

NUEVAS TECNOLOGÍAS
APLICADAS A LA GESTIÓN (E66)
5º INGENIERÍA EN INFORMÁTICA

Tema 6.
La Seguridad en
las Tarjetas Inteligentes.

- 1.- Introducción.
- 2.- Seguridad Hardware.
- 3.- Seguridad Software.
- 4.- Identificación del Usuario.
- 5.- Cifrado de Información.
- 6.- Autenticación y Firma Digital.
- 7.- Manejo de Claves.

(Capítulos 3, 6 y 9 del Zoreda)

(Capítulo 8 del RankI)

INTRODUCCIÓN

Planteamiento

- Una de las ventajas más importantes de las tarjetas inteligentes es el nivel de seguridad que suministran.
- Esta característica es la fundamental para el uso de esta tecnología frente a otro tipo de tarjetas.
- Los aspectos de seguridad se enfocan desde puntos de vista muy diferentes.
- Desde un punto de vista hardware, el objetivo es el diseño de un circuito que no pueda ser falsificado.
- Para ello se deben incorporar al circuito todos los elementos que eviten una manipulación no adecuada.
- Desde un punto de vista software se requiere un control sobre la ejecución de ordenes en la tarjeta.
- Este control debe prevenir la modificación de zonas de memoria reservadas y el acceso de usuarios no autorizados.
- En este último aspecto, resulta de gran interés el método de identificación del usuario y la autenticación del terminal y de la tarjeta.
- También se debe controlar que el diálogo con la tarjeta sea correcto y sin interferencias.
- El manejo de claves de acceso, así como el uso de algoritmos de cifrado son elementos básicos de estos aspectos.

SEGURIDAD HARDWARE

Planteamiento

- Existen una gran variedad de metodologías que permiten proteger al microprocesador de una tarjeta inteligente.
- Estas soluciones se pueden englobar en dos clases,
 - Soluciones Pasivas. En donde no resulta necesario que la tarjeta esté alimentada.
 - Soluciones Activas. Requieren que la tarjeta esté alimentada.
- La idea de las primeras es mejorar el proceso de fabricación de la tarjeta con el objeto de proteger los diferentes elementos de la tarjeta de un análisis externo.
- Las segundas se asocian con un conjunto de sensores activos que se integran con el resto de elementos de la tarjeta.
- Las medidas de estos sensores se controlan en el funcionamiento normal de la tarjeta, aunque sólo son útiles si la tarjeta esta conectada .
- Normalmente, estos sensores son de uso muy específico, por lo que sólo son útiles en la detección de un único ataque externo.
- Además, incluso puede suceder que un valor tomado como peligroso se deba a un simple cambio en el entorno.
- Por tanto la elección de el número y la función de los sensores utilizados es fundamental.

ATAQUES Y SOLUCIONES PASIVAS

Presentación

- La mayoría de los ataques hardware que sufre una tarjeta inteligente utilizan un equipamiento de alta tecnología.
- Algunos de los más utilizados son microscopios, cortadores láser, micromanipuladores, útiles para la separación química de componentes, y computadores de altas prestaciones para el análisis de los datos.
- El objetivo de estos ataques es la memoria EEPROM, ya que en ella se encuentra toda la información de la tarjeta inteligente.
- La lectura de la memoria permitiría el posterior manejo de la tarjeta para su modificación, ya que sería posible leer la copia cifrada del PIN, y descifrarlo utilizando la función de cifrado que también aparece en la memoria.
- Existen diferentes opciones para posibilitar estos ataques,
 - Cambio de Estado de la Tarjeta.
 - Acceso Directo a la Memoria.
- Otro tipo de ataques hardware, se refiere a la generación de números aleatorios.
- Estos números son utilizados en el proceso de autenticación, que permite verificar el diálogo con un terminal.

ATAQUES Y SOLUCIONES PASIVAS

Cambio de Estado

- El microprocesador de las tarjetas inteligentes puede pasar a un modo de test en el que es posible acceder a toda la memoria EEPROM sin ningún tipo de control.
- Este modo es útil en el proceso de fabricación y para realizar ciertas tareas internas.
- El paso a este modo se controla por un fusible físico, que se funde cuando se verifica el funcionamiento de la tarjeta en la última etapa del proceso de fabricación.
- Este fusible fundido aparece como una gran superficie plana en el circuito, que al menos teóricamente, puede ser cortocircuitado de modo mecánico.
- Para resolver este problema, aparece en las tarjetas una zona de la EEPROM que permite complementar la tarea del fusible.
- Esta zona de la EEPROM funciona como un fusible lógico respecto del tránsito al estado de test.
- Dado que el acceso a la EEPROM requiere la desactivación de los dos fusibles, y el fusible lógico se encuentra en la propia memoria EEPROM, se bloquea el tránsito al modo de test.

ATAQUES Y SOLUCIONES PASIVAS

Acceso Directo a la Memoria

- Este tipo de ataque requiere la extracción de la superficie de silicio de su envoltorio, para lo cual es necesario aplicar distintas técnicas.
- Dicha operación requiere gran delicadeza, ya que cualquier maniobra inadecuada podría romper el circuito.
- La escala de integración actual imposibilita un ataque directo sobre los bits de la memoria, por lo que resulta necesario abordar el problema desde otro punto de vista.
- Una posibilidad, aunque realmente compleja, es el acceso directo a las pistas que conectan los diferentes componentes de la tarjeta.
- De este modo es posible leer las memorias ROM y EEPROM sin necesidad de alimentarlas eléctricamente.
- Este ataque resulta poco probable ya que las técnicas micromecánicas que lo posibilitarían, están poco desarrolladas.
- En cualquier caso, los circuitos están provistos de técnicas para preverlo, como el cambio en el orden de las pistas en los buses.
- También es posible leer el contenido de una memoria ROM mediante la utilización de un microscopio óptico.
- Para evitar este problema, la memoria ROM no se encuentra en la capa superior del circuito, reduciendo el riesgo de este ataque.

ATAQUES Y SOLUCIONES PASIVAS

Generación de Números Aleatorios

- Los números aleatorios son utilizados por la tarjeta y por el terminal en la autenticación.
- La idea de este mecanismo es verificar que se puede descifrar un número que ha sido cifrado por el otro comunicante, comprobando que ambos poseen el mismo algoritmo de cifrado.
- El principal objetivo de esta tarea es asegurar la individualización de un diálogo entre una tarjeta y un terminal.
- De este modo se imposibilita la reproducción de una sesión anterior, que pudiera haber sido grabada.
- Un posible ataque fuerza a la tarjeta a generar una secuencia de números aleatorios que sea lo suficientemente grande para que llegue a ser predecible.
- Para resolver este problema, el generador de la tarjeta posee un periodo que mayor que la longevidad de la propia tarjeta.
- Otra posibilidad es generar una secuencia de números aleatorios tan grande que llegue un momento en el cual el generador de números aleatorios se bloquee y siempre genere el mismo número.
- En este caso, la tarjeta imposibilita posteriores procesos de autenticación, que tendría una influencia directa sobre el funcionamiento de la tarjeta.

ATAQUES Y SOLUCIONES ACTIVAS

Descripción

- Los circuitos suelen estar recubiertas de una envoltura de material pasivo que le protege contra la oxidación u otros procesos químicos.
- Cuando se desea manipular el circuito, resulta necesario retirar esta capa pasiva.
- Para controlar la existencia de esta capa, se incluye un sensor que verifica la resistencia o capacitancia que dicha capa genera.
- Dicho sensor genera una señal que bloquea el circuito si detecta una medida errónea.
- También es posible incluir un Regulador de la Tensión cuyo objeto es asegurar que la tarjeta funcione a los niveles adecuados.
- Una tensión fuera de los límites podría cambiar el valor de ciertas zonas, como el contador de programa, lo que originaría un funcionamiento aleatorio.
- Una frecuencia de reloj inadecuada podría permitir un análisis pormenorizado de la tarjeta, incluyendo el consumo de potencia, de modo que se pudiera predecir su funcionamiento.
- Para evitar este análisis, también aparece un Regulador de la Frecuencia de Reloj.
- También podrían aparecer otros circuitos en la tarjeta, como un Supervisor de Temperatura, aunque su utilidad no está asegurada.
- El circuito resultante depende en gran medida de la aplicación donde se vaya a utilizar.

SEGURIDAD SOFTWARE

Planteamiento

- La seguridad software hace referencia a los diferentes mecanismos de seguridad que la tarjeta posee para imposibilitar un acceso a la memoria no deseado.
- Existen diferentes tipos de ataques que deben ser previstos y corregidos.
- Algunos se restringen al funcionamiento interno de la tarjeta, en donde las diferentes zonas de memoria se encuentran protegidas para evitar acceso no deseados.
- Otras se refieren a la conexión externa de la tarjeta y pueden incluir,
 - La manipulación del diálogo con el terminal.
 - Emulación de la tarjeta o del terminal para detectar los fundamentos del diálogo.
- También es posible realizar una evaluación externa del comportamiento de la tarjeta, que se puede centrar en
 - Consumo de Potencia de la Tarjeta, con el objeto de detectar cuando se produce una escritura en la EEPROM.
 - Coste Temporal en efectuar una respuesta, que permite deducir la operación realizada.
- También resulta de interés, el modo en el que las propias aplicaciones se defienden contra el ataque externo.
- **Bloqueo por parte del sistema operativo.**

SEGURIDAD SOFTWARE

Funcionamiento Interno

- La nueva generación de tarjetas inteligentes permiten la inclusión de código objeto en la memoria EEPROM para el desarrollo de tareas específicas a una aplicación.
- Esta mayor versatilidad permite la inclusión de "caballos de Troya" que pueden modificar el contenido de la tarjeta.
- Para evitar este problema, se proponen las siguientes dos técnicas.
- Todas las zonas que contienen información de uso reservado para el sistema operativo están protegidos por un Código de Detección de Errores.
- Si se modificara el valor de algunas de estas zonas sin actualizar el código asociado, sería fácilmente detectable mediante el cálculo del código.
- Esta metodología también se utiliza para la detección de errores que pudieran aparecer en estas zonas.
- El acceso inadecuado de un caballo de Troya también es evitado, encapsulando la memoria accesible por una aplicación en un DF.
- Cualquier acceso a otra zona de memoria es detectado e imposibilitado por el gestor de ficheros.

SEGURIDAD SOFTWARE

Manipulación del Diálogo

- La única vía de comunicación de la tarjeta con el mundo exterior se produce a través de uno de sus contactos, el contacto I/O.
- Por tanto una alteración de su flujo de datos podría llegar a introducir ordenes en las que se modificara el contenido de la memoria.
- Una posibilidad es la inclusión de un dispositivo formado por dos contactos separados por un material aislante.
- Uno de ellos se situaría sobre el contacto I/O de la tarjeta y el otro estaría conectado a un ordenador de altas prestaciones.
- De este modo el ordenador podría eliminar e incorporar instrucciones y datos, de modo que se alterara el diálogo del terminal y la tarjeta.
- Una solución a este problema es la inclusión de un obturador que imposibilitara la existencia de un cable conectado a cualquier contacto.
- Pero dado que existe esta posibilidad, y que en el futuro puede desarrollarse con mayor vigor, resulta necesario incluir alguna técnica que resuelva estos problemas.
- Éstas se denominan de modo genérico como Control de I/O, y en ellas participan diferentes elementos del sistema operativo.
- Uno de ellos es el Gestor de Transporte que es el encargado de verificar que el diálogo entre el terminal y la tarjeta es válido.

SEGURIDAD SOFTWARE

Emulación de la Tarjeta o del Terminal

- Una vía de ataque es la emulación de alguno de los elementos del diálogo.
- Mediante la emulación de la tarjeta es posible averiguar que operaciones solicita el terminal, y su posterior análisis puede llegar a desarrollar una tarjeta que responda a estas ordenes.
- El problema aparece en el momento se inicia un proceso de autenticación, ya que la clave no es conocida por el terminal.
- Esta solución se complementa con el control del número de serie de las tarjetas válidas en las que se excluyan las tarjetas que tengan un funcionamiento sospechoso.
- La emulación del terminal permite verificar el juego de instrucciones de la tarjeta, mediante la transmisión de todos los valores posibles de los bytes que las definen.
- Este dato permite conocer el rango válido de los parámetros y otras instrucciones que no estén documentadas.
- También es posible deducir las claves relativas al proceso de autenticación controlando el coste temporal del descifrado del mensaje.
- Para evitar este problema, la implementación de estos procesos aseguran que el coste es independiente de la clave y del mensaje.
- Otra opción es incluir un contador que controle el número de errores en la autenticación.

SEGURIDAD SOFTWARE

Evaluación Externa

- La operación de escritura sobre la memoria EEPROM utiliza la Bomba de Carga que genera un aumento en el consumo de potencia de la tarjeta.
- Este consumo puede ser detectado mediante la inclusión de una resistencia en el contacto Vcc de la tarjeta.
- Por lo tanto, un incremento en el consumo de potencia suficiente infiere una intención de realizar una escritura en la memoria EEPROM.
- Este conocimiento puede ser utilizado para la búsqueda del PIN, o cualquier otra clave, de la tarjeta.
- Normalmente la tarjeta comprueba el valor de la clave y posteriormente actualiza el valor del campo de errores producido, antes de enviar el código de error correspondiente.
- Si esta situación es detectada se puede llegar a desactivar la tarjeta con el objeto de evitar que el decremento del contador se produzca.
- Existen dos posibles soluciones,
 - La primera es incrementar siempre el valor del contador antes de comparar el valor de la clave, que será decrementado si la clave es correcta.
 - Otra posibilidad es escribir en una zona de memoria no útil si la clave es correcta.

SEGURIDAD SOFTWARE

Seguridad de las Aplicaciones

- Todos los esfuerzos realizados por el sistema operativo para proteger a la tarjeta contra ataques externos pueden ser insuficientes.
- Por esta razón, resulta necesario definir algún tipo de seguridad propio de la aplicación.
- La primera solución es manejar un conjunto de tarjetas cuyo número de serie sea único, que se puede complementar con una lista de las tarjetas cuyo funcionamiento sea dudoso.
- Algunas de las técnicas descritas para evitar ataques, se fundamentan en la repetición de una misma experiencia, hasta que ésta genere un valor correcto.
- Por esta razón se suele imposibilitar el intento de ejecutar una instrucción no adecuada.
- Los ficheros de protocolo asociados a una aplicación, en el que aparecen las incidencias asociadas a una sesión, facilitan la seguridad de la aplicación.
- De este modo se mantiene la integridad de la información almacenada en la tarjeta.
- El cifrado de la información es una herramienta básica, pero no puede ser utilizada en exceso, ya que su uso indiscriminado para ralentizar el funcionamiento de la tarjeta.
- Su uso se debe restringir a la transmisión de las claves y al proceso de autenticación, que controlan el acceso adecuadamente.

IDENTIFICACIÓN DEL USUARIO

Planteamiento

- Desde el principio de los tiempos, la búsqueda de un medio de identificación no ambiguo ha sido uno de los objetivos de la humanidad.
- El método más sencillo es la incorporación de una foto y/o una firma en una tarjeta, que es utilizado como identificación entre personas.
- Este planteamiento debe ser modificado en el ámbito de la tecnología de la información, ya que no existe una persona que identifique.
- Es por ello que se requieren otras técnicas que resuelvan dicho problema, que se agrupan en,
 - Uso de Información Confidencial.
 - Tenencia de un Objeto Físico.
 - Medida de Características Biológicas.
- En la primera y la segunda opciones,
 - El usuario debe ayudar para que la técnica funcione.
 - Su desarrollo en diferentes ámbitos puede llegar a ser muy complejo para el usuario.
 - Su uso infiere un beneplácito del usuario en realizar la comunicación.
- Mediante el uso de una tecnología suficiente, el uso de la tercera opción resuelve las dos primeras cuestiones pero puede llegar a incumplir la tercera, por lo que su un correcto desarrollo de la técnica es fundamental.

IDENTIFICACIÓN DEL USUARIO

Memorización de Información

- El método más común de memorización de información es el Número de Identificación.
- El estándar ISO 9564-1 aconseja que el PIN de estar compuesto de entre 4 y 12 caracteres alfanuméricos.
- Pero habitualmente se utilizan 4 dígitos, que resulta más cómodo para el usuario y además simplifica el teclado de los terminales.
- El uso del PIN permite identificar al usuario, pero no suministra ningún control sobre el terminal sobre el que se introduce.
- La inclusión del proceso de autenticación ha resuelto este problema.
- Una posible solución se podría implementar del modo siguiente,
 - El usuario guarda un código secreto en un fichero de la tarjeta.
 - Cuando la tarjeta se introduce en el terminal se desarrolla la autenticación.
 - Posteriormente el terminal accede al fichero donde se encuentra el código secreto y lo visualiza.
 - Cuando el usuario observa el código en la pantalla del terminal, lo reconoce como válido e introduce el PIN.

MÉTODOS BIOMÉTRICOS

Planteamiento

- La memorización de información puede llegar a ser muy molesta cuando se tienen diferentes tarjetas o alguna de ellas se utiliza con poca frecuencia.
- En estos casos resulta interesante la utilización de métodos de identificación biométricos, ya que facilita al usuario su utilización.
- Pero en cambio presenta inconvenientes que deben tenerse en cuenta,
 - La implementación de éstas técnicas suele tener un coste computacional muy alto.
 - Las técnicas no son absolutamente seguras, pudiendo producirse ciertos errores.
- Para resolver el primero de los problemas, se debe mejorar las prestaciones del terminal, que será el encargado de procesar de modo adecuado la señal recibida.
- Esto requiere una fuerte inversión que, como en otros casos, permitirá mejorar las prestaciones del sistema.
- El segundo de los problemas se aborda a través de la mejora de las técnicas actuales, que permitirá mejorar su nivel de certeza.
- Cuando estos condicionantes se satisfagan completamente, el uso de la memorización de información pasará a un segundo plano.

MÉTODOS BIOMÉTRICOS

Aceptación del Usuario

- La aceptación por parte del usuario es uno de los problemas básicos es la introducción de los métodos biométricos.
- Una característica biológica se puede utilizar habitualmente en una sociedad como medio de identificación, pero es posible que no sea aceptada en el ámbito de las tarjetas.
- Un caso típico son las huellas digitales que son utilizadas en el ámbito policial.
- Los problemas médicos que pueden producir las técnicas de medida, tanto por un contagio como por una lesión, también influye sobre la aceptación de los métodos.
- En ambos aspectos se requiere una mejora del proceso de medida y una fase de información al usuario que elimine cualquier sombra de duda que pueda tener.
- En algunos casos, el proceso de medida de una característica se puede producir sin el previo consentimiento del usuario.
- Es por ello que el proceso de medida siempre debe incluir un consentimiento expreso por parte del usuario.

MÉTODOS BIOMÉTRICOS

Seguridad de la Medida

- Por definición, los procesos de medida no son fiables, sino que presenta cierta incertidumbre inherente que debe ser considerada.
- Dicha incertidumbre resulta proporcional a la complejidad del propio proceso de medida, que suele ser bastante alta en la medida de características humanas.
- La probabilidad de que una medida se ajuste a su valor real se representa mediante una campana de Gauss.
- Para resolver esta problemática, el valor de referencia se obtiene como la media de una serie de mediciones de la característica.
- Posteriormente, la identificación se produce mediante la comparación de una medida con el valor de referencia.
- Debido a la incertidumbre de la medida, la comparación debe admitir como correctas medidas con un cierto nivel de error.
- Es por ello que se debe definir un umbral ,que varía con la aplicación y con la técnica de identificación utilizada.
- Este valor debe resolver el solapamiento de la campana de Gauss de dos individuos, que puede llevar a una interpretación inadecuada de la información.
- En muchos casos se opta por un umbral que sea ajustable.

MÉTODOS BIOMÉTRICOS

Clasificación de los Métodos

- Una técnica biométrica se fundamenta en una característica biológica que debe cumplir las siguientes premisas.
 - Identifica de modo único a una persona.
 - Su falsificación resulta imposible.
 - El envejecimiento de la persona no modifica su valor.
 - Su evaluación es viable, tanto por el método utilizado como en el coste computacional y monetario.
 - La cantidad de datos generados debe ser pequeña, de hasta unos cientos de bytes.
 - El método y la característica seleccionados serán adecuados para sus usuarios futuros.
- Las características puede agruparse en,
 - Características Fisiológicas.
 - Características de Comportamiento.
- Las primeras incluyen las relacionadas con el cuerpo humano y las que no se refieren a un patrón de comportamiento consciente.
- Por su parte las segundas se refieren a las que se refieren al comportamiento consciente, y que por tanto pueden variar dentro de unos límites.
- Seguidamente se describen las características más utilizadas de cada uno de los grupos.

CARACTERÍSTICAS FISIOLÓGICAS

Planteamiento

- La elección de una característica fisiológica es compleja, ya que sus valores no deben variar a lo largo de la vida del usuario.
- Ejemplos de características cuyo valor es fijo son las huellas digitales o los vasos sanguíneos de la retinas.
- En cambio, la imagen facial de la cara puede sufrir varios cambios, entre los cuales aparecen el volumen del cabello y su peinado, así como la existencia de bigote y/o barba.

Características Faciales

- Externamente la imagen de la cara de una persona puede variar sobremanera, pero aún así puede ser utilizado en este contexto.
- Se puede demostrar que el procesamiento de la fotografía bien iluminada de una persona puede generar una serie de parámetros que la identifiquen de modo único.
- El procesamiento requiere la utilización de ordenadores de altas prestaciones, así como técnicas específicas como lógica difusa o redes neuronales.
- En la actualidad, el desarrollo de las técnicas asociadas no son muy seguras, por lo que su uso no está muy extendido, aunque lo estarán en el futuro próximo.

CARACTERÍSTICAS FISIOLÓGICAS

Características de la Retina

- La estructura de vasos sanguíneos de la retina, tanto sus nodos como sus capilares, es único para cada persona.
- Para medir esta estructura se aplica un rayo infrarrojo sobre la retina y la radiación reflejada es medida por una cámara específica que envía la imagen a un computador.
- Este método tiene una fiabilidad muy alta, pero cuenta con una aceptación muy baja, que impide su utilización, en la que influye la proximidad a la que debe situarse el lector sobre el ojo del usuario.
- Otro inconveniente es la utilización de lentes de contacto que modifica los valores de la medida obtenida.

Utilización del Iris

- El iris es un diagrama variable que corta los rayos alcanzando la retina.
- Como el caso de la retina, da lugar a una medida que es única y por tanto muy válida.
- A diferencia de la técnica anterior, se puede medir a mayor distancia, por lo que presenta una mejor aceptación.
- Pero como en el caso anterior, la utilización de lentes de contacto modifica su medida.

CARACTERÍSTICAS FISIOLÓGICAS

Geometría de la Mano

- Las propiedades geométricas de la mano se utilizan desde los 70, ya que se implementa de modo muy sencillo, dando una medida única.
- Para ello se realizan mediciones de diferentes características tridimensionales de la mano o de parte de ella.
- Entre las características que se pueden medir aparecen,
 - Longitud de los Dedos.
 - Diámetro de los Dedos.
 - Radio de la Punta de los Dedos.
- Para obtener un identificador único, sólo hace falta tener un conjunto reducido de medidas, como por ejemplo 5.
- Por lo tanto, el procesamiento de las medidas suele ser bastante sencilla y rápida.
- En el proceso de medida se utilizan LEDs de luz infrarroja y fotodiodos, que pueden medir los diferentes valores, explotando el bloqueo parcial o total de los rayos.
- Debido a la sencillez del método, y dado que su uso es muy sencillo, su nivel de aceptación es muy alto.

CARACTERÍSTICAS FISIOLÓGICAS

Huellas Digitales

- El uso de las huellas digitales se encuentra muy extendido en diferentes ámbitos, siendo una de las características más utilizadas.
- Tradicionalmente, la huella digital requería la impregnación de la punta del dedo con tinta, y su posterior impresión sobre papel.
- La utilización de técnicas electrónicas reduce la complejidad de este sistema, de modo que sólo es necesario situar la punta del dedo sobre una superficie transparente.
- La comparación se basa en la clasificación de Henry que se fija en los arcos, las curvas y las espirales de la huella.
- Realmente sólo 20 de estos valores se utilizan como valores de referencia en la tarjeta.
- El proceso de medida puede fallar por la aparición de pequeñas heridas que alteren los valores de la huella.
- Su aceptación es muy alta, aunque presenta cierto rechazo por su utilización en el ámbito policial.
- El aparato de medida se compone de un lector óptico que graba la huella, y una serie de sensores que aumentan su fiabilidad.
- Un ejemplo es un sensor de temperatura y de pulso que evita la identificación válida de dedos amputados.

CARACT. DE COMPORTAMIENTO

Planteamiento

- Una de las propiedades básicas de estas características es su evolución a lo largo de la vida de una persona.
- Dicha evolución debe ser considerada en la en el desarrollo de la técnica, de modo que se pueda identificar a una persona aún cuando se hayan producido ciertos cambios.
- Es por ello, que habitualmente se desarrollan procedimientos adaptativos que detectan y corrigen los cambios producidos.

Ritmo de Escritura

- El modo en el que cada persona escribe sobre un teclado es diferente.
- Estas diferencias se fundamentan en las pausas producidas cuando se presionan diferentes teclas.
- Para medir estas pausas se procede de modo siguiente,
 - Se define una cadena de caracteres, que puede ser especificada por el terminal o es conocida por el usuario.
 - El usuario introduce esta cadena sobre el teclado del terminal.
 - El terminal mide las pausas.
- La utilización de esta técnica no requiere la modificación del hardware del terminal.

CARACT. DE COMPORTAMIENTO

Características de la Voz

- De igual modo que las características faciales permiten identificar una persona, también es posible utilizar su voz.
- La voz humana es simplemente un sonido, por lo que puede ser tratada como una señal más, sobre la cual es posible aplicar un análisis de Fourier.
- Como resultado de este análisis se obtiene el espectro característico de una persona que puede ser almacenado en la tarjeta para una posterior identificación.
- Este análisis requiere una potencia de cálculo bastante importante, así como herramientas adicionales como la lógica difusa y las redes neuronales.
- Uno de los problemas típicos a considerar es la reproducción de un mensaje anterior, por lo que el terminal siempre debe cambiar el mensaje que enuncia el usuario.
- También debe considerarse algunos aspectos externos como el estado de salud del usuario o el ruido ambiental, para lo cual es necesario mejorar las técnicas asociadas.
- Esta técnica tiene un nivel de aceptación por parte del usuario muy alta, por lo que a pesar de sus problemas técnicos, será una de las más utilizadas en el futuro.

CARACT. DE COMPORTAMIENTO

Firma Dinámica

- Usualmente se utiliza una firma como el medio de identificar a una persona.
- Lógicamente, el usuario debe realizar la firma delante del persona que tiene que verificar su identidad, ya que de otro modo un impostor podría presenta la fotocopia de una firma.
- Por la misma razón, un terminal que utilice esta técnica debe contener los elementos que permitan al usuario realizar su firma.
- Para poder realizar las medidas oportunas es necesaria la inclusión de ciertos elementos en el terminal como,
 - Lápices Especiales.
 - Plantillas Sensitivas.
- Estos elementos pueden llegar a medir los siguientes aspectos,
 - Forma de la Firma.
 - Velocidad y Aceleración de la Escritura.
 - Presión Ejercida sobre la Plantilla.
 - Tiempo para la Realización de la Firma.
- Como en los casos anteriores, ciertos valores de referencia se almacenan en la tarjeta, que se deben comparar con los procesados en el proceso de identificación.

MÉTODOS BIOMÉTRICOS

Experiencias

- En los últimos años se han realizado diversas experiencias que integran diferentes métodos de identificación en las tarjetas inteligentes.
- En la EXPO'92 se implementó un sistema de identificación basado en huellas digitales, que se utilizó en las tarjetas de los empleados y en los pases de visita semestrales.
- La idea de los pases semestrales fue impedir el bloqueo de la venta de pases diarios, lo que permitiría un mayor número de visitantes.
- Resultaba fundamental que estos pases fueran utilizados únicamente por su propietario, por lo que se introdujo este sistema de identificación.
- El problema fue el coste de la identificación, cuyo valor debía ser 8 seg. siendo su valor inicial de 30 seg. llegando hasta 15 seg.
- En Barcelona'92 se utilizó un sistema basado en la firma dinámica para el acceso a la torre de control de tráfico aéreo de su aeropuerto.
- El proceso de identificación se basaba en la comparación de la firma introducida por el usuario con el valor medio de los parámetros de tres firmas almacenadas en la tarjeta.
- Tras una identificación correcta, se sustituía la firma más antigua por la nueva, con el objeto de tener una batería de firmas actualizada.
- El número de intentos del usuarios se limitaba para impedir un proceso de prueba y error.

CIFRADO DE INFORMACIÓN

Introducción

- Desde el principio de los tiempos, el cifrado ha sido utilizado para proteger la transferencia de información confidencial.
- Su utilización en una tarjeta inteligente permite aumentar la seguridad del sistema.
- El campo de la ciencia que estudia este tema es la Criptología que se divide en,
 - Criptografía, que estudia métodos para el cifrado y descifrado de información.
 - Criptoanálisis, en el que se estudian técnicas para el descifrado fraudulento de mensajes.
- En este apartado, se describen los sistemas criptográficos, que poseen dos objetivos,
 - Seguridad, es decir, la información no se puede acceder fraudulentamente.
 - Autenticidad, que indica que la información sólo puede proceder de un único emisor.
- Los sistemas actuales se basan en el principio de Kerckhoff, que afirma que la seguridad de un algoritmo se encuentra en la seguridad de la clave y no en el propio algoritmo.
- Es por ello, que la mayoría de algoritmos están publicados, e incluso patentados, ya que su confidencialidad no es fundamental.
- Aplicando esta norma, aparecen tres tipos de datos en un algoritmo de cifrado: el Mensaje Original, el Mensaje Cifrado y la Clave.

CIFRADO DE INFORMACIÓN

Introducción

- Las operaciones que pueden aparecer en un sistema criptográfico son,
 - Cifrado de Información, en el que se obtiene el mensaje cifrado utilizando una clave y el mensaje original.
 - Descifrado de Información, que tiene como objeto la obtención del mensaje original a partir de una clave y el mensaje cifrado.
 - Función de Resumen, cuyo objetivo es la obtención de una versión más compacta del mensaje original mediante la utilización de una clave.
- El cifrado y descifrado de información están relacionados, de modo que todo algoritmo de cifrado tiene un algoritmo de descifrado asociado, que a veces es el mismo.
- Existen diferentes tipos de algoritmos, que se diferencian por el número y modo en el que se utilizan las claves,
 - Los Sistemas Simétricos, en los que se utiliza la misma clave para cifrar y descifrar el mensaje.
 - Los Sistemas Asimétricos, en donde la clave de cifrado y descifrado es diferente.
- Por lo que respecta a la función de resumen, es posible que más de un mensaje genere el mismo resumen, y por tanto se puede afirmar que estas funciones son irreversibles.

SISTEMAS SIMÉTRICOS

Introducción

- La simetría de estos sistemas se fundamentan en el hecho que el cifrado y el descifrado de información utilizan la misma clave.
- Es por ello, que la confidencialidad de la clave resulta básica para asegurar la seguridad de estos sistemas, que sólo debe ser conocida por el emisor y el receptor del mensaje.
- Por esta razón, estos sistemas también toman el nombre de sistemas de Clave Privada.
- Mediante estos sistemas se aseguran los dos objetivos básicos de estos sistemas,
 - La seguridad aparece por la privacidad de la clave.
 - Si el receptor sabe descifrar el mensaje, sabe que ha sido enviado por el emisor.
- El manejo de las claves es básica, ya que ellas aportan al sistema seguridad y autenticidad.
- Por tanto su intercambio debe realizarse del modo más seguro posible.
- Otro problema es el número de claves que son necesarias para conectar todos los usuarios de un sistema.
- Se puede comprobar que siendo n el número de usuarios, el número de claves es $n * (n-1)$.

SISTEMAS SIMÉTRICOS

El Sistema DES

- El sistema simétrico más común es el DES o Estándar de Cifrado de Datos, que cifra bloques de 8 bytes.
- La clave también es un bloque de 8 bytes, cada uno de los cuales contiene un bit de paridad, por lo que el número de claves distintas es 2^{56} .
- Dicho sistema se basa en dos operaciones,
 - Confusión, que intenta desligar los valores estadísticos de los caracteres del mensaje original y del cifrado.
 - Difusión, en donde el resultado depende del mayor número de bits del valor inicial.
- Existen tiene cuatro modos de funcionamiento de este sistema, de los que se destacan,
 - Libro de Códigos Electrónicos (ECB), en el que cada bloque de datos se cifra de modo independiente.
 - Cifrado de Bloques Encadenado (CBC), en donde el cifrado de un bloque depende del cifrado de los anteriores.
- Para aumentar la seguridad del sistema, se definió una variante del método el Triple-DES, cuyo objetivo es unir fases de cifrado.
- Las propiedades algebraicas del sistema obligan a que esta unión intercale cifrados y descifrados.

SISTEMAS ASIMÉTRICOS

Introducción

- Estos sistemas utilizan dos claves distintas para el cifrado y descifrado de la información.
- Cada usuario de estos sistemas posee dos claves diferentes,
 - La Clave Privada que sólo es conocida por el usuario.
 - La Clave Pública que es conocida por todos los usuarios que pueden recibir el mensaje.

Por lo que también se les denomina Sistemas de Clave Pública.

- El uso de estos sistemas sólo pueden asegurar uno de los objetivos de la criptografía,
 - Si el emisor usa la clave pública del receptor, el mensaje sólo puede ser descifrado por éste, aunque puede haber sido enviado por cualquier emisor.
 - Si utiliza su clave privada se asegura que el mensaje sólo puede haber sido enviado por el emisor, pero puede ser descifrado por cualquier receptor.
- Para conseguir tanto la Seguridad como la Autenticidad, resulta necesario aplicar dos procesos de cifrado, cada uno asegurando uno de los objetivos anteriores.

SISTEMAS ASIMÉTRICOS

El Sistema RSA

- Este sistema se fundamenta en la aritmética de grandes números enteros, y sobretodo en la dificultad de factorizar el producto de dos números grandes que son primos.
- El cifrado y el descifrado de la información se realiza del mismo modo,
 - En primer lugar, se calcula la exponencial respecto de una de las claves.
 - Posteriormente, se aplica el módulo definido por el producto de dos números primos.
- El producto utilizado en la operación módulo también es un valor público, que se relaciona con el valor de las claves.
- El coste de estas operaciones suele ser alto, aunque se puede resolver con circuitería de uso específico.
- En concreto, las claves se calculan como sigue,
 - Se obtienen dos números primos, p y q , y con ellos su producto, n .
 - La clave pública e es el número que cumple que el máximo común divisor respecto de $z=(p-1)(q-1)$ es 1.
 - La clave privada d cumple que el módulo respecto de z del producto d por e es 1.
- El método funciona para cualquier tamaño de la clave, por lo que se suelen utilizar claves muy grandes que aumentan su seguridad.

FUNCIONES DE RESUMEN

Planteamiento

- En algunos casos resulta interesante obtener una versión reducida de un mensaje, como en el caso de las firmas digitales.
- Dado un mensaje que puede tener cualquier tamaño, las funciones de resumen obtienen un valor de tamaño fijo.
- Para que estas funciones sean eficientes, es necesario que cumplan las propiedades,
 - Longitud Fija del Valor Resultante, para cualquiera de los mensajes procesados.
 - Sencillez del Cálculo del Valor Resultante, lo que permitirá aumentar su rendimiento.
 - Irreversible, de modo que sea imposible obtener el mensaje original desde el valor resultante de la función de resumen.
 - Resistente a las Colisiones, es decir, que la posibilidad de encontrar dos mensajes con el mismo valor resultante sea muy complejo.
- Estas funciones pueden sufrir dos ataques,
 - Dada un mensaje con un valor resultante, buscar otro mensaje con sentido que tenga el mismo valor resultante.
 - Definir dos mensajes que tengan mismo valor resultante, con la inclusión de caracteres especiales, y alternar el envío de cada uno.
- El segundo es más efectivo, ya que los dos documentos son conocidos de antemano.

AUTENTIFICACIÓN

Introducción

- El objetivo de este proceso es la identificación de uno de los participantes en un diálogo por el otro participante.
- La base del proceso es una información que es secreta y común a ambos participantes.
- En este ámbito se refiere a la identificación de la tarjeta o del terminal, y se fundamenta en un intercambio de información entre ambos.
- Existen diferentes modos de clasificar estos procesos.
- Uno de los criterios estudia el valor de los datos transmitidos, permitiendo obtener dos clases,
 - Estático, si los datos no cambian.
 - Dinámico, si el valor de los datos es variable.
- También se clasifica por los participantes que son identificados en,
 - Unidireccionales, si sólo se identifica a uno de los participantes.
 - Bidireccional, si se identifican ambos.
- Por último, el sistema de cifrado utiliza permite obtener,
 - Simétricos, si utilizan un sistema simétrico.
 - Asimétricos, si utilizan estos sistemas.
- Seguidamente se describen los procesos más comunes.

AUTENTIFICACIÓN

Simétrico Unidireccional

- En este caso se desea identificar a uno de los participantes, que tienen en común la clave utilizada en la transmisión de información.
- El proceso se resume como sigue,
 - La parte que desea identificar genera un número aleatorio y lo envía.
 - La otra parte cifra el número y lo envía.
 - El valor recibido es descifrado y comparado con el número original.
- Dado que el valor transmitido es un número aleatorio, se imposibilita la grabación externa de la sesión, con el objeto de replicarla.
- La seguridad está en la clave sobre la cual hay que incluir mecanismos seguridad.
- El primero es utilizar una clave individualizada para cada tarjeta, de este modo se evita que su descubrimiento revele todo el sistema.
- Normalmente esta clave puede ser calculada por el terminal a partir del número de serie de la tarjeta que es único.
- Habitualmente, parte del número de serie es la versión cifrada de la clave utilizada en este proceso, mediante la utilización de la clave maestra, que sólo es conocida por el terminal.
- Por tanto la seguridad de la clave maestra es básica para un correcto funcionamiento de la autenticación.

AUTENTIFICACIÓN

Simétrico Bidireccional

- Esta doble identificación se podría realizar mediante el desarrollo de dos procesos simétricos unidireccionales.
- Pero el coste temporal sería demasiado alto para considerar esta posibilidad.
- Además se puede comprobar que el sistema es más seguro, ya que desde el exterior no se puede interferir las dos fases del proceso.
- De un modo resumido, la metodología es la siguiente,
 - El terminal obtiene el número de serie de la tarjeta para calcular su clave.
 - El terminal genera un número aleatorio, n_1 , y solicita un número aleatorio de la tarjeta, n_2 .
 - El terminal cifra la concatenación de n_1 y n_2 , y envía el resultado a la tarjeta.
 - La tarjeta descifra el mensaje y compara el valor de n_2 con el valor local de n_2 .
 - La tarjeta cifra la concatenación de n_2 y n_1 , y envía al terminal el resultado.
 - El terminal descifra el mensaje y compara el valor de n_1 con su valor local.
- Una mejora al anterior sistema es el envío, por parte de la tarjeta, del número aleatorio y del número de serie en un único mensaje.

AUTENTIFICACIÓN

Asimétrico Estática

- La utilización de una autenticación asimétrica resulta interesante, ya que en su violación es necesario localizar dos claves.
- El coste de la inclusión de una unidad para el cifrado asimétrico en una tarjeta inteligente, aconsejó en un primer momento la utilización de una autenticación estática.
- El funcionamiento es el siguiente,
 - En la tarjeta se almacena una información y su cifrado mediante un sistema asimétrico.
 - EL terminal puede leer ambos valores con el objeto de verificar su validez, mediante la utilización de una clave pública.
- Uno de los problemas básicos de este sistema, es que puede ser reproducido, reduciendo el nivel de seguridad.
- Además se plantea el problema de la clave elegida en su desarrollo.
 - Si siempre se utiliza la misma clave pública, y la clave privada asociada es descubierta, todo el sistema es descubierto.
 - La mejor opción es utilizar pares de claves diferentes para cada tarjeta.
- Utilizando la segunda opción, la tarjeta incluye la clave pública a utilizar junto con su valor cifrado que puede ser descifrado por una clave pública común.

AUTENTIFICACIÓN

Asimétrico Dinámica

- Si la inclusión de una unidad para el cifrado asimétrico no presenta un coste demasiado alto, resulta aconsejable la utilización de una autenticación dinámica.
- En estos casos, el terminal genera un número aleatorio que se convierte en el punto de inicio del proceso.
- Dicho número aleatorio es cifrado en la tarjeta utilizando la clave privada, y posteriormente enviado al terminal.
- El terminal sólo tiene que descifrar el mensaje utilizando la clave pública correspondiente, y comparando el resultado con el número que él había generado.
- Este sistema se puede implementar, tanto si existe una única pareja de claves, como si existe una pareja asociada a cada tarjeta.
- En este segundo caso se incluiría la fase inicial comentada en la versión estática.

FIRMA DIGITAL

Introducción

- Usualmente se han utilizado las firmas para determinar que un documento es auténtico.
- Cuando la información se transmite a través de cualquier medio electrónico, resulta necesario verificar que dicha información no es alterada.
- La utilización de la firma puede resolver este problema, aunque su definición debe variar.
- En este ámbito se entiende como un bloque que se añade al propio mensaje, y que el receptor puede volver a calcular para verificar la autenticidad del mensaje.
- La firma debe permitir verificar, a cualquiera de sus receptores, que el mensaje proviene del emisor y que no se ha modificado.
- Por esta razón, el valor de la firma depende del contenido del mensaje y de un valor que sólo es conocido por el emisor.
- Ambos criterios puede ser cubiertos mediante la utilización de un sistema criptográfico, que utilice una clave que sólo sea conocida por el emisor del mensaje.
- La utilización de un sistema asimétrico es más versátil ya que la firma podrá ser verificada por cualquier receptor que posea la clave pública del emisor.
- Los sistemas simétricos sólo permiten verificar la autenticidad del mensaje a los receptores que conozcan la clave.

FIRMA DIGITAL

Sistemas Simétricos

- La menor versatilidad de estos sistemas, ya que el mensaje sólo puede ser verificados por un número reducido de receptores, aconseja la utilización de otra terminología.
- Por esta razón, los bloques obtenidos cuando se utilizan estos sistemas se suelen denominar simplemente Firmas o también Códigos de Autenticación de Mensajes.
- El sistema más comúnmente utilizado es el DES en su modo CBC, ya que presenta un nivel de difusión más amplio y por tanto los cambios son más complejos.
- Dado que el tamaño de la firma modifica el coste de comunicación del mensaje, resulta interesante reducir el máximo su tamaño.
- Con este fin, la firma sólo contiene los últimos 4 bytes del último bloque cifrado por el sistema de cifrado.
- Esta información es más que suficiente para la verificación del emisor del mensaje.
- El problema se presenta cuando en el diálogo aparecen más de dos comunicantes, ya que cualquiera de ellos puede ser el emisor del mensaje.
- Por esta razón, resulta necesaria la existencia de una clave para cada una de las posibles comunicaciones.

FIRMA DIGITAL

Sistemas Asimétricos

- La utilización de estos sistemas da lugar a las firmas digitales propiamente dichos.
- Como en el caso de los sistemas simétricos, resulta de gran importancia reducir el tamaño de la firma.
- En este caso, la solución más interesante es la utilización de una función de resumen.
- La metodología sería la siguiente,
 - El emisor aplica la función de resumen sobre el mensaje, y cifra el resultado mediante la utilización de su clave privada que es la firma
 - EL emisor envía el mensaje y su firma.
 - El receptor aplica la función de resumen al mensaje y descifra la firma, comparando los dos valores resultantes.
- Además del sistema RSA, también es posible utilizar otros tipos de sistemas para generar una firma digital.
- Uno de ellos es el Algoritmo de Firma Digital, o DSA, que no puede utilizarse para el cifrado de información.
- En el ámbito de las tarjetas inteligentes, la verificación de información remota puede dividirse entre la tarjeta y el terminal.
- La tarjeta se encarga de descifrar la firma y el terminal aplica la función de resumen.

MANEJO DE CLAVES

Introducción

- En los sistemas de cifrado de información, que se utilizan en los procesos de autenticación y de firma digital, resulta fundamental el uso de claves.
- La privacidad de éstas resulta básica por lo que el desarrollo de técnicas que la aumenten son fundamentales.
- Una de las filosofías más comunes es aumentar el número de claves, de modo que resulte más complejo el acceso fraudulento.
- Seguidamente se describen las técnicas más comunes para preservar la privacidad de las claves.

Claves Derivadas

- Las tarjetas inteligentes pueden sufrir un análisis profundo lejano al terminal que puede llegar a descubrir su conjunto de claves.
- Si la tarjeta no posee una clave maestra que permita un control completo, dicho análisis es menos productivo.
- En estos casos, la clave maestra aparece en el terminal, y las claves de la tarjeta se obtienen a partir de la clave maestra y de información propia de la tarjeta, como el número de serie.
- Para el cálculo de la clave suele utilizarse un algoritmo de cifrado como el DES o también el triple DES.

MANEJO DE CLAVES

Múltiples Claves y Versiones de Claves

- En la multiplicación de las claves se asigna una clave para cada uno de los procesos que utilicen sistemas de cifrado.
- Normalmente, cada clave se obtienen de una clave maestra, para aumentar el nivel de seguridad.
- La privacidad de una clave maestra no es eterna, y dado que de su valor dependen las claves de todo un sistema, resulta fundamental la actualización de su valor.
- Dicha actualización puede realizarse cuando la clave resulta comprometida, o mediante una planificación predefinida.

Claves Dinámicas

- Para evitar el acceso fraudulento a las claves, su valor puede variar en cada sesión.
- El método más genérico es el cálculo de la clave como el cifrado de un número aleatorio mediante la utilización de una clave derivada.
- De este modo se consiguen las ventajas de las claves derivadas pero personalizadas a una única sesión.
- Si esta técnica se utiliza en las firmas digitales, el número aleatorio deber ser almacenado para realizar comprobaciones posteriores.

MANEJO DE CLAVES

Datos de las Claves

- Dada la gran variedad de claves existentes en un sistema, resulta básica la utilización de una serie de parámetros que permitan identificar una determinada clave.
- De este modo se evita que una clave sea empleada para un uso no deseado.
- Normalmente los sistemas operativos permiten la enumeración de las claves de acuerdo con su posterior utilización.
- También resulta de interés la inclusión de la versión de la clave, con el objeto de permitir una correcta identificación.
- En algunos casos, se imposibilita la utilización de versiones antiguas de claves, para evitar usos inadecuados de la tarjeta.
- El control de número de errores producidos en la presentación de una clave resulta básica para evitar un análisis de su valor basado en un sistema de prueba y error.
- Dicho control se realiza mediante dos valores,
 - Contador de Errores.
 - Número Máximo de Errores.
- El primero se inicializa a cero cuando la clave es introducida correctamente.
- Cuando el primero alcanza un valor igual al segundo, la tarjeta se bloquea.