(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 485 501**

(51) Int. CI.:

G06F 21/00 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **12.08.2009 E 09167708 (8)**

(97) Fecha y número de publicación de la concesión europea: **30.04.2014 EP 2157526**

(54) Título: **Lector de RFID con heurísticas de detección de ataques incorporadas**

(30) Prioridad:

14.08.2008 US 88778 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
13.08.2014

(73) Titular/es:

ASSA ABLOY AB (100.0%)
P.O. Box 70340
107 23 Stockholm , SE

(72) Inventor/es:

DAVIS, MICHAEL

(74) Agente/Representante:

CURELL AGUILÁ, Mireia

DESCRIPCIÓN

Lector de RFID con heurísticas de detección de ataques incorporadas.

Campo de la invención

La presente invención se refiere en general a lectores con capacidad de leer credenciales legibles por máquina y ataques dirigidos contra dichos lectores y las comunicaciones entre lectores y otros dispositivos. Más específicamente, la presente invención proporciona métodos para detectar intentos de comprometer la seguridad y medidas de autenticación usadas por lectores de RFID y sus contramedidas.

Antecedentes

Los sistemas de control de acceso usan invariablemente un lector para leer y, en ocasiones, escribir credenciales legibles por máquina, tales como una banda magnética, Proximidad a 125 kHz, tarjetas inteligentes sin contacto de 13,56 MHz, etcétera. A medida que la comunidad de piratas informáticos se hace más sofisticada, se divulgan cada vez más *exploits* que pueden comprometer la información que es leída por un lector y transmitida posteriormente a un dispositivo de aguas arriba tal como un panel de control de acceso, un controlador de puertas, un ordenador anfitrión, etcétera. Los *exploits* son publicados no solamente por la comunidad de piratas informáticos sino por investigadores en seguridad e instituciones educativas legítimos. Así mismo, las personas curiosas estudian las fortalezas y debilidades de los sistemas y componentes de control de acceso. En ocasiones, las debilidades y los detalles descubiertos de los *exploits* se publican de una manera irresponsable y, con la disponibilidad de largo alcance de Internet, surge una amenaza provocada por la disponibilidad ampliamente extendida de esta información. Esta información puede permitir que individuos que no poseen la pericia o conocimiento ellos mismos, se aprovechen de sistemas, por ejemplo, los *script kiddies*. De hecho, varios de estos *exploits* se han expuesto recientemente en las Conferencias de *DEFCON and Black Hat*, por parte de participantes tales como Zac Franken con sus dispositivos Gecko y Chamaleon, el dispositivo de clonación de RFID Proxmarkii de Jonathan Westhues, y la RFIDIOt de Adam Laurie (RFIDIOt es una biblioteca python de código abierto que se puede usar para clonar transpondedores de RFID).

Sin cuestionar los motivos de cualquier individuo o institución que estudie dichos sistemas, existe una preocupación real de que sujetos con intenciones dudosas puedan aprovecharse de algunas de las debilidades publicadas y descubiertas para perpetrar crímenes contra personas o instituciones.

Todavía peor es el individuo u organización que desarrolla dichos *exploits* y, en lugar de publicarlos, los usa con fines perversos o incluso los vende a terceros por beneficios económicos.

El documento US-A-6 084 977 da a conocer un método de protección de un sistema de ordenador contra brechas de seguridad de grabación-reproducción.

El documento WO 2005/038633 da a conocer un dispositivo y un método para proteger y monitorizar datos protegidos.

El documento EP 1 209 551 da a conocer un sistema y un método para evitar el acceso no autorizado a recursos de ordenadores.

Sumario

Aunque ningún sistema puede ser siempre 100% eficaz contra dichas amenazas especialmente puesto que “no se sabe lo que no se sabe” (Confucio), una de las intenciones de la presente invención es probar y frustrar o paliar estos ataques o, por lo menos detectarlos y proporcionar una notificación apropiada de manera que pueda llevarse a cabo una acción correctiva.

Los sistemas y métodos de control de acceso de acuerdo con la invención se definen en las reivindicaciones.

Si los métodos y contramedidas de detección, según se define en las reivindicaciones, se implementan en el lector, entonces formas de realización de la presente invención pueden proporcionar una ventaja significativa en la renovación de la seguridad de dispositivos heredados, situados aguas arriba, en los cuales los microprogramas no pueden ser actualizados o no se actualizarán debido a los costes o al hecho de que el fabricante ya no presta soporte a dicho sistema. Aunque, para estos métodos de detección, su incorporación en el lector es óptima, los mismos también se pueden incluir en el dispositivo de aguas arriba. Para sistemas heredados en los cuales ni el lector ni el dispositivo de aguas arriba se pueden actualizar para incorporar dichos mecanismos de detección o sustituir con un dispositivo que ya incorpore dichos mecanismos de detección, se puede instalar un dispositivo que reside entre un lector y el dispositivo de aguas arriba y que incorpora estos mecanismos de detección.

Estas y otras ventajas se pondrán de manifiesto a partir de la exposición de la(s) invención(es) contenida(s) en la

presente. Las formas de realización que se describen posteriormente y las configuraciones antes descritas no son ni completas ni exhaustivas. Tal como se apreciará, son posibles otras formas de realización de la invención que utilicen, de manera individual o combinada, una o más de las características expuestas anteriormente o que se describen de forma detallada posteriormente.

Breve descripción de los dibujos

La figura 1 representa un sistema ejemplificativo de control de acceso de acuerdo con por lo menos algunas formas de realización de la presente invención.

Descripción detallada

Tal como puede observarse en la figura 1, un módulo de detección de ataques 104 se puede incorporar en uno o más componentes de un sistema de acceso seguro 100. Más específicamente, se puede proporcionar un único módulo de detección de ataques 104 en un lector de RFID 108, un panel anfitrión o de control 112, y/o un dispositivo intermedio 116 que resida entre el lector 108 y el panel de control 112. El lector 108 está adaptado en general para intercambiar mensajes con un dispositivo o credencial de IDentificación por Radiofrecuencia (RFID) 120 usando técnicas de comunicación conocidas de RF. Alternativamente, el lector 108 puede estar adaptado para leer datos biométricos (por ejemplo, llevar a cabo un escaneo de retina y obtener datos de la retina, llevar a cabo un escaneo de huellas dactilares y obtener datos de huellas dactilares, llevar a cabo un escaneo facial y obtener datos faciales, u obtener cualquier otro tipo de firma biométrica conocida) directamente de un usuario, en lugar de leer una credencial 120 llevada por un usuario. No obstante, tal como pueden apreciar los expertos en la materia, las comunicaciones entre la credencial 120 y el lector 108 se pueden basar en el contacto o pueden estar basadas en el magnetismo. Como ejemplo, la credencial 120 puede comprender una banda magnética o similar, y la credencial 120 se desliza a través de un lector de bandas magnéticas del lector 108 para efectuar un intercambio de mensajes. Con frecuencia, las comunicaciones entre la credencial 120 y el lector 108 son aprovechadas por atacantes en un intento de comprometer el sistema 100. Otras veces, durante un ataque se aprovechan las comunicaciones entre el lector 108 y el dispositivo intermedio 116 y/o el panel de control 112.

Según por lo menos algunas formas de realización de la presente invención, se puede proporcionar una pluralidad de módulos de detección de ataques 104 en una pluralidad de componentes diferentes para actuar en cooperación y detectar ataques potenciales sobre el sistema 100. En algunas formas de realización, la lógica de un único módulo de detección de ataques 104, que se describe de forma más detallada posteriormente, se puede distribuir entre una pluralidad de módulos de detección de ataques 104 ó se puede incorporar en un único módulo de detección de ataques 104, en función de los requisitos del sistema.

Los siguientes son métodos de detección de ataques, riesgos, y otros intentos ilícitos de comprometer la integridad de una credencial, un lector o su trayecto de comunicaciones en un intento por obtener acceso ilícito a unas instalaciones protegidas por sistemas de control de acceso físico conectados a dicho lector. Se puede proporcionar un módulo de detección de ataques 104 o una combinación de dichos módulos para ejecutar estos métodos y detectar dichos intentos de ataque.

- Dosificación de las transacciones: Se utiliza un sistema de *dosificación* para limitar la velocidad con la que se puedan leer credenciales. Por ejemplo, típicamente una persona tarda 3 ó más segundos en presentar su credencial a un lector, subsiguientemente reaccionar al LED del lector y a continuación abrir la puerta y avanzar a través de ella, suponiendo que se ha concedido acceso a la credencial presentada. La evitación de una nueva lectura de tarjetas antes de 3 segundos únicamente ralentiza la producción masiva de un número elevado de iteraciones por parte de un dispositivo atacante de fuerza bruta diseñado para generar credenciales ilícitas cuya identidad ha sido suplantada, en un intento por descubrir una credencial válida. Evidentemente, 3 segundos es simplemente un ejemplo, y el mismo debería ajustarse para su adecuación al contexto apropiado de la puerta específica. Si se detecta un ataque de fuerza bruta (es decir, el lector está leyendo tarjetas a una velocidad mayor que 3 segundos), este tiempo se puede incrementar dinámicamente y, después de que se haya alcanzado un periodo de tiempo predeterminado, el lector se puede deshabilitar completamente hasta que el mismo sea reinicializado por intervención humana.

- Aplicación de fuerza bruta en el número de tarjeta: Las credenciales utilizan varios campos para contener información específica. Por ejemplo, la mayoría de credenciales usadas en el control de acceso tiene un campo *número de tarjeta*. Aunque la opción de la presentación consecutiva de dos credenciales con un número de tarjeta que difiera en uno no está completamente fuera de la realidad, las probabilidades de que tres personas presenten credenciales que son consecutivas y que difieran solamente en uno son esencialmente nulas. Cuando se produce un evento de este tipo, puede suponerse que se está utilizando un generador de fuerza bruta. Ampliando todavía más esta detección heurística, se pueden detectar patrones de dichos datos, por ejemplo, el valor absoluto de la distancia numérica entre tarjetas sucesivas es siempre un número fijo *n*.

- Aplicación de fuerza bruta en los códigos de sitio: El *código de sitio* (*side code*) es un campo que es siempre

el mismo para cualquier instalación dada y se usa para garantizar que las credenciales de un sitio no funcionan en un sitio al otro lado de la calle. A diferencia del campo del número de tarjeta, si este campo difiere con respecto a la credencial previa en un patrón observable tan siquiera una vez, existe una alta probabilidad de que se esté llevando a cabo un ataque de fuerza bruta. Ciertamente, lo más probable es que los patrones crecientes y decrecientes sean provocados por un dispositivo atacante de fuerza bruta.

- Filtración de los códigos de sitio: puesto que el campo de código de sitio es siempre invariablemente el mismo para cualquier instalación dada, un lector podría memorizar el primer código de sitio leído después de que se haya encendido y rechazar todas las credenciales que son leídas subsiguientemente y que contienen un código de sitio diferente. En el caso en el que se esté usando más de un código de sitio en una instalación dada, se podría almacenar una lista. El número de entradas de esa lista se limitaría de manera que una vez que se encuentre un código de sitio diferente que no está en la lista, el lector superaría el número máximo de códigos de sitio permitidos; en otras palabras, el lector ha detectado un problema. Alternativamente, el código de sitio se podría programar en el lector mediante una tarjeta de órdenes o cualquier otro método y, en el caso de que, en una instalación, se utilice más de un código de sitio, en el lector se podría programar una lista de códigos de sitio válidos. La detección de un código de sitio no presente en la lista no se producirá a no ser que algo vaya mal, y la detección de *más de un* código de sitio no presente en la lista indica con certeza que se ha detectado alguna clase de ataque. También pueden utilizarse umbrales más altos para códigos de sitio no reconocidos. Una vez que se detecta una situación de este tipo, se puede generar un mensaje o informe para su transmisión a un administrador de seguridad o el lector 108 se puede apagar temporalmente, frustrando así todo intento de ataque posterior.

- Cierre por formatos permitidos: Los *formatos* se usan en la industria del control de acceso para describir la lista de *campos* que están presentes en el flujo continuo de datos de salida correspondiente a datos decodificados de una tarjeta que han sido leídos por un lector. Cada *campo* es una colección de bits con un tipo y una longitud de datos definidos. Por ejemplo, en el formato Wiegand de 26 bits más popular, según se define en la Norma de Control de Acceso SIA AC-01 cuyo contenido en su totalidad se incorpora por la presente a este documento a título de referencia, el campo de número de tarjeta se define de manera que es un número de 16 bits en el intervalo de 0 a 65.535.

  1 SIA AC-01-1996.10, Protocolo de Normas de Control de Acceso para la Interfaz de Lectores Wiegand de 26 bits. Esta norma se enumera también como referencia normativa en la TWIC Reader Hardware and Card Application Specification del Departamento de Seguridad Nacional de Estados Unidos, 30 de mayo de 2008

  Existen varias formas de incrementar la seguridad de un sistema de control de acceso en el contexto de formatos. Uno de estos ejemplos consiste en únicamente permitir que el propio lector acepte formatos que son usados realmente en unas instalaciones. Pueden ser un único formato o varios formatos. Cuando se lee un formato que no está permitido, el lector sabe que *podría* tratarse de un problema. Sin embargo, si se lee más de un formato erróneo en un intervalo de tiempo predeterminado, entonces las probabilidades de que se esté produciendo (por ejemplo, que se esté intentando un ataque de fuerza bruta) un problema son relativamente mayores. La detección de un evento de este tipo puede dar como resultado la generación de un mensaje de alerta que se transmite a un administrador de seguridad o puede dar como resultado que el lector 108 se apague temporalmente (es decir, la interrupción de servicios).

- Cierre por formatos no permitidos: De manera similar a tener una lista de formatos aceptados, otra técnica es la inversa en la cual todos los formatos posibles son aceptados por el lector *excepto* uno o más formatos. Por ejemplo, el formato Wiegand de 26 bits es tan popular que siempre hay disponibles tarjetas para muchos lectores populares en eBay y otros sitios de comercio en línea basados en la web. Con la disponibilidad tan ampliamente extendida de este popular formato, puede que no sea una buena idea usar el mismo para un sistema particular de control de acceso y, por lo tanto, puede que resulte deseable hacer que el lector *excluya* este formato. Nuevamente, tal como se ha descrito anteriormente, cuando se leen tarjetas en formatos de la lista de exclusión, esto indica que puede estar produciéndose un ataque, y, ciertamente, si se lee más de un formato excluido en cualquier periodo de tiempo dado, entonces es casi seguro que se está produciendo un ataque de alguna clase. La detección de un evento de este tipo puede dar como resultado la generación de un mensaje de alerta que se transmite a un administrador de seguridad o puede dar como resultado que el lector 108 se apague temporalmente (es decir, la interrupción de servicios).

- Vulneración del formato: Los datos codificados en credenciales, según se ha descrito previamente, obedecen a las reglas definidas por un formato particular. Si se lee una credencial que vulnera las reglas del formato, existe una alta probabilidad de que haya algo incorrecto. Todo error de transmisión de datos entre la tarjeta y el lector ya habrá sido abordado antes de que se examinen los datos concretos. Muchos lectores simplemente se aseguran de que los datos que han sido leídos son idénticos para por lo menos dos o más veces sucesivas. Otros métodos de detección de errores incluyen sumas de comprobación, CRC, y ECC por nombrar algunos. Sin embargo, si los datos han sido leídos correctamente y los mismos vulneran las reglas del formato, entonces puede estar en juego una credencial impostora que fue creada por alguien que no acababa de entender el formato – especialmente si se utiliza un formato privativo y relativamente oculto. Los

Sistemas de Control de Acceso que utilizan formatos privativos hacen que resulte más difícil para los infractores obtener suficientes tarjetas de fuentes ilegítimas para su estudio y para la aplicación de ingeniería inversa en los detalles del formato. Si se detecta una credencial impostora, entonces se puede activar la generación de un mensaje de alerta. A continuación, el mensaje de alerta se puede transmitir a un administrador de seguridad. Esto se puede hacer en solitario o en combinación con la deshabilitación temporal del lector 108 por parte de sí mismo.

- Detección de comunicaciones impostoras: Para lectores que pueden monitorizar comunicaciones entre ellos mismos y el dispositivo de aguas arriba (por ejemplo, el panel de control 112 o el dispositivo intermedio 116), la detección de mensajes que son diferentes de mensajes enviados así como mensajes "fantasmas" que ni siquiera fueron enviados por el lector es un problema serio. Para lectores que utilizan el protocolo Wiegand, esta es una posibilidad real y ya ha sido desvelada. El protocolo Wiegand es susceptible de sufrir este tipo de ataque puesto que utiliza señalización de colector abierto la cual permite comunicaciones de "línea compartida". La adición de la capacidad de leer datos sobre sus líneas de señalización de datos D0 y D1 es una mejora de hardware sencilla para cualquier lector basado en el Wiegand. Por lo tanto, una de las formas de realización de esta invención prevé la monitorización y detección de mensajes impostores. Además, cuando se inicia la transmisión de un mensaje impostor, en función de la interfaz de comunicaciones que se use, el lector puede de hecho destruir o dañar el mensaje impostor de modo que no será recibido por el dispositivo de aguas arriba. Para lectores que usan el protocolo Wiegand, mantener simplemente a nivel bajo una de entre D0 y D1, o las dos, durante uno o más periodos de tiempo TPW y TPI y/o añadir bits adicionales que provoquen un error de longitud del mensaje es una cuestión sencilla. La detección de una transmisión impostora puede dar como resultado la generación de un mensaje de alerta que se transmite a un administrador de seguridad, o puede dar como resultado que el lector 108 se apague temporalmente (es decir, interrupción de servicios).

- Mecanismos de detección de anomalías de RF: Otro mecanismo potencialmente eficaz que se puede utilizar es distinguir entre un Dispositivo de Suplantación de Identidad de RF (RFSD) y una credencial genuina. La mayoría de dispositivos electrónicos de suplantación de identidad estarán alimentados con baterías ya que requieren funcionalidad más allá de simplemente simular ser una credencial de RFID legítima. Existen varios mecanismos que se pueden utilizar tal como se expresa a continuación en líneas generales:

  Una prueba sencilla que se puede realizar es apagar la portadora de RF del lector después de que se haya leído una credencial. Probablemente un RFSD continuaría transmitiendo si se tratase de un dispositivo activo alimentado por baterías y no realizase un "seguimiento" de la portadora de RF. De este modo, esta forma de realización apaga la portadora de RF y muestrea la circuitería de recepción para asegurarse de que un dispositivo ya no está transmitiendo. Si el lector detecta que el dispositivo todavía está transmitiendo, entonces el lector puede tener la capacidad de considerar que el dispositivo es un dispositivo ilícito que intenta causar daño en el lector o el dispositivo de aguas arriba. La detección de un evento de este tipo puede dar como resultado la generación de un mensaje de alerta el cual se transmite a un administrador de seguridad o puede dar como resultado que el lector 108 se apague temporalmente (es decir, interrupción de los servicios).

  Si el RFSD se activa cada vez que detecta una portadora en la frecuencia apropiada, entonces, o bien antes o bien después de que se lea una credencial legítima, el campo de RF emitido por el lector puede generar una portadora que puede activar el inicio de la transmisión por parte del RFSD pero que sería suficientemente diferente en cuanto a potencia, frecuencia, fase, etcétera, de manera que una credencial genuina de RFID no funcionase, por ejemplo, una onda sinusoidal con un ciclo de trabajo muy bajo. Así, por ejemplo, si esto se realiza en el comienzo de un ciclo de lectura de la tarjeta, y el lector recibe datos de RF, entonces es probable que haya una credencial no legítima en el campo de RF del lector. De modo similar, si se realiza al final de un ciclo de lectura de la tarjeta, los datos de RF que se reciben deberían detenerse si se tratase de una credencial legítima. Si se efectúa aleatoriamente en el comienzo *o* en el final, le resultaría más difícil de superar a un atacante pero sería igual de fácil de administrar.

  Otro método para detectar si se está presentando un RFSD con respecto a una credencial genuina, es alterar alguna característica de RF transmitida por el lector, por ejemplo, la amplitud, la frecuencia, o la fase o bien en el inicio o bien al final del ciclo de lectura de la tarjeta. Por ejemplo, si se altera la frecuencia, entonces una credencial de RF legítima presentaría un cambio observable en los datos recibidos que realizan un "seguimiento" de la característica eléctrica que se está haciendo variar. Si la credencial 120 no cambia su respuesta, entonces se puede considerar que se está presentando una credencial ilegítima al lector 108. La detección de un evento de este tipo puede dar como resultado la generación de un mensaje de alerta que se transmite a un administrador de seguridad o puede dar como resultado que el lector 108 se apague temporalmente (es decir, interrupción de los servicios).

  Aunque los métodos expresados en líneas generales en esta sección no son infalibles, especialmente si el creador del RFSD es muy inteligente y sofisticado, elevan la seguridad del lector y probablemente detectarán atacantes aficionados sobre el lector. Probablemente, el atacante más sofisticado intentará

encontrar otra manera de comprometer un sistema de control de acceso.

- Datos con multi-tecnología redundante: A medida que la tecnología de las credenciales cambia, con frecuencia una credencial contendrá los mismos datos o datos muy similares en diferentes tecnologías legibles por máquina. Esto es especialmente prevalente en la industria del control de acceso en la medida en la que se refiere a credenciales de RFID. A medida que la tan popular tecnología heredada de 125 kHz se sustituye con credenciales de tarjetas inteligentes sin contacto de 13,56 MHz más modernas y sofisticadas, aparecen varias estrategias de migración para el periodo provisional en el que un sitio dispone de credenciales tanto de Proximidad como de tarjetas inteligentes sin contacto y/o de lectores tanto de Proximidad como de tarjetas inteligentes sin contacto. En general existen dos maneras de facilitar la estrategia de migración. Un método utiliza la aplicación de lectores de multi-tecnología con capacidad de leer los dos tipos de credenciales, y el otro método consiste en crear una única credencial con las dos tecnologías presentes, habitualmente con datos similares o idénticos. En todo caso, cuando la totalidad de los lectores se sustituye con un lector de multi-tecnología, el fabricante de los lectores da órdenes al usuario para deshabilitar la tecnología más antigua. Una de las razonas citadas es por motivos de seguridad, es decir, el lector de multi-tecnología sigue aceptando la tecnología más antigua la cual puede ser no tan segura como la credencial de la tecnología más nueva. Esta es una argumentación correcta. No obstante, si en el sitio se despliegan también credenciales con multi-tecnología que tienen los mismos datos o datos similares en las dos tecnologías, una estrategia mejor consiste en leer de hecho las dos tecnologías y comparar los datos leídos de cada tecnología para asegurarse de que los datos coinciden. Esto hace realmente que se incremente la seguridad global ya que resulta más difícil realizar un dispositivo electrónico de suplantación de identidad de credenciales que pueda soportar múltiples tecnologías en la misma unidad. Asimismo, dichos dispositivos de suplantación de identidad también serán de un tamaño sustancialmente mayor, de manera que será más difícil ocultarlos. Además, incluso si se vence la complejidad aumentada del dispositivo de suplantación de identidad, se eleva el listón sin ningún coste adicional para el administrador del sistema puesto que la credencial ya dispone de las dos tecnologías.

La invención reivindicada es el mecanismo de detección de tarjetas nulas: se basa en el hecho de que, invariablemente, todos los dispositivos situados aguas arriba envían una señal de vuelta al lector de tarjetas cuando se lee una tarjeta válida y se permite el acceso. Para lectores que se comunican con su dispositivo de aguas arriba usando el protocolo Wiegand, el dispositivo de aguas arriba lleva invariablemente la señal LEDCTL a un nivel bajo para credenciales válidas. Esto se realiza para alertar al usuario de que se le está concediendo acceso y, típicamente, adopta la forma de un indicador visual, tal como un LED, en el lector, que cambia de rojo a verde. Si se ha leído un número arbitrario de credenciales durante un periodo de tiempo arbitrario y el dispositivo de aguas arriba *no* ha señalizado al lector que se trataba de una credencial válida, entonces existe un alto grado de certeza de que hay algo incorrecto. Más particularmente, si se leen más de *n* tarjetas *nulas* en un cierto intervalo de tiempo, entonces el lector se puede apagar en correspondencia con una penalización de tiempo cada vez mayor. Una tarjeta nula se detecta por el hecho de que las tarjetas válidas obtienen un acuse de recibo al llevarse a un nivel bajo la línea de LEDCTL.

En la totalidad de los métodos anteriores de detección de ataques, es deseable disponer de contadores de eventos de detección y penalizaciones de retardo de tiempo usados individualmente o en combinación y de manera simultánea con umbrales ajustables. Las penalizaciones de retardo de tiempo pueden ser dinámicas y se incrementan cada vez que se detecta un “evento”. Podría haber una penalización de tiempo máxima en la cual no tiene lugar ningún incremento adicional o podría haber un contador de eventos que deshabilita el lector hasta que algún mecanismo externo reinicializa la condición de deshabilitación del lector, o podría haber una combinación en la cual se dispone de penalizaciones de tiempo cada vez mayores y, cuando se alcanza un umbral predeterminado, el lector se deshabilita. Adicionalmente, los contadores de eventos se pueden reinicializar si se ha alcanzado el umbral de activación en un cierto intervalo de tiempo. Por ejemplo, tres códigos de sitio erróneos en un periodo de 24 horas pueden ser permisibles y, después de que hayan transcurrido 24 horas desde el evento más reciente, el contador se inicializa (es decir, se reinicializa). Es importante señalar que la mayoría de lectores de tarjetas *no* disponen de relojes de tiempo real que conozcan la hora real del día, pero a la mayoría de lectores se les puede dotar de relojes de tiempo transcurrido que son sencillos de implementar sin ningún microprograma adicional. No obstante, debe tenerse cuidado de que estos contadores se mantengan en memoria no volátil de manera que un infractor no pueda apagar y volver a encender en un intento por superar ciertas contramedidas asociadas a la utilización y la reinicialización del reloj.

Además, todo evento que se ha detectado debería comunicarse de vuelta al dispositivo de aguas arriba usando cualquier interfaz y protocolo de comunicaciones que esté disponible en el lector. Adicionalmente, cuando se detecta un evento importante, el lector podría señalizar este hecho usando cualquier indicador audible y visual disponible, para intentar atraer la atención sobre el lector y ahuyentar a un infractor sospechoso.

En un escenario alternativo, puede que se desee realmente dejar a un infractor que entre en unas instalaciones si ello está siendo grabado, por ejemplo, con un sistema de CCTV, como prueba. En este caso, la detección del evento se puede usar para iniciar la grabación, y señalarla en un registro de pistas de auditoría con una marca de tiempo con los detalles que incluyen fecha, hora, ubicación, y tipo de evento sospechoso. De esta manera, estos eventos se

pueden encontrar en datos históricos e investigar si se trata realmente o no de un problema. El hecho de que los lectores dispongan de cualquiera de las formas de realización de esta invención junto con la activación de la CCTV se puede hacer público a los usuarios, de manera que actúe como un freno adicional a este tipo de actividad.

Todavía en otro escenario, si el sistema anfitrión está siendo monitorizado en vivo por personal de seguridad in situ, se puede enviar de hecho una persona al lector en cuestión de modo que se pueda coger “con las manos en la masa” al posible infractor.

Además, estos mecanismos de detección y reacción de ataques se pueden proporcionar en un dispositivo que incluye la funcionalidad tanto de lector como de dispositivo de aguas arriba. A dicho dispositivo se le hace referencia en general como dispositivos “autónomos”. Estos constituyen una categoría de lectores de control de acceso que disponen tanto del lector 108 como del dispositivo de aguas arriba en una única unidad. A los mismos se les denomina comúnmente dispositivos “autónomos” ya que no necesitan nada más – disponen de autonomía, es decir, son autosuficientes. Una solución autónoma es aquella en la que la totalidad de la electrónica de control se sitúa en el teclado o lector. Los sistemas compactos constituyen unos medios, fáciles de administrar y rentables, para controlar el acceso a un edificio. No obstante, en la medida en la que la electrónica de control está alojada toda ella en el lector o teclado, este tipo de sistema no se puede recomendar para puertas exteriores o interiores de alta seguridad.

Obsérvese que algunas instalaciones únicamente cierran la puerta fuera del horario comercial normal. Durante el horario comercial normal, en el cual la puerta no está cerrada, un LED u otro indicador visual del lector se puede iluminar de color verde para señalar este hecho. Durante este tiempo, no es necesario leer tarjetas para obtener acceso y se recomienda que el dispositivo de aguas arriba ignore completamente cualesquiera datos provenientes del lector. Esto debería realizarse de manera que al infractor no se le proporcione ninguna realimentación o pista en relación con la validez de una credencial o formato presentado al lector. Casi invariablemente, todos los lectores proporcionan siempre alguna indicación visual al usuario (típicamente con una opción de entre un pitido audible corto o un indicador visual o ambos) de que una tarjeta ha sido leída satisfactoriamente, y a continuación envían los datos de la credencial al dispositivo de aguas arriba para tomar la decisión de si al titular de la credencial se le concederá o no el acceso. Una de las formas de realización de esta invención consiste en incluir esta funcionalidad sin realimentación en el propio lector de manera que cada vez que el dispositivo de aguas arriba informe al lector de que la puerta está desbloqueada, el lector ni siquiera acusará recibo de ninguna tarjeta presentada a un lector en modo alguno, audible o visual. Si se desea, el lector podría realizar su detección heurística de anomalías de credenciales y enviar “eventos” al dispositivo de aguas arriba como pista de que pueda haber algo incorrecto – sin embargo, no debería proporcionarse ningún acuse de recibo al usuario.

En un conjunto de reglas de detección de ataques particularmente sencillo de implementar, el lector se puede adaptar para determinar si al mismo se le ha presentado más de un número predeterminado de tarjetas en un periodo de tiempo predeterminado, y para determinar además que no se le concedió acceso a ninguna de las tarjetas presentadas durante ese tiempo. Si el lector determina esto, entonces el mismo puede determinar que se está llevando a cabo un ataque sobre el lector. El lector también puede ser suficientemente inteligente para determinar que algunas de las presentaciones de las tarjetas se produjeron durante un periodo de tiempo relativamente corto y, por lo tanto, puede agrupar todos esos intentos en un único intento de usuario. No obstante, si las tarjetas presentadas en el breve periodo de tiempo tenían un valor diferente en uno o más campos (por ejemplo, código de sitio, número de tarjeta, etcétera), el lector puede atribuir cada intento independiente a un intento de usuario diferente. De este modo, en algunas formas de realización, el lector se puede adaptar para determinar que se ha producido un número predeterminado de intentos de usuario en un periodo de tiempo predeterminado, y puede correlacionar esta determinación con un posible ataque sobre el sistema. Si el lector detecta un evento o una serie de eventos de este tipo, entonces el mismo puede responder deshabilitándose durante un periodo de tiempo predeterminado o emitiendo un mensaje de alerta para las autoridades encargadas de la seguridad.

Todas las formas de realización anteriores se pueden implementar en una tabla de reglas que se almacena de forma segura en el módulo de detección de ataques 104 o en memoria del dispositivo que almacena el módulo de detección de ataques 104. A medida que se aprenden nuevos *exploits*, estas reglas se pueden actualizar en el módulo de detección de ataques 104 o bien por medio de una conexión segura entre el dispositivo de aguas arriba y el lector o bien usando algún tipo mecanismo de *sneaker-net* tal como tarjetas de órdenes. Además, ciertas reglas se pueden habilitar o deshabilitar automáticamente según un horario planificado, por medio de una orden del dispositivo de aguas arriba, o localmente usando algún método manual. Además de que las propias reglas sean actualizables y en efecto según se requiera, también se pueden modificar de manera similar los contadores, las penalizaciones de tiempo, y otros criterios asociados a reglas individuales.

Tal como pueden apreciar los expertos en la materia, el módulo de detección de ataques 104 se puede implementar en forma de microprogramas en un lector 108, un panel de control 112, y/o un dispositivo intermedio 116. De manera alternativa, o adicional, el módulo de detección de ataques 104 se puede proporcionar como una aplicación o instrucciones almacenadas en un soporte legible por ordenador que resida en un dispositivo de ese tipo. Las instrucciones del módulo de detección de ataques 104 pueden ser leídas y ejecutadas por un procesador local, dando como resultado así la ejecución de uno o más de los métodos de detección de ataques antes descritos.

Debería apreciarse que el formato en el cual se proporciona el módulo de detección de ataques 104 en el lector 108, el panel de control 112, y/o el dispositivo intermedio 116 no se limita necesariamente a ningún formato particular, sino que puede variar de acuerdo con las capacidades del dispositivo en el cual resida y las funciones llevadas a cabo por el módulo de detección de ataques 104.

Los sistemas, métodos y protocolos de esta invención se pueden implementar en un ordenador de función especializada además o en lugar del equipo de comunicaciones descrito, un microprocesador o microcontrolador programado y elemento(s) de circuito integrado periférico(s), un ASIC u otro circuito integrado, un procesador digital de la señal, un circuito lógico o electrónico de conexión permanente tal como un circuito de elemento discreto, un dispositivo de lógica programable tal como PLD, PLA, FPGA, PAL, un dispositivo de comunicaciones, tal como un servidor, un ordenador personal, cualesquiera medios comparables, o similares. En general, cualquier dispositivo con capacidad de implementar una máquina de estados que, a su vez, tenga la capacidad de implementar la metodología ilustrada en la presente, se puede usar para implementar los diversos métodos, protocolos y técnicas de comunicación según esta invención.

Además, los métodos dados a conocer se pueden implementar fácilmente en software usando entornos de desarrollo de software de objetos u orientado a objetos, que proporcionan código fuente portable el cual se puede usar en una variedad de plataformas de ordenadores o estaciones de trabajo. Alternativamente, el sistema dado a conocer se puede implementar parcial o totalmente en hardware usando circuitos lógicos normalizados o diseño de VLSI. El uso de software o hardware para implementar los sistemas de acuerdo con esta invención depende de los requisitos de velocidad y/o eficiencia del sistema, de la función particular, de los costes, y de los sistemas de software o hardware o sistemas de microprocesador o microordenador particulares que se estén utilizando. Los sistemas, métodos y protocolos de análisis ilustrados en la presente se pueden implementar fácilmente en hardware y/o software usando cualesquiera sistemas o estructuras, dispositivos y/o software conocidos o desarrollados posteriormente por aquellos con conocimientos habituales en la técnica pertinente, a partir de la descripción funcional proporcionada en la presente y con un conocimiento básico general de las técnicas de comunicación.

Por otra parte, los métodos dados a conocer se pueden implementar fácilmente en software que se puede almacenar en un soporte de almacenamiento, ejecutado en un ordenador programado de propósito general con la cooperación de un controlador y memoria, un ordenador de función especializada, un microprocesador, o similares. En estos casos, los sistemas y métodos de esta invención se pueden implementar como un programa incorporado en un ordenador personal, tal como una miniaplicación, JAVA®, o un lenguaje específico del dominio, en forma de un recurso que resida sobre un servidor o estación de trabajo de ordenador, en forma de una rutina incorporada en un sistema o componente de sistema de comunicaciones dedicado, o similares. El sistema también se puede implementar incorporando físicamente el sistema y/o método en un sistema de software y/o hardware, tal como los sistemas de hardware y software de un dispositivo o sistema de comunicaciones.

Por lo tanto, se pone de manifiesto que se han proporcionado, de acuerdo con la presente invención, sistemas, aparatos y métodos para detectar ataques sobre un sistema de control de acceso o componentes del mismo. Aunque esta invención se ha descrito en combinación con una serie de formas de realización, es evidente que, para aquellos con conocimientos habituales en las técnicas pertinentes, se pondrán o ponen de manifiesto muchas alternativas, modificaciones y variaciones. Por consiguiente, la intención es abarcar todas aquellas alternativas, modificaciones, equivalentes y variaciones que se sitúan dentro del alcance de esta invención.

REIVINDICACIONES

1. Sistema de control de acceso, que comprende:

un lector de tarjetas adaptado para obtener información de permisos de acceso leyendo uno o más de entre (a) credenciales legibles por máquina, (b) datos biométricos de un individuo, y (c) una entrada de usuario basada en el conocimiento;

un dispositivo situado aguas arriba en comunicación con el lector; y

un módulo de detección de ataques adaptado para determinar que el lector ha transmitido información obtenida por el lector al dispositivo de aguas arriba, determinar que no se ha recibido una señal de LEDCTL en el lector desde el dispositivo de aguas arriba en un periodo de tiempo predeterminado después de que el lector transmitiera la información al dispositivo de aguas arriba, y, basándose en la determinación de que no se ha recibido la señal de LEDCTL en el periodo de tiempo predeterminado, determinar que se ha intentado un ataque sobre el lector.

2. Sistema según la reivindicación 1, en el que el módulo de detección de ataques está contenido en el lector, o en el que el módulo de detección de ataques está contenido tanto en el lector como en el dispositivo de aguas arriba, o en el que el módulo de detección de ataques está adaptado además para comunicar un ataque intentado al personal de seguridad llevando a cabo por lo menos una de las siguientes etapas (i) generar un mensaje de alerta y transmitir el mensaje de alerta a un dispositivo de comunicaciones operado por el personal de seguridad, (ii) hacer sonar una alarma, e (iii) iluminar una fuente de luz, o en el que el módulo de detección de ataques está adaptado además para deshabilitar el lector durante un periodo de tiempo predeterminado, como respuesta a la detección de un ataque intentado.

3. Sistema de la reivindicación 1, en el que la señal de LEDCTL se detecta como no recibida en el lector en el periodo de tiempo predeterminado mediante la determinación de que una línea de LEDTCL no se ha llevado a nivel bajo en el periodo de tiempo predeterminado.

4. Sistema según la reivindicación 1, en el que la señal de LEDCTL se detecta como no recibida en el lector en el periodo de tiempo predeterminado mediante la determinación de que un indicador de LED en el lector no se activa cuando se presenta una tarjeta al lector y una puerta controlada por el lector está en un estado desbloqueado.

5. Método, que comprende:

leer, en un lector de tarjetas, información de autenticación proveniente de uno o más de entre (a) una credencial legible por máquina, (b) datos biométricos de un individuo, y (c) una entrada de usuario basada en el conocimiento, y, sobre la base de la lectura, obtener permisos de acceso;

transmitir, por parte del lector de tarjetas, los permisos de acceso de la información de autenticación a un dispositivo de aguas arriba;

determinar, por parte de un módulo de detección de ataques, que el lector de tarjetas ha transmitido los permisos de acceso al dispositivo de aguas arriba y que, en el lector de tarjetas, no se ha recibido ninguna señal de LEDCTL desde el dispositivo de aguas arriba en un periodo de tiempo predeterminado después de que el lector de tarjetas transmitiera los permisos de acceso de la información de autenticación al dispositivo de aguas arriba; y

basándose en la determinación de que la señal de LEDCTL no se ha recibido en el periodo de tiempo predeterminado, determinar que se ha intentado un ataque sobre el lector de tarjetas.

6. Método según la reivindicación 5 que comprende además:

generar un mensaje de alerta; y

provocar que el mensaje de alerta sea presentado de manera audible y/o visual.

7. Método según la reivindicación 6, en el que el mensaje de alerta se presenta en el lector, o en el que provocar que el mensaje de alerta se presente de manera audible y/o visual comprende transmitir el mensaje de alerta a un dispositivo operado por personal de seguridad, de tal manera que el dispositivo operado por el personal de seguridad presente el mensaje de alerta al personal de seguridad.

8. Método según la reivindicación 5, que comprende además deshabilitar funciones del lector durante un periodo de tiempo predeterminado.

9. Método según la reivindicación 8, en el que el mensaje de alerta se presenta en el lector, o en el que provocar que el mensaje de alerta se presente de manera audible y/o visual comprende transmitir el mensaje de alerta a un dispositivo operado por personal de seguridad, de tal manera que el dispositivo operado por el personal de seguridad presente el mensaje de alerta al personal de seguridad.

10. Método según la reivindicación 7, que comprende además deshabilitar funciones del lector durante un periodo de tiempo predeterminado.

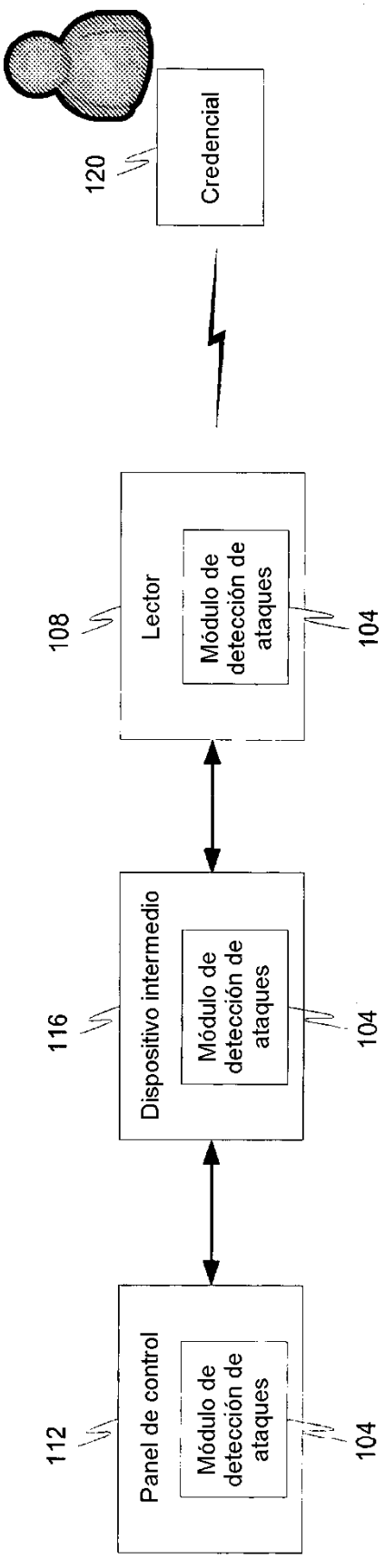
120
Credencial
108
Lector
Módulo de detección de ataques
104
116
Dispositivo intermedio
Módulo de detección de ataques
104
112
Panel de control
Módulo de detección de ataques
104

Fig. 1