Conociendo la Seguridad ENTRUST, una Tecnología que Facilita el Entorno Empresarial

Knowing the ENTRUST Security, a Technology that Facilitates the Business Environment

Conhecendo a ENTRUST Segurança, uma tecnologia que facilita o Ambiente de Negócios.

Omar A. Urrutia Rincón[1], Jorge L. Barajas Mendivelso[2], John A. Bohada
Grupo de Investigación MUISCA, Facultad de Ingeniería, Fundación Universitaria Juan de Castellanos, Tunja, Colombia.
[1]urrutia.omar60@gmail.com, [2]lyonnardobarmen@gmail.com, [3]jbohada@jdc.edu.co

Recibido / Received: 12/03/2015 – Aceptado / Accepted: 19/06/2015

Resumen

La finalidad de esta investigación es sensibilizar a las personas y empresarios, sobre la importancia de adquirir sistemas de seguridad que permitan la conservación y preservación de la información en sus compañías, de igual forma, que garanticen la distribución y protección de datos que las organizaciones tienden a dejar al descubierto, por tal motivo, se plantean algunas propuestas de mejora en los procedimientos para que las empresas implementen de acuerdo a su criterio. La deficiencia en el manejo de las comunicaciones y de la información, se ve reflejada en el éxito de las organizaciones, pues no tienen la suficiente eficiencia y eficacia en sus transacciones. En este sentido, la tecnología Entrust IdGuard, ofrece una serie de controles asistenciales personalizados, de fácil acceso a los sistemas de información, con el fin de buscar vulnerabilidades que permitan infiltraciones que arriesguen la continuidad del negocio.

Palabras clave: Tecnología Entrust IdGuard, Acceso Biométrico, Vulnerabilidades, Protección de Datos Informáticos e Internet de las Cosas (IOT).

Abstract

The purpose of this research is to sensitize people and entrepreneurs about the importance of acquiring security systems for the conservation and preservation of information in their companies, likewise, to ensure distribution and data protection organizations tend to expose, for that reason, some proposals for improvements in procedures arise for companies to implement according to their criteria. The deficiency in the management of communications and information is reflected in the success of organizations, they do not have enough efficiency and effectiveness in their transactions. In this sense, the Entrust ID Guard technology offers a number of personalized care controls with easy access to information systems, in order to look for vulnerabilities that allow infiltration that risk business continuity.

Keywords: Entrust ID Guard Technology, Biometric Access, Vulnerabilities, Protection of Computer Data, and Internet of Things (IOT).

Resumo

O objetivo desta pesquisa é sensibilizar as pessoas e empresários sobre a importância da aquisição de sistemas de segurança que permita a conservação e preservação da informação em suas empresas, da mesma forma, para garantir a distribuição e proteção de dados que as organizações tendem a expor, por essa razão, surgir algumas propostas para melhorias nos procedimentos para as empresas programar de acordo com seus critérios. A deficiência na gestão da comunicação e informação se reflete no sucesso das organizações, pois elas não têm a eficiência e a eficácia suficiente em suas transações. Neste sentido, a tecnologia Entrust ID Guard, oferece uma série de controles de cuidados personalizados, com fácil acesso a sistemas de informação, a fim de olhar para as vulnerabilidades que permitem infiltrações que pôr em perigo a continuidade dos negócios.

Palavras-chave: Tecnologia Entrust ID Guard, acesso biométrico, vulnerabilidades, proteção dos dados do computador e da Internet das Coisas (IOT).

I. Introducción

Según los estudios realizados a través de la historia [1], se ha demostrado que cerebros humanos desarrollados y con pocas armas, han logrado sobrepasar las innovaciones tecnológicas de avanzada, mediante la utilización de elementos capaces de afectar y modificar la integridad de la información, las comunicaciones y los servicios que ofrecen las organizaciones, costándoles la credibilidad, estabilidad y hasta la permanencia en los mercados globales. Por consiguiente, esta investigación se enfoca en la conveniencia del uso de tecnologías que permitan salvaguardar tanto los datos como la información esencial para cualquier organización, todo ello basado particularmente en la Tecnología Entrust IdGuard [2], la cual está diseñada para mitigar los riesgos de la información contenida en las empresas.

La Tecnología Entrust IdGuard [2] cuenta con diversos dispositivos móviles y procedimientos de protección, que garantizan confiabilidad y disponibilidad de los datos que migran a diferentes áreas o sectores, brindando soluciones y respondiendo de forma adecuada a las expectativas y necesidades de disponibilidad, conservación y reserva de la información de las organizaciones, con altos niveles de confianza y aprovechamiento tecnológico.

II. Metodología

Para el desarrollo de la investigación, se procedió a la recopilación de información de diversas fuentes bibliográficas, explorando cuidadosamente los avances en el perfeccionamiento de sus métodos y los aportes que, desde los años 90, la tecnología Entrust IdGuard ha brindado al desarrollo de las personas y organizaciones[3]. Aunque, desde sus comienzos, este sistema no fue la mejor opción para salvar y proteger la información de las organizaciones, siempre se apoyó en la tecnología de la época para fortalecerse y tomar fuerza en la calidad de sus servicios de control, acceso, autenticación fuerte, localidad GPS, códigos y diseños de encriptación pseudo-aleatorio, generador de números criptográficamente seguros (CSPRNG, por sus siglas en inglés) [4]-[5], para relevación de contraseñas y otras actividades, haciendo posible la creación de la tecnología Entrust IdGuard.

A. Tecnología Entrust IdGuard en el Pasado

David Wagner fue el creador de la tecnología Entrust IdGuard, a comienzos de los noventas [6]. Él vio la necesidad de proteger de una mejor forma la información de los usuarios, por lo que a comienzos de siglo, hizo posible la primera infraestructura de clave pública en el mercado (PKI, por sus siglas en inglés), convertida hoy en día en el prototipo base

de todas las técnicas utilizadas [6]. Estados Unidos la implementó como Puente Federal de Autoridad de Certificación (FBCA, por sus siglas en inglés) [6], constituyéndose en componente esencial de la infraestructura de seguridad, basándose en las comunicaciones mundiales seguras. Con la tecnología PKI, Entrust se convirtió en proveedor de FBCA.

Entrust adquirió un servicio relacionado con gestión de riesgos (AmikaNow!), en el año 2004, permitiéndole un amplio conocimiento, análisis y control de la tecnología, catalogando de forma instantánea correos electrónicos según el contenido basado en su significado contextual, remplazando en forma tradicional el uso de dicho proceso [6]. A medida de que se fue implementando el servicio, también se fue adaptando un entorno corporativo hacia las políticas, obedeciendo leyes de privacidad y valores, como lo son Health Insurance Portability and Account ability Act (HIPAA, por sus siglas en inglés), Ley Gramm-Leach-Bliley, Protección de la Información Personal y Documentos Electrónicos y diversos delitos en la comisión de bolsa de valores de Estados Unidos (SEC, por sus siglas en inglés), para su diverso funcionamiento.

A medida que Entrust fue cambiando, logró obtener conversaciones con proveedores de soluciones para la detección de fraudes y claves públicas, conquistando el terreno en la industria de la seguridad, proporcionando a sus clientes un enfoque más moderno en la protección de información de sus organizaciones en el año 2006. En julio de 2007, esta compañía proyectó el inicio de una tecnología PKI basada en códigos abiertos a través de Sun Microsystems, Inc. y la Fundación Mozilla [6], suministrando certificados bajo licencia libre. Entrust fue invitada en septiembre de 2008, a ser parte de una tecnología relacionada con pasaportes electrónicos en control de acceso extendido (EAC, por sus siglas en inglés) en República Checa, debido a su éxito en los últimos años, llamando la atención del Grupo de Interoperabilidad de Bruselas (BIG, por sus siglas en inglés) y el Centro Común de Investigación de la Comisión Europea.

Dentro de esta participación y la protección de las funciones EAC, se permitió realizar pruebas en países Europeos para experimentar la aprobación de pasaportes electrónicos de segunda generación que contienen datos biométricos de huellas dactilares, verificando la interoperabilidad de cruce entre sistemas de inspección EAC y pasaportes electrónicos de diferentes países [6]. Después de un tiempo, la comprobación relacionada con los pasaportes electrónicos obtuvo grandes experiencias y beneficios para la compañía, su traspaso a Thomas Bravo redundó en el mejoramiento de su calidad desde 2009, permitiendo a sus clientes y socios brindar mejores beneficios en entornos altamente acoplados, desarrollando un número aproximado de 125 patentes en diferentes campos empresariales, permitiéndole distribuir servicios en las áreas de acceso lógico/físico, certificados digitales, localidad GPS, biometría, entre otros, perfeccionado la eficacia y eficiencia de resguardo de la información con innovadores componentes tecnológicos, y convirtiéndose en una de las organizaciones más poderosas del mundo.

B. Funcionamiento de la Tecnología Entrust IdGuard

La tecnología Entrust IdGuard se fundamenta en tres clases de servicios de autenticación distintos, los cuales justifican un rendimiento favorable para la administración de la información de las organizaciones, cuya base se encuentra en los criterios de la seguridad conocida en los años 90 [6] y que permiten reducir vulnerabilidades, amenazas y riesgos que puedan surgir en un entorno organizacional [7]-[13], siendo de esa manera un proceso transparente y limpio para el usuario. Los tres servicios de autenticación en los que se basa la tecnología Entrust son los que se detallan en la Tabla 1.

TABLA 1. TIPOS DE AUTENTICACIONES UTILIZADAS POR ENTRUST IDGUARD

AUTENTICACIÓN MULTIFACTOR	AUTENTICACIÓN MUTUA	AUTENTICACIÓN FUERTE
Se basa en lo que el usuario sabe, es y tiene.	Se basa en lo que el usuario sabe y tiene.	Se basa en lo que el usuario sabe, tiene y es.
Su funcionalidad está derivada por capas para debilitar a una persona no deseada.	Satisface a clientes en seguridad local por un contexto establecido, para poder iniciar sección, interpretando al usuario con un proveedor de seguridad.	Esta autenticación presenta un avance desde el año 2012, permitiendo elegir una atractiva oferta de seguridad en la nube.
Interpreta una autenticación con dos, para utilizarla en una red o bases de datos.	Para su funcionamiento, utiliza una arquitectura cliente servidor con un protocolo de seguridad denominada kerberos.	Es capaz de interpretar más de tres factores para su utilización, mejorando la seguridad en las empresas.
Para su uso, es característico visualizarlos en tarjetas inteligentes (chip), conexión a la web mensajes SMS, huellas dactilares tokens, entre otros dispositivos.	Donde se ve más común esta autenticación es en plataformas web login con sistema de seguridad respectivo.	Los servicios en lo que se aplica esta autenticación están vistos en los dispositivos móviles con avances biométricos y cloud servicies.

Estas tres autenticaciones permiten que la tecnología Entrust conserve una buena operación para las organizaciones, prestándole un excelente servicio y rendimiento al hardware, reducción de riegos y solución de relevancias, evitando fraudes en un entorno laboral, tal y como se evidenció en la Tabla 1. De ese modo, la autenticación mutua ayuda a los sistemas a alcanzar una mayor facilidad para obtener los datos de una forma más ágil y guiada para el usuario, en cambio, la autenticación multifactor obedece a un entorno más difícil para acceder al sistema, llevando al usuario a realizar procesos más complejos. Por otro lado, la autenticación fuerte demuestra un gran avance en su funcionalidad, ya que exige al usuario un manejo aún más variado en el ingreso a la información, debido a su utilización en la computación en la nube [7]-[13], ofreciendo servicios de alta calidad, en un sofisticado software token para móviles y EGRID [14], encargados de enviar y recibir transacciones que son evaluadas por el sistema para brindar acceso a él.

C. Técnicas y Estrategias de la Tecnología Entrust IdGuard

Como se ha indicado, el funcionamiento de la tecnología Entrust está en la forma de proteger los datos, su capacidad de supervisión logra un conocimiento previo del entorno organizacional donde esta opere [15] [16], para así identificar las falencias y debilidades, dado que las amenazas inundan nuestros sistemas sin que se pueda apreciar. Para evitar esa clase de fallas, el procedimiento a seguir consiste en identificar y detectar la forma de cómo se pone en riesgo nuestra información y procesos. Es por ello que, se ha fortalecido la forma de entregar a las empresas la seguridad y tranquilidad que ellas requieren, por medio de estrategias bien estructuradas y clasificadas en diferentes etapas que ayudan a soportar los mecanismos de ataques, aprovechando vulnerabilidades que se puedan detectar en el proceso de identificación de usuarios, definiéndolo como autenticación robusta a una solución que tiene en cuenta las inseguridades encontradas en las plataformas [17]-[20], constituyéndose en amenazas constantes por la variedad de canales que quieren tomar la información y datos que se obtienen sensiblemente por identidades verdaderas, ofreciendo una flexibilidad para complacer los requerimientos más exigentes, con aseguramiento severo, una normativa eficaz en la integridad de la información, siendo mucho más amigable con el cliente, accediendo con gestiones de identidad digital y colocando en su desarrollo un incremento en ventas con seguridad y tranquilidad, afirmando flexibilidad a los empleados y socios, mientras que el logro de la

eficiencia operativa maximiza el retorno de la inversión, controlando aún más la sostenibilidad del negocio.

Como aplicación de estas estrategias, se observó la utilización de etapas encargadas de diferentes entornos, las cuales se muestran en la Tabla 2 y que hasta el momento se han manejado en la tecnología.

TABLA 2. SOLUCIONES APLICADAS Y UTILIZADAS EN ORGANIZACIONES

AUTENTICACIÓN BASADA EN CONOCIMIENTO	IP- GEO LOCALIZACIÓN	TOKENS	CERTIFICADOS DIGITALES	BIOMETRÍA
Son modelos de calificación orientados en preguntas con respuestas interpretativas para logar un acceso. Son utilizadas más que todo para la recuperación de claves de correo electrónico, aplicaciones web, bancos (para realizar transacciones en línea). Muchas veces esta estrategia es apoyada con autenticación mutua, tokens y biometría para brindar el acceso a un sistema en general.	Ayuda a localizar objetos y personas por satélites espaciales. Su primera utilización fue en la milicia como estrategia de guerra. Su utilización está marcada por la web, correos electrónicos, hardware en los móviles para que puedan ingresar desde cualquier lugar, siendo de mucha utilidad para detectar intrusos por dirección IP. La geolocalización, para su óptimo rendimiento es mezclado con la biometría por bancos, multinacionales y móviles para su buen control de autentificación.	Son estructurados con contraseña de una sola vez. Son utilizados en Redes locales, servicios en la nube, sistema con login, empresas multinacionales, bancos. Estos objetos pueden ayudar con otros métodos, como lo son los certificados digitales, la geolocalización, sistemas móviles y actualmente con la biometría, convirtiéndose en la solución más eficaz para muchas empresas.	Son archivos enviados por correos electrónicos con forma digital para garantizar la integridad de un dato. Su utilización está basada en documentos digitales enviados por correos electrónicos para validar la autenticidad de unos datos proporcionados por empresas, bancos, instituciones, entidades gubernamentales, entre otras. Estas certificaciones no funcionan por sí solas, necesitan de un respaldo para poder dar acceso a un sistema, esta puede ser por medio de tokens, biométrica u otras estrategias para lograr su objetivo.	Es un medio que se utiliza para reconocer a una persona por su aspecto físico, huella retina, voz, etc. Está siendo utilizada para identificar personas por medio de la huella, por primera vez en china, utilizado luego para identificar criminales. Hoy en día, es muy utilizado por toda clase de empresas, especialmente bancos, entidades gubernamentales, en la milicia, servicios sociales y hospitales. La biometría se destaca más aun con apoyo de la atención mutua, certificados digitales y token, fortaleciendo su autorización en un sistema.

Las estrategias presentadas anteriormente son aplicadas en diversas organizaciones [21]-[32], fortaleciendo de forma práctica sus datos e información, conservando una mejora continua en sus procesos y permitiendo la selección de diferentes características que ayudan a encontrar tácticas, tales como Tokens, Biométrica, Geolocalización, entre otras. Estas tácticas ayudan a minimizar los fraudes, como por ejemplo, las contraseñas para organizaciones, tales como las bancarias, donde el acceso autorizado y seguro es vital para su normal funcionamiento.

III. Resultados

Del análisis de cada uno de los métodos de aplicación de la tecnología Entrust IdGuard [33]-[37], se prestó especial atención en la implementación y manejo, teniendo en cuenta el grado de complejidad en el uso, ya que a pesar de la seguridad y confiabilidad que ofrecen, se ha llegado a la conclusión de que un individuo especializado en infiltración de sistemas, podría explorar con facilidad las vulnerabilidades de los métodos, especialmente el biométrico, por ser uno de los más nuevos y menos experimentados.

Sin embargo, lo que se ha visto hasta el momento es que ha sido lo contrario, la tecnología Entrust ha beneficiado a muchas empresas, brindándoles múltiples soluciones de acuerdo a las necesidades que cada una requiere [38]-[41]. En este sentido, los diferentes métodos ofrecen seguridad y confianza, dando especial atención al método de la biométrica, puesto que se ha cruzado con técnicas modernas y actualizadas, forjándose un método confiable y eficaz para la seguridad de una organización, o los métodos de autenticación mutua y robusta, que juntos logran un buen desempeño de seguridad contrarrestando las barreras vulnerables que aparecen en un sistema.

Con respecto a la seguridad de la información en Colombia, la forma como se ha desempeñado no ha sido muy favorable tecnológicamente hablando, dado que Entrust no ha enfocado su visión en el país, permitiendo inseguridad en sus sistemas, es decir, sus políticas de seguridad no son suficientes para resguardar la información, sin embargo, algunas multinacionales como Claro, Telefónica, Microsoft, Cisco, BBVA, entre otras, que están aplicando estos innovadores métodos, han mejorado su calidad de servicio y, por consiguiente, se cree que Entrust IdGuard debería globalizarse y extenderse a países aceptando que la tecnología pueda conservar estabilidad de perfeccionamiento y orden a la hora de determinar una tarea específica para brindar un mejor servicio [42]-[45].

De igual forma, las entidades gubernamentales han venido experimentando técnicas como el sistema de votaciones, que consiste en realizar un registro de código de barras, para este caso de la cédula de ciudadanía, que asegura la información suministrada mediante un sensor-lector, el cual ha sido utilizado en las principales ciudades del país durante procesos de elecciones. De acuerdo con lo anterior, el objetivo es simplificar el proceso y verificar la información de los votantes de manera ágil y eficaz, sin embargo, los resultados de las pruebas no han sido los esperados, por lo que se ha considerado implementar el sistema de autenticación multifactor que provee la tecnología Entrust, ya que este proporciona con seguridad un ágil manejo del sistema orientado a dispositivos móviles, web y tradicional, administrado por métodos de biometría, geolocalización y contraseñas aleatorias, autorizándole al usuario realizar su voto desde casa [45]-[49].

IV. Discusión

Se sabe que los avances tecnológicos en seguridad y facilidad de la información, han llevado a que el ser humano avance en el logro de sus ambiciones y alcances, a tal punto que el uso de las nuevas tecnologías lo absorban y dominen por completo [49]-[53], sin que haya forma de defenderse y liberarse de ellas, pues la dependencia se ha convertido en necesidad no solo de intercomunicarse con el resto del planeta, sino de realizar operaciones, inclusive sin la intervención humana, por ejemplo, neveras inteligentes, las cuales permiten controlar productos y pedirlos directamente al supermercado; vasos inteligentes, que permiten el pago del servicio y la descripción de la bebida; pulseras inteligentes, que permiten mostrar un reporte de la salud del usuario; Near Field Communication (NFC), que permite la lectura de etiquetas e ingresa a la información multimedia y servicio; Cloud Computing, el cual es el almacén permanente de la información, su escalabilidad permite adaptarse a la gran cantidad de información generada por los objetos y por los humanos, y su alta disponibilidad da confianza y fiabilidad, además de bajos costes de mantenimiento.

Así como los del ítem anterior, existen múltiples dispositivos que se pueden conectar a la red para alcanzar altos niveles de información obtenidas de las bases de datos que están disponibles en la nube, por lo que el volumen de información almacenada ha aumentado considerablemente, dejando en ries-

go la integridad y la confiabilidad que puede tener una organización. Teniendo en cuenta lo anterior, la tecnología Entrust ha decidido fortalecer su investigación en internet, cerrando puertas vulnerables que dejan los paquetes de servicio en la nube. Esta investigación demuestra que cada sistema y tipo de ataque requiere de un medio de protección o inclusive de la combinación de varios de ellos, que eviten los riesgos y amenazas. Sin embargo, estos mismos conllevan igualmente a soluciones adecuadas para proteger la información proporcionada por las organizaciones.

V. Conclusiones

Como se puede ver, las aplicaciones de Entrust han estado actualizando e implementado distintos mecanismos para mejorar la seguridad y protección de la información de las organizaciones y sus entornos de tecnología.

Gracias a estos avances, se ha podido establecer que son fundamentales los procesos que permitan estandarizar los niveles de seguridad, mejorando su inclusión dentro de una organización que realice periódicamente intercambio de técnicas de autenticación, que hagan que un delincuente no complete su deseo de sustraer información.

En la web, aún se ven distintos sistemas o aplicaciones que solamente utilizan un medio de seguridad inestable, permitiendo el ingreso sin restricción alguna, de ahí que la tecnología Entrust procura evolucionar sus controles de acceso, soportando diferentes formas de acceder a los sistemas.

El condicionamiento de las tecnologías que han surgido para que se haga más fácil el manejo de los servicios desde cualquier lugar, sin tener que transportarse al sitio específico y pedir un servicio que llegue al instante y realice pagos, ha sido posible y se ha seguido mejorando con circuitos y sensores que son capaces de realizar una comunicación por cuenta propia, para el beneficio del ser humano.

Para resumir, la investigación nos ha llevado a la conclusión de que con la tecnología Entrust IdGuard se garantiza una mayor seguridad y confiabilidad para las empresas, ya que permite superar anomalías de suplantación de identidad, y asume responsabilidades de protección y detracción de intrusos para mitigar los riesgos causados por delincuentes.

Referencias

[1] S. J. Costas, Seguridad Informatica, Bogotá: Ediciones de la U, 2011, pp. 19-25.

[2] Entrust 1000 Innovation Drive Ottawa, Entrust IdentityGuard PIV Credential FIPS 140-2 Cryptographic Module Security Policy, 1nd ed. vol. 1. Canadá: Entrust Public Material, 2013.

[3] Latinus. net, Latinus, 2014. [Online]. Available: http://latinus.net/.

[4] A. Maioramo, Criptografia Técnicas de desarrollo para profesionales, Buenos Aires: Alfaomega, 2009, pp. 10-15.

[5] Centrodeartigos.com, Generador de números pseudaoaleatorios criptográficamente seguro, Requerimientos. Un poco de historia, Diseños, Normas, 2014. [Online]. Available: http://www.centrodeartigo.com/articulos-noticias-consejos/article_129211.html.

[6] Entrust, Entrust, 2014. [Online]. Available: http://en.wikipedia.org/wiki/Entrust.

[7] Latinus. net, Entrust Identity Guard, 2014. [Online]. Available: http://www.latinus.net/paginas/soluciones_entrust.html.

[8] Corp ZOHO, Manageengine, Mdm_device_authentication, 2014. [Online]. Available: http://www.manageengine.com/products/desktop-central/help/mobile_device_management/mdm_device_authentication.html.

[9] Entrust. net, Cms authentication, 2014. [Online]. Available: http://www.entrust.net/certificate-services/cms-authentication.htm.

[10] Entrust. com, Mobile Smart Credential, 2014. [Online]. Available: http://www.entrust.com/products/mobile-smart-credential/.

[11] A. Molina Coballes, Datateca, Autenticación de Usuario Mediante Contraseña, 2014. [Online]. Available: http://datateca.unad.edu.co/contenidos/233011/233011Exe/leccin_8_autenticacin_de_usuario_mediante_contrasea.html.

[12] Ordenador. wingwit. com, Protocolo de Autenticación Mutua, 2014. [Online]. Available: http://ordenador.wingwit.com/Redes/network-security/76007.html.

[13] Technet. microsoft, Mutual Authentication, 2014. [Online]. Available: http://technet.microsoft.com/en-us/library/cc961730.aspx.

[14] Entrust. com, Gridcard, 2014. [Online]. Available: http://www.entrust.com/gridcard/.

[15] M. G. Piattini Emilio del Peso, Auditoría Informática, un Enfoque práctico, México, D. F. :Alfaomega, 2001, pp. 20-31.

[16] C. Headnagy, Ingeniería Social el arte del Hacking personal. Madrid: Anaya multimedia, 2011, pp. 40-47.

[17] I. Ramos, L. Pérez, F. Picouto, G. Moran, J. P. Ramos, andA. A. Varon, Haching y Seguridad en Internet, México, D. F.: Alfaomega, 2008, pp. 175-180.

[18] M. Snort, and R. Ligtweigt, INtrusion Detection for Networks, 1999, pp. 32-42.

[19] Oposcaib, Medidas de seguridad en conectividad a redes, Sistemas de detección de intrusos, 2014. [Online]. Available: http://oposcaib.wikispaces.com/file/view/Tema+41+-+Sistemas+de+Detecci%C3%B3n+Intrusos.pdf.

[20] Y. Vandoorselaere, L. L. Prelude, An Open Source, Hybrid Intrusion Detection System, 2011.

[21] M. Diodati, blogs. gartne, Mobile Device Certificate Enrollment: Are You Vulnerable?, 2014. [Online]. Available: http://blogs.gartner.com/mark-diodati/2012/07/02/mobile-device-certificate-enrollment-are-you-vulnerable/.

[22] Experian. com, Knowledge IQSM, 2014. [Online]. Available: http://www.experian.com/decision-analytics/identity-and-fraud/knowledge-based-authentication. html.

[23] Hidgloba. hidgloba, Tokens con contraseña de un solo uso (OTP) ActivID®, 2014. [Online]. Available: http://www.hidglobal.mx/products/cards-and-credentials/actividl/one-time-password-tokens.

[24] International VASCO Data Security, Vasco, Validacion de transacciones, 2014. [Online]. Available: https://www.vasco.com/solutions/application_security/e-signatures/e-signature_for_transaction_validation_and_document_signing. aspx.

[25] Misbiometrics, Wikidot, MIS Biometrics Home, 2008. [Online]. Available: http://misbiometrics.wikidot. com/.

[26] Mi-Token, Soft Tokens, 2014. [Online]. Available: http://mi-token.com/feature/authentication-options/mobile-soft-tokens/.

[27] Phnea Ellyne zdnet, Transaction signing progress held back by user resistance, 2014. [Online]. Available: http://www.zdnet.com/transaction-signing-progress-held-back-by-user-resistance-2062304306/.

[28] Safenet inc, One-Time Password (OTP) Authentication, 2014. [Online]. Available: http://www.safenet-inc.com/multi-factor-authentication/authenticators/one-time-password-otp/.

[29] Searchsecurity. techtarget, Digital certificate, 2014. [Online]. Available: http://searchsecurity.techtarget.com/definition/digital-certificate.

[30] Information Technology Services, Utexas. edu, Digital Certificates, 2014. [Online]. Available: http://www.utexas.edu/its/help/digital-certificates/845.

[31] Whereisip, Generador de números pseudoaleatorios criptográficamente seguro, Requerimientos, Un poco de historia, Diseños, Normas, Tu IP es, 2014. [Online]. Available: http://www.whereisip.net/cualesmiip/.

[32] SEAT, seguridad y equipos de alta tecnologia, s. f., Objetivos de la Biometría en la seguridad, 2014. [Online]. Available: http://seguridadseat.com/articulos-seguridad/objetivos-seguridad-biometrica.html#.VRXdEtLoTgt

[33] FRAX Informáticos S. A., Normas de la Inspección del Trabajo, 2014. [Online]. Available: http://www.biometricos.cl/equipos_biometria/aspectos_legales_control_de_asistencia_biometrico.php.

[34] FRAX Informáticos S. A., Quienes Somos, 2014. [Online]. Available: http://www.biometricos.cl/equipos_biometria/quienes_somos_frax.php.

[35] FRAX Informáticos S. A., Aplicaciones de la Biometría, 2014. [Online]. Available:http://seguridadseat.com/articulos-seguridad/aplicaciones-de-la-biometria.html#. VQhCbI6G_n8.

[36] J. Solé i Casals, investigacionyciencia, Aplicaciones de la Biometria, 2014. [Online]. Available: http://www.investigacionyciencia.es/blogs/tecnologia/20/posts/biometra-aplicada-a-la-salud-y-a-la-seguridad-11242.

[37] Diario Financiero, signalstelecomnews s. f., La Biometría en Dispositivos Samsung, 2014. [Online]. Available: http://signalstelecomnews.com/toc-desarrollara-identificacion-biometrica-en-dispositivos-samsung.

[38] Seguridadseat. com, Aplicaciones de la Biometría en Sistemas de Seguridad Electrónica, 2014. [Online]. Available: http://seguridadseat.com/articulos-seguridad/aplicaciones-de-la-biometria.html#. VUvMo_l_NBf.

[39] E. Dave, Internet de las cosas, Cómo la próxima evolución de Internet lo cambia todo. Barcelona:Cisco, 2011.

[40] Lovelle and J. M. Cueva, Intenet de las cosas, Bogota: idk, 2014.

[41] NetMediaEurope, siliconweek, Internet de las cosas enganchada al internacional, 2014. [Online]. Available: http://www.siliconweek.es/projects/internet-de-las-cosas-engancharа-al-international-ces-2015-72766.

[42] International Telecommunication Union, All rights reserved Privacy Policy Reprints & Permissions, 2014. [Online]. Available:https://itunews.itu.int/es/4503-Internet-de-las-cosas-Maquinas-empresas-personas-todo. note.aspx.

[43] FORTINET, hay canal s. f, El Internet de las Cosas y la Biometríca son un reto para el 9 de cada 10 responsables de TI españoles, 2014. [Online]. Available: http://www.haycanal.com/noticias/6460/El-Internet-de-las-Cosas-y-la-Biometrica-son-un-reto-para-el-9-de-cada-10-responsables-de-TI-espanoles.

[44] ITU NEWS, Internet de las cosas - **Máquinas**, empresas, personas, todo, 2014. [Online]. Available: https://itunews.itu.int/es/4503-Internet-de-las-cosas-Maquinas-empresas-personas-todo. note.aspx.

[45] Prnewswire.com, Internet de las cosas para luchar contra el crimen, 2014. [Online]. Available: http://www.prnewswire.com/news-releases/agt-international-apalanca-el-internet-de-las-cosas-para-luchar-contra-el-crimen-y-reforzar-la-seguridad-publica-en-mexico-295742261.html.

[46] Ideca, Internet de las cosas, 2014. [Online]. Available: http://www.ideca.gov.co/sites/

default/fi les/files/Presentaciones/Presentaciones_III%20Foro_2014/19_Internet%20de%20las%20Cosas.pdf.

[47] Registraduría, Nuestra Huella, 2015. [Online]. Available: http://www.registraduria.gov.co/rev_electro /2013/rev_elec_junio/revista_junio2013.html.

[48] El Tiempo.com, Desde enero, todo trámite notarial se tendrá que realizar con huella, 2015. [Online]. Available: http://www.eltiempo.com/politica/gobierno/sistema-biometrico-en-colombia/15024394.

[49] Enter.co, Así construye Colombia su política de ciberseguridad y ciberdefensa, 2015. [Online]. Available: http://www.enter.co/chips-bits/seguridad/ciberdefensa-colombia-politica

[50] Investigación y ciencia, Biometría aplicada a la salud y a la seguridad, 2014. [Online]. Available: http://www.investigacionyciencia.es/blogs/tecnologia/20/posts/biometra-aplicada-a-la-salud-y-a-la-seguridad-11242.

[51] El Espectador.com, Sin cables ni contraseñas, 2015. [Online]. Available: http://www.elespectador.com/noticias/economia/sin-cables-ni-contrasenas-articulo-538375.

[52] Colombia digital, Adiós suplantación, bienvenida la biometría, 2015. [Online]. Available: http://colombiadigital. net/opinion/columnistas/certicamara/item/5734-adios-suplantacion-bienvenida-la-biometria. html.

[53] Colombia.com, Biohacker asegura que nosotros mismos seremos el internet de las cosas, 2015. [Online]. Available: http:// www. colombia. com/tecnologia/informatica/sdi/108104/biohacker-asegura-nosotros-mism os-seremos-el-internet-de-las-cosas.