ISSN 2346-9307

SKOPEIN

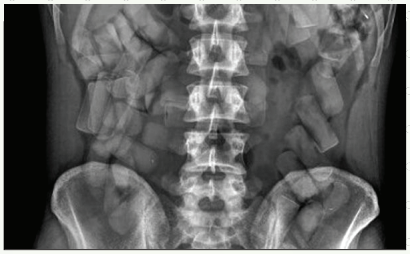
La Justicia en Manos de la Ciencia

Armas de Fuego "Inteligentes" o "Personalizadas"

María Elena Recagno

Posible Revisión de la Pena para los Ingestados

Gabriela S. Sosa



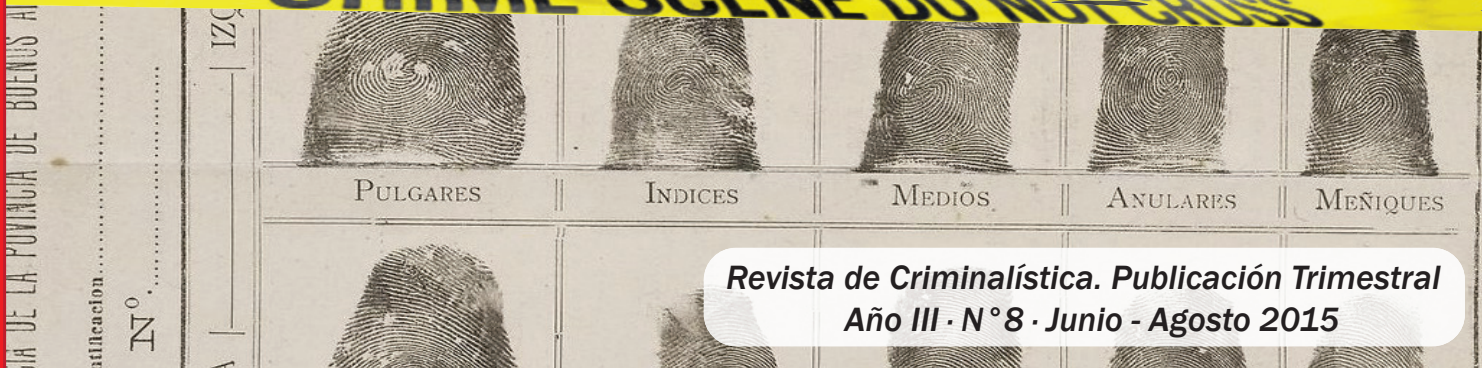
Skopein Presente! en el IX Congreso Argentino de Derecho Informático

Dra. Adriana Oliva

La especialista en entomología forense e investigadora del CONICET nos habla del caso Carrasco

¡ENTREVISTA EXCLUSIVA!

CRIME SCENE DO NOT CROSS



Revista de Criminalística. Publicación Trimestral
Año III · N°8 · Junio - Agosto 2015

Imágenes de portada

Radiografía de mulas: http://co-secharoja.org/wp-content/uploads/2014/04/radro-graf%C3%ADa-mulas.jpg
Escopeta "inteligente": Greene, M. (Junio 2013). A Review of Gun Safety Technologies (NCJ 242500).

Cod. registro SafeCreative: 1506154335917

N° de Edición

Año III, N° 8,
Junio 2015

Edición Gratuita

ISSN
2346-9307

AVISO LEGAL

Skopein® es una revista de difusión gratuita en su formato online, sin fines de lucro, destinada al público hispanoparlante de todas partes del mundo, ofreciéndoles a estudiantes, graduados y profesionales, un espacio para publicar sus artículos científicos y divulgativos, con su respectivo registro digital de propiedad intelectual, detallado en el siguiente apartado. Por lo tanto, la revista no se hace responsable de las opiniones y comentarios que los lectores expresen en nuestros distintos medios (como el foro), ni de las opiniones y comentarios de los colaboradores que publican dentro de la misma, y en ningún caso representando nuestra opinión, ya que la misma sólo se verá reflejada dentro de las notas de la Editorial.

El equipo revisa el contenido de los artículos publicados para minimizar el plagio. No obstante, los recursos que manejamos son limitados, por lo que pueden existir fallas en el proceso de búsqueda. Si reconoce citas no señaladas de la manera debida comuníquese con nosotros desde la sección de contacto, o regístrese en nuestro foro para participar dentro del mismo.

Registro de propiedad Intelectual

ESTEREOSCOPIO

Proviene de las raíces griegas "Stereo", que significa sólido, y del verbo "Skopein", que significa observar, examinar, considerar.

[1]

"Aparato óptico en el que, mirando con ambos ojos, se ven dos imágenes de un objeto, que, al fundirse en una, producen una sensación de relieve por estar tomadas en un ángulo diferente para cada ojo" - *Real Academia Española, 2001*

Para publicar* en Skopein, realizar consultas y sugerencias:

info@skopein.org

*mayor información en www.skopein.org/publicarskopein.html

[1] Ejemplo de imagen obtenida con un estereocopio

NOTA EDITORIAL

Hemos llegado al mes de junio, y para el hemisferio en el que nos encontramos, es el frío el encargado de recordarnos que ya ha finalizado la primera mitad del año 2015, sin embargo estamos contentos de poder anunciar algunas novedades particulares provenientes de quienes hacemos Skopein.

Por un lado, el cuerpo editorial felicita a uno de sus directores, Carlos M. Diribarne, por obtener recientemente su título de Lic. en Criminalística, al haber aprobado con elogios su tesina; en este número hemos incluido la segunda parte resumida del tema desarrollado en la misma.

Por el otro, también queremos felicitar al director Diego A. Alvarez, por haber sido distinguido como miembro honorario de la Sociedad de Tecnólogos Forenses (SOTEMFOR) del Perú, para lo cual agradecemos particularmente al Dr. Angelo Ascarza Gallegos, su presidente fundador, por este otorgamiento, y la realización de un convenio de mutua colaboración académica entre Revista Skopein y SOTEMFOR.

Desde Skopein, también participamos en la 1° Feria de Editoriales y Revistas Independientes en la Facultad de Humanidades y Ciencias de la Educación, organizada por la Universidad Nacional de La Plata.

Pero las novedades de esta primera parte del año no serán nada comparado a los proyectos que venimos preparando para la segunda mitad del 2015. Uno de ellos será la realización de las JACFA, primeras jornadas organizadas por Skopein, y que habíamos adelantado en el número anterior. Estas Jornadas Argentinas de Ciencias Forenses Aplicadas, que se llevarán a cabo los días 13 y 14 de Agosto en CABA, serán de entrada libre y gratuita. Conforme pasen las semanas, informaremos el procedimiento de inscripción y más novedades mediante las redes sociales. En la página oficial del evento podrán encontrar más información: www.skopein.org/jacfa

La segunda novedad es la primer publicación especial de Revista Skopein, que será temática sobre Asesinos Seriales Históricos, con dos excelentes investigaciones, una sobre Jack el Destripador y otra sobre el Petiso Orejudo, y que se publicará a principios de Agosto.

En este número podrán apreciar una entrevista a una reconocida entomóloga forense, la Dra. Adriana Oliva, a quien agradecemos su predisposición e interés en participar en Skopein. También hemos llevado la cobertura del "IX Congreso Argentino de Derecho Informático" (ADIAr 2015), invitados por cortesía del abog. Miguel Summer Elías, director de Informática Legal.

Como ya es costumbre, agradecemos a todos los lectores y suscriptos que siguen nuestras publicaciones y dan el apoyo para continuar escribiendo con constancia, y esperamos que las distintas notas les sean de interés.

Skopein

Armas de Fuego
"Inteligentes" o "Personalizadas" 6
Por: María E. Recagno

Entrevista Exclusiva a:
Adriana Oliva 16
Entomóloga forense e investigadora del CONICET

Posible Revisión de la Pena para los Ingestados 26
Por: Gabriela S. Sosa

Animaciones y Recreaciones Crimino-Dinámicas en 3D 31
Por: Fabrizzio Theiler Gioia

¡Skopein Presente! en...
IX Congreso Argentino de Derecho Informático 37

RUIV, Reconstrucción de la Última Imagen Visual (Parte II) 44
Por: Carlos M. Diribarne

Skopein Responde 50

Robo de Mercadería en Tránsito 53
Por: Daniel P. Amarillo

Armas de Fuego "Inteligentes" o "Personalizadas"

*María Elena Recagno**

marierecagno@hotmail.com

Introducción

La presente investigación parte de la problemática en la que se encuentran involucradas las armas de fuego. Con frecuencia las personas adquieren armas con la idea de la autodefensa y seguridad personal o familiar; sin embargo, hay pruebas contundentes de que las armas de fuego en realidad ponen en peligro a quienes las poseen: muchos delincuentes actúan a través del "factor sorpresa" y si la víctima está armada, aumenta la probabilidad de que la hieran o maten. Otro punto importante son los accidentes fatales que ocurren cuando hay armas en los hogares y no se toman los recaudos necesarios, las víctimas por lo general son los menores o las personas que no poseen los conocimientos pertinentes en el manejo de éstas.

Desde el año 1990 aproximadamente, numerosos equipos han desarrollado armas de fuego con una avanzada tecnología de seguridad llamadas armas de fuego "inteligentes" o "personalizadas", con distintos grados de evolución tecnológica. Estas armas están diseñadas para contener sistemas de autorización que generalmente combinan un mecanismo de autenticación con un mecanismo de bloqueo en un proceso ininterrumpido y rápido, lo que aporta gran fiabilidad y seguridad ya que permiten operar o disparar el arma exclusivamente a un usuario autorizado o conjunto de usuarios y desactivarla automáticamente bajo circunstancias específicas, reduciendo las posibilidades de uso accidental o intencional por un usuario no autorizado. Es decir que únicamente podrán ser utilizadas por su legítimo usuario.

A continuación, si bien es información de público conocimiento, creo necesario aclarar quienes se consideran "legítimos usuarios" en nuestro país. Existen dos circunstancias: la tenencia que autoriza al legítimo usuario a tener el arma en su poder, transportarla (siempre descargada y tomando las precauciones necesarias) para utilizarla con fines lícitos tal como la caza, el tiro deportivo, etc.; y la portación que se basa en poseer el arma de fuego cargada, lista para ser usada, en un lugar público. La autorización para esta última, es de carácter restrictiva: sólo la poseen los integrantes de las Fuerzas de Seguridad o empresas de seguridad que han pasado por infinidad de controles del RENAR.

Tecnologías utilizadas para la autorización del usuario

* *Estudiante avanzada de la Licenciatura en Criminalística (IUPFA).*

Un sistema de autorización general, combina un mecanismo de autenticación que acciona un mecanismo de bloqueo en un proceso ininterrumpido diseñado para tomar menos tiempo que la manipulación y el disparo de un arma convencional.

Los mecanismos de autenticación utilizan identificación por radiofrecuencia (RFID), biometría, o alguna otra tecnología que se pueda utilizar para establecer una identidad única. No es necesario que ésta "identidad única" sea algo intrínseco del usuario, tal como la huella digital, sino que podría ser un código único de difusión a distancia muy corta dada por un token[1] de RFID usado por el operador como un anillo, pulsera o reloj.

Una vez que el usuario es identificado y autenticado, los sistemas de autorización por lo general, energizan un circuito electrónico que produce un cambio físico, por ejemplo la eliminación de un bloque mecánico para permitir que el arma se pueda disparar. Los mecanismos de bloqueo que se han empleado incluyen solenoides[2], motores y dispositivos piezoeléctricos[3] que se utilizan como actuadores que responden a las señales del mecanismo de autenticación.

Tecnologías Basadas en Token

Las Tecnologías Basadas en Token requieren el uso adicional de un elemento físico tal como un anillo, reloj, tarjeta, o pulsera para permitir la operación del sistema. Estas fichas pueden ser transportadas, usadas, o incluso implantadas en el usuario autorizado. Este objeto externo requiere que el usuario recuerde tenerlo siempre consigo y es susceptible al robo por parte de personas no autorizadas. Sin embargo, existen medidas de seguridad adicionales como por ejemplo un código PIN (Número de Identificación Personal) que puede resolver el inconveniente.

Identificación por Radiofrecuencia (RFID)

La Tecnología RFID consiste en el uso inalámbrico de campos electromagnéticos de radiofrecuencia para transferir datos a los efectos de identificación y seguimiento automático de etiquetas asociadas a los objetos. Algunas etiquetas no necesitan batería y funcionan a distancias cortas por inducción electromagnética[4], se denominan "etiquetas pasivas"; otras usan una fuente de alimentación local y emiten ondas de radio, se denominan "etiquetas activas".

La etiqueta contiene información almacenada electrónicamente que puede ser leída desde varios metros de distancia. La ventaja que posee ante un código de barras, es que no es necesario que esté dentro de la línea de visión del lector y además, puede ser colocada en objetos de diversa naturaleza sin inconvenientes.

Con respecto al funcionamiento, los sistemas constan de etiquetas o tags, lectores y software para procesar datos. Los tags se aplican a los objetos y son capaces de almacenar varios tipos de datos, como números, letras, instrucciones de configuración, datos obtenidos por sensores como la temperatura, la presión, etc. Los lectores pueden ser unidades autónomas o estar integrados a un terminal portátil.

[1] Testigo.- Paquete de datos que circula a través de una red local y que determina qué nodo puede iniciar una transmisión. (Electrónica2000, s.f).
[2] Selenoide: en electrotecnia, se conoce con dicho nombre un arrollamiento en forma de hélice cilindrica de alambre conductor en cuyo interior se produce la formación de un campo magnético. (Diccionario. Motorgiga, s.f).
[3] Piezoelectricidad.- Propiedad de algunos cristales, particularmente el cuarzo, por la que aplicando a los mismos una fuerza mecánica se obtiene una tensión eléctrica. Y viceversa, la aplicación de una tensión eléctrica produce en ellos una fuerza mecánica. (Electrónica2000, s.f).
*[4] Inducción electromagnética: en física, este vocablo indica generalmente aquellos fenómenos por los cuales un cuerpo (inducido) acusa los efectos producidos por otro cuerpo (*inductor). La inducción electromagnética se manifiesta especialmente como producción de fuerza electromotriz, denominada también corriente inducida, en un conductor sometido a un campo magnético de flujo variable. (Diccionario. Motorgiga, s.f).*

En lo que respecta a la seguridad y confiabilidad, las etiquetas de RFID son sumamente difíciles de falsificar: se requieren avanzados conocimientos de ingeniería inalámbrica, algoritmos de codificación y técnicas de cifrado. Además, se pueden aplicar distintos niveles de seguridad a los datos almacenados.

En el contexto de este trabajo, la tecnología basada en token y RFID establece un canal de comunicación entre el arma de fuego y el objeto adicional. El lector RFID del arma emite una señal en busca de un tag, entonces otra señal codificada es enviada desde el objeto (que contiene el tag) hacia el arma que autorizará el disparo o no. Cabe señalar que cualquier tecnología de RFID podría ser afectada por interferencias, pero dependerá de factores tales como la frecuencia y el régimen de funcionamiento; los rangos utilizados en estos casos son muy poco susceptibles a la interferencia debido a la corta distancia del funcionamiento.

Tecnologías Magnéticas

En estas tecnologías se utiliza simplemente un imán para mover magnéticamente el mecanismo de bloqueo situado en el interior del arma de fuego. Este sistema no ha sido ampliamente adoptado. Las interferencias son abundantes debido a que es común hallar otros imanes en el lugar. Es inespecífico.

Tecnologías Biométricas

La palabra biometría proviene del griego “bios” (vida) y “metron” (medida), es la ciencia que se dedica al análisis estadístico de las características cuantitativas de los seres vivos como el peso, la longitud, etc. Un elemento biométrico es un rasgo fisiológico o de comportamiento mensurable de una persona viva, utilizado para identificar a una persona o verificar una identidad declarada (autenticación). Dado que el elemento biométrico está ligado a una sola persona, constituye un factor más que determinante.

Los sistemas de seguridad utilizan tres métodos de autenticación:

- Algo que la persona sabe: clave secreta/contraseña, número de identificación (PIN).

- Algo que la persona tiene: llaves, tarjeta de proximidad, tarjetas inteligentes, token, etc.

- Algo que la persona es: un dato personal biométrico (huella dactilar, geometría de la mano, etc).

Un sistema biométrico, es un sistema informático de reconocimiento que funciona extrayendo un patrón algorítmico de los datos biométricos aportados por un individuo en primera instancia, y luego comparando el mismo contra una plantilla previamente almacenada en una base de datos fija o en un dispositivo transportable como ser un token o tarjeta inteligente, dependiendo de su aplicación.

Los períodos del análisis biométrico son:

- Fase de registro: el individuo otorga un elemento biométrico, del cual se extrae una representación matemática de los datos que éste contiene. Este modelo es almacenado.

- Fase de verificación: el dato biométrico adquirido por el sistema mediante el confronte es analizado tanto para la autenticación como para la identificación.

Entonces, las tecnologías biométricas utilizan características únicas de los individuos como "clave" para identificar a los usuarios autorizados. Algunos ejemplos de tecnologías biométricas incluyen huellas

digitales, impresión de la palma, la voz, la cara y el patrón venoso, aunque no todos ellos son utilizados para la autorización del arma de fuego. Además, se utilizan sensores o lectores electrónicos adecuados para recoger los datos biométricos y compararlos con los de los usuarios autorizados, que han sido previamente almacenados en la memoria de un ordenador.

Tecnologías de Huella Digital

Para iniciar la autorización, el usuario coloca su dígito en un sensor de huellas dactilares; éste se encuentra en un área de acceso natural que requiere poco o ningún esfuerzo consciente para lograr la posición adecuada, como en la empuñadura, donde el dedo se apoya normalmente. Una vez que la huella digital se escanea, se produce rápidamente la comparación con una base de datos de huellas dactilares de los usuarios autorizados almacenada internamente. Si encuentra coincidencia, el arma de fuego se activa; de lo contrario, permanece bloqueada.

Tecnologías de Impresión Palmar

Funcionan al igual que las tecnologías de huellas dactilares pero con el uso de la impresión de la palma de la mano como única identificación. Hasta la actualidad, esta tecnología no ha podido ser integrada con éxito como sistema de autorización en un arma de fuego.

Tecnologías de Agarre Dinámico

El Reconocimiento de Agarre Dinámico (DGR) es un método que utiliza biometría dinámica, es decir que no se basa en un rasgo físico del individuo, tal como una huella digital, sino más bien en los comportamientos de agarre que pueden ser utilizados como una actividad identificable que se mide durante un período de tiempo. Las características que podrían medirse como parte del DGR incluyen el tamaño de la mano, la geometría de la mano y la presión o la fuerza. La investigación sobre DGR permanece a prueba y todavía no ha sido ampliamente aceptada en la práctica.

Tecnologías de Agarre Estático

El Reconocimiento de Agarre Estático (SGR) es un método de autenticación biométrica basado en el comportamiento humano de agarre en un momento fijo en el tiempo. El SGR simplemente mide la presión aplicada sobre la empuñadura del arma de fuego. Esta tecnología también se encuentra a prueba.

Tecnologías Ópticas

Son técnicas de autorización que utilizan métodos ópticos para la identificación por medio de datos espectroscópicos, tales como las variaciones leves del color de la piel, o datos de imagen, como el patrón de las venas en el reconocimiento de la palma de la mano. Este enfoque tecnológico no ha sido ampliamente adoptado.

Prototipos

Diversos fabricantes han comenzado a desarrollar esta nueva tecnología de seguridad llegando a crear con éxito armas de fuego completas, accesorios o sólo diseños que se seguirán estudiando. La mayoría con la ayuda de subsidios del Instituto Nacional de Justicia de los Estados Unidos.

- Armatix de Alemania ha desarrollado el “Smart System” que se compone de dos partes principales: la iP1 que es una pistola

calibre .22 que se activa por el iW1, un dispositivo que se lleva en la muñeca como un reloj. Se comunican utilizando identificación por radiofrecuencia (RFID).

○ Industrias Kodiak de Utah creó el "Intelligun", un sistema de bloqueo basado en huellas dactilares instalado en una pistola M1911 calibre .45 que desbloquea el funcionamiento únicamente para los usuarios autorizados.

○ En 1997 Colt's Manufacturing Company, Inc. de Hartford, CT desarrolló un arma inteligente basada en la comunicación por radiofrecuencia. Consistía en una pulsera que se comunicaba con el arma de fuego y le permitía actuar mecánicamente cuando se encontraba cerca. Los prototipos resultaron ser poco fiables y no estaban construidos lo suficientemente sólidos como para permitir el disparo.

○ iGun Technology Corporation de Florida desarrolló en 1998 la "M-2000", una escopeta que se podría considerar la primera arma de fuego personalizada por ir más allá de un prototipo. El operador lleva un anillo con una etiqueta RFID pasiva incrustada que se comunica mediante un código específico con un lector de RFID a bordo de la escopeta.

○ Entre 2000 y 2005, Smith & Wesson de Springfield, MA, exploró diferentes métodos de autenticación incluyendo códigos PIN, biometría (huellas digitales), enfoques espectroscópicos del tejido epidérmico y también un sensor de agarre que era incorporado en la empuñadura de la pistola.

○ Entre 2000 y 2006, FN Manufacturing, Inc., de Columbia, Carolina del Sur, una sucursal de FN Herstal, presentó un informe técnico completo y un prototipo diseñado, desarrollado e integrado que se habilitaba mediante RFID llamado "Secure Weapon System" (SWS). El sistema se componía de un anillo que contenía una etiqueta RFID incrustada y un mecanismo piezoeléctrico integrado en la pistola que evitaba que el arma se disparara cuando el anillo estuviera fuera de la proximidad. Al probar los prototipos se observaron errores en el sistema de autorización y en la fuerza mecánica contundente, que anulaba el pasador de bloqueo electromecánico controlador. A falta de una financiación adicional para continuar con la investigación y las pruebas, el proyecto no tuvo éxito.

○ Entre 2004 y 2008 el Instituto de Tecnología de New Jersey (NJIT) desarrolló una tecnología de autenticación de usuario basada en el reconocimiento dinámico de agarre. El diseño "Child Safe Personalized Weapon" utilizaba múltiples sensores de presión situado en las almohadillas de agarre izquierdo y derecho en la empuñadura de la pistola.

○ TriggerSmart, con sede en Irlanda asociado con el Instituto de Tecnología de Georgia, desarrolló un dispositivo basado en la tecnología RFID consistente en una pieza de recambio a cargo del usuario que podría ser utilizada en cualquier tipo de arma de fuego.

○ Safe Gun Technology (SGT), de Columbus, GA, desarrolló una versión de la escopeta Remington 870, "prototype user-authorized", con un sistema de autorización que utilizaba un sensor de identificación de huellas dactilares. El sistema contaba con un paso de "autorización única" para preparar el arma, que permanecía en un estado de armado mientras una mano aplicaba presión en la empuñadura. Si se liberaba la presión por más de un segundo o el arma se caía, el sistema se desautorizaba.

Finalmente, con el objetivo de difundir las tecnologías existentes, se hará un breve desarrollo de algunos de los sistemas que existen en la actualidad y cuya evolución tecnológica ha llegado al nivel máximo conformando un diseño y prototipo avanzado que ha superado las pruebas de funcionamiento y fiabilidad adecuadas.

IGUN TECHNOLOGY CORPORATION

La escopeta iGun M-2000 fue desarrollada en 1998. El operador lleva un anillo con una etiqueta RFID pasiva incorporada que responde a un código específico cuando se energiza por el lector RFID a bordo de la escopeta. Si el código coincide con el arma, se solicita una segunda verificación, y sólo si la segunda verificación se corresponde, el arma activa el mecanismo de disparo.

Como se muestra en la Figura 1, la iGun M-2000 fue diseñada como un sistema integrado, no como un accesorio o una modificación del arma de fuego.

El prototipo comenzó a desarrollarse en 1995 e involucró la utilización de imanes para prevenir el uso no deseado, pero estos no eran "inteligentes" y la operación se podía ver afectada por cualquier otro imán. El concepto fue revisado en 1998 para utilizar la tecnología RFID.

Para disparar la M-2000, el usuario pulsa una tecla ubicada en la culata de la escopeta, posicionado por la colocación natural de una mano. La palanca activa el sistema electrónico integrado que emite una señal de radiofrecuencia a una distancia máxima efectiva de dos pulgadas (5 cm aprox.). El arma busca una respuesta por el chip RFID incrustado en un anillo que usa el usuario. Dos códigos son solicitados por el arma desde el chip, y con más de 18 billones de combinaciones disponibles, hay pocas posibilidades de error en la identificación. Cuando el anillo proporciona una respuesta positiva al arma, el usuario escuchará un suave "clic" (por dentro y fuera), así como un indicador rojo visual, como se ve en la fig. N° 1, y a continuación podrá efectuar el disparo.

La M-2000 funciona rápidamente al ser accionada (<0,25 segundos), y el sistema se apaga de inmediato cuando el usuario suelta el agarre del arma o cuando el chip RFID del anillo se retira de la proximidad (dos pulgadas), utilizando un diseño patentado de doble solenoide para bloquear la cola del disparador. El objetivo es proteger al usuario autorizado en el caso de que la escopeta se le quite y se le vuelva en su contra.

La batería se ha diseñado para operar a través de un uso normal durante 10 años y es fácilmente reemplazable. Tienen medidas especiales y circuitos que advierten que queda poca carga a través de una señal acústica para dar al usuario el tiempo adecuado para reemplazarla.

En caso de querer manipular dolosamente el arma, ésta se vuelve inoperable. Por ejemplo, la eliminación de los componentes electrónicos o el mecanismo de bloqueo dejarían al arma incapaz de disparar. Intervenir en el sistema mediante el uso de energía para activar el arma o para tratar de forzar el sistema de un modo operativo probablemente quemaría los componentes electrónicos. Una persona tendría que tener un conocimiento sustancial del sistema para accionar el mecanismo de bloqueo.

Al igual que un arma de fuego tradicional, la M-2000 no es impermeable ni totalmente resistente al impacto pero puede

Fig. N°1. Escopeta iGun M-2000.
Greene, M. (Junio 2013). A Review of Gun Safety Technologies (NCJ 242500).

ser reparada en algunos casos. La susceptibilidad a la corrosión de la electrónica es limitada, ya que se encuentra encerrada en la culata lejos de los lugares comúnmente expuestos, además se encuentra lejos de las áreas que se limpian y lubrican.

Esta tecnología podría adaptarse a cualquier otra arma de fuego. El fabricante decidió comenzar con una escopeta, que tiene la característica de necesitar un golpe e impulso fuerte por lo que la migración a otros modelos sería más sencilla.

ARMATIX GmbH

Armatix ha desarrollado un sistema inteligente que consiste en un arma de puño diseñada originalmente (iP1) y un transpondedor a modo de reloj pulsera (iW1). El sistema inteligente utiliza RFID activa para establecer la comunicación entre el transpondedor que se lleva en la muñeca y el arma de fuego. Además, el transpondedor requiere una identificación con un código que es un número personal y hace de entrada antes de transmitir una señal de autorización al arma.

El iP1 es una pistola calibre .22 de doble acción con un cargador de 10 cartuchos, como se muestra en la Figura 2. Armatix diseñó el arma con el fin de integrar el sistema de autorización a nivel del diseño, en lugar de tratar de incorporar el sistema en un arma de fuego ya disponible comercialmente. La pistola utiliza un mecanismo de bloqueo integrado que le permite disparar sólo si recibe una señal de autorización desde el transpondedor de la pulsera. Se requiere la sincronización entre varios componentes mecánicos y electrónicos.

La pulsera autoriza al usuario a través de un código PIN de cinco dígitos, y también parece y funciona como un reloj digital (ver Figura 3). Para activar el sistema, el usuario introduce el código PIN usando cuatro botones ubicados en el reloj. Si el código PIN es incorrecto, aparecerá la palabra "FAIL" en la pantalla del reloj. Si el código PIN es correcto, aparecerá la palabra "GOOD" y además debe introducirse un "tiempo restante" de autorización (ocho horas como máximo, una hora como mínimo). El reloj entonces envía una señal a la pistola que le permite ser disparada por el período de tiempo especificado. Una vez transcurrido el tiempo establecido, la pistola se desactivará; asimismo se lo puede hacer manualmente antes de que transcurra el tiempo. La pistola también se desactivará si se mueve más allá del rango de la guardia (15 pulgadas) y se activará automáticamente de nuevo cuando vuelva a la distancia de activación.

Cuando las baterías se insertan por

Fig. N° 2 . iP1 (pistola calibre .22) Greene, M. (Junio 2013). A Review of Gun Safety Technologies (NCJ 242500).

Fig. N° 3. Armatix iW1 Reloj-pulsera Greene, M. (Junio 2013). A Review of Gun Safety Technologies (NCJ 242500).

Fig. N° 4. Luces indicadoras en el iP1 mostrando el arma de fuego en un estado no autorizado (rojo) y un estado autorizado (verde) durante un disparo de prueba del sistema inteligente en el Laboratorio de Ciencia Forense de la Policía del Estado de Maryland, en febrero de 2013. Greene, M. (Junio 2013). A Review of Gun Safety Technologies (NCJ 242500).

primera vez en el Sistema Inteligente (dos AAA estándar en la pistola y CR2032 en el reloj), el reloj y la pistola deben estar sincronizados, un procedimiento que tarda unos segundos. Una pantalla LED en el arma de fuego indica el estado siguiente:

• Azul: No se insertaron (el arma no se dispara, incluso si hay cartucho en recámara).

• Rojo: La pistola no está lista para disparar (no autorizada o no sincronizada).

• Verde: La pistola está lista para disparar.

• Indicador Intermitente - Batería baja.

El reloj y el arma deben tener un juego de códigos PIN, que se proporcionan a los clientes en las tarjetas de seguridad PIN. Si un reloj se pierde o destruye, un nuevo reloj debe ser reprogramado con el código PIN de la pistola. Para aplicaciones en las fuerzas policiales, es posible tener un reloj que autoriza a más de un arma de fuego, así como tener un arma de fuego operada por más de un reloj.

Armatix tiene proyectos en curso para el desarrollo de fusiles de cerrojo, semiautomáticos y automáticos, rifles, escopetas y revólveres. También ha puesto a prueba una pistola de 9 mm y un revólver calibre .44 y prevé hacer estos modelos disponibles para el mercado en el futuro.

Industrias KODIAK

Industrias Kodiak lanzó un arma de fuego con identificación biométrica llamada “Intelligun” en 2012. Es pistola calibre .45 M1911 que tiene instalado un sistema de bloqueo basado en huellas digitales, que utiliza un diseño patentado para bloquear completamente la operación de la pistola cuando no está en uso, mientras que la desbloquea inmediatamente (en una fracción de segundo) para los usuarios autorizados.

La Intelligun se compone de una empuñadura blindada cerrada y un muelle principal combinado con tornillos especiales de seguridad para evitar la manipulación del sistema. La unidad está sellada, es resistente químicamente y con planes futuros para la impermeabilización.

El sistema se activa cuando la persona aplica presión a través de la sujeción del arma

mediante sensores instalados en la empuñadura, en un proceso natural. El usuario del sistema coloca el dígito mayor en el sensor biométrico y tan pronto como el sistema haya completado el arranque, lee la huella dactilar y la compara con los usuarios autorizados. El sistema seguirá funcionando siempre y cuando permanezca el agarre por parte del usuario. Todo el proceso tarda una fracción de segundos.

La pistola también posee otro sistema de seguridad de funcionamiento basado en la presión, que trabaja mediante la desactivación de la capacidad de disparar tan pronto como se libera el agarre. Además se puede ajustar la duración en que el sistema sigue en funcionamiento cuando un usuario autorizado detiene el agarre. El arma entrará en un modo de "alta seguridad" si una persona no registrada intenta utilizarla varias veces (3x); y con el fin de devolver el arma de fuego a un estado operativo, el administrador debe volver a activar el sistema a través de una secuencia específica de pasos.

La unidad tiene tres luces emitidas por diodos (LED) que son indicadores de estado -rojo, amarillo y verde- para proporcionar el estado del sistema, la duración de la batería, y la información operativa. Un botón permite visualizar el estado del sistema y de la batería. Cuando se mantiene pulsado este botón, se atenúan los indicadores LED para uso nocturno, y si el proceso se repite, se vuelve al funcionamiento diurno.

Después de la compra, la primera persona que empuñe y coloque el dígito en el sensor de huellas dactilares comenzará la inscripción de administrador en el sistema; sólo hay un administrador, y sólo él puede agregar nuevos usuarios. Durante la inicialización y las nuevas adiciones de usuarios, el sistema requerirá captar múltiples (de tres a cinco) huellas digitales para inscribir adecuadamente a una persona; esto permitirá que el sistema reconozca mejor la huella digital, incluso si no está completamente sobre el sensor biométrico en el momento de uso. Si desea, el administrador del arma puede realizar un barrido que eliminará a todos los usuarios excepto a él; sólo un reinicio de fábrica puede eliminar por completo todos los usuarios incluyendo al administrador original y volver el sistema a un estado inactivo.

La batería de iones de litio debe durar alrededor de un año mientras que su uso sea de dos a tres veces por semana (o aproximadamente 800 horas). Se carga a través de un puerto estándar micro USB.

También requiere una instalación para zurdo o diestro debido al sensor y el indicador de posicionamiento; aunque Kodiak está trabajando en planes para desarrollar una versión ambidiestro del sistema, si su progresión tecnología lo permite. Inclusive, un registro de usuario o funciones de GPS podrían ser añadidos en el sistema si la demanda de mercado lo requiere en el futuro, pero no son

Fig. N° 5. Sistema Intelligun - pistola M1911.
Greene, M. (Junio 2013). A Review of Gun Safety Technologies (NCJ 242500).

parte de la unidad actual Intelligun.

El desarrollo original del sistema se dirige a las fuerzas de seguridad y militares, y se ha explorado el uso para aplicaciones de seguridad aérea. La comercialización incluye a las familias que buscan opciones más seguras de armas de fuego.

Conclusión

Al mencionar los beneficios que aportan estos nuevos sistemas de seguridad, debemos considerar que su mayor propósito es atenuar los riesgos asociados con el uso o mal uso de las arma de fuego. Evitar lesiones o la muerte por disparos accidentales, por el mal manejo o uso indebido de un inexperto o persona no autorizada, como es el caso de los niños, e impedir el funcionamiento del arma cuando está en posesión ilegal y se pretende usar con fines delictivos.

Ahora bien, con respecto a la fiabilidad de estas armas llamadas “inteligentes” o “personalizadas”, la habitual preocupación se centra en el rendimiento y en la aceptación de estas nuevas tecnologías. Puede existir cierta desconfianza debido al temor de que en una situación límite, de vida o muerte, se produzca el mal funcionamiento del arma o que el sistema no cumpla con su función de inhabilitarla en los casos en que fuera necesario. Pero la desconfianza se debe a que estos sistemas aún se encuentran en vías de desarrollo y no han alcanzado un gran reconocimiento por parte de la sociedad, cuestión que será subsanada en el futuro.

A pesar de lo expuesto, insisto en que tenemos que ser conscientes de que ninguna nueva tecnología de seguridad podrá eliminar completamente las consecuencias negativas que muchas veces acarrean los errores producidos por el factor humano. Los riesgos están siempre latentes.

Bibliografía

Arbelo, F.R. y Freire Pazó, C. (2004). Biometría y Seguridad. Revista Ciencia Policial, Nº 72, 61-71.

Ballestin, A. (1 de febrero de 2010). Armatix presenta una pistola con identificación biométrica. Engadget. Recuperado de http://es.engadget.com/2010/01/31/armatix-presenta-una-pistola-con-identificacion-biometrica/. Consultado 12 de septiembre de 2014.

Blázquez del Toro, L.M. Sistemas de Identificación por radiofrecuencia (Código: 10.8). Recuperado de http://www.it.uc3m.es/jmb/RFID/rfid.pdf. Consultado 18 de octubre de 2014.

Electronica2000 (s.f). Piezoelectricidad. Recuperado de http://www.electronica2000.com/dic_elec/p.htm. Consulado 28 de mayo de 2015.

Electronica2000 (s.f). Token. Recuperado de http://www.electronica2000.com/dic_elec/t.htm. Consultado 28 de mayo de 2015.

Greene, M. (Junio 2013). A Review of Gun Safety Technologies (NCJ 242500). Whashington, DC: U.S. Department of Justice, Office of Justice Programs, National Institute of Justice. Recuperado de https://www.ncjrs.gov/pdffiles1/nij/242500.pdf. Consultado 12 de septiembre de 2014.

Intermec. Conceptos básicos de RFID: Conocimiento y uso de la identificación por radiofrecuencia. Recuperado de http://www.intermec.com.mx/learning/content_library/white_papers/localized/wpABC_MX.pdf. Consultado 18 de octubre de 2014.

Motorgiga (s.f). Inducción- definición- significado. Recuperado de http://diccionario.motorgiga.com/diccionario/induccion-definicion-significado/gmx-niv15-con194447.htm. Consultado 28 de mayo de 2015.

Motorgiga (s.f). Solenoide- definición- significado. Recuperado de http://diccionario.motorgiga.com/diccionario/solenoide-definicion-significado/gmx-niv15-con195603.htm. Consultado 28 de mayo de 2015.

RENAR (s.f). Diferencia entre tenencia y portación. Recuperado de https://www.renar.gov.ar/faq3.htm. Consultado 28 de mayo de 2015.

Tapiador Mateos, M. y Singüenza Pizarro, J. A. (2005). Tecnologías Biométricas Aplicadas a la Seguridad. México: Alfaomega Grupo Editor, S.A.

Tecnología biométrica inteligente para uso más seguro de armas de fuego (16 de mayo de 2013). IDNoticias. Recuperado de http://www.idnoticias.com/2013/05/16/tecnologia-biometrica-inteligente-para-uso-mas-seguro-de-armas-de-fuego#top. Consultado 12 se septiembre de 2014.

Thill, E. (2011). Biometrías. Buenos Aires: Jefatura de Gabinete de Ministros-Presidencia de la Nación.