través de medios como cables y señales electromagnéticas, por lo que su seguridad puede ser comprometida al conectar dispositivos externos, desconectar dispositivos internos o interceptar sus comunicaciones.

Las amenazas de intercepción de hardware pueden ocurrir por diversos tipos de vulnerabilidades, las más frecuentes ocurren cuando existen deficientes perímetros de seguridad que provocan el robo de equipo de cómputo. Por otro lado, el ataque TEMPEST[1] es otro ejemplo de ataque de intercepción; el cual

[1] El término TEMPEST no es un acrónimo, es el nombre clave que se refiere a las investigaciones y estudios de emisiones electromagnéticas comprometedoras.

aprovecha la vulnerabilidad de los dispositivos electrónicos de fugar señales electromagnéticas al procesar la información.

La interrupción de los dispositivos del hardware es otro tipo de amenaza que ocurre cuando deja de funcionar algún dispositivo ocasionando la denegación de servicios (DoS). Este tipo de amenaza puede ocurrir de manera no deliberada a través de fallas en el suministro eléctrico o la destrucción de dispositivos por causas de fenómenos naturales. De esta manera es imposible garantizar la integridad del hardware, pero si disminuir las posibilidades de pérdida administrando los riesgos.

A diferencia de las amenazas anteriores, la fabricación y modificación de hardware son amenazas menos comunes pero igual de dañinas, ocurren cuando de manera deliberada se construye o se altera el dispositivo electrónico provocando errores de procesamiento y generando otras amenazas como la intercepción.

Vulnerabilidades de software

El software es la parte lógica de los sistemas de cómputo que principalmente controla y administra los recursos de hardware; y transforma los datos a información, por lo cual es recurso primario de ataques y amenazas como la modificación, interrupción, etc. (Cuadro 1.1).

La intercepción de software se manifiesta como la copia ilegal de software, este problema es muy común y no ha sido solucionado de manera satisfactoria, pues involucra aspectos legales y éticos.

Otro problema común de seguridad del software es la modificación, la cual se manifiesta a través de ataques realizados por “software malicioso” (**malware**) como virus, gusanos y troyanos que alteran la integridad del software; o bien códigos maliciosos que aprovechan las vulnerabilidades de los programas como: “puertas traseras” (**backdoors**), **rootkits** (combinación de programas para tomar el control principal del sistema) o **exploits** (código, datos o comandos que explotan vulnerabilidades).

De la misma manera, la fabricación de software espurio contribuye a que se vulneren los equipos de cómputo y la información que procesan. Esta amenaza surge porque generalmente no se autentican los programas, ocasionando que no se pueda garantizar que el software original sea el solicitado.

Por otro lado, la interrupción del software es ocasionada comúnmente por errores de uso por parte de los usuarios. Sin embargo, también es común que el malware sea el causante de la pérdida de este recurso.

Cuadro 1.1 Categorías de amenazas de software			
Tipo	Descripción	Propiedad comprometida	Objetivos
Interrupción	Suspensión de la ejecución de un programa. Degradación del desempeño de un programa. Eliminación del programa.	Disponibilidad	Denegación de servicio (DoS). Sabotaje.
Modificación	El software es alterado intencionalmente por una entidad no autorizada con código malicioso.	Integridad.	Acceso de privilegios. Obtener comportamientos que vulneren los controles de acceso. Obtención de información confidencial.
Intercepción	El software o parte del software es obtenido por una entidad no autorizada. Los detalles técnicos son revelados a través de técnicas de ingeniería inversa.	Control de acceso. Confidencialidad.	Crear una copia ilegal de software. Obtener conocimiento de la construcción del software para elaborar un ataque.
Fabricación	Un software espurio es creado para imitar las características de su original.	Autentificación.	Engañar al usuario para obtener información confidencial.

Cabe mencionar que la taxonomía de las vulnerabilidades de software ha sido una de las actividades más persistentes en la seguridad de software, la cual tiene como intención categorizar y clasificar las vulnerabilidades en un sistema para su identificación única y de esta manera anticipar el reconocimiento de fallas (Bishop y Bailey, 1996). Estos estudios iniciaron formalmente a principio de los años 70s con el proyecto "Investigación en sistemas operativos seguros" (RISOS por sus siglas en inglés) y actualmente se han presentado iniciativas sin que alguna de ellas sea formalmente un estándar (Landwehr *et al*., 1994).

Vulnerabilidades del recurso humano en las TIC

El recurso humano que utiliza las tecnologías de la información también es vulnerable a ataques que comprometen los recursos informáticos, incluyendo aquellos que ocurren de manera no deliberada. Estos ataques ocurren cuando los usuarios usan irresponsablemente el software, el hardware y los datos; cuando no se tiene una cultura de seguridad, o bien, cuando no se tienen los conocimientos adecuados para la administración de los recursos.

La ingeniería social es un ejemplo de ataque al recurso humano por falta de cultura de seguridad, se perpetra a través de utilizar el engaño y el convencimiento a los usuarios, con el motivo de obtener información importante; como contraseñas, programas, esquemas, etc. Este tipo de ataque constituye aproximadamente el 3.7% de los ataques a servidores en todo el mundo (www.zone-h.org, 2008).

Del mismo modo, la mala configuración de equipos es otro error común del personal de cómputo y constituye el 19.3% de todos los ataques a servidores (www.zone-h.org, 2008), lo cual lo coloca en el error de cómputo más utilizado para atacar los sistemas de información.

De esta manera, la suma de estos dos problemas de seguridad del recurso humano constituye un desfavorable 23% de los incidentes que ocurren con más frecuencia. ¿Cuál es el costo de las pérdidas con este 23%? Esta pregunta nos invita a reflexionar la importancia de una capacitación en el tema de seguridad informática tanto para los usuarios como para los administradores.

En conclusión, las vulnerabilidades que sufren el hardware, software, datos y el recurso humano involucrado en las TIC, son las deficiencias de seguridad que ponen en riesgo a la información, la cual es el activo fundamental que se gestiona. Es por esto que se necesitan esquemas donde intervengan medidas tecnológicas, legales y sociales que en conjunto protejan la confiabilidad de la

información. A estos esquemas se les denomina ambientes de cómputo confiable.

Cómputo confiable

La visión más común de seguridad en cómputo es la de aseverar que no existe sistema de protección inquebrantable, afirmación que resulta ser verdadera pero no alentadora. Por esto es importante considerar que aunque resulta ser cierto lo anterior, el trabajo se concreta en reducir el **riesgo**[2] de manera que la realización de un ataque sea impráctica y no viable.

Para realizar esta tarea se deben conectar los diferentes aspectos que intervienen en la seguridad informática: tecnología, leyes y sociedad de manera que el uso de la información en las TIC sea confiable. Esta conexión de tecnología, leyes y sociedad se logra a través de **políticas de seguridad**.

Estas políticas de seguridad se basan en la importancia o valor de la información, las leyes que regulan a la información y las características tecnológicas de los diversos ambientes de cómputo; y se definen en los diferentes estados de la información: creación, adquisición, almacenamiento, procesamiento y transmisión.

Por lo tanto estas políticas identifican las propiedades y cualidades que mantienen confiable a la información y su nivel de confianza necesarios para integrar los mecanismos de seguridad.

Posteriormente a conocer los mecanismos de seguridad que implementan la confiabilidad de la información, es necesario asegurar la confiabilidad del software, hardware y datos que intervienen en el ambiente de cómputo. Para lo cual se realiza el análisis de las vulnerabilidades de software, hardware y datos al diseño de esquemas que los interconecten de manera segura. Estos esquemas tienen que ser configurados de acuerdo a los distintos ambientes en los que operan las tecnologías de la información, por ejemplo el multimedia.

De lo anterior, el papel principal de la ingeniería en la seguridad informática es conocer y aplicar los principios de este ámbito (criptografía, esteganografía, patrones de ataque, etc.) y generar diseños que integren herramientas de manera eficiente, considerando situaciones legales, culturales, de costo, efectividad, necesidad e incertidumbre con el objetivo de mantener confiable a la información.

[2] La fórmula clásica para evaluar el riesgo es *Riesgo = Probabilidad de ataque * Tamaño de la pérdida.*

Propiedades y cualidades de la información confiable

La información se ve vulnerada cuando se atenta en contra de las propiedades y cualidades que la hacen confiable. Las propiedades fundamentales que definen la confiabilidad de la información son las siguientes:

- Integridad: es la propiedad que define que la información no carece de alguna de sus partes.
- Autenticidad[3]: es la propiedad que define que la información es genuina o verdadera.

Las cualidades que caracterizan a la información confiable son:

- Confidencialidad: es la cualidad que caracteriza a la información como reservada o secreta para las entidades no autorizadas.
- Disponibilidad: es la cualidad que define a la información como accesible y usable bajo demanda de una entidad.
- Responsabilidad: es la cualidad que caracteriza que la información se relacione con la acción o la entidad que la originó. Esta cualidad sirve para proporcionar la prueba ante una tercera parte autorizada que alguna entidad ha participado en algún evento.
- Accesibilidad: es la cualidad que caracteriza a la información como tratable, comunicable y usable.

Por lo cual, las acciones que resguardan o verifican las propiedades y cualidades de la información confiable son indispensables en un ambiente de cómputo confiable. Estas acciones se conocen como servicios de seguridad, por otra parte a los procesos que implementan dichos servicios se denominan mecanismos de seguridad.

Servicios y mecanismos de seguridad en dispositivos electrónicos

En cómputo, un servicio es un conjunto de una o más funciones, tareas o actividades realizadas para alcanzar uno o más objetivos que benefician a un usuario o proceso (IATAC, 2007).

[3] Del griego *αυθεντικός* = verdadero o genuino.

De esta manera, los servicios de seguridad (Fig. 1.2) son aquellas prácticas que protegen las propiedades y cualidades fundamentales para la seguridad. Estos servicios son un modelo de referencia para el diseño de una arquitectura de seguridad, de los seis, cinco están estandarizados por la Organización Internacional para la estandarización (ISO) (ISO 7498-2, 1988).

Figura 1.2 Servicios de seguridad.

1. Servicios de autenticación o autentificación[4]

   Estos servicios proporcionan la autenticación de las entidades en una comunicación (communicating peer entity) y de la fuente de datos ISO 7498-2, 1988).

2. Servicio de Integridad

   Es el conjunto de funciones y tareas que se desempeñan para saber (verificar) si la integridad de un recurso ha sido alterada o destruida de una manera no autorizada. Además este servicio puede incluir los mecanismos para recuperar el total o parte de la información perdida.

3. Servicio de no repudio

   Es el conjunto de funciones y tareas que se desempeñan para proporcionar la prueba, ante una tercera parte autorizada, de responsabilidad de la participación de cada entidad en una comunicación.

4. Servicio de confidencialidad

[4] Con este mismo sentido se ha creado modernamente el verbo *autentificar*, que se considera también válido; Diccionario panhispánico de dudas, "autenticar".

Estos servicios proporcionan la protección contra la revelación de datos no autorizada (ISO 7498-2, 1988).

5. Servicio de control de acceso.

   Es el conjunto de funciones y tareas que se desempeñan para prevenir el acceso no autorizado de un recurso, incluyendo la prevención del uso del recurso de una manera inadecuada.

Servicio de disponibilidad

Es el conjunto de funciones y tareas que se desempeñan para procurar la disponibilidad de un recurso bajo demanda de una entidad autorizada. Este servicio no está normalizado debido a la imposibilidad de asegurarlo a través de mecanismos de seguridad. Por lo que para lograr disminuir el riesgo de indisponibilidad es necesario implementar los servicios estandarizados.

Posteriormente, los servicios de seguridad deben ser implementados a través de mecanismos los cuales deben ser eficientes y eficaces. Por esto, las técnicas más utilizadas para implementar los servicios de seguridad son las criptológicas (criptografía y esteganografía, específicamente). Sin embargo, la implementación de estos mecanismos debe ser confiable, pues las vulnerabilidades de programación son generalmente la principal falla de estos.

Métodos de defensa del recurso humano

La cultura de seguridad informática es el conjunto de costumbres, conocimientos, hábitos y desarrollo tecnológico de seguridad en el uso de las tecnologías de la información. Por lo que su desarrollo no solo depende de las tecnologías. Por ello es importante que se concientice del uso de buenas prácticas para el manejo de las TIC

Estas prácticas abarcan desde el desarrollo de políticas y estándares hasta el compromiso de seguirlos, lo cual se refleja en la siguiente fórmula empírica de seguridad:

$$S = C\,[(P_L\,E\,F)^{2} + (P_R\,T\,H)]$$

Donde:

S representa seguridad.
C representa compromiso.
P_L representa políticas.
E representa estándares.
F representa esquemas de trabajo (Frameworks).
P_R representa procedimientos.
T representa las técnicas.

H representa Herramientas.

De esta manera, la fórmula anterior pondera el compromiso, los modelos y las metodologías indicando que si no hay compromiso, la seguridad es cero. Esto ocurre cuando no se siguen los protocolos establecidos o no se utilizan las herramientas para la protección de información valiosa.

La selección y administración de contraseñas por parte de los usuarios representa un caso clave para la seguridad debido a que los ataques que aprovechan las vulnerabilidades de contraseñas débiles, representan el 7.9% de los ataques a sistemas de cómputo.

Por otro lado, la instalación de software legal, software libre de calidad, software obtenido de fuentes autenticadas, la instalación de hardware autorizado y compatible son prácticas indispensables llevadas a cabo por los usuarios para el aseguramiento de los recursos informáticos.

Como se revisó anteriormente, la información confiable se ve vulnerada cuando las defensas de software, hardware, datos y el recurso humano involucrado en las TIC son deficientes, para solucionar este problema se han desarrollado métodos para disminuir las debilidades en cada uno de los elementos que conforman a un sistema de cómputo.

Métodos de defensa para hardware

Hoy en día se tienen diversos dispositivos electrónicos que proporcionan seguridad, entre ellos se encuentran tarjetas inteligentes que implementan criptografía, cableado que disminuye el riesgo de intercepción, elementos que filtran el tráfico de comunicaciones (cortafuegos) y dispositivos de almacenamiento que respaldan la información.

De la misma manera se han creado controles físicos de seguridad como circuitos cerrados de televisión, puntos de control de revisión, arquitecturas que disminuyen la fuga de emisiones electromagnéticas (generalmente con información importante), etc. Por lo tanto, se debe realizar un modelo físico adecuado de las tecnologías de la información y la comunicación para controlar las amenazas de hardware.

Métodos de defensa para software

Los métodos de defensa para el software confiable son mecanismos legales y técnicos que protegen la integridad del software y regulan el software de calidad.

En México, el aspecto legal no involucra normas que obligan la creación de software de calidad. Pese a este problema, sí se dispone de leyes que norman cualquier agravio en contra de su integridad y de su propiedad intelectual.

Estas leyes protegen a los programas de cómputo (sistemas operativos y aplicaciones) en su contenido (código fuente o código objeto), sus características y las funciones que realizan[5] . Además consideran como causal de infracción importar, vender, arrendar o realizar cualquier acto que permita tener un dispositivo o sistema cuya finalidad sea desactivar los dispositivos electrónicos de protección de un sistema de cómputo[6] (Parets, 2007).

Por otro lado, el aspecto técnico es esencial debido a que las vulnerabilidades de software constituyen más del 50% de los métodos de ataques en la actualidad (www.zone-h.org, 2008), provocando que sea la manera más frecuente de comprometer los recursos en cómputo.

Para evitar este escenario se han creado programas internos de control y de protección. Sin embargo la manera más adecuada de proteger el software es integrar metodologías de seguridad desde su diseño, es decir dentro del ciclo de vida para el desarrollo de software (SDLC por sus siglas en inglés).

Modelo de amenazas en el ciclo de vida del desarrollo de software (SDLC).

Requerimientos

En esta etapa es importante establecer o conseguir los requerimientos de seguridad y crear un esquema de casos de abusos que permitan la identificación de escenarios negativos en etapas futuras. También es recomendable la clasificación del valor e importancia de datos.

Diseño

En esta etapa es importante integrar mecanismos de seguridad en el diseño, valorar si el diseño del software no es vulnerable a niveles de riesgo inaceptables a través de un modelo de amenazas y utilizar estándares de seguridad para elevar la calidad del software.

El modelo de amenazas para el desarrollo de software consiste en representar los tipos de amenazas, sus puntos de entrada, los riesgos y las defensas con las

[5] Artículo 102 de la Ley Federal de Derechos de Autor.

[6] Artículo 231 de la Ley Federal de Derechos de Autor.

que cuenta el sistema y posteriormente implementar medidas necesarias para minimizar el riesgo.

Implementación

Algunas actividades en esta etapa son analizar y revisar que tipo de código es seguro y qué tipo de bibliotecas no son vulnerables, por ejemplo a los desbordamientos de buffer, puertas traseras, etc.

Pruebas

Es importante realizar durante esta etapa, pruebas de penetración y ataques deliberados (**Ethical Hacking**) para calificar los mecanismos de protección e identificar vulnerabilidades no contempladas.

Implantación

En esta etapa se debe valorar el impacto de la interacción con aplicaciones externas y valorar la seguridad en diferentes tipos de configuración.

Operación

Medir los problemas de seguridad existentes durante la operación para retroalimentarlos para versiones futuras del software.

Los beneficios de utilizar un modelo de amenazas durante el desarrollo del software son el incremento de la calidad del software y la confianza por parte de los usuarios. Las estadísticas son registros de lo que está pasando.

Métodos de defensa de datos

Como ya se revisó anteriormente, los datos son los elementos principales que conforman la información. Dentro de las TIC, estos datos son administrados por el software y comunicados a través de canales de comunicación o bien en medios físicos como papel. Es por esto que son necesarios mecanismos legales y técnicos que protejan sus propiedades.

En el aspecto legal hay que tomar en cuenta que existen leyes y normas referentes al manejo y almacenamiento de información digital importante (revisar Sarbanes-Oxley Act of 2002, 2002), que en sí mismas, estas leyes son mecanismos de defensa de datos para ambientes de cómputo confiable. Por lo que un sistema que maneje información de alta seguridad debe considerar estas normas.

En el aspecto técnico, la primera tarea que se debe considerar para realizar un modelo de defensa para los datos, consiste en modelar qué tipo de datos se almacenan temporalmente, a largo plazo o permanentemente en nuestro

sistema. Para ello hay que representar los datos que fluyen en el software, en los canales de comunicación e incluso fuera de estos.

Además se cuenta con modelos matemáticas que protegen la confidencialidad de los datos. El desarrollo de estos modelos de confidencialidad es una rama de las matemáticos llamada criptografía.

La criptografía es un aspecto importante para la protección de datos y las propiedades de la información confiable, ya que los datos bien disfrazados (galimatías) hacen que la información no sea entendible, modificable o fabricada fácilmente.

Por otra parte, la criptografía no solo aporta sistemas que protegen la confidencialidad de datos. También desarrolla modelos que implementan cuatro de los servicios de seguridad mencionados anteriormente, los cuales son: el servicio de autenticación, integridad, confidencialidad y control de acceso.

Capítulo II
Criptografía

La criptología es la disciplina que estudia y diseña sistemas de secreto para la ocultación de información, se divide en criptografía, criptoanálisis y esteganografía; en donde intervienen áreas del conocimiento de la ciencia, la matemática y la ingeniería.

La criptografía y la esteganografía tienen el objetivo de diseñar sistemas para la ocultación de información. Sin embargo, la criptografía oculta a través de transformaciones matemáticas (algoritmos) y la esteganografía encubre la información a través de embeberla en otro medio. En contraste, el criptoanálisis analiza los sistemas criptográficos para encontrar fallas que comprometan su eficacia.

Actualmente las técnicas criptográficas tienen un uso extendido en las comunicaciones, en las transacciones del comercio electrónico y en la protección de software y datos de las tecnologías de la información. Esto se debe a que los algoritmos y protocolos criptográficos desarrollados en décadas recientes, proporcionan los servicios de autenticación, confidencialidad, comprobación de la integridad y no repudio.

No obstante, las primeras técnicas de encriptación sólo proporcionaban el servicio de confidencialidad y eran desarrolladas manualmente o con la ayuda de máquinas no electrónicas. Estos mecanismos de cifrado utilizaban operaciones elementales como sustituciones o permutaciones del alfabeto para ocultar el mensaje y eran ampliamente usados para establecer comunicaciones seguras durante encuentros bélicos, o bien, para mantener en secreto información importante. Algunos ejemplos de estos criptosistemas son: El cifrado César, uno de los sistemas de cifrado por sustitución más conocidos y el cifrado Vigenère, un algoritmo de cifrado de sustitución poli alfabética del siglo XIX (ver cita; Pfleeger y Pfleeger, 2003).

Por su parte, el criptoanálisis ha evolucionado a la par de la criptografía, con técnicas que lograron “romper” con los primeros criptosistemas a través de las propiedades inherentes de los lenguajes como la redundancia de los símbolos y sus patrones. Estos sucesos tuvieron consecuencias que influyeron en hechos históricos como la segunda guerra mundial, pues se creé que los criptoanalistas británicos y americanos adelantaron 2 años el término de la guerra (Kahn, 1967).

La criptografía moderna comenzó cuando se construyó la base matemática de la teoría de la información y la comunicación con los trabajos de Claude Elwood Shannon (Shannon, 1948) el cual dió un soporte teórico a la criptología en general y a partir de ese momento se generaron criptosistemas que cambiaron el rumbo de la criptografía.

El interés en el uso de la criptografía por parte de la industria y de los sectores no militarizados como el bancario, orilló a que países como Estados Unidos estandarizaran un algoritmo criptográfico para el uso público. Fue así que la National Bureau of Standards (NBS) por sus siglas en inglés ahora conocido como (NIST), adoptó al algoritmo "cifrado de datos estándar" (DES por sus siglas en inglés) en 1976 (NBS, 1977), con el objetivo de regularizar el uso público de la criptografía.

Otro hecho que cambio la forma de hacer criptografía fue el desarrollo de la criptografía Asimétrica o de llave pública (Diffie y Hellman, 1976) y de esta manera nacieron conceptos como la firma digital, la integridad de datos y el no repudio.

Por su parte, el criptoanálisis moderno se enfocó en desarrollar técnicas como el criptoanálisis diferencial, el cual puso a prueba muchos algoritmos como DES, ocasionando que se fueran adoptando nuevos estándares y se reforzaran las técnicas criptográficas del momento. De esta manera, DES fue perfeccionado a triple DES y en 2001, el NIST adoptó el algoritmo AES (Advanced Encryption Standard) como nuevo estándar criptográfico (NIST, 2001).

Hoy en día han surgido una serie de algoritmos criptográficos fuertes que son utilizados ampliamente en mecanismos de encriptación, como RSA; un algoritmo de llave pública que forma parte del dominio público desde septiembre de 2000 y que hasta el momento se considera seguro en llaves mayores a 1024 bits, ya que supercomputadoras utilizadas por criptoanalistas han logrado "romper" con el algoritmo en llaves menores a los 640 bits (ver The RSA Factoring Challenge, www.rsa.com, 2007).

Aunado a esto, surgieron políticas para el uso y la exportación de criptografía, que causaron controversia en la utilización de la criptografía fuerte y la realización de herramientas que las implementen. Ejemplo de esta situación fue la restricción por parte de Estados Unidos de exportar criptografía mayor de 40 bits, antes de 2004.

En síntesis, el desarrollo de la criptografía moderna comienza sus pasos y transforma el modo en el que usamos las tecnologías de la información y la comunicación. Por su parte, el desarrollo tecnológico cambia la forma en que se diseñan los criptosistemas porque en general, estos dependen de la posibilidad computacional de realizar operaciones complejas.

Criptosistema

La criptografía se concreta a la elaboración de un criptosistema (Fig. 2.1) que define dos algoritmos. Un algoritmo de cifrado (E_k) que transforma un mensaje (m) a un mensaje secreto (C) a través de una llave (k) para definir la transformación del mensaje (m); y analógicamente un algoritmo de descifrado (D_k), que a partir de la función definida por una llave (k) particular, revierte el proceso.

La llave es un arreglo de bytes que entran en el criptosistema y sirve para transformar el mensaje llano en el texto cifrado. Donde la fortaleza del texto cifrado depende de la complejidad de dicha llave, es decir del tamaño del arreglo de bytes y la dificultad de adivinar cada bit del arreglo (aleatoriedad).

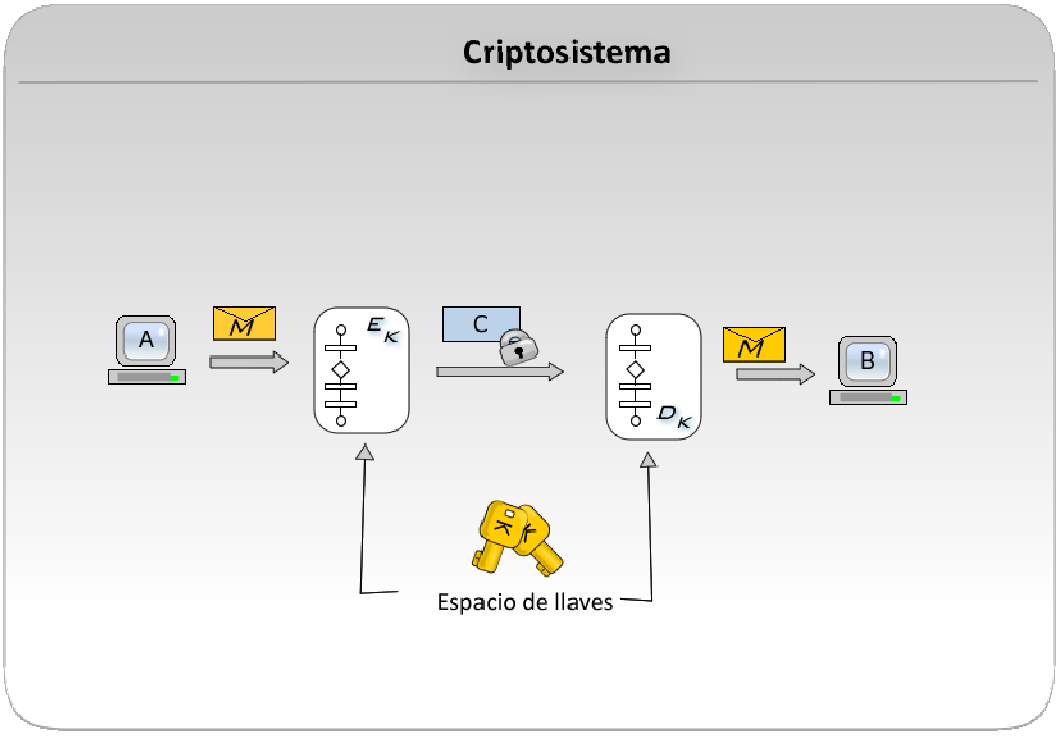

Figura 2.1 Criptosistema.

Estos criptosistemas se clasifican bajo diversos criterios, los más utilizados son por el número de llaves (espacio de llaves) y el otro por el modo de procesamiento. Por el número de llaves se clasifican en:

- **Algoritmos de llave simétrica o llave secreta:** la llave utilizada para cifrar y descifrar es la misma (una sola llave).
- **Algoritmos de Llave asimétrica o llave pública:** la llave que cifra es diferente a la que descifra (dos llaves diferentes).

- **Funciones Hash o algoritmos de digestión:** no requieren llave, por lo tanto el proceso de descifrado (D_k) no existe.

La importancia de conocer y clasificar estos algoritmos radica en identificar las "bondades" de cada tipo de criptosistema y utilizar los algoritmos adecuados para realizar protocolos y herramientas criptográficas que conectarán e implementarán los servicios de seguridad necesarios para el cómputo confiable.

Aunque cada llave depende del tipo de criptosistema y algoritmo, la administración segura de las llaves es una tarea importante en la utilización de cualquier criptosistema, por lo que es importante considerar:

- La protección de las llaves en el momento en que son utilizadas.
- El almacenamiento seguro cuando no son usadas.
- La sustitución de las llaves cuando han sido comprometidas (perdidas o copiadas).
- La variedad de tamaños y formas de las llaves dependiendo del criptosistema.

Primitivas criptográficas

Las primitivas criptográficas son los elementos principales que constituyen la criptografía moderna. Estas primitivas, junto con algoritmos, protocolos y estándares; implementan los mecanismos de seguridad.

De esta manera las primitivas criptográficas son los bloques más pequeños en la construcción de estructuras criptográficas más complejas. Estas primitivas son los algoritmos de llave simétrica o llave secreta; los algoritmos de llave asimétrica o llave pública; y los algoritmos de compendio, digestión o funciones Hash.

Algoritmos de Llave simétrica

Los algoritmos de llave simétrica como AES (ver Fig. 2.1.2) y triple DES basan su diseño en la combinación de transformaciones elementales como transformaciones y permutaciones, logrando eficiencia y rapidez en comparación con los algoritmos de llave asimétrica, por lo que su seguridad depende del tiempo y los recursos de computo. Es por esto que son empleados generalmente en:

- Cifrado de información no clasificada generalmente almacenada en medios electrónicos como discos duros.
- Autenticación en sistemas electrónicos.

Por el modo de procesamiento son:

- **Algoritmos de bloque:** el mensaje (M) se procesa en bloques del mismo flujo.
- **Algoritmos de flujo:** el mensaje se procesa como un todo.

Figura 2.1.2 Cifrado AES-128 de la imagen aragon.jpg.

En la Figura 2.1.2 se muestra el proceso de cifrado de llave secreta, en donde se cuenta con un archivo en claro (1) que se cifra utilizando el algoritmo AES a través de la biblioteca de programación OpenSSL y una contraseña que sirve para generar la llave secreta (2). El resultado de este proceso es un conjunto de datos inteligibles (3) que ocultan la información. Finalmente, los datos cifrados se pueden descifrar utilizando la misma llave (4) para obtener la información original (5).

Algoritmos de Llave asimétrica

Los algoritmos de llave pública como RSA o DSS son diseñados con base en la imposibilidad computacional de resolver problemas matemáticos como la factorización de números grandes (mayores de 100 dígitos). Por lo que su seguridad depende de la resolución de los problemas matemáticos. Generalmente se emplean para:

- Acordar llaves de criptografía simétrica.
- Firma digital.
- Cifrar información no muy grande o información clasificada como ultra secreta (necesitan tener un uso eficiente).

Funciones Hash

Los algoritmos de funciones Hash como SHA-1 ó MD5 (Fig. 2.2) poseen propiedades únicas al no contar con llaves de descifrado y son utilizados en combinación con los otros criptosistemas. Su seguridad se fundamenta en la imposibilidad computacional de encontrar la manera de ser reversibles, de manera que son fáciles de calcular pero difíciles de revertir su proceso. De esta manera dependen del tiempo y equipo de cómputo. Son utilizados para:

- Comprobación de la integridad de los datos.
- Normalizar índices de información a un mismo tamaño.
- Autenticación.

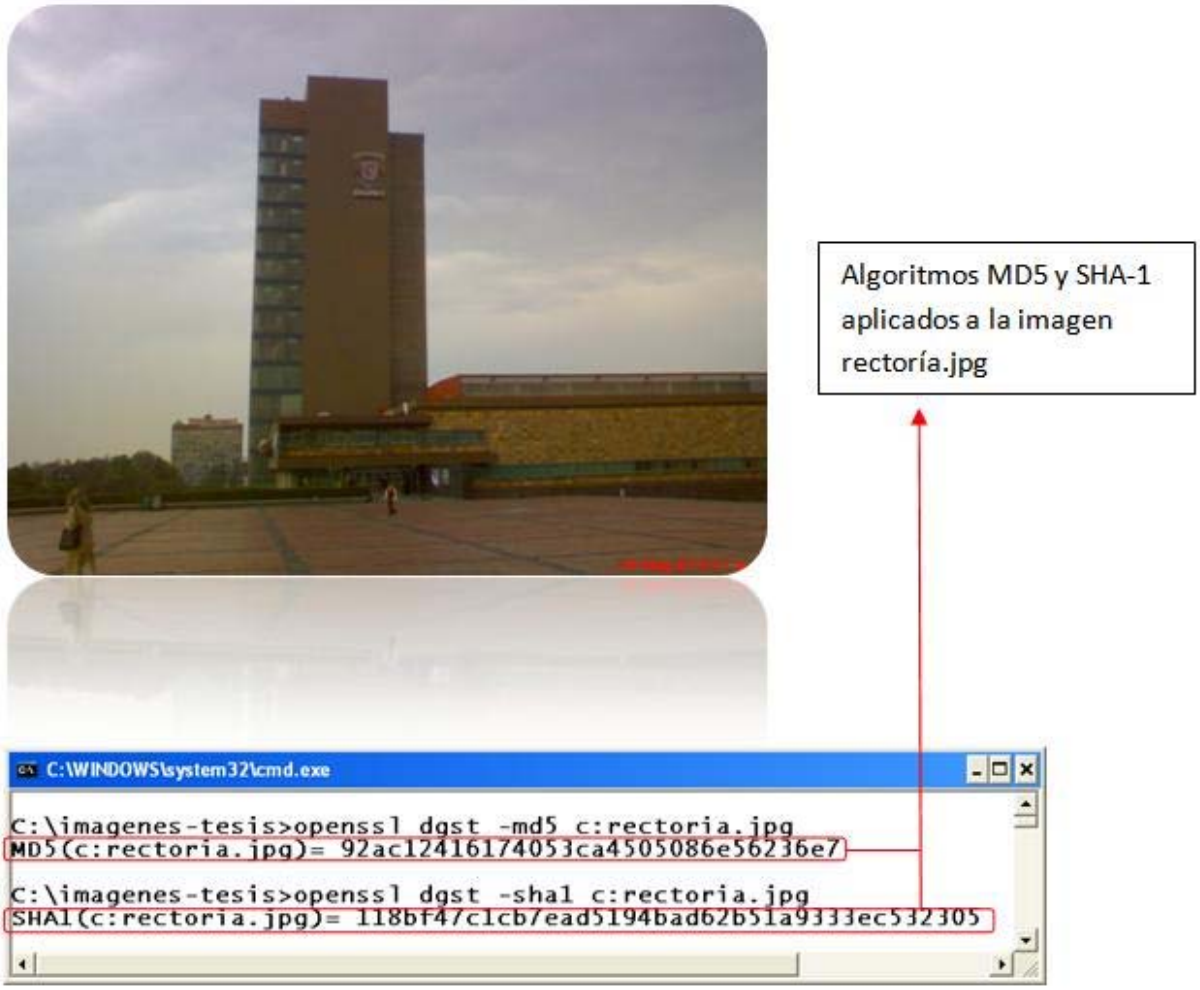

Figura 2.2 Algoritmos de Resumen.

Técnicas criptográficas

Los algoritmos criptográficos no proporcionan los servicios de seguridad por sí solos, es necesario desarrollar e implementar protocolos criptográficos que los conecten con otros algoritmos, procedimientos, estándares y especificaciones para realizar los servicios de autenticación, confidencialidad, integridad y no repudio (Cuadro 2.1).

Firma digital

La firma digital es un procedimiento criptográfico que incorpora algunas propiedades de la firma autógrafa relacionando un documento con una llave criptográfica. La idea básica es que la firma de un mensaje pueda ser creada por una persona y verificada por cualquiera.

Formalmente la firma digital es una transformación realizada por una función de firma F que relaciona al mensaje o documento (M) y una llave privada (Ek) que posee únicamente la entidad firmante. Se realiza aplicando una función de compendio al documento, la cual es cifrada con la llave privada del firmante, logrando de esta manera que el proceso de verificación se realice con la llave pública y que la firma digital brinde los servicios de autenticación, integridad y no repudio.

Además, la firma digital es dependiente del documento y computacionalmente imposible de imitar a partir de su llave pública. Situación que no ocurre con la firma autógrafa que es independiente del documento y es reproducible, ya que puede existir una persona con la suficiente habilidad para imitarla.

Actualmente se recomienda que la firma digital se implemente con la combinación de los algoritmos RSA – SHA1 ó bien DSS – SHA1 (Moyle Y Kelley, 2005), debido a que se han encontrado debilidades en el algoritmo de digestión MD5 (Wang *et al*., 2005) (Fig. 2.3).

Cuadro 2.1 Mecanismos de seguridad	
Autenticación	Protocolos criptográficos
Confidencialidad	Criptografía
Integridad	Funciones Hash (criptografía)
No repudio	Firma digital

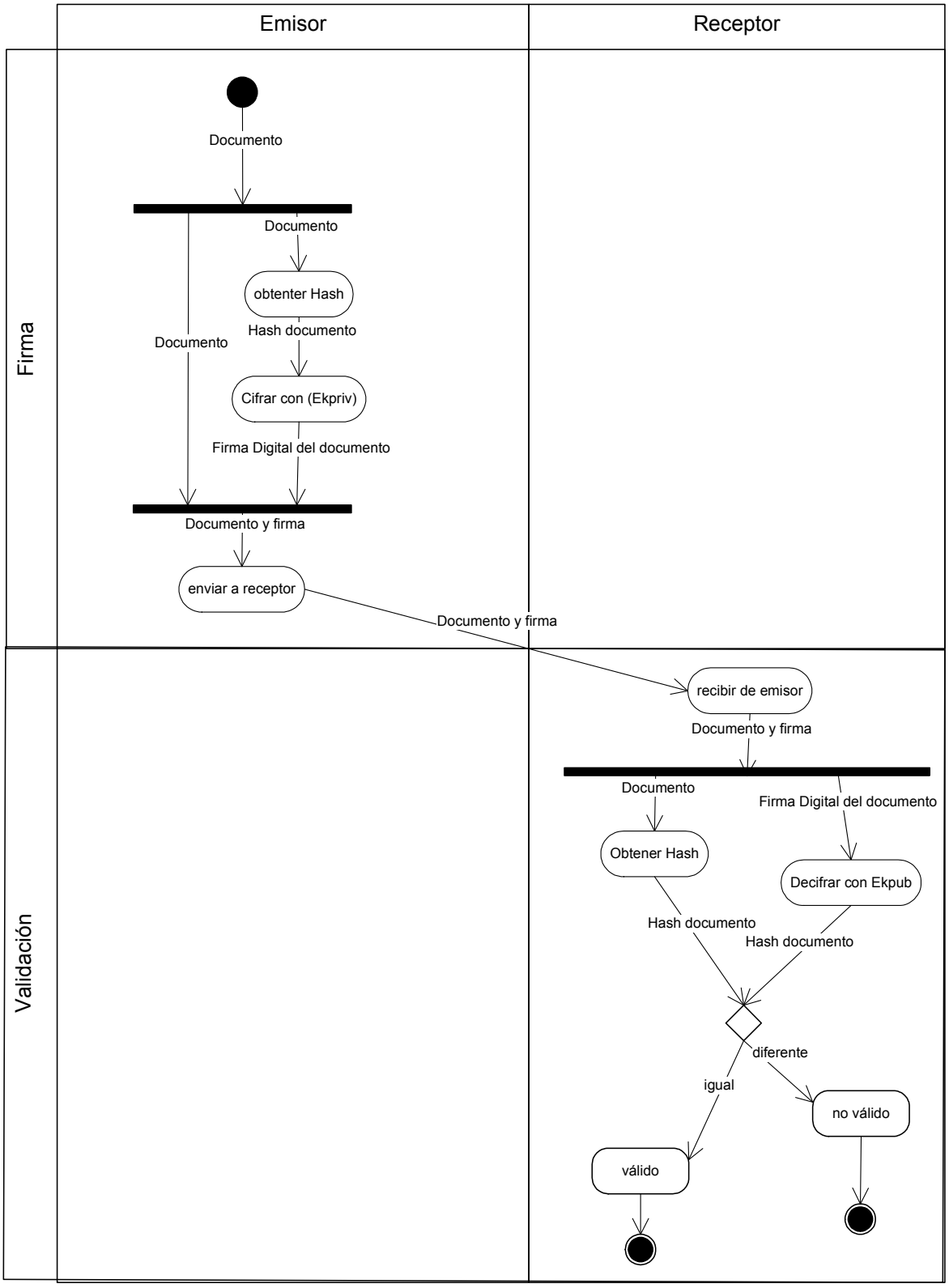

Figura 2.3 Diagrama de actividades UML de la firma.

Sin embargo, la implementación de la firma digital conlleva los problemas de la administración de llaves y la autentificación de la llave pública, dificultades inherentes en el cifrado asimétrico. Estos problemas surgen porque las llaves caducan o cambian y porque un atacante puede suplantar la llave pública (ataque por hombre en medio).

Es por esto, que surge el concepto de autoridad certificadora (AC), quien es un tercero confiable que autentica la llave pública a través de un certificado digital (CD), el cual es un documento digital que relaciona a una llave pública con su propietario.

Finalmente, el uso de diversas técnicas criptográficas como la firma digital se utiliza para construir capas de seguridad en los ambientes de cómputo.

Técnicas criptográficas en ambientes de cómputo

El uso de las técnicas criptográficas debe configurarse para los distintos ambientes de cómputo, por ejemplo: En las redes computacionales se implementan en el manejo de puntos de conexión (sockets), logrando así una capa de seguridad conocida como SSL (Secure Sockets Layer). De la misma manera en otras áreas de cómputo como: base de datos, sistemas operativos, multimedia, entre otras.

Capítulo III
Seguridad multimedia

En cómputo el multimedia es la integración transparente de texto, sonido, imágenes de todo tipo y software de control dentro de un único ambiente de información digital (Feldman, 1994). Por lo tanto es una obra derivada de diferentes tipos de contenidos digitales y del software que los integra; interviniendo de esta manera: autores, productores, diseñadores, programadores, usuarios finales y más personas en una misma obra multimedia.

Por lo tanto la obra multimedia es una producción colectiva, que requiere de un ambiente de cómputo que dé certidumbre en el uso adecuado de los recursos tecnológicos y artísticos; por ejemplo, la protección de los privilegios que posee cada uno de los creadores de la obra y el usuario final de la misma.

De lo anterior, la **seguridad multimedia** es el conjunto de mecanismos (tecnológicos, legales y sociales) que intervienen para el desarrollo de un ambiente confiable en la tecnología multimedia. Es decir que el objetivo de la seguridad multimedia es proteger a través de la tecnología y con un respaldo legal contra el abuso de los contenidos, a las tecnologías empleadas y a las personas involucradas en la creación, producción, venta y uso de las obras multimedia.

En el aspecto legal, los contenidos como la fotografía y la música pueden reflejar cualidades impresas por decisiones del autor que definen su originalidad e interpretación, cualidades protegidas por el **derecho de autor**.

De la misma manera, el multimedia puede ser una obra colectiva que contiene una obra original y obras derivadas que en ocasiones poseen permisos explícitos y no explícitos. Por lo tanto, un objetivo muy importante para la seguridad multimedia corresponde en diseñar mecanismos que logren que la tecnología ayude en la aplicación de los mecanismos legales para la **propiedad intelectual**.

Además estos contendidos interactúan dinámicamente con otros contenidos de forma transparente siguiendo un guión de presentación, siendo necesario proteger la obra; así como su presentación.

Por lo que la perspectiva técnica de la propiedad intelectual se puede visualizar como un conjunto dinámico de políticas de manejo de los contenidos, las cuales son definidas por varias entidades como el autor, coautores y titulares; cada uno de ellos con roles y permisos diferentes del contenido.

Esta característica de la propiedad intelectual de los contenidos; sumado al dinamismo y versatilidad que tienen las obras multimedia, originan que los mecanismos de protección deban ser: seguros, dinámicos y flexibles.

La flexibilidad de los mecanismos se ve delimitada por las cualidades técnicas con las que son implementadas las obras multimedia. Por ejemplo, en ocasiones, los contenidos son tolerantes a pérdida de datos siempre y cuando no afecten significativamente su calidad porque algunos contenidos son más prioritarios que otros, lo que obliga a que los mecanismos de seguridad deban ser eficaces en su objetivo, pero flexibles a esta característica.

Marco legal de la seguridad multimedia: Propiedad Intelectual de los contenidos multimedia

La propiedad intelectual es el conjunto de mecanismos legales que protegen las creaciones del intelecto humano. Se divide en el derecho de autor; que protege las obras literarias y artísticas, así como las creaciones en el campo de los denominados "derechos conexos" y la propiedad industrial; que protege las invenciones (OMPI, 2007).

Estos mecanismos sirven para incentivar la creación y la invasión a través de la originalidad y no de la copia. La **originalidad** es la impresión de las características del autor en la creación o invención, que en su conjunto reflejan la personalidad o la inventiva de este.

Sin embargo, el derecho de autor, protege únicamente la expresión de las ideas y no a las ideas, procedimientos, métodos de operación o conceptos matemáticos en obras como: libros, pinturas, fotografías, programas de cómputo, entre otras.

Por otro lado, la propiedad industrial protege a las ideas nuevas que dan solución a un problema técnico, las cuales no necesitan estar representadas en un elemento físico.

De lo anterior, el derecho de autor es un mecanismo que protege la expresión de las ideas (presentación) en la obra multimedia y la expresión de las ideas en los contenidos que la integran. Y se otorga desde la incorporación de letras, números, signos, sonidos, imágenes y demás elementos en que se haya expresado la obra, o de las representaciones digitales de aquellos, que en cualquier forma o soporte material, incluyendo los electrónicos, que permiten su percepción, reproducción u otra forma de comunicación (ver Ley Federal Del Derecho De Autor, LFDA, 2003).

El derecho de autor en la seguridad multimedia

Jurídicamente, el derecho de autor es el reconocimiento que hace el Estado en favor de todo creador de obras literarias y artísticas, en virtud del cual otorga su protección para que el autor goce de prerrogativas y privilegios exclusivos de carácter personal y patrimonial. Los primeros integran el llamado derecho moral y los segundos, el derecho patrimonial (ver Ley Federal Del Derecho De Autor, LFDA, 2003).

Los **derechos morales** son los privilegios inalienables, imprescriptibles, irrenunciables e inembargables que posee el autor con su obra, los cuales son los siguientes:

1. Derecho de paternidad de la obra: es el reconocimiento de la calidad de autor en todo momento y en todo acto de reproducción. Relaciona la obra con el autor (su nombre, pseudónimo o anónimo).
2. Derecho de Integridad: es el privilegio que tiene el autor de exigir el respeto a su obra en la forma en que fue concebida y creada, es decir, el derecho a oponerse o aprobar la deformación, modificación o mutilación de la obra.
3. Derecho de divulgación de la obra: es el privilegio que tiene el autor a decidir que su obra sea divulgada o permanezca en forma inédita (que no sea pública).
4. Derecho a retirar la obra del comercio: es el derecho a decidir que la obra no sea objeto de explotación (retirar la obra del comercio).

De la misma manera, los **derechos patrimoniales** son los privilegios del autor de explotar de manera exclusiva sus obras, o de autorizar a otros su explotación, en cualquier forma, dentro de los límites que establece la presente Ley y sin menoscabo de la titularidad de los derechos morales (tomado de; LFDA, 2003).

De lo anterior, los titulares de los derechos patrimoniales podrán autorizar o prohibir:

1. La reproducción, publicación, edición o fijación material de una obra en copias o ejemplares, efectuada por cualquier medio ya sea impreso, fonográfico, gráfico, plástico, audiovisual, electrónico, fotográfico u otro similar.
2. La comunicación pública de su obra a través de cualquiera de las siguientes maneras:

    a) La representación, recitación y ejecución pública en el caso de las obras literarias y artísticas.

b) La exhibición pública por cualquier medio o procedimiento, en el caso de obras literarias y artísticas.

c) El acceso público por medio de la telecomunicación.

3. La transmisión pública o radiodifusión de sus obras, en cualquier modalidad, incluyendo la transmisión o retransmisión de las obras por

   a) Cable

   b) Fibra óptica

   c) Microondas

   d) Vía satélite

   e) Cualquier otro medio conocido o por conocerse

4. La distribución de la obra, incluyendo la venta u otras formas de transmisión de la propiedad de los soportes materiales que la contengan, así como cualquier forma de transmisión de uso o explotación. Cuando la distribución se lleve a cabo mediante venta, este derecho de oposición se entenderá agotado efectuada la primera venta, salvo en el caso expresamente contemplado en el artículo 104 de esta Ley.
5. La importación al territorio nacional de copias de la obra hechas sin su autorización.
6. La divulgación de obras derivadas, en cualquiera de sus modalidades, tales como la traducción, adaptación, paráfrasis, arreglos y transformaciones.
7. Cualquier utilización pública de la obra salvo en los casos expresamente establecidos por la Ley.

Marco tecnológico de la seguridad multimedia

Técnicas criptográficas en multimedia

Las técnicas criptográficas en el multimedia tienen la función de aplicar las primitivas criptográficas junto con técnicas de procesamiento de imagen, video, audio; protocolos criptográficos y estándares para la implementar los servicios de seguridad en las aplicaciones y en los contenidos multimedia.

Hay que tomar en cuenta que los servicios de seguridad tienen características específicas en el ámbito multimedia, por ejemplo una característica del multimedia es que es tolerante a la pérdida de datos en ciertas circunstancias,

por lo que el servicio de integridad debe ser adaptado a esta exigencia, por ejemplo:

- Los contenidos pueden estar en diferentes formatos con diferentes características (a veces hay que transformalos).
- Los contenidos pueden estar distribuidos en diversos medios por ejemplo: el reproductor (player); el software que ejecuta el guión, puede estar en una computadora diferente a la de los contenidos.
- Los contenidos pueden viajar por diferentes medios o canales de comunicación.
- El software multimedia puede tener la exigencia de procesar imágenes de manera eficiente al mismo tiempo que audio y datos.
- Los canales pueden tener la exigencia de transmitir información en tiempo real.
- Los contenidos pueden estar almacenados en hardware especializado como reproductores de audio y video.

Es decir, la eficacia y la eficiencia de estas técnicas criptografías puede comprometerse por dichas particularidades, por lo que algunas de las cualidades que se requieren considerar son:

- La complejidad de la técnica de cifrado.

  Esta característica impacta directamente en la rapidez del proceso de cifrado, descifrado y generalmente en la seguridad del criptosistema.

- La degradación del contenido a consecuencia de la técnica criptográfica.

  Esta característica impacta en la calidad del contenido según la técnica criptográfica[7].

- La resistencia de la técnica criptográfica a la tolerancia de error.

  Esta característica impacta en el tipo de criptosistema a elegir.

Para disminuir la complejidad de la técnica de cifrado en un entorno multimedia se puede procesar la información en algoritmos de compresión y de esta manera disminuir la cantidad de datos que se cifran. Este proceso de compresión y cifrado se puede realizar de las siguientes maneras:

[7] El problema de la degradación depende de las técnicas de procesamiento de datos que conforman la técnica criptográfica.

a) El contenido se cifra y posteriormente se comprime: Este proceso no disminuye significativamente la complejidad del cifrado además de disminuir la eficiencia del proceso de compresión. Sin embargo la seguridad del contenido es significativa.

b) El contenido se comprime y posteriormente se cifra: este proceso disminuye la complejidad de cifrado además de mantener seguro el contenido.

c) El contenido sufre una transformación, posteriormente se comprime y se cifra: este proceso disminuye la complejidad del proceso de cifrado significativamente, sin embargo la compresión y la seguridad dependen del tipo de transformación del contenido.

Sin embargo, en cualquiera de los tres procesos anteriores, el contenido original no puede ser entendible hasta revertir el proceso, el cual involucra a todo el contenido. Es por esto que se manejan esquemas donde solo partes del contenido son cifradas y de esta manera se pueden entender los encabezados de los contenidos y el proceso inverso es menos costoso.

Cifrado selectivo de contenidos (Selective encryption)

Es la técnica criptográfica que cifra sólo parte de los datos y el resto permanece en claro con el objetivo de reducir el tiempo empleado para el descifrado de grandes cantidades de información. Esta técnica es empleada principalmente en aplicaciones en tiempo real que transmiten grandes cantidades de información como video conferencia y videoteléfono.

Existen diversos esquemas de cifrado selectivo que dependen del contenido y cuáles de sus elementos se cifran, algunos de los esquemas más comunes son los que se enlistan en el Cuadro 3.3 (adaptado de Liu & Eskicioglu, 2003).

Ventajas:

- El tiempo de descifrado es menor.
- El tamaño del flujo de datos original pocas veces es variable.

Desventajas:

- Hay un decremento en el nivel de seguridad.
- Hay un decremento en la tasa de compresión del contenido.
- En algunos esquemas se pierde la compatibilidad con los estándares actuales.

En resumen, las técnicas criptográficas empleadas para la protección de la información multimedia deben ser eficientes para sus particularidades, esto ocasiona que se deban manejar diversas técnicas de procesamiento a los

contenidos además de seleccionar las técnicas criptográficas más adecuadas. Este problema compromete la seguridad de los contenidos cuando se necesita que el proceso de descifrado sea menos costoso.

Cuadro 3.3 Esquemas de cifrado selectivo			
Medio	Dominio	Elemento cifrado	Algoritmo de cifrado
Imagen	Frecuencia	Pixel set related significance information in the two highest pyramid levels of SPIHT	No especificado
		Los bits que indican el signo y la magnitud de los coeficientes diferentes de cero de la DCT.	DES, tripleDES e IDEA
		Estructura de la sub-banda de descomposición	AES
	Espacio	Estructura Quadtree	No especificado
		Mapa de bits menos significativos	XOR
		Mapa de bits más significativos	AES
Video	Frecuencia	Cabeceras, pates de los I-blocks, todos los I-blocks, I-frames del flujo MPEG	DES, RSA
	Espacio	I-frames, sequence headers and ISO end code of the MPEG stream	DES
		Coeficientes de la DCT	Permutaciones, DES
		Cada bit alternado del flujo de datos	XOR, premutaciones e IDEA
		Bit de signo de la DCT	XOR
		Bits de signo de los vectores de movimiento	IDEA
		Every nth I-macroblock, headers of all the predicted macroblocks, header of every nth predicted macroblock	DES
		Pixel and set related significance information in the two highest pyramid levels of SPIHT in the residual error	Ningún algoritmo especificado
		Selective bit scrambling, block shuffling, block rotation of the transform coefficients (wavelet and JPEG) and JPEG motion vectors	Permutación, XOR
		Quadtree structure of motion vectors and quadtree structure of residual Errors	Ningún algoritmo especificado
	Códec de Entropía	Encryption of data by multiple Huffman coding tables and multiple state indices in the QM coder	Multiple Huffman tables, multiple state indices in the QM coder

Aunado a esto, las técnicas de criptoanálisis en multimedia no solo atacan las deficiencias del algoritmo de cifrado, generando que el contenido sea recuperado al romper el algoritmo (criptoanálisis completo). También es posible que se recupere perceptualmente un contenido con una calidad aceptable (criptoanálisis perceptual) u obtener parte de la información del contenido sin necesidad de recuperar la llave (criptoanálisis local).

Esto se debe a que los ataques no solo explotan las vulnerabilidades de los criptosistemas, también las vulnerabilidades de las técnicas criptográficas para el multimedia, como las correlaciones que existen entre las diferentes porciones de un mismo contenido en el cifrado selectivo o bien ocultando de la vista las porciones cifradas para lograr un ataque perceptual.

Otros mecanismos de seguridad no criptográficos

Existen diferentes mecanismos no criptográficos útiles para la protección de contenidos digitales, estos mecanismos son tecnologías no criptográficas que en combinación con los mecanismos criptográficos dan el soporte tecnológico a la seguridad multimedia.

Entre estos mecanismos se encuentran:

- Marcas de agua digital.
- Metadatos.

Marca de agua digital

La marca de agua digital es una técnica esteganográfica que tiene como objetivo prestar los servicios de autenticación e integridad de contenidos digitales. Funciona introduciendo información referente a la autoría de los datos dentro del mismo contenido digital. De esta manera se puede demostrar su autenticidad e integridad al revisar que la marca de agua exista y que no haya sido alterada.

Para introducir una marca de agua en un archivo digital es necesario realizar transformaciones al contenido original aprovechando el mismo canal de comunicación para incrustar la marca de agua. Por lo tanto es una técnica adecuada para los diferentes tipos de contenido multimedia. Por ejemplo las imágenes, el video, texto y sonido.

Metadatos

Los metadatos son otro tipo de esteganografía que permite la inserción de información dentro de un archivo digital. La función principal es almacenar información referente al mismo archivo digital (meta información). A diferencia

de la marca de agua, los metadatos no se incrustan en el mismo canal de comunicación, sino en estructuras bien definidas dentro del formato del archivo digital.

Por lo tanto, los metadatos son una tecnología que puede ser utilizada para almacenar datos referentes a la seguridad del recurso digital que los contenga.

Seguridad informática en el uso de los contenidos multimedia

Finalmente para crear una conexión entre el aspecto legal y social del uso de los contenidos multimedia con la seguridad informática, se pueden relacionar los servicios de seguridad expuestos en el primer capítulo (autenticación, integridad, confidencialidad, no repudio, control de acceso y disponibilidad) con los derechos morales y patrimoniales otorgados al autor de un contenido multimedia (Cuadro 3.1).

Cuadro 3.1 Políticas de seguridad a través de derechos morales

Derecho de autor	Políticas de seguridad	Propiedades de seguridad	Servicios de seguridad
Derechos morales	Derecho de paternidad	Responsabilidad (relaciona al autor con los bits de la imagen)	No repudio
	Derecho de integridad	Integridad	Integridad
	Derecho de divulgación	Confidencialidad	Confidencialidad
	Derecho de comercialización	Disponibilidad	Disponibilidad

De tal manera que los derechos morales sirven como un conjunto de **políticas dinámicas de seguridad** (variables según las conveniencias del autor) que

impactan en los mecanismos de seguridad que se implementan para hacer funcionales dichos privilegios.

Por otro lado, los derechos patrimoniales especifican la manera en que la obra puede ser explotada especificando los controles de acceso de los recursos (Cuadro 3.2).

Cuadro 3.2 Controles de acceso a través de derechos patrimoniales

Derecho de autor	Políticas de seguridad	Propiedades de seguridad	Servicios de seguridad
Derechos patrimoniales	Derecho de fijación de copias	Autenticación Responsabilidad Accesibilidad Disponibilidad	Autenticación No repudio Control de acceso
	Derecho de comunicación pública	Accesibilidad confidencialidad	Control de acceso
	Derecho de transmisión pública	Disponibilidad Accesibilidad	Control de acceso
	Derecho de distribución (venta)	Disponibilidad Accesibilidad	Control de acceso
	Derecho de traducción, adaptación, paráfrasis, arreglos y transformaciones.	Integridad Accesibilidad	Control de acceso

De esta manera, el mapeo entre las políticas de uso (creadas por los derechos de autor y el modelo de negocio o contrato de uso) y la seguridad informática permite establecer qué mecanismos (como la criptografía, las marcas de agua y los metadatos) son adecuados para proteger un contenido multimedia.

De lo anterior se puede concluir que se requieren de herramientas que sean capaces de gestionar las políticas de uso de los contenidos multimedia, protegerlos y así, difundir el uso correcto de las tecnologías multimedia.

Capítulo IV
Diseño e implementación a través de software

Como se revisó anteriormente, el caso de la piratería informática ha provocado la desconfianza en la tecnología, específicamente donde se afectan los derechos de autor. Por otro lado, no existe una conexión clara entre esta tecnología y los aspectos legales del derecho de autor, menos aún, un esquema donde se fomente la cultura del uso correcto de la tecnología y la propiedad intelectual de los contenidos.

Es por esto que en este trabajo se presentan metodologías y técnicas para la protección de la propiedad intelectual (en objetos multimedia), así como una aplicación que implemente servicios de seguridad dentro de una Interfaz gráfica, con el objetivo de fomentar el uso de herramientas simples, generar una cultura del cómputo seguro e implementar políticas o prácticas y procedimientos de seguridad multimedia institucionales u organizacionales.

En este primer desarrollo se propone un mecanismo que englobe un conjunto de técnicas y metodologías de alta disponibilidad, con el objetivo de proporcionar servicios de seguridad para la protección de la propiedad intelectual y de contenidos multimedia, promoviendo de esta manera una cultura que respete la autoría de los contenidos.

Objetivos del proyecto

1. Utilizar la tecnología de metadatos, técnicas criptográficas y esteganográficas para la protección de contenidos multimedia.
2. Verificar la integridad de contenidos multimedia.
3. Uso de firmas digitales en los contenidos.
4. Marcado de agua.
5. Lectura y edición de metadatos con un estándar con alta disponibilidad.

Metas del proyecto:

1. Gestión de políticas de uso: lograr que el sistema permita implementar políticas institucionales correspondientes al uso de obras multimedia.

2. Protección: servir como una herramienta útil para la protección de la propiedad intelectual.

3. Difusión:

    - Fomentar una cultura de seguridad en el uso de medios digitales.

    - Conseguir que la funcionalidad del sistema sea la adecuada para transacción y verificación del comercio multimedia.

Descripción del proyecto

Esta primera fase del proyecto abarca los contenidos en imágenes compatibles con el estándar Exif, ya que es un estándar que tiene alta disponibilidad y compatibilidad; también combina esta tecnología con técnicas criptográficas y de marcado de agua.

El proyecto de desarrollo (ver Fig. 4.2) incluye componentes que prestan los servicios de seguridad y una aplicación gráfica que implementa los procedimientos de seguridad multimedia. Esta aplicación está diseñada para facilitar la seguridad multimedia a través de una metáfora multimedia. La intensión es fomentar las buenas prácticas de seguridad en multimedia, dentro de un entorno de cómputo confiable; para ello la interfaz gráfica promueve con su diseño (priorización y señalización de metadatos), registro de niveles de seguridad (señalización, ayuda y recomendaciones sobre áreas sensibles) en los contenidos, e interactividad con modelos de usuario (ayuda para alcanzar los objetivos de seguridad del usuario).

El uso de metadatos en la primera etapa responde a la facilidad de adquisición, ya que los fabricantes de cámaras digitales incluyen un chip que genera automáticamente las etiquetas en el estándar usado. Esto permite que el usuario aproveche esta tecnología como una primera aproximación o introducción a la seguridad multimedia. Para fomentar y explicar prácticas más sofisticadas, rigurosas, pero también más exigentes o complicadas, la aplicación maneja niveles de seguridad que se consiguen con técnicas criptográficas sobre las etiquetas de metadatos y técnicas de marcas de agua robustas.

Requerimientos de la aplicación

Gestión de políticas de uso, esto es:

1. Definir a las personas que intervinieron en la obra digital, por ejemplo: autor, coautor, editor, etc. Además de los privilegios que tienen con la misma.

2. Definir políticas de uso de la obra multimedia como: política de copia, distribución, obra derivada, etc.

3. Colocar candados de seguridad como: firma digital, marcado de agua digital, restricción de copias, para asegurar las políticas.

4. Evaluar si los mecanismos de seguridad son los convenientes y notificar posibles fallos de seguridad.

5. Verificar los malos usos de los contenidos digitales.

Funcionalidades

(ver Fig. 4.1)

1. Capacidad de abrir y procesar colecciones de contenidos multimedia.

2. Capacidad de definir a las personas involucradas en una obra multimedia y definir sus privilegios sobre la misma.

3. Capacidad de definir, editar o eliminar políticas de uso y asociarles un mecanismo de seguridad, los cuales son:

    a. Inspección de la integridad del contenido al conocer si ha sido modificado inadecuadamente, registrar la última fecha de modificación, las veces que ha sido alterado el original y las veces que se ha realizado una copia.

    b. Restricción visual de contenido al ocultar los bits de la imagen a las personas no autorizadas.

    c. Autenticar a través de una firma digital a las personas con privilegios sobre la obra.

    d. Capacidad de reconocer al dueño de una copia del contenido multimedia

e. Capacidad de transformar la obra digital (reducción de dimensiones, colores o resolución) y regresar al estado original a través de contraseña.

f. Realizar un marcado de agua digital robusto, capaz de resistir escaneo o “pantallazo”.

g. Capacidad de restringir la visión de las características importantes del contenido digital a las personas no autorizadas para preservar originalidad.

4. Capacidad de mostrar las propiedades del contenido digital como sus propiedades, comentarios e información referente.

5. Capacidad de mostrar las políticas de uso a través de un manifiesto integrado al archivo multimedia, con el objetivo de que el usuario al leerlo conozca las políticas de uso.

6. Contar con indicaciones que orienten al usuario acerca de:

    a. Qué tipo de políticas de uso puede ingresar (estas se basarán con las de la propiedad intelectual).

    b. Qué tipo de obligaciones tiene el usuario de acuerdo a las políticas de la imagen.

    c. Explicar la utilidad y cómo usar cada mecanismo de seguridad.

Indicar de que tipos de abusos fue objeto un contenido multimedia, y explicar cómo funciona la evidencia de tal incidente.

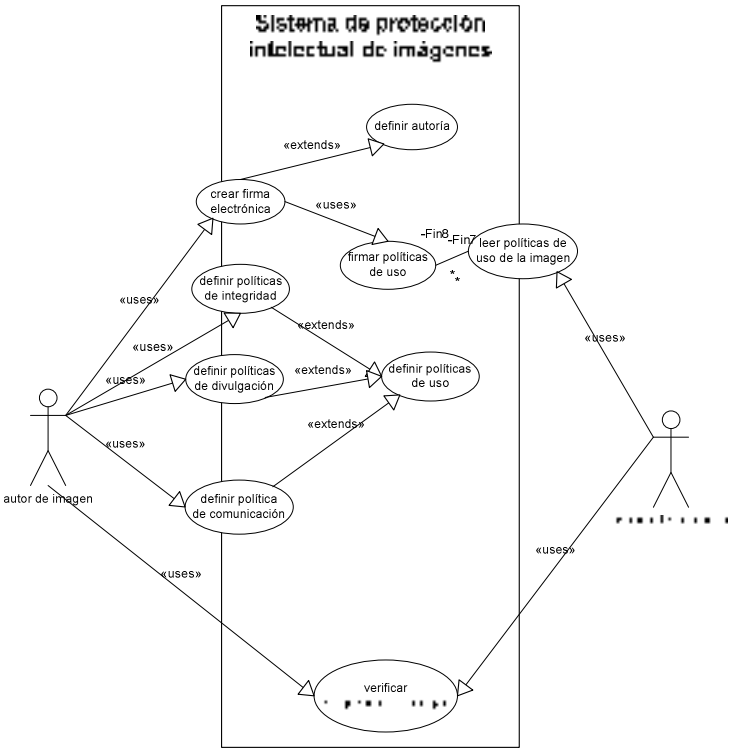

Figura 4.1 Diagrama de casos de uso de la aplicación.

Arquitectura

Para cumplir con los requerimientos del sistema se optó por una arquitectura de componentes que presten los servicios de seguridad, manejo de metadatos e información de la imagen y el marcado de agua digital.

Estos componentes dan el soporte de seguridad al programa principal que implementa la gestión de las políticas de uso.

Servicios del componente que implementa el estándar Exif

La aplicación permite leer y modificar información de etiquetas Exif (Exchangeable Image File Format), un estándar para el almacenamiento de información (metadatos) dentro de imágenes, que tiene una alta disponibilidad en dispositivos como cámaras digitales y en diferentes tipos de reproductores de imágenes. Este estándar permite la lectura y edición de información referente al contenido (ver Fig. 4.2), por lo que se aprovecha esta tecnología como herramienta para almacenar datos referentes a la seguridad de los

contenidos digitales y propiciar un ambiente donde los creadores de contenidos puedan incorporar información referente a la autoría de sus producciones.

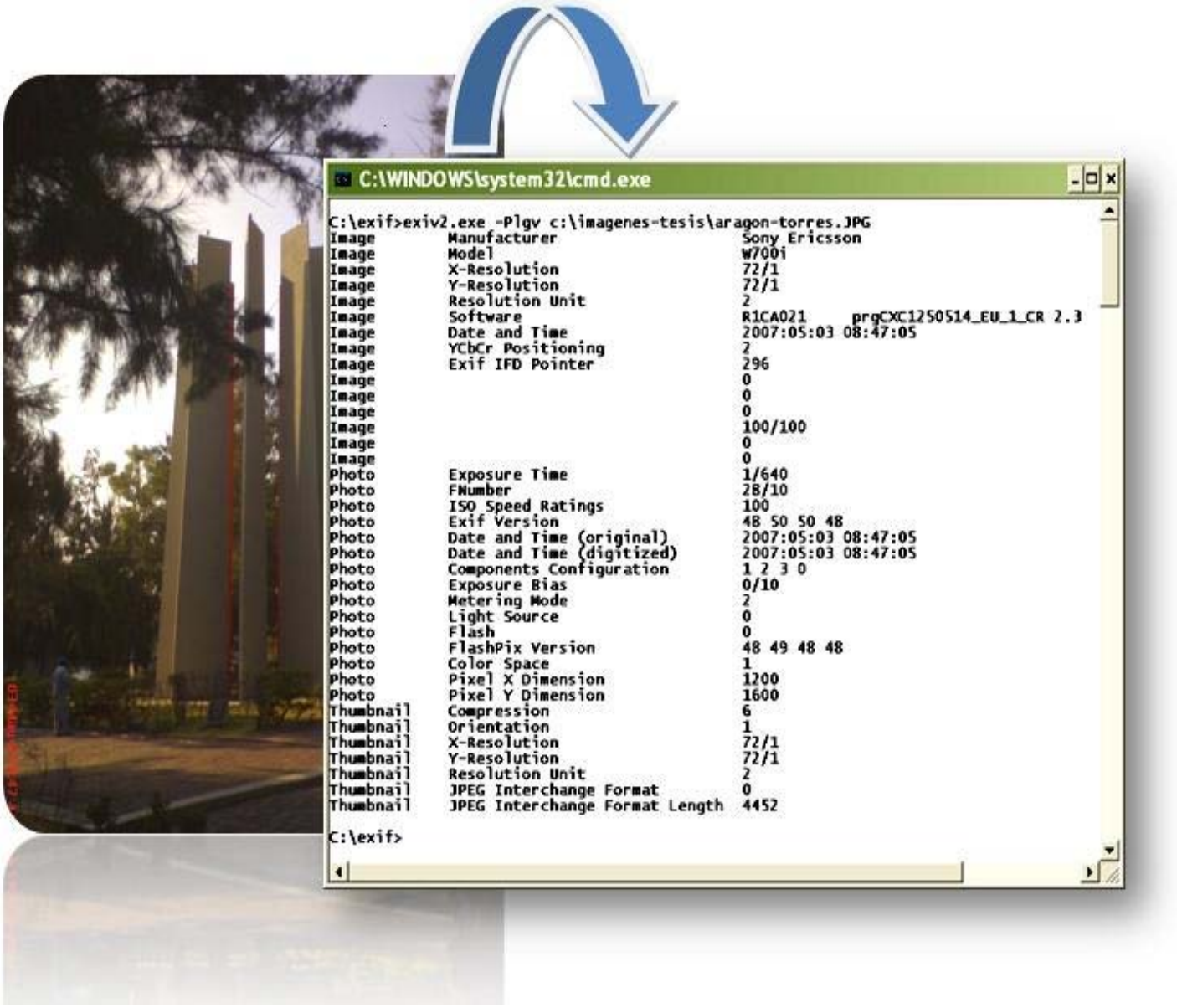

Figura 4.2 Etiquetas Exif de la imagen Aragón-torres.jpg.

Servicios del componente que implementa los mecanismos criptográficos de seguridad

La aplicación brinda los servicios de seguridad para la protección de la imagen: autenticación, confidencialidad, control de acceso, integridad y no repudio. Para implementar estos servicios de seguridad, se emplean técnicas criptográficas

(firma digital y cifrado de datos) y esteganográficas (marcado de agua digital). El conjunto de estas técnicas refuerzan la seguridad al actuar en sinergia.

Para la implementación de estos mecanismos de seguridad se usó la biblioteca de código abierto OpenSSL, la cual implementa algoritmos de cifrado simétrico como AES, algoritmos Hash como: SHA-1 y MD5 para la verificación de integridad; y algoritmos de llave pública como RSA para el uso de firmas digitales. Además, esta biblioteca tiene la ventaja de estar programada en el lenguaje de programación C, por lo que permite la implantación en diferentes plataformas.

Servicios de componente que preste los servicios de marcado de agua digital

La aplicación fomenta el uso de Marca de agua digitales no visibles en las imágenes de los usuarios, ya que el uso de estas técnicas brinda al autor una manera de comprobar su propiedad intelectual, y así darle confianza en la publicación de contenidos en los canales públicos. Esta marca de agua debe ser invisible para el ojo humano, debe ser capaz de resistir ataques como la compresión de imagen, etc; dicha marca de agua deberá contener la información referente al autor.

Las técnicas criptográficas como la firma digital y las funciones Hash dan el soporte de los servicios antes mencionados; las técnicas esteganográficas de marcado de agua y el uso de metadatos refuerzan su seguridad debido a las propiedades que poseen.

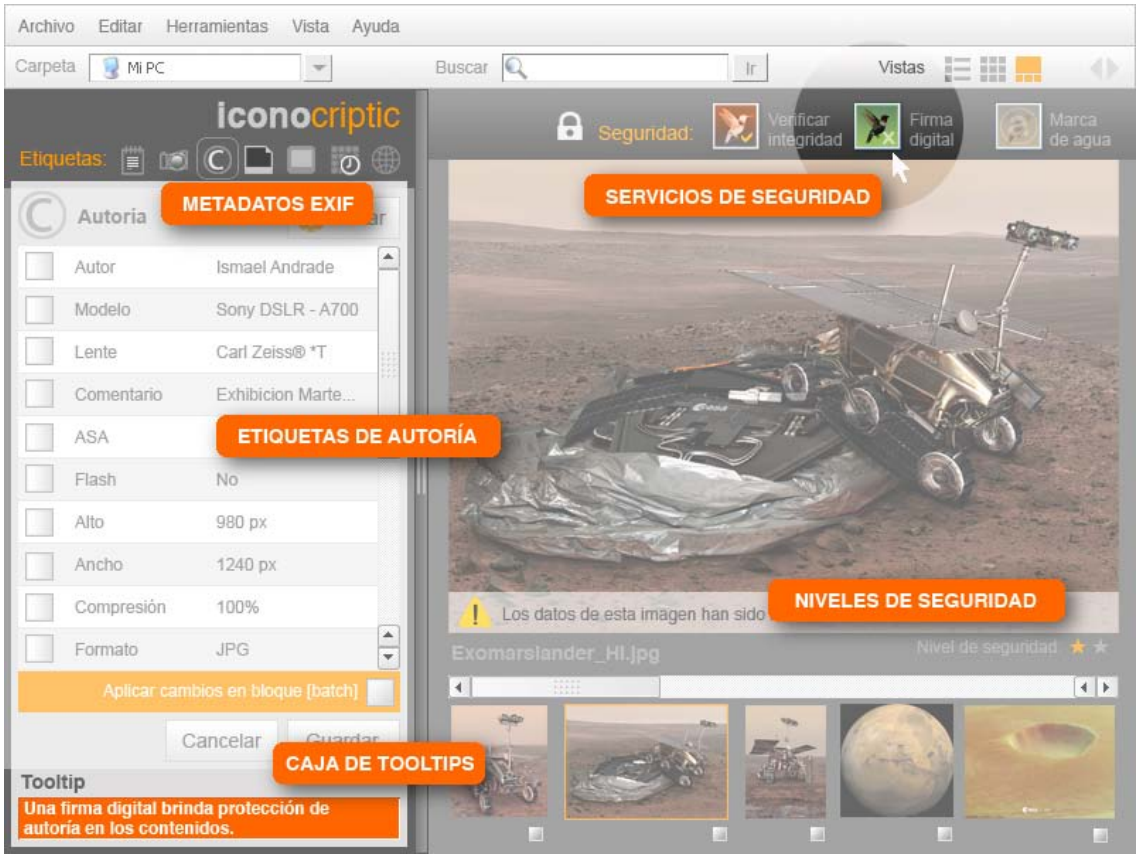

Figura 4.3 Prototipo de la aplicación.

Resultados y conclusiones

Solución de caso práctico

Actualmente las obras multimedia distribuidas sobre el Web son un ejemplo de tecnologías que requieren un ambiente de cómputo confiable, ya que se ha propiciado un ambiente donde no se tiene un control sobre la propiedad intelectual y el uso correcto de los contenidos.

Un caso particular de este tipo de problemas es el de las agencias de venta de fotografías por internet, debido a que necesitan gestionar diferentes políticas de uso, las cuales sólo se implementan de manera legal y no de manera tecnológica.

En este caso práctico, aunque hipotético, la agencia de fotografías necesitó que se gestionaran los diferentes tipos de licencia con los que cuentan. Estas licencias administran los privilegios que tiene el usuario con la fotografía y de la misma manera, también establecen las condiciones en que los fotógrafos deben entregar sus contenidos.

Las licencias y obligaciones que maneja la agencia son las siguientes:

Licencia RF (Royalty Free)

Con esta licencia el comprador solo puede usar la fotografía para uso personal, presentaciones o publicidad no lucrativa (campañas humanitarias y sociales). Además sólo puede realizar hasta 10,000 copias de la fotografía en cualquiera de sus usos.

El modo de implementar estas políticas es con un contrato que se acepta al momento de descargar la imagen del sitio, pero no existe un mecanismo tecnológico para llevar el control del número de copias y un mecanismo para relacionar la fotografía con el autor.

Licencia P-EL (reventa)

Con esta licencia el comprador puede revender impresiones de la fotografía original hasta un número menor a 10,000 copias.

De igual manera que la licencia anterior, la implementación es a través de un contrato con el usuario, de tal manera que el usuario es quien lleva el control de las copias y el uso que le da.

Licencia E-EL (Editorial)

Con esta licencia el comprador sólo puede utilizar la fotografía para fines editoriales como periódicos, revistas o documentales. Por lo tanto el comprador tiene la garantía que la imagen no ha sido alterada por software de edición, comprometiéndose de la misma manera a no retocar la imagen más allá de su redimensionamiento.

La implementación de esta política es sólo por contrato y a través de la opinión de un experto que da fe que la imagen no ha sido retocada. Sin embargo no hay medios tecnológicos que aseguren la autenticidad de la imagen.

Licencia SR-EL (venta de derechos)

Con esta licencia el comprador adquiere la posesión de los derechos patrimoniales de la fotografía. Es decir que la agencia ya no puede revender la fotografía y el comprador tiene todos los derechos de divulgación, comercialización y edición.

La implementación de esta política es a través de la firma de varios contratos por parte del fotógrafo al comprometerse a no vender la fotografía adquirida bajo esta modalidad. Por otro lado la agencia también firma un acuerdo que restringe la venta de la copia después de la fecha de compra por parte del consumidor.

Obligaciones del fotógrafo

La agencia requiere que el trabajo del fotógrafo sea original, que posea los contratos de cesión de imagen en caso de retratos (que la fotografía contenga imágenes reconocibles) y no edite con software la fotografía en el caso de las licencias editoriales.

Obligaciones del consumidor

La agencia requiere que las fotografías no sean utilizadas en temas sensibles o perjudiciales al autor o a las personas involucradas en la fotografía. Por ejemplo en imágenes referentes a pornografía, crimen, drogadicción, entre otros similares.

Resultados de la Implementación con el sistema de protección de autoría

El sistema propuesto tiene mecanismos tecnológicos que dan un soporte al acuerdo legal de contratos y al manejo de evidencia que comprueba el tipo de uso que se haya dado al contenido multimedia. Además, el manejo adecuado de la información favorece un aprendizaje en cuanto al respeto de los derechos de autor, estos mecanismos se explican en el cuadro 5.1

Cuadro 5.1 Resultados de la implementación de políticas a través del sistema

Licencia	Soporte técnico	Soporte legal	Soporte cultural
Royalty Free Reventa.	Se lleva control del número de copias a través de los metadatos Exif Se firma digitalmente la copia.	El contrato de uso que se firma es insertado en la imagen de igual manera se da la evidencia en caso de la realización de una copia ilegal.	El usuario puede saber las obligaciones que tiene al usar la imagen y de esta manera asegurar que da un uso adecuado.
Editorial.	Se verifica que la imagen no haya sido retocada a través de la etiqueta Exif del software de edición. Se verifica la integridad de la imagen con una función hash.	Se da la evidencia para comprobar que la imagen no haya sido alterada de manera no autorizada.	El usuario tiene la certeza a cerca de la autenticidad lo mostrado en la imagen.
Venta de derechos.	Se cifra la imagen original de manera que solo el comprador pueda descifrarla.	La imagen sólo puede ser descifrada por el comprador por lo	Se da la certeza al comprador que posee una copia inédita.

	Se verifica integridad y se firman todas las copias antes de la venta de los derechos.	cual se da la evidencia de que solo el puede manipularla. En caso de que se encuentre una copia no autorizada se tiene la evidencia de quien la realizó a través de la firma digital.	
Obligaciones del fotógrafo	El sistema puede advertir al fotógrafo en caso de que haya alterado la imagen. El sistema podría tener la capacidad de analizar rostros reconocibles y advertir al fotógrafo de la necesidad de contratos de cesión de imagen. El uso de las etiquetas Exif puede demostrar si dos fotografías fueron tomadas con las mismas propiedades de fotografía.	Da evidencia de una violación del contrato al momento de editarse la fotografía. Da evidencia a una tercera parte que una imagen posee la misma composición fotográfica que otra similar. Además de mostrar las fechas de creación de las mismas.	Da certidumbre al fotógrafo y al consumidor de que la fotografía cumple con los requerimientos acordados.
Obligaciones del consumidor	El uso de metadatos permite al fotógrafo definir en qué temas sensibles se puede utilizar la fotografía.	En caso del mal uso del contenido, existe la evidencia ante una tercera parte de los temas	Da la certidumbre al fotógrafo a cerca del uso de la fotografía. Da la certeza al

		sensibles en los que la fotografía podía ser utilizada.	usuario que en cualquier controversia puede demostrar los privilegios que contaba con la fotografía.

Conclusiones

Los ambientes de cómputo confiable son una pieza fundamental para el desarrollo de tecnologías de la información, los cuales dan la certidumbre del uso adecuado de la información a la sociedad.

Para desarrollar estos ambientes de cómputo se necesita un trabajo interdisciplinario para que la tecnología resuelva los problemas técnicos y dé soporte a los marcos jurídicos y a la sociedad en el manejo seguro de la información.

En cuanto a este soporte tecnológico, hoy en día existen herramientas informáticas que brindan el soporte electrónico de evidencias y de protección a datos, suficientes para combatir el problema de los delitos informáticos. Estos mecanismos que han penetrado en la sociedad desde hace poco tiempo son el trabajo de décadas en materia del aseguramiento de la información.

Sin embargo, estas metodologías no han sido explotadas de manera adecuada por lo que es necesario el análisis multidisciplinario para integrar estos mecanismos de seguridad digital a las tecnologías de la información y la comunicación

Un ejemplo claro de este fenómeno es el de la piratería informática que atenta contra los derechos de autor y la propiedad intelectual. Ya que los mecanismos empleados actualmente han sido ineficaces al problema.

Por lo que el enfoque planteado en este trabajo pretende desarrollar un ambiente cooperativo entre la tecnología, el marco jurídico y la sociedad para combatir este problema que si continua provocará grandes consecuencias a la sociedad de la información.

Trabajo futuro

El trabajo que se planteo en los capítulos anteriores expone un enfoque para el desarrollo de ambientes de cómputo seguro y a la vez los implementa con una herramienta para la gestión de políticas de uso en fotografías digitales.

Sin embargo el desarrollo de ambientes de cómputo seguro requiere formalizar estas ideas en un framework para poderse aplicar en cualquier área de cómputo y que esto sea parte del desarrollo de tecnologías de la información.

El diseño de este framework debe contener desde la formalización de las políticas, el diseño a través de métricas de seguridad y la programación segura a través de buenas prácticas.

Por otro lado la aplicación planteada en este trabajo debe extender su funcionalidad a la gestión de audio, video y texto, ya esto tendría más impacto en obras colectivas.

Literatura citada

Bishop, M. y Bailey, D. 1996. A critical analysis of vulnerability taxonomies. CSE-96-11, Department of Computer Science, University of California, E.U.A.

Diffie, W. Y Hellman, M. E. 1976. New Directions in Cryptography. IEEE Transactions on Information Theory, 22,6 pp: 644-654 (Noviembre).

Feldman, T. 1994. Multimedia. Chapman and Hall, pp. 135. Londres.

IATAC. 2007. Software Security Assurence: A State-of-the-art Report (SOAR). Information Assurance Technology Analisys, pp. 396, (julio).

International Organization for Standarization (ISO). 1989. Information processing systems – Open Systems interconnection – Basic Reference Part 2: Security Architecture. ISO 7498-2, (Febrero).

Kahn, D. 1967. The Codebreakers: The Story of Secret Writing. The Macmillan Co., E.U.A.

Landwehr, C. Bull, A. Mcdermott, J. Y Choi, W. 1994. A taxonomy of computer program security flaws. ACM comput. Surv. 26, 3 pp. 211–255.

Liu, X. y Eskicioglu, A. 2003. Selective Encryption of Multimedia Content in Distributed Networks: Challenges and New Directions, IASTED Communications, Internet & Information Technology (CIIT), November 2003.

Moyle, E. Y Kelley, D. 2005. Cryptographic Libraries for Developers. Charles River Media, pp.512. E.U.A.

NBS (U.S. National Bureau of Standars). 1977. Data Encryption Standard. FIPS, Publ. 46, (Enero).

NIST (U.S. National Institute of Standards & Technology). 2001. Specification for the Advanced Encryption System AES. FISP, Publ, 197.

Parets, J. G. 2007. El proceso administrativo de infracción intelectual. SISTA Editorial., México.

Pfleeger, C. y Pfleeger, S. 2003. Security in Computing. Prentice Hall PTR, E.U.A.

Rsa Security 2007. http://www.rsa.com

Shannon, C. E. 1948. A mathematical theory of communication. The Bell System Technical Journal , 27, pp. 379–423, 623–656, (Julio, Octubre).

Wang, X.Y. Guo, F.D. Lai, X.J. Y Yu, H.B. 2004. Collisions for hash functions MD4, MD5. HAVAL-128 and RIPEMD, rump session of Crypto'04, E-print.

Zone-h.org http://www.zone-h.org/content/view/14928/30/

Glosario

AES (Advanced Encryption Standard): es un criptosistema de llave secreta de 128 bits desarrollado por los belgas Joan Daemen y Vincent Rijmen

Amenaza: es un conjunto de circunstancias o entidades que tienen la posibilidad de causar eventos de daño o pérdida de los recursos informáticos.

Ataque: es un conjunto de eventos deliberados que explotan las vulnerabilidades del sistema de cómputo para interceptar, modificar, fabricar y/o eliminar información.

Autenticación o autentificación: es la propiedad que define que una entidad, información y/o la fuente de información es genuina o verdadera.

Confidencialidad: es la cualidad que caracteriza a la información como reservada o secreta para las entidades no autorizadas.

Control de acceso: es el conjunto de funciones y tareas que se desempeñan para prevenir el acceso no autorizado de un recurso, incluyendo la prevención del uso del recurso de una manera inadecuada

Criptoanálisis: es la disciplina que estudia la eficacia y la eficiencia de los criptosistemas.

Criptografía: es la disciplina que estudia y diseña sistemas de secreto (criptosistemas) para la ocultación de información.

DES (Data Encryption Standard): es un sistema de criptografía de clave secreta. Usa bloques de datos de 64 bits y clave de 56 bits.

Disponibilidad: es el conjunto de funciones y tareas que se desempeñan para procurar la disponibilidad de un recurso bajo demanda de una entidad autorizada.

Disponibilidad: es la cualidad que define a la información o a la fuente de información como accesible y usable bajo demanda de una entidad.

E-crime: es la actividad criminal que emplea como herramienta a las tecnologías de la información y la comunicación.

Esteganografía: es la tecnología que introduce información en un canal de información externo con el fin de ocultarla.

Ethical Hacking (hackeo ético): es una disciplina de la seguridad informática que se sustenta en el hecho de que para estar protegido se debe conocer cómo operan y qué herramientas usan los hackers

Exif (Exchangeable image file format): es una especificación para formatos de archivos de imagen usado por las cámaras digitales. Fue creado por la Japan Electronic Industry Development Association (JEIDA). La especificación usa los formatos de archivos existentes como JPEG, TIFF Rev. 6.0, y RIFF el formato de archivo de audio WAVE, a los que se agrega tags específicos de metadatos.

Exploit: es el conjunto de código, datos o comandos que explotan vulnerabilidades

Firewall (cortafuegos):son los elementos de software y hardware que filtran el tráfico de comunicaciones.

Firma Digital: es un conjunto de información cifrada que relaciona al autor de un documento electrónico y autentifica que es quien dice ser, además de comprobar la integridad del documento firmado.

Framework: es un conjunto de APIs y herramientas destinadas a la construcción de un determinado tipo de aplicaciones de manera generalista. Modela las relaciones generales de las entidades del dominio. Provee una estructura y una metodología de trabajo la cual extiende o utiliza las aplicaciones del dominio.

Gusano (worm): es un programa informático que se autoduplica y autopropaga. En contraste con los virus, los gusanos suelen estar especialmente escritos para redes.

Hardware: es el conjunto de artefactos que conforman la parte física del sistema de cómputo, estos dispositivos se interconectan comúnmente a través de medios como cables y señales electromagnéticas.

Integridad: es la propiedad que define que la información no carece de alguna de sus partes.

Malware: es el conjunto de programas cuyo objetivo es causar daños al software, a la información y, por extensión, a sus usuarios.

MD5 (Message-Digest Algorithm 5), es un algoritmo de funciones hash o funciones criptográficas de resumen.

Metadatos: del griego *μετα*, *meta*, «después de» y latín *datum*, «lo que se da», «dato» ; literalmente «sobre datos», son datos que describen otros datos.

Rootkit: es el conjunto de programas que sirven para tomar el control principal del sistema.

SHA-1 (Secure Hash Algorithm); es un algoritmo de funciones Hash que produce una cadena de 160-bits que es irreversible o computacionalmente dificil de revertir.

Software: es la parte lógica de los sistemas de cómputo que principalmente controla y administra los recursos de hardware; y transforma los datos a información.

TEMPEST: es el nombre clave que se refiere a las investigaciones y estudios de emisiones electromagnéticas comprometedoras.

Trapdoors o backdoor (puertas traceras): es una sección oculta de un programa de computadora, que sólo se pone en funcionamiento si se dan condiciones o circunstancias muy particulares en el programa.

Troyano (trojan): es un programa malicioso que se presenta como software legítimo y benigno. Obtiene su nombre del Caballo de Troya.

Virus: es un programa que se duplica a sí mismo en un sistema informático incorporándose a otros programas con el objetivo de comprometer la información.

Vulnerabilidad: es una debilidad de seguridad generada por una falla o deficiencia en el diseño, en la implementación y/o en su uso, que aumenta el riesgo de pérdidas o errores.