CIBSI

ECUADOR 2015

CIBSI

FULL PAPER

VIII CONGRESO IBEROAMERICANO DE SEGURIDAD INFORMÁTICA

III Taller Iberoamericano de enseñanza e innovación educativa en seguridad de la información

10-12 NOV 2015
UNIVERSIDAD DE LAS FUERZAS ARMADAS DEL ECUADOR - ESPE
Sangolquí, ECUADOR

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

Con la Organización de

ESPE-InnOvativa EMPRESA PÚBLICA

CRIPTORED

Fundación In-n-va Centro de Innovación

Modelo PERIL. Repensando el gobierno de la seguridad de la información desde la inevitabilidad de la falla.

Full Paper

Miércoles, 11 Noviembre

Bloque Gobierno de la Seguridad y Aspectos Generales de la Ciberseguridad

Jeimy Cano

Resumen/Abstract

La práctica actual de seguridad de la información en las organizaciones ha estado marcada por un ejercicio de aplicación virtuoso de estándares para asegurar una gestión eficiente y efectiva de la protección de la información, el cual busca alcanzar certezas, pocos defectos y actuaciones predecibles antes eventos inesperados.

Sin embargo, el contexto actual marcado por un entorno VICA - Volátil, Incierto, Complejo y Ambiguo, demanda actualizar la forma como se gobierna la seguridad de la información para lo cual se introduce el modelo PERIL, que fundado en la incertidumbre, la debilidad y las fallas permite dar cuenta de un ejercicio complementario de la seguridad de la información que fortalece.

Palabras clave/Keywords

incertidumbre, estándares, gobierno de la seguridad, gestión de la seguridad, inseguridad de lainformación.

Importancia de la Cultura de la Seguridad en las PYMES para la correcta Gestión de la Seguridad de sus Activos.

Full Paper

Miércoles, 11 Noviembre

Bloque Gobierno de la Seguridad y Aspectos Generales de la Ciberseguridad


Luis Enrique Sánchez Crespo


Ismael Caballero


Daniel Mellado


Eduardo Fernández-Medina


Antonio Santos-Olmos

Resumen/Abstract

La sociedad de la información cada vez depende más de los Sistemas de Gestión de la Seguridad de a Información (SGSI), y poder disponer de estos sistemas ha llegado a ser vital para la evolución de las PYMES. Sin embargo, este tipo de compañías requiere de SGSIs adaptados a sus especiales características, y que estén optimizados desde el punto de vista de los recursos necesarios para implantarlos y mantenerlos. En este artículo se presenta la importancia que dentro de los SGSIs tiene la cultura de la seguridad para las PYMES y cómo se ha introducido el concepto de cultura de seguridad dentro de la metodología de gestión de la seguridad en las pequeñas y medianas empresas (MARISMA). Este modelo está siendo aplicado directamente a casos reales, consiguiendo así una constante mejora en su aplicación.

Palabras clave/Keywords

Ciberseguridad, Sistemas de Gestión de Seguridad de la Información, SGSI, Cultura de la Seguridad, PYMES, ISO27001, ISO27002.

Con la Organización de

CIBSI ECUADOR 2015

ESPE UNIVERSIDAD DE LAS FUERZAS ARMADAS INNOVACION PARA LA EXCELENCIA

Analysis of dynamic complexity of the Cybersecurity Ecosystem in Colombia.

Full Paper

Miércoles, 11 Noviembre

Bloque Gobierno de la Seguridad y Aspectos Generales de la Ciberseguridad


Angélica Flórez Abril


Lenin Javier Serrano Gil


Urbano Eliécer Gómez Prada


Luis Eduardo Suárez Caicedo


Alejandro Villarraga Plaza


Hugo Armando Rodríguez Vera

Resumen/Abstract

This paper presents two proposals for the analysis of dynamic complexity of the Cybersecurity Ecosystem in Colombia, which allows the understanding of the synergy between the legal entities working in Cybersecurity in Colombia and the distinct components of it.

The complexity of the Cybersecurity Ecosystem in Colombia is shown in the form of influence diagrams from System Dynamics and domain diagrams from Software Engineering. The resulting model presents Cybersecurity as a strategic component in national security.

Palabras clave/Keywords

cybersecurity, cyberspace, ecosystem, influence diagram, domain model, system dinamics, software engineering

El uso de contraseñas, un mundo lejos de la extinción: Un Estudio Empírico

Full Paper

Miércoles, 11 Noviembre

Bloque Gobierno de la Seguridad y Aspectos Generales de la Ciberseguridad

Rolando P. Reyes Ch.

Óscar Dieste

Efraín R. Fonseca C.

Resumen/Abstract

Antecedentes. En la actualidad los sistemas de información utilizan distintos mecanismos de seguridad para permitir el acceso a sus funcionalidades a usuarios identificados, siendo las contraseñas el modo más común de validación. Existen varias políticas y normas (unas más estrictas que otras) para la creación de contraseñas; sin embargo, éstas aún siguen siendo vulnerables.

Objetivo. Conocer las vulnerabilidades de diferentes niveles de complejidad de contraseñas propuestos para el presente estudio, así como conocer los tipos de contraseñas usados en los ataques, tipos de atacantes y su procedencia.

Método. Esta investigación fue llevada a cabo a través de un estudio empírico basado en un experimento controlado. El estudio se fundamentó en la utilización de *honeypots* para emular un servidor SSH, el cual fue expuesto al internet durante un tiempo aproximado de 30días.

Resultados. Se registró un gran número de ataques, los cuales no llegaron a vulnerar ningún nivel de complejidad de contraseñas propuestos.

Conclusión. A pesar que no fueron vulnerados los niveles de complejidad propuestos, se considera que un incremento en el factor tiempo, podría permitir que dichos niveles sean vulnerados.

Palabras clave/Keywords

experimento controlado, vulnerabilidad, contraseña, entropía, ataque, honeypot.

CIBSI ECUADOR 2015

ESPE UNIVERSIDAD DE LAS FUERZAS ARMADAS INNOVACION PARA LA EXCELENCIA

Towards a Security Model for Big Data

Full Paper

Miércoles, 11 Noviembre

Bloque Seguridad en Base de Datos

Julio Moreno

David García Rosado

Ismael Caballero

Manuel Ángel Serrano

Eduardo Fernández-Medina

Resumen/Abstract

Big Data technologies describe a new generation of technologies and architectures, designed so organizations can economically extract value from very large volumes of a wide variety of data by enabling high-velocity capture, discovery, and/or analysis. This new technology raises new risks due to more volume and variety of data. Issues related to data security and privacy are one of the main concern in today's era of "big data." It is necessary to know before of involving in big data, which are the most important security needs, requirements and aspects to assure a high security level in our applications, transactions, data processing and decision management. In this paper we analyze the most important privacy and security aspects and requirements found in Big Data and we establish a security model aligned with security quality factor where the most relevant security and privacy aspects considered in Big Data are defined.

Palabras clave/Keywords

Big Data, Security, Information Model, security requirements.

Mitigación de Ataques DDoS a través de Redundancia de Tablas en Base de Datos

Full Paper

Miércoles, 11 Noviembre

Bloque Seguridad en Base de Datos

Diego
Romero Vásconez

Christian
Bastidas Espinosa

Walter
Fuertes Díaz

Mauro
Silva

Resumen/Abstract

La cantidad de ataques de tipo Denegación de Servicios a las pequeñas y medianas empresas, se han triplicado en el año 2014, con respecto al año 2013. El presente estudio es un aporte a este tipo de empresas para que en lugar de realizar inversiones económicas en software de seguridad, modifiquen el funcionamiento de sus gestores de bases de datos. Para llevarlo a cabo, en una fase inicial, el experimento se realizó en una sola máquina. Sin embargo, los resultados no fueron los esperados, pues las consultas a la BDD no eran eficientes en el tiempo, pues los recursos eran compartidos por el software utilizado. Luego se decidió crear un entorno físico con tres máquinas que tengan la base de datos redundante, dentro de una red inalámbrica. En esta topología se inyectaron ataques para denegar el servicio de manera distribuida. Luego se realizaron varias pruebas con sus respectivas mediciones variando el número de clientes (i.e. de un cliente a dos simultáneos), comparándose luego los efectos. Los resultados muestran que al aumentar el número de consultas simultáneas, el motor de la base de datos se apodera del procesador y no permite que se realicen otras tareas. Además el conector ODBC inserta una capa intermedia denominada nivel de interfaz de cliente SQL, entre la aplicación y el gestor de la base de datos que finalmente termina siendo bloqueado, manteniendo los servidores en funcionamiento.

Palabras clave/Keywords

Balanceo de carga, Denegación de Servicio,Denegación Distribuida de Servicios, Mitigación.

CIBSI ECUADOR 2015

ESPE UNIVERSIDAD DE LAS FUERZAS ARMADAS INNOVACION PARA LA EXCELENCIA

Evaluación de Ataques a las Aplicaciones Web tipo Inyección SQL a Ciegas utilizando Escenarios Virtuales como Plataforma Experimental

Full Paper

Miércoles, 11 Noviembre

Bloque Seguridad en Base de Datos


Santiago Hidalgo


Diego Jaramillo


Víctor Olalla


Becket Toapanta


Walter Fuertes Díaz

Resumen/Abstract

Los ataques a ciegas por Inyección SQL a las aplicaciones Web, también conocidos como Blind SQL Injection Attacks, tienen el propósito de obtener acceso sin restricciones a la base de datos empresariales para conseguir información potencialmente sensible. Ante este problema, el presente estudio ha evaluado diversas herramientas de software útiles para la generación de ataques y justipreciar cómo afectan al rendimiento de los servidores para conseguir acceso a la base de datos. Las herramientas probadas fueron Absinthe, BSQL Hacker y The Mole, que funcionan sobre las plataformas Windows y Linux respectivamente. Luego, se diseñó e implementó un entorno virtual de red como plataforma experimental, con segmentación LAN que impide el acceso interno al servidor Web. Además, se desarrolló un aplicativo utilizando el framework CodeIgniter para PHP, sobre un servidor Apache y se conectó a una BDD Microsoft SQL 2008. A continuación se modificó la lógica de programación y se utilizó la clase llamada Active Record como parte de la mitigación, donde se evidenció que ninguna de las herramientas logró vulnerar la base de datos. Finalmente se midió la carga sobre el procesador, la memoria y la red para determinar cuál de estas herramientas es más contundente al ejecutar un ataque en estas condiciones.

Palabras clave/Keywords

Ataques de seguridad, Virtualización, Sql Injection, Absinthe, BSQL Hacker, The Mole.

CIBSI ECUADOR 2015

ESPE UNIVERSIDAD DE LAS FUERZAS ARMADAS INNOVACION PARA LA EXCELENCIA

MONOCLE – Extensible open-source forensic tool applied to cloud storage cases.

Full Paper

Miércoles, 11 Noviembre

Bloque Seguridad en Cloud y Patrones

Jorge Rodríguez-Canseco

José María de Fuentes

Lorena González-Manzano

Arturo Ribagorda

Resumen/Abstract

Current forensic tools highly depend on the analyst awareness of evidences in order to retrieve them by means of a proactive search methodology. This paper presents MONOCLE, an open-source extensible framework for automated forensic analysis. MONOCLE provides automation over the forensic procedure by means of user created plugins, reducing the complexity of evidence retrieval in target's machine hard disk and memory. The software makes use of external tools such as the Volatility Framework in order to provide extended functionality to the executed plugins. To show the applicability of the proposal, in this paper MONOCLE is applied to two userside cloud storage scenarios: iCloud and Box. Results show that MONOCLE is able to retrieve relevant information regarding end-users systems and cloud services interaction in the client machine.

Palabras clave/Keywords

Computer forensics, analysis, memory forensics, software tools.

CIBSI ECUADOR 2015

ESPE UNIVERSIDAD DE LAS FUERZAS ARMADAS INNOVACIÓN PARA LA EXCELENCIA

Actividad de Diseño en el proceso de migración de características de Seguridad al Cloud

Full Paper

Miércoles, 11 Noviembre

Bloque Seguridad en Cloud y Patrones


Luis Márquez


David García Rosado


Haralambos Mouratidis


Daniel Mellado


Eduardo Fernández-Medina

Resumen/Abstract

La importancia de Cloud Computing se está incrementando enormemente y recibe una gran atención por parte de la comunidad científica. El Cloud Computing ofrece un amplio conjunto de beneficios, pero también supone un gran reto desde el punto de vista de la seguridad, siendo la seguridad el principal freno para su completo éxito. La migración de sistemas heredados a la nube nos devuelve la esperanza de que podamos retomar el control sobre la seguridad pobremente integrada en los sistemas heredados o que no había sido incorporada en el diseño inicial de los mismos. El proceso denominado SMiLe2Cloud pretende resolver el problema de la migración con seguridad a la nube de sistemas de información heredados. El presente artículo pretende exponer un caso práctico sobre el diseño de la migración de las características de seguridad de una aplicación heredada a proveedores Cloud utilizando para ello el proceso denominado SMiLe2Cloud.

Palabras clave/Keywords

Cloud, seguridad, migración, diseño, CSA.

CIBSI ECUADOR 2015

ESPE UNIVERSIDAD DE LAS FUERZAS ARMADAS INNOVACION PARA LA EXCELENCIA

Cloud Privacy Guard (CPG): Security and Privacy on Data Storage in Public Clouds

Full Paper

Miércoles, 11 Noviembre

Bloque Seguridad en Cloud y Patrones

Vitor H. G. Moia

Marco A. A. Henriques

Resumen/Abstract

Cloud data storage is an interesting service that offers several advantages for users. However, the risks involved in the outsourcing of data storage can be a barrier to the adoption of this model by those concerned with privacy. Cryptography is being used as a solution to overcome such risks and gain the trust of users who want more security for their data. Still, several cloud service providers that offer cryptography services do not fulfill some security requirements essential in a secure and reliable service, raising questions about the effective security obtained. In this paper, we propose a cryptography system to overcome the most common security risks in cloud data storage and show how it can satisfy some important security requirements that will be presented and discussed.

Palabras clave/Keywords

Cloud computing, security, privacy, cryptography.

A Post-Quantum Set of ompact Asymmetric Protocols using a General Linear Group

Full Paper

Miércoles, 11 Noviembre

Bloque Criptografía

Pedro
Hecht

Resumen/Abstract

This paper presents an original and unified set of compact asymmetric and arbitrated protocols developed with the same general linear group. As a computational secure one way function we use the generalized symmetric decomposition problem. By unified we mean that all protocols share the same algebraic structure and by compact that they use only single precision modular arithmetic that can be ported into low capabilities platforms like 8 and 16 bit processors. They are arbitrated since they use a trusted third party (TTP), but this feature needs not be a drawback. The appealing feature of this approach is that for this kind of non-commutative algebraic primitives and one way functions, there are no known sub exponential time complexity or quantum algorithm attacks as with traditional commutative fields. Our chosen structure was a Hill matrix group; specifically order eight square matrices with 8 bit elements under Z251 arithmetic; because it can be fitted into smartcards, cell phones, USB cryptographic keys and similar devices. The module was selected as it is the greatest prime fitting into 8 bits. We present asymmetric protocols including key exchange, key transport, ciphering, digital signature and ZKP authentication. As it will be proven, their simplicity does not affect the cryptographic security level which is conjectured to be around 64 bits. We believe that the protocols could be a good choice for low performance environments without sacrificing security.

Palabras clave/Keywords

post-quantum cryptography, asymmetric cryptography, non-commutative cryptography, cryptographic protocols, general linear groups, algebra.

CIBSI ECUADOR 2015

ESPE UNIVERSIDAD DE LAS FUERZAS ARMADAS INNOVACION PARA LA EXCELENCIA

Modelización lineal de generadores de secuencias basados en decimación

Full Paper

Miércoles, 11 Noviembre

Bloque Criptografía

Sara
Díaz Cardell

Amparo
Fúster-Sabater

Resumen/Abstract

Entre los generadores de secuencia basados en decimación se encuentra el generador auto-shrinking, un generador criptográfico no lineal de secuencia binaria que se utiliza principalmente en aplicaciones de cifrado en flujo para protección de la información. En este trabajo, la secuencia de salida de dicho generador, llamada secuencia auto-shrunken, se puede obtener como una de las secuencias de salida de un modelo lineal basado en autómatas celulares. Estos autómatas son lineales, uniformes, nulos y usan la ley 60 como función de transición. La linealidad de estas estructuras puede aprovecharse ventajosamente para llevar a cabo un criptoanálisis del generador auto-shrinking.

Palabras clave/Keywords

generador auto-shrinking, secuencia auto-shrunken, autómata celular, ley 60, cifrado en flujo, criptografía.

CIBSI ECUADOR 2015

ESPE UNIVERSIDAD DE LAS FUERZAS ARMADAS INNOVACION PARA LA EXCELENCIA

Halve-and-add in type II genus 2 curves over binary fields

Full Paper

Miércoles, 11 Noviembre

Bloque Criptografía


Ricard Garra


Josep M. Miret


Jordi Pujolás

Resumen/Abstract

We give a method to compute multiples *kD* of a divisor in the Jacobian variety of a genus 2 curve in characteristic 2 based on halving algorithms. Our method is competitive compared to the classic algorithms based on double-and-add, and also compared to analogous for other curves over binary fields. We present explicit halving formulae for each possible divisor class for type II curves (those with $h(x) = x$), detailing all the process to obtain them. We improve the fastest known formulae for some divisor classes in the studied type of curves.

CIBSI ECUADOR 2015

ESPE UNIVERSIDAD DE LAS FUERZAS ARMADAS INNOVACION PARA LA EXCELENCIA

Zero-Knowledge Proof Authentication using Left Self Distributive Systems: a Post-Quantum Approach

Full Paper

Miércoles, 11 Noviembre

Bloque Criptografía

Pedro Hecht

Resumen/Abstract

This paper presents an original and theoretical approach to zero-knowledge authentication, using left selfdistributive (LD) algebraic systems like Laver tables. The reason for using Laver tables is that their combinatorial properties seem quite complicated and, as cited, involve necessarily fast growing functions. Post-Quantum cryptography explores solutions whosesecurity do not rely over traditional numeric fields one way trap functions based on integer factorization or discrete logarithm problems. The paper shows at first the method, after that it states as a theorem that the authentication protocol complies with a zero-knowledge proof and finally proves it. No attempt or effort has been made to develop a practical instance and the paper focus only the theoretical aspect of the question. Despite this, we sketch the potential use of Laver tables.

Palabras clave/Keywords

post-quantum cryptography. zero-knowledge proofs, ZKP, non-commutative cryptography, cryptographic protocols, left-self distributivity. Laver tables, LD-systems.

Proceso Ágil para la realización de Análisis y Gestión de Riesgos sobre la ISO27001 orientado a las PYMES

Full Paper

Miércoles, 11 Noviembre

Bloque Gestión de la Seguridad e Infraestructuras Críticas

Antonio Santos-Olmos

Luis Enrique Sánchez Crespo

Esther Álvarez González

Mónica Karel Huerta

Eduardo Fernández-Medina

Resumen/Abstract

La sociedad de la información cada vez depende más de los Sistemas de Gestión de la Seguridad de la Información (SGSI), y poder disponer de estos sistemas ha llegado a ser vital para la evolución de las PYMES. Sin embargo, este tipo de compañías requiere de SGSIs adaptados a sus especiales características, y que estén optimizados desde el punto de vista de los recursos necesarios para implantarlos y mantenerlos. En este artículo se presenta el método propuesto para realizar un análisis de riesgos simplificado, que sea válido para las PYMES, y enmarcado dentro de la metodología de gestión de la seguridad en las pequeñas y medianas empresas (MARISMA). Este modelo está siendo aplicado directamente a casos reales, consiguiendo así una constante mejora en su aplicación.

Palabras clave/Keywords

Ciberseguridad, Sistemas de Gestión de Seguridad de la Información, SGSI, Analisis de Riesgos, PYMES, ISO27001, ISO27005.

CIBSI ECUADOR 2015

ESPE UNIVERSIDAD DE LAS FUERZAS ARMADAS INNOVACION PARA LA EXCELENCIA

El defecto de la seguridad por defecto en SCADA y SHODAN

Full Paper

Miércoles, 11 Noviembre

Bloque Gestión de la Seguridad e Infraestructuras Críticas

Manuel Sánchez Rubio

José Miguel Gómez Casero Marichal

Resumen/Abstract

This paper presents a potential threat that exists when both developers and companies deploy SCADA for critical infrastructures without taking care about security. In this paper we will talk about the search engine Shodan and its job when attackers gather information about a target or when they are searching for an asset to attack. We will end the research with a proof of concept simulating an attack to these SCADA systems, following the steps of a normal attacker, from the search query into the Shodan search engine until the access granted successfully into a critical infrastructure.

Palabras clave/Keywords

scada, default security, critical infrastructure, shodan, footprinting.

Propuesta Metodológica para la Gestión de la Seguridad Informática en Sistemas de Control Industrial.

Full Paper

Miércoles, 11 Noviembre

Bloque Gestión de la Seguridad e Infraestructuras Críticas

Fabián Bustamante

Paúl Díaz

Walter Fuertes Díaz

Resumen/Abstract

Los últimos reportes Internacionales de incidenciasde seguridad han difundido un creciente número de ataques cibernéticos a Sistemas de Control Industrial (SCI). A estos informes se suma el aumento de implementaciones de informática en procesos de manufactura y la escasa oferta de soluciones de Seguridad de Información de los fabricantes y profesionales involucrados. Por otro lado se ha visto que la seguridad informática está especialmente destinada a usarse en el área administrativa de las empresas, siendo ISO-27000 el estándar favorito. Además se ha determinado que ISO no es aún un estándar idóneo para un SCI, ya que no fue concebido para estos sistemas. El objetivo de este estudio es diseñar y poner en funcionamiento una metodología para la gestión de la seguridad informática de los SCI de empresas industriales, basada en estándares expedidos por el Instituto Nacional de Estándares y Tecnología de Estados Unidos. La metodología propuesta, presenta el desarrollo de una serie de fases las cuales dan como aportaciones: (1) Un conjunto de estrategias para mitigar riesgos; y (2) Un manual de políticas y normas para lagestión efectiva de la seguridad informática, que puede ser aplicado a cualquier empresa de este tipo.

Palabras clave/Keywords

Sistemas de Control Industrial, Seguridad de Información, Automatización, SGSI, SCADA, DSC, PLC, ISO 27000, NIST.

Aplicación del método de Investigación-Acción para desarrollar una Metodología Agil de Gestión de Seguridad de la Información

Full Paper

Miércoles, 11 Noviembre

Bloque Gestión de la Seguridad e Infraestructuras Críticas

Luis Enrique Sánchez Crespo

Antonio Santos-Olmos

David García Rosado

Eduardo Fernández-Medina

Mario Piattini

Resumen/Abstract

La sociedad de la información cada vez depende más de los Sistemas de Gestión de la Seguridad de la Información (SGSI), y poder disponer de estos sistemas ha llegado a ser vital para la evolución de las PYMES (Pequeñas y Medianas Empresas). Sin embargo, este tipo de compañías requiere de SGSIs adaptados a sus especiales características, y que estén optimizados desde el punto de vista de los recursos necesarios para implantarlos y mantenerlos, con unos costes muy reducidos y periodos de implantación muy cortos. En este artículo se analizan los diferentes ciclos realizados utilizando el método científico investigación en acción que han permitido desarrollar una metodología de gestión de la seguridad válida para las PYMES, con la que se han podido automatizar procesos y reducir los tiempos de implantación de los SGSIs.

Palabras clave/Keywords

Ciberseguridad, Sistemas de Gestión de Seguridad de la Información, SGSI, Investigación en acción, Mejora de procesos, Reducción de coste, Reducción de tiempo, PYMES, ISO27001, ISO27002.

Evaluación de ataques DDoS generados en dispositivos móviles y sus efectos en la red del ISP

Full Paper

Miércoles, 11 Noviembre

Bloque Seguridad en Redes y Análisis Forense

Carlos Andrés Almeida

Liliana Chacha

Christian Torres

Walter Fuertes Díaz

Resumen/Abstract

Los ataques de Denegación de Servicio distribuido (DDoS) generados en dispositivos móviles, se han incrementado notablemente debido a la masificación de los mismos y a la vulnerabilidad de los Sistemas Operativos. Los estudios actuales se centran en analizar y evaluar el efecto de los ataques de DDoS sobre los clientes. El presente trabajo se enfoca en cambio en evaluar que sucede en la red del ISP durante un ataque generado a través de varios dispositivos móviles que actúan como Botnets. Para llevar a cabo esta investigación, se diseñó e implementó un entorno virtual de red controlado haciendo uso de herramientas de software libre para producir ataques desde un dispositivo móvil. Posteriormente se evaluó el ancho de banda del proveedor de servicio hacia sus Tier 1 y se constató los efectos sobre la red del ISP. Esto permitió concluir que durante el ataque, no solo se ve afectada la víctima, sino que también se comprometen los recursos de ancho de banda del proveedor de servicios, creando así un efecto rebote de ataque hacia otros clientes del mismo proveedor de servicios.

Palabras clave/Keywords

Denegación de Servicio, Redes Móviles, Botnet, Proveedor de Servicios de Internet

CIBSI ECUADOR 2015

ESPE UNIVERSIDAD DE LAS FUERZAS ARMADAS INNOVACION PARA LA EXCELENCIA

Detección de Malware en Dispositivos Móviles mediante el Análisis de Secuencias de Acciones

Full Paper

Miércoles, 11 Noviembre

Bloque Seguridad en Redes y Análisis Forense

Jorge
Maestre Vidal

Ana Lucila
Sandoval Orozco

Luis Javier
García Villalba

Resumen/Abstract

The recent sharp increase in popularity of mobile devices has led to the emergence of new and varied forms of malware. These novel specimens are characterized for its sophistication and ease of propagation. Hence, different organizations for cyber defense have warned about the need to develop more effective defenses. In order to contribute to this purpose, we introduce a malware detection system for mobile devices based on sequence alignment algorithms. The use of this methodology allows an exhaustive study in real time of sequences of system calls executed by applications. As demonstrated in experimentation, most of the malicious activities may be unmasked accurately in the boot process. Consequently, to launch programs in secure and isolated environment in order to distinguish legitimate and malicious content is possible.

Palabras clave/Keywords

Android, IDS, Information Security, Intrusion Detection System, Malware, Mobile Device, Sequence Alignment.

CIBSI ECUADOR 2015

ESPE UNIVERSIDAD DE LAS FUERZAS ARMADAS INNOVACION PARA LA EXCELENCIA

Método Anti-Forense para Manipular la Fuente de Adquisición de una Imagen de Dispositivo Móvil

Full Paper

Miércoles, 11 Noviembre

Bloque Seguridad en Redes y Análisis Forense

Jocelin
Rosales Corripio

Anissa
El-Khattabi

Ana Lucila
Sandoval Orozco

Luis Javier
García Villalba

Resumen/Abstract

Nowadays digital images play an important role in oursociety. The mobile device camera presence is growing at an unstoppable rate, causing that most of digital imagescome from this kind of devices. While the developing technology makes image generation process easier, at the same time it facilitates forgery; therefore, image forensics is gaining relevance. In this paper we propose a pair of algorithms that are based on sensor noise and the wavelet transform, the first to eliminate the possibility of identifying the mobile device (maker and model) that generated an image and the second to forge the identity of a given image.

Palabras clave/Keywords

Counter Forensics, Forensics Analysis, Image Anonymity, Image Forgery, PRNU, Wavelet.

CIBSI ECUADOR 2015

ESPE UNIVERSIDAD DE LAS FUERZAS ARMADAS INNOVACIÓN PARA LA EXCELENCIA

Ocultación de código malicioso en Google Play. Monitorización y detección temprana

Full Paper

Jueves, 12 Noviembre

Bloque Web y Redes Sociales

Alfonso Muñoz

Antonio Guzmán

Resumen/Abstract

Las estrategias actuales para la distribución de malware o adware agresivo para móviles parecen propias de una factoría de software. Esta maquinaria está perfectamente engrasada y se aprovecha de las laxas medidas de seguridad que se aplican en la mayoría de los markets de aplicaciones móviles. Esta investigación pone el foco en la forma y modo que tiene un desarrollador para crear y distribuir código malicioso en Google Play dificultando la detección de malware si se utiliza esteganografía para ocultar el código malicioso. El trabajo destaca la dificultad de la tecnología actual para detectar estegomalware en Google Play. Las conclusiones de esta investigación toman como referencia más de 2 millones de aplicaciones móviles de Google Play.

Palabras clave/Keywords

Estegomalware, Google Play, market móvil, malware.

Con la Organización de ESPE-InnOvativa EMPRESA PÚBLICA CRIPTORED fundación IN-N-VA Centro de Innovación

CIBSI ECUADOR 2015

ESPE UNIVERSIDAD DE LAS FUERZAS ARMADAS INNOVACION PARA LA EXCELENCIA

Búsqueda de Relaciones entre Vulnerabilidades de Aplicaciones Web

Full Paper

Jueves, 12 Noviembre

Bloque Web y Redes Sociales

Fernando Román Muñoz

Luis Javier García Villalba

Resumen/Abstract

In a previous paper the authors described a new method to map web vulnerability issue classifications. That method is based on shorting issue descriptions to a set of two or three words. Then specific queries are send to the Internet to find the relationships. The result are a new mapping between classifications that can be kept updated and a new web vulnerability classification. In this paper are described the implementation of the method and the results of testing it. The test results indicate that the propose method find real relationships in most cases, and also some new ones.

Palabras clave/Keywords

Classification Mappings, Vulnerability Classification,Web Vulnerability, Web Vulnerability Relationships.

Con la Organización de ESPE-InnOvativa EMPRESA PÚBLICA CRIPTORED fundación IN-N-VA Centro de Innovación

CIBSI ECUADOR 2015

ESPE UNIVERSIDAD DE LAS FUERZAS ARMADAS INNOVACION PARA LA EXCELENCIA

Extracción de Características de Redes Sociales Anónimas a través de un Ataque Estadístico

Full Paper

Jueves, 12 Noviembre

Bloque Web y Redes Sociales

Alejandra Guadalupe Silva Trujillo

Javier Portela García-Miguel

Luis Javier García Villalba

Resumen/Abstract

Social network analysis (SNA) has received growing attention on different areas. SNA is based on examine relational data obtained from social systems to identify leaders, roles and communities in order to model profiles or predict a specific behavior in users' network. This information has a huge impact on research areas such as terrorism, financial crimes, analysis of fraud, and sociological studies because SNA helps to understand the dynamics of social networks. The aim of our work is develop a statistical disclosure attack and show the results and information obtained from a social network composed of a university community. **n**

Palabras clave/Keywords

Anonymity, Graph Theory, Privacy, Social Network Analysis, Statistical Disclosure Attack.

CIBSI

ECUADOR 2015

CIBSI

SHORT PAPER

VIII CONGRESO IBEROAMERICANO DE SEGURIDAD INFORMÁTICA

III Taller Iberoamericano de enseñanza e innovación educativa en seguridad de la información

10-12 NOV 2015

UNIVERSIDAD DE LAS FUERZAS ARMADAS DEL ECUADOR - ESPE

Sangolquí, ECUADOR

ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

Con la Organización de

ESPE-InnOvativa EMPRESA PÚBLICA

CRIPTORED

Fundación In-n-va Centro de Innovación

CIBSI ECUADOR 2015

ESPE UNIVERSIDAD DE LAS FUERZAS ARMADAS INNOVACION PARA LA EXCELENCIA

Procedimiento metodológico para la Implementación de Seguridades contra Ataques de Inyección SQL en PYMES

Short Paper

Martes, 10 Noviembre

Bloque Seguridad en Base de Datos


Francisco Gallegos


Pablo Herrera


Rosa Ramirez


Silvana Vargas


Walter Fuertes Díaz

Resumen/Abstract

Este artículo presenta un procedimiento metodológico para implementar seguridades en redes de pequeñas y medianas empresas que permita mitigar ataques de Inyección SQL. Para lograrlo fueron identificados las tareas, recursos y fases requeridas para el análisis, planificación, organización, dirección y control de los aspectos que debe tener una red básica segura. Como plataforma experimental se utilizó un entorno de red virtualizado con una Aplicación Web. Con ello se inyectaron ataques de Inyección SQL obteniéndose la línea base. Esto permitió determinar los daños y nivel de intrusión del atacante al tener acceso a la base de datos de la Aplicación Web. A continuación se procedió a configurar un muro de fuegos de aplicaciones Web de código abierto llamado ModSecurity. En él se mejoraron las políticas de seguridad y se evaluó la seguridad que ofrece, verificándose que todos los ataques de inyección sean neutralizados. Como fundamento se aplicaron las reglas básicas provistas por el Proyecto abierto de seguridad de aplicaciones Web OWASP. Los resultados muestran que esta solución es adecuada para PYMES que tienen un presupuesto limitado.

Palabras clave/Keywords

SQL Injection, ModSecurity, SQLMap, Seguridad Informática, Ciberseguridad.

CIBSI ECUADOR 2015

ESPE UNIVERSIDAD DE LAS FUERZAS ARMADAS INNOVACION PARA LA EXCELENCIA

SecBP&P: Hacia la obtención de Artefactos UML a partir de Procesos de Negocio Seguros y Patrones de Seguridad

Short Paper

Martes, 10 Noviembre

Bloque Seguridad en Cloud y Patrones


Matías Zapata


Alfonso Rodríguez


Angélica Caro

Resumen/Abstract

La incorporación de conceptos de seguridad dentro de los modelos de procesos de negocio ha resultado ser un factor interesante para el proceso de desarrollo de software. Esta especificación temprana de requisitos permite evitar problemas relacionados con la seguridad que sería costoso corregir en etapas posteriores. Por otro lado, dentro del área de la seguridad en ingeniería de software, existen los patrones de seguridad, que son importantes pues guían el proceso de desarrollo de software seguro. En este trabajo se utilizarán, en conjunto, los modelos de proceso de negocio con especificaciones de seguridad y los patrones seguridad, con el objeto de generar artefactos valiosos para la construcción de software. Específicamente, se crearán un conjunto de clases de análisis UML que incluyan la seguridad.

Palabras clave/Keywords

Proceso de Negocio Seguro, Patrones de Seguridad

A Diffie-Hellman Compact Model Over Non-Commutative Rings Using Quaternions

Short Paper

Miércoles,11 Noviembre

Bloque Criptografía

Jorge Kamlofsky

Pedro Hecht

Óscar Hidalgo Izzi

Samira Abdel Masih

Resumen/Abstract

The key exchange cryptographic protocol created by Whitfield Diffie and Martin Hellman was one of the pioneers of asymmetric cryptography (AC). Many of the asymmetric cryptography protocols are based on operations performed in commutative algebraic structures. Today many of them are vulnerable to subexponential or quantum attacks. The development of algorithms in noncommutative structures can strengthen these protocols. This line of development is an actual growing trend. In particular Hecht (2009) has presented a key exchange model based on the Diffie-Hellman protocol over noncommutative rings using matrices of order four with Z256 elements, particularly interesting to provide cryptographic security to devices with low computing power. The set of quaternions, like the set of all the matrices form non-commutative ring structures. However, quaternions have more compact notation and shown lower runtimes in many comparable operations. In this paper we propose the use of quaternions in this key exchange protocol, and present experimental results showing lower run-times in this cryptosystem when using quaternions at equivalent security.

Palabras clave/Keywords

Asymmetric cryptography, quaternions in cryptography, quaternions, non-commutative cryptography, post-quantum cryptography.

Quitando el Velo a la Memoria: Estructuras Ocultas y Malware

Short Paper

Miércoles,11 Noviembre

Bloque Gestión de la Seguridad e Infraestructuras Críticas


Ana Haydee Di Iorio


Gonzalo Ruiz de Angeli


Juan Ignacio Alberdi


Bruno Constanzo


Ariel Podestá


Hugo Armando Rodríguez Vera

Resumen/Abstract

Forensic analysis of a computer's volatile memory has become a major area of interest, with relatively few solutions outside closed commercial packages. This branch of digital forensics is full of challenges: the memory has a different layout depending onthe Operating System, hardware architecture and even on features of the microprocessor. After extensive research, the BIP-M project is close to presenting a framework for the forensic analysis of RAM memory, and a tool built on top of it.

Palabras clave/Keywords

Análisis forense en memoria, estructuras ocultas, malware, hooks.

CIBSI ECUADOR 2015

ESPE UNIVERSIDAD DE LAS FUERZAS ARMADAS INNOVACION PARA LA EXCELENCIA

Detección de Ataques de Denegación de Servicio en Tor

Short Paper

Miércoles,11 Noviembre

Bloque Seguridad en Redes y Análisis Forense

Ignacio
Gago Padreny

Jorge
Maestre Vidal

Luis Javier
García Villalba

Resumen/Abstract

To protect our privacy, Tor, a popular anonymity system, forwards traffic through multiple relays. This network has been subject of numerous attacks trying to disclose user identities, being denial of service attacks one of the most widespread. Not only this attacks have been very popular on Tor, but also on the Internet. In the present work, an anomalybased detection system is proposed for detecting such attacks. Traffic is analized without concerning user's privacy and from it some metrics are extracted which enable to model traffic as time series in order to find out anomalies.

Palabras clave/Keywords

Anomalies, DDoS, Entropy, Predictive Models, Time Series, Tor.

CIBSI ECUADOR 2015

ESPE UNIVERSIDAD DE LAS FUERZAS ARMADAS INNOVACION PARA LA EXCELENCIA

Algoritmo para el Mapeo de Clasificaciones de Vulnerabilidades Web

Short Paper

Jueves, 12 Noviembre

Bloque Web y Redes Sociales

Fernando
Román Muñoz

Luis Javier
García Villalba

Resumen/Abstract

Due to the widespread use of the World Wide Web, the amount and kinds of application level web vulnerabilities have increased. In order to sort web vulnerabilities, many web vulnerabilityclassifications have been developed. There are also mappings that relate the vulnerabilities of various classifications. Until the authors' knowledge any full mapping between web vulnerability classifications has been done. In this paper a new method to map web vulnerability classifications is proposed. As classifications change over time, this new method could be executed when the existing classifications change or when new classifications are developed. The result of get the mappings between web vulnerability classifications also involves a process to simplify each web vulnerability description into a unique and small group of words. The vulnerabilities describe this way can also be seen as a web vulnerability classifications that includes all vulnerabilities in the classifications taken into account.

Palabras clave/Keywords

Classification Mappings, Vulnerability Classification, Web Vulnerability, Web Vulnerability Relationships.

CIBSI ECUADOR 2015

ESPE UNIVERSIDAD DE LAS FUERZAS ARMADAS INNOVACION PARA LA EXCELENCIA

Ataque y Estimación de la Tasa de Envíos de Correo Electrónico mediante el Algoritmo EM

Short Paper

Jueves, 12 Noviembre

Bloque Web y Redes Sociales

Alejandra Guadalupe Silva Trujillo

Javier Portela García-Miguel

Luis Javier García Villalba

Resumen/Abstract

Monitoring a communication channel is an easy task, with appropriate tools anyone can gain information, an attacker can eavesdrop the communication such that the communicators cannot detect the eavesdropping. An attacker is capable of observing the network and deduces users' communication patterns, even when data is incomplete, communication patterns can be used to infer information about a specific subject. The attacker is able to know who communicates whom, what time, frequency, among others. Traffic analysis is a powerful tool because it is difficult to safeguard against. The purpose of this work is to develop an attack and estimate the sending rate of an email system using the EM algorithm.

Palabras clave/Keywords

Anonymity, EM Algorithm, Privacy, Statistical Disclosure Attack.

CIBSI

ECUADOR 2015

TIBETS

FULL PAPER

VIII CONGRESO IBEROAMERICANO DE SEGURIDAD INFORMÁTICA

III Taller Iberoamericano de enseñanza e innovación educativa en seguridad de la información

10-12 NOV 2015

UNIVERSIDAD DE LAS FUERZAS ARMADAS DEL ECUADOR - ESPE

Sangolquí, ECUADOR

ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

Con la Organización de

ESPE-InnOvativa EMPRESA PÚBLICA

CRIPTORED

Fundación In-n-va Centro de Innovación

Proyecto MESI en Centro América: Los primeros pasos

Full Paper

Jueves, 12 Noviembre

Bloque Sesión 1 TIBETS

Héctor Jara

Alejandro Sobko

Resumen/Abstract

La oferta asociada a las carreras relacionadas con la seguridad de la información es difícil de encontrar por el común de los estudiantes que buscan desarrollar su carrera profesional en esta disciplina. En España, el Proyecto MESI es un excelente trabajo que tiene como uno de sus pilares, el relevamiento de las distintas opciones académicas en dicho campo. El presente artículo tiene por objetivo extender el trabajo realizado en España a Centro América, indicando las distintas opciones que disponen los estudiantes, como así también los nuevos desafíos que se presentaron al momento de realizar la investigación. Finalmente se presenta una versión Beta de una herramienta desarrollada para tal fin.

Palabras clave/Keywords

information security, education, security education, universities, MESI, Central America.

CIBSI ECUADOR 2015

ESPE UNIVERSIDAD DE LAS FUERZAS ARMADAS INNOVACIÓN PARA LA EXCELENCIA

Desarrollo de un Sistema Experto para la valoración del Curriculum de los alumnos a partir de las competencias

Full Paper

Jueves, 12 Noviembre

Bloque Sesión 1 TIBETS

Luis Enrique Sánchez Crespo

Antonio Santos-Olmos

Esther Álvarez González

Mónica Karel Huerta

Eduardo Fernández-Medina

Resumen/Abstract

Durante la reforma de los grados de ingeniería informática, la aparición del concepto de competencias no ha aportado ventajas a las empresas a la hora de poder seleccionar candidatos más adecuados para sus puestos de trabajo. Este articulo pretende mostrar parte de la investigación que se ha realizado para determinar las causas por las que las empresas no encontraron útiles estas competencias y cómo se pueden alinear ambas. Por último se muestra el desarrollo de un Sistema Experto orientado a facilitar a las empresas la selección adecuada de candidatos para sus puestos de trabajo, teniendo en cuenta competencias personales y sociales, así como conocimientos técnicos. Este prototipo servirá de base para alinearlo con las competencias definidas en las mallas curriculares, permitiendo un auténtico alineamiento entre las carreras y las necesidades de perfiles profesionales de las empresas.

Palabras clave/Keywords

Espacio Europeo de Educación Superior EEES, Grado en Ingeniería Informática, CompetenciasGenerales, Competencias Generales Específicas, Sistemas Expertos, e-GRH

Cátedra en Seguridad de Datos como una aproximación desde la arquitectura empresarial

Full Paper

Jueves, 12 Noviembre

Bloque Sesión 2 TIBETS

Claudia P.
Santiago

Resumen/Abstract

Este artículo presenta el diseño del curso de Seguridad de Datos, el cual fue concebido como una aproximación de la seguridad de la información desde la arquitectura empresarial – AE, de tal manera que durante el diseño de las arquitecturas de negocio, datos, aplicaciones y tecnología se hiciera una revisión de los aspectos de seguridad relacionados y así conseguir un diseño de seguridad alineada directamente al negocio, sus estrategias, sus metas y sus fortalezas, y apoyada en tecnologías de información – TI. Adicionalmente, en el artículo se presentan resultados de la puesta en operación del curso, en donde los estudiantes llevaron a la práctica los conceptos aprendidos obteniendo resultados de divulgación y de introducción o mejora para las organizaciones en donde trabajan.

Palabras clave/Keywords

Arquitectura empresarial, seguridad de datos, seguridad de la información, arquitectura de seguridad.

La importancia de las TIC y los Ingenieros en Informática para las empresas en España

Full Paper

Jueves, 12 Noviembre

Bloque Sesión 2 TIBETS

Antonio Santos-Olmos

Luis Enrique Sánchez Crespo

Mónica Karel Huerta

Esther Álvarez González

Eduardo Fernández-Medina

Resumen/Abstract

La adopción y utilización de las TIC tiene un impacto positivo sobre la productividad, el crecimiento económico y el bienestar social, ya que las tecnologías traen consigo la aparición de oportunidades para el desarrollo de nuevos negocios y la mejora de los procesos de los ya existentes. La posibilidad de reducir costes, la utilización eficiente de recursos y de ampliar mercados ha contribuido a que los ciudadanos se estén beneficiando de productos de mayor calidad a precios más bajos. No obstante, la penetración de las TIC en el entorno empresarial se está realizando lentamente en el caso Español, ya que no existe un consenso entre el uso de las TIC y el aumento de productividad. El desconocimiento, la falta de formación en nuevas tecnologías y la falta de personal adecuado son los principales obstáculos con los que se enfrentan las empresas, que no perciben la utilidad para su negocio al estimar que las tecnologías no se adaptan a sus necesidades. En este artículo se dan las claves para entender cómo las tecnologías de la información y comunicación pueden ayudar a mejorar la productividad de las empresas, y cómo este aumento de productividad debe ir precedido de un aumento y especialización en la formación del personal relacionado con las TIC.

Palabras clave/Keywords

Espacio Europeo de Educación Superior EEES, Grado en Ingeniería Informática, Competencias Generales, Competencias Generales Específicas.

CIBSI ECUADOR 2015

ESPE UNIVERSIDAD DE LAS FUERZAS ARMADAS INNOVACION PARA LA EXCELENCIA

Valoración de las Competencias en la carrera de Ingeniería del Software para la orientación curricular de los alumnos

Full Paper

Jueves, 12 Noviembre

Bloque Sesión 3 TIBETS


Luis Enrique Sánchez Crespo


Antonio Santos-Olmos


David García Rosado


Daniel Mellado


Eduardo Fernández-Medina

Resumen/Abstract

Durante la reforma de los grados de ingeniería informática, la aparición del concepto de competencias no ha ayudado a los alumnos a entender mejor en qué medida alcanzan los objetivos de las diferentes asignaturas, ni a tomar mejores decisiones sobre los pasos a seguir en su carrera profesional. En este artículo se pretende mostrar los resultados obtenidos durante la investigación realizada, que ha tenido como objetivo desgranar las competencias generales y específicas del Grado en Ingeniería Informática, centrándonos en las relacionadas con la Seguridad Informática, con el objetivo de buscar un acercamiento mucho más concreto y detallado con las asignaturas y, consecuentemente, que pueda justificarse adecuadamente la forma en que las asignaturas permiten alcanzar parcial o completamente las competencias para el grado. Este enfoque, y su orientación a obtener métricas sobre las que valorar el grado en que se han alcanzado los objetivos, también permitirá que los alumnos puedan tomar mejores decisiones a la hora de seleccionar las diferentes asignaturas del grado y conocer para qué competencias están mejor cualificados.

Palabras clave/Keywords

Espacio Europeo de Educación Superior EEES, Grado en Ingeniería Informática, Competencias Generales, Competencias Generales Específicas, Métricas.

CIBSI ECUADOR 2015

ESPE UNIVERSIDAD DE LAS FUERZAS ARMADAS INNOVACION PARA LA EXCELENCIA

Propuesta de Educación y Concientización en Seguridad Informática en Base a Paremias

Full Paper

Jueves, 12 Noviembre

Bloque Sesión 3 TIBETS

Leobardo Hernández Audelo

Daniel Baltazar Alemán

Raúl Alejandro Díaz Rosas

Ángel Leopoldo Moreno Olivares

Adrián Alberto Romero Granados

José Roberto Romero Granados

Resumen/Abstract

This paper presents the design, development and implementation of an educational and awareness project about Information Security, based in reworking of paremias, proverbs, adagios, sentences and aphorisms that have been used over time to transmit, with a short sentence or phrase, a very broad message, easy to remember and learn, but contextualized to Security Information. We present software developed educational and awareness material that, using information technologies (IT), offer to students fundamental knowledge in Information Security. These material integrate applications such as animations, audio and video, all of which will be used to start a diffusion campaign to make awareness about the security relevance and needs in college, business, and institutional environments; and also all interested people.

Palabras clave/Keywords

Information security, teaching of security, security awareness, paremias of security, maxims, aphorism, information security laboratory

CIBSI
ECUADOR 2015

TIBETS
SHORT PAPER

VIII CONGRESO IBEROAMERICANO DE SEGURIDAD INFORMÁTICA

III Taller Iberoamericano de enseñanza e innovación educativa en seguridad de la información

10-12 NOV 2015
UNIVERSIDAD DE LAS FUERZAS ARMADAS DEL ECUADOR - ESPE
Sangolquí, ECUADOR

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

Con la Organización de

ESPE-InnOvativa EMPRESA PÚBLICA

CRIPTORED

Fundación IN-N-VA Centro de Innovación

CIBSI ECUADOR 2015

ESPE UNIVERSIDAD DE LAS FUERZAS ARMADAS INNOVACIÓN PARA LA EXCELENCIA

Objetivos de las competencias curriculares para mejorar la orientación profesional de los alumnos

Short Paper

Jueves, 12 Noviembre

Bloque Sesión 3 TIBETS


Luis Enrique Sánchez Crespo


Antonio Santos-Olmos


David García Rosado


Ismael Caballero


Eduardo Fernández-Medina

Resumen/Abstract

Durante la reforma de los grados de ingeniería informática, la aparición del concepto de competencias no ha ayudado a los alumnos a entender mejor en qué medida alcanzan los objetivos de las diferentes asignaturas, ni a tomar mejores decisiones sobre los pasos a seguir en su carrera profesional. De igual forma, tampoco han sido de utilidad para las empresas a la hora de seleccionar los mejores candidatos para sus puestos de trabajo. En este artículo se pretenden mostrar las principales deficiencias que se han encontrado hasta el momento en la aplicación de estas competencias y en su alineación con la empresa privada, y los objetivos que hemos planteado para dar solución a esas problemáticas, alineando mejor las competencias de los alumnos con las necesidades de las empresas. Este nuevo enfoque guiado por competencias y alineado con las empresas permitirá a los alumnos tomar mejores decisiones y guiarles mejor en su futura orientación profesional a la hora de realizar su carrera.

Palabras clave/Keywords

Espacio Europeo de Educación Superior EEES, Grado en Ingeniería Informática, Competencias Generales, Competencias Generales Específicas, Métricas.

Intercambio seguro de datos entre banco central y sistema financiero

Short Paper

Jueves, 12 Noviembre

Bloque Sesión 2 TIBETS

Edy Milla

Alberto Dams

Hugo Pagola

Resumen/Abstract

Este trabajo es el resultado de la búsqueda de casos reales en nuestra catedra que motiven a los alumnos a realizar prácticas de laboratorio con tecnologías de seguridad asociadas a las PKI. Para ello se seleccionó un caso de estudio de intercambio de datos confidenciales entre una banca central y sus entidades financieras.

El sistema financiero intercambia información con la banca central para el desarrollo de sus actividades funcionales como por ejemplo el reporte del manejo de moneda extranjera, estados de cuenta y financieros, etc. Se requiere tener la certeza que el intercambio electrónico de datos es efectuado de una manera segura.

Conscientes de esta necesidad, la industria ha desarrollado especificaciones bajo estándares que permiten efectuar el intercambio de forma segura. En este documento se propone utilizar un sobre electrónico como el que brinda la especificación S/MIME (Secure Multipurpose Internet Mail Extensions) y el objeto CMS (Cryptographic Message Syntax) en conjunto con la confianza entre organizaciones que se puede establecer utilizando la funcionalidad de certificación cruzada de X.509 (RFC5280). Como veremos en este artículo, este conjunto de herramientas apoyándose en el uso de PKI permite obtener autenticación, integridad, confidencialidad y no repudio (prueba de origen) de la información.

El caso de uso se implementó utilizando las herramientas que provee OpenSSL y se implementaron guías de laboratorio que permiten llevar a cabo un modelo de la infraestructura PKI del Banco Central (BC), Instituciones Financieras (IF), su relación de confianza y la generación de los mensajes CMS para el intercambio de datos de forma segura. Estas guías fueron utilizadas con éxito en el desarrollo de la materia Seguridad en Redes de la Maestría en Seguridad Informática de la Universidad de Buenos Aires.

Palabras clave/Keywords

Infraestructura de clave pública, S/MIME,CMS, PKI, confianza, intercambio seguro, integridad, confidencialidad, autenticación, no repudio.