Publicación quincenal editada por el Departamento de Telecomunicaciones y Telemática del Instituto Superior Politécnico José Antonio Echeverría
Auspiciada por el Ministerio de la Informática y las Comunicaciones

Año VII No. 21

ISSN: 1729-3804

Telem@tica

Enero 30, 2009
"Año del 50 aniversario del triunfo de la Revolución"

REVISTA DIGITAL DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

FRASE DE LA SEMANA

"Intenta no volverte un hombre de éxito, sino volverte un hombre de valor."

Albert Einstein

SUMARIO

Contáctenos

REVISTA TELEM@TICA
Departamento de Telemática
Facultad de Ingeniería Eléctrica

Instituto Superior Politécnico
José Antonio Echeverría

Calle 114, No. 11901, entre 119 y 127, Municipio Marianao, Habana,Cuba

Teléfono:
+53 (7) 2606279 / 2679880

Fax:
+53 (7) 2671576

Telematica@revistas.cujae.edu.cu

Sitio Web:
http://www.cujae.edu.cu/revistas/telematica

IR al SUMARIO

NOTA DEL EDITOR

Estimado lector:

Con el objetivo de encontrar una vía para realizar un módulo de Seguridad de un Sistema de Supervisión y Control de Datos (SCADA: Supervisory Control And Data Acquisition) bajo licencias de software libre o Licencia Pública General (GPL: General Public License) para el diseño e implementación del mismo, se realizó este trabajo, el cual cuenta como temas principales explicar brevemente las ventajas de disponibilidad y mejora de un sistema trabajando bajo GPL, explicar detalladamente los requerimientos y la arquitectura del sistema recorriendo sus diferentes subsistemas y las funcionalidades que tienen los mismos en el módulo de Seguridad de un SCADA. También se muestra una breve explicación de las técnicas modernas para lograr una mayor seguridad en el sistema.

Nos encontraremos nuevamente en el próximo número.

Los Editores.

TÉCNICAMENTE HABLANDO

Implementación: Poner en funcionamiento, aplicar métodos, medidas, etc., para llevar algo a cabo.

Arquitectura: Es el diseño conceptual y la estructura operacional fundamental de un system.

Caso de uso: En ingeniería del software, un caso de uso es una técnica para la captura de requisitos potenciales de un nuevo sistema o una actualización de software. Cada caso de uso proporciona uno o más escenarios que indican cómo debería interactuar el sistema con el usuario o con otro sistema para conseguir un objetivo específico.

Seguridad: Consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida así como su modificación sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

Subsistema: Sistema que es parte de un sistema más grande.

ARTÍCULO

SEGURIDAD DE SISTEMAS SCADA BAJO GPL

INTRODUCCIÓN

¿Por qué GPL?

Dado el alto precio de los sistemas software en el mercado, unido al precio de los servicios de licencias y soporte que éstos exigen; dada la crítica situación en la que se encuentra nuestro país con el bloqueo en el mundo informático, donde no se le permite realizar compras de determinados productos necesarios para nuestro desarrollo informático ni de comercializar nuestros productos en la mayoría de los casos si contienen licencias privativas, Cuba se proyecta la estrategia de migrar al software libre (SWL). Nosotros, como estudiantes y trabajadores de la Universidad de las Ciencias Informáticas (UCI), estamos ya en una etapa madura de ese proceso; y con ese fin, además de otras situaciones políticas presentadas, nos trazamos como objetivo realizar el módulo Seguridad del sistema SCADA que se está desarrollando en la universidad en software libre, bajo licencias GPL (General Public License).
Durante el desarrollo de nuestro sistema, se ha ido garantizando que su diseño cumpla con las 4 libertades básicas que establece la Fundación de Software Libre, o Free Software Fundation como más se conoce (FSF). De esta forma se respalda el soporte y actualizaciones que se hagan luego de su primera liberación de nuestro sistema. Además de estar basado en herramientas libres para su desarrollo, diseño, gestión y documentación.
Contar con esas licencias y cumplir con estas políticas nos brinda la ventaja de trabajar con bibliotecas de código abierto con una comunidad de soporte, intercambio y ayuda. Brinda autonomía, derecho y posibilidad libre de desarrollo. Aunque muchos consideran que el ser código abierto pudiera comprometer la seguridad de un sistema, nuestro módulo prueba todo lo contrario, pues como mismo en los algoritmos de encriptación existe en código abierto y son utilizados dado que la seguridad yace en la complejidad de su clave, nuestro módulo provee de una estructura lógica capaz de disipar todo tipo de brechas en su desempeño.

Sistema Operativo (SO) Debian GNU/Linux

Debian se una distribución basada en el conocido y distribuido núcleo de Linux y bajo la licencia General Public Licence (LGPL), además de ser una de las distribuciones de GNU/Linux mantenida solamente por voluntarios, sin un enfoque comercial. La misma se actualiza diariamente apareciendo paquetes nuevos de software constantemente. Al mismo tiempo, existe un compromiso de calidad, no se desea distribuir software con errores, por lo que es un SO muy profesional.
Por estas razones, esta distribución tiene un mayor componente técnico que otras distribuciones; aunque también es posible que ciertos paquetes no estén tan actualizados como debieran, quizás porque sus desarrolladores han dejado de actualizarlos y nadie se ha hecho cargo.
Se decidió usar la distribución Debian porque es una distro[1] de desarrollo muy estable, por lo que los paquetes que se desarrollen en él y quieran ejecutarse utilizando cualquier distribución siempre serán estables.. A diferencia de otras distribuciones tiene un magnífico soporte de estabilidad en las aplicaciones. Los módulos del LDAP (Lighweight Directory Access Protocol) se pueden ejecutar sin problemas permitiendo que los usuarios usen sus sesiones en cualquier máquina dentro del área de trabajo, ahorrando recursos de hardware.

Iliana Pérez Pupo
INSTRUCTOR RECIEN GRADUADO.
FACULTAD #5 (UCI)

Iperez@uci.cu

Ruben Gomez Johnson
INSTRUCTOR RECIEN GRADUADO.
FACULTAD #5 (UCI)

Rjohnson@uci.cu

Enrique Reyes Bermúdez
Estudiante (UCI)

Ereyes@estudiantes.uci.cu

IR al SUMARIO

IDE a utilizar: Eclipse

El Eclipse es un Entorno Integrado de Desarrollo[2] (IDE) multiplataforma libre para crear aplicaciones clientes de cualquier tipo.
El IDE de Eclipse emplea módulos (en inglés plug-in) para proporcionar toda su funcionalidad, a diferencia de otros entornos monolíticos donde las funcionalidades están todas incluidas, las necesite el usuario o no. El mecanismo de módulos permite que el entorno de desarrollo soporte varias tecnologías como Java, C/C++, XML, el Subversion para el desarrollo integrado, bibliotecas para la programación visual como Gtk y Qt, soporte a bases de datos. En general, existen módulos para añadir un poco de todo.
Se decidió usar el IDE de Eclipse porque nos permite realizar trabajo en equipo, realizar actualización teniendo el control de las versiones anteriores y nos facilita la integración del módulo Seguridad con el resto del sistema sólo con agregarlos en forma de plug-in. La gestión del proyecto se torna muy cómoda.
La definición que da el proyecto Eclipse acerca de su software es: "una especie de herramienta universal - un IDE abierto y extensible para todo y nada en particular".

Módulo Seguridad de un sistema SCADA

La Seguridad en el Control Industrial es un tema novedoso y en desarrollo actual en la rama de la especializada mundial del Control Automático, tanto para fabricantes de tecnologías, diseñadores de la ingeniería de sus aplicaciones, como para las organizaciones profesionales que se orientan en el planteamiento de su normativa y regulación.
La vulnerabilidad de la Seguridad de los Sistemas de Control y Adquisición de Datos es un hecho y reto mundial.
Estos sistemas de control proveen gran eficiencia y el más amplio de los usos en su aplicabilidad, sin embargo, constituyen también un riesgo si no son atendidas las vulnerabilidades a la seguridad que implícitamente poseen.
Es importante el señalar que la Arquitectura de la Seguridad se debe tratar desde el principio, que a diferencia de los sistemas informáticos corporativos, la prioridad de las tareas en los SCADA es Disponibilidad, Seguridad y Confiabilidad, minimizando el impacto en el desempeño de las tareas que presentan restricciones de tiempo real.

Con el fin de garantizar los principios antes expuestos, se diseñó una arquitectura para el módulo de Seguridad de un SCADA realizado bajo GPL, de la cual se provee una descripción comprensiva, mostrando a través de las vistas de casos de uso y lógica todas las soluciones que permitan el desarrollo e integración con los restantes módulos del sistema.

1. Vista de casos de uso.

En esta vista se documenta tanto los casos de uso que afectan a la Arquitectura del sistema como aquellas funcionalidades identificadas como requerimientos funcionales (figura 1)

2. Vista lógica.

Es un subconjunto del modelo de análisis/ diseño del sistema que presenta los elementos significativos para la arquitectura, subsistemas así como las interrelaciones que existen entre ellos.

---

1 Distribución de GNU/Linux.
2 IDE: Integrated Development Environmen. Entorno Integrado de Desarrollo.

IR al SUMARIO

Vista de casos de uso

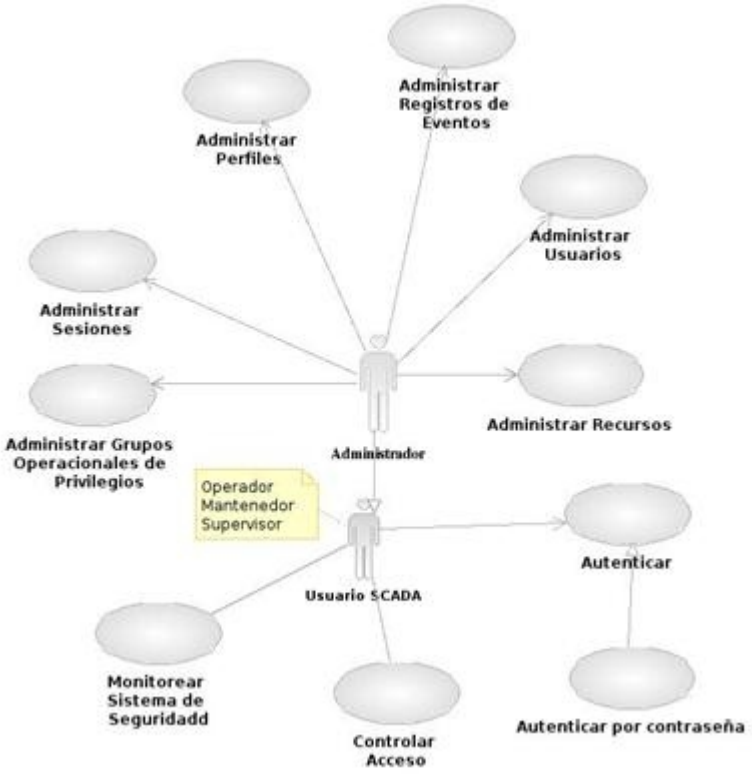

Figura 1. Diagrama de casos de uso

En esta sección serán descritos los casos de uso que afectan a la arquitectura del sistema y las funcionalidades identificadas como requerimientos funcionales.

Prioridades y descripción de los casos de uso.

- Autenticar usuario.

La autenticación describe el proceso de identificar positivamente los potenciales usuarios de un SCADA, usando una combinación de diversos factores de autenticación como contraseña, información biométrica y credenciales de identificación, siendo requisito esencial para conceder el acceso a los recursos en el sistema. Sobre la base de la información del perfil de Usuario, se le otorga los privilegios correspondientes e inicia una sesión con el tiempo de expiración adecuado a su perfil.

- Control de acceso.

Describe el proceso de conceder o negar peticiones específicas para la obtención y uso de información y servicios de procesamiento. Se concederá o no el control solicitado por el usuario al recurso según los permisos definidos a su perfil.

- Administrar usuarios.

Este caso de uso permite definir, modificar y eliminar los usuarios de un sistema SCADA.

- Administrar perfiles.

Este caso de uso permite definir, modificar y eliminar los perfiles de usuarios de un sistema SCADA.

- Administrar Registro de eventos.

Este caso de uso permite definir, modificar y eliminar los registros de eventos (log) relacionados con la seguridad del sistema SCADA Nacional.

- Administrar sesión.

Este caso de uso permite definir, modificar y eliminar sesiones para los usuarios de un sistema SCADA, además de bloquearla en caso de haberse detectado alguna acción anómala realizada por el usuario dueño de la sesión.

- Validar.

Este caso de uso permite realizar validaciones de los datos entrados por el usuario, además de garantizar el las contraseñas cumplan com las políticas de seguridad establecidas por el SCADA[3].

---

3 Para conocer las políticas de seguridad estasblecidas por el grupo de desarrolladores del módulo Seguridad del SCADA, ver el documento “Políticas de Seguridad”.

- Encriptar.

Este caso de uso permite garantizar la confiabilidad de los datos como contraseñas y otras informaciones sensibles del sistema mediante la encriptación.

Entre los actores identificados para el sistema están:

- Usuarios SCADA

Conceptualiza a los módulos internos o externos del SCADA así como los usuarios de estos módulos, que requieran interactuar con los servicios de Autenticación y Control de acceso. Entre los tipos de Usuarios SCADA pueden estar Operador, Mantenedor y el Supervisor.

- Administrator

Conceptualiza al usuario encargado de instar los casos de usos asociados al quitar administrador.
En la figura 1 se muestra un diagrama que relaciona cada una de estas funcionalidades con los actores del sistema.

Vista Lógica
Esta sección describe las partes más significativas de la arquitectura en un modelo de diseño, para cada subsistema significativo su descomposición en clases, las clases arquitectónicamente significativas y la descripción de sus responsabilidades así como las relaciones más importantes, operaciones y sus atributos.
Paquetes de diseño arquitectónicamente significativos.
1. Persistence Control Subsystem
2. Credential Generator Subsystem
3. Session Control Subsystem
4. Privileges Control Subsystem
5. Authentification Control Subsystem
6. Log Control Subsystem
7. Monitor Control Subsystem
8. Validation Subsystem
9. Encriptation Subsystem

Descripción de los Paquetes de Diseño Arquitectónicamente Significativos.

- Persistence Control Subsystem

Este subsistema se centra en la persistencia de todos los datos necesarios para el mantenimiento de la seguridad y que estará soportado en una base de datos. El subsistema debe permitir guardar de forma ordenada y segura estos datos permitiendo un rápido acceso a ellos, garantizando además la disponibilidad, integridad y seguridad de los mismos, independientemente del comportamiento del sistema.

- Credential Generator Subsystem

Éste genera las credenciales de los recursos, usuarios, grupos de usuarios y los grupos de recursos, garantizando que éstas sean únicas.

- Session Control Subsystem

Este subsistema se encarga de la administración y control de todos los datos de todos aquellos usuarios que estén en el sistema en ese momento, los datos que se almacenan del mismo son: credencial y tablas de permisos. Además se encargan de la eliminación, inserción y cambio de estado de las sesiones.

- Privileges Control Subsystem

Este subsistema administra y controla el acceso de los usuarios del SCADA Nacional a los recursos, permite que los recursos no sean accedidos o utilizados de forma incorrecta por cualquier usuario.

- Authentication Control Subsystem

Este subsistema administra y controla las entradas al sistema SCADA Nacional de forma que siempre garantice que sea solamente para personal autorizado. Se encarga de crear una nueva sesión y de cargar las tablas de privilegios para la nueva sesión. Se apoya en el Persistence Subsystem, User Subsystem y Session Subsystem, y de este se desprende el subsistema: Validation Subsystem.

- Validation Subsystem.

Es el encargado de validar los datos del usuario que desea entrar al sistema, o sea verificar la validez de los mismos.

IR al SUMARIO

- Monitor Control Subsystem

Este subsistema se encarga de realizar monitoreos a los usuarios on-line del sistema, es decir, a los que se encuentran autenticados. De ellos llevará el control de la ip desde donde se conectan, el tiempo inicial que realizaron la conexión, el nombre del usuario concectado y su tiempo de expiración, que no es más que el tiempo que le queda por tener su sesión abierta.
En la figura 2 se representan los subsistemas descritos anteriormente, la relación entre ellos y la forma de comunicación con el medio exterior, a través de la interfaz ISecurity, responsable del flujo de información entre éstos con los del resto de los módulos del sistema.

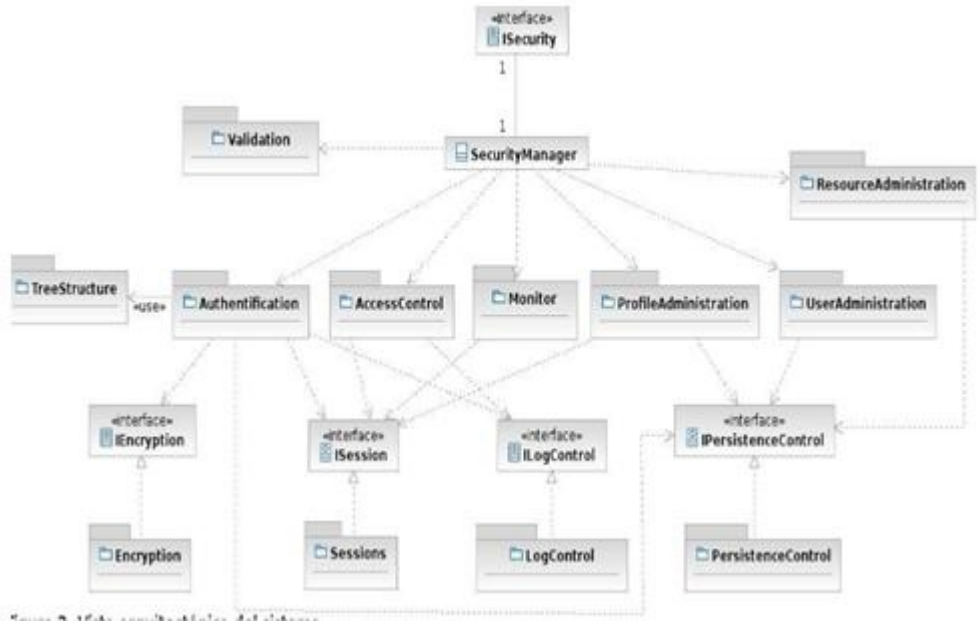

Figura 2. Vista arquitectónica del sistema.

Realización de los Casos de Uso

- Descripción del Caso de Uso ”Autenticar”

Es el proceso de verificación de la identidad del usuario de un sistema SCADA, como requisito esencial para conceder el acceso a los recursos en el sistema.
El resultado de este proceso de autenticación se convierte entonces en la base para permitir o negar acciones futuras que permita o no el potencial acceso del usuario a los recursos.

- Descripción del Caso de Uso ”Controlar Acceso”

La autorización es el proceso de determinar, a quién y a qué se le debe permitir el acceso a un recurso particular según el perfil asociado: control de acceso es el mecanismo para cumplir la autorización.
Los controles de acceso proporcionan políticas y procedimientos para especificar el uso de los recursos del sistema SCADA por solamente los usuarios de dicho sistema. Especifica los controles para administrar las cuentas del sistema. Los controles cubren asuntos de fortalecimiento del acceso tales como la separación de tareas, privilegios mínimos, intentos de entrada al sistema infructuosos, notificación de uso del sistema, notificación previa de entrada al sistema, control coincidente de cierre y cese de la sesión. Se insertarán controles que tratan el uso de dispositivos portátiles y remotos para acceder al sistema, así como el uso de las capacidades de acceso remoto y la implementación de tecnologías inalámbricas.

- Descripción del Caso de Uso “Monitorear”

Se encarga de mostrar y administrar las sesiones activas en el sistema, permitiendo además el control por parte de los administradores del sistema, previniendo posibles fallas o ataques al sistema tales como múltiples autenticaciones. Además se encarga de mostrar al usuario cuándo una sesión está por caducar para lo que se le brinda además la opción de extender su tiempo de expiración operación que solo podrá ser desarrollada en dos intentos. En caso de que una sesión expire el monitoreo eliminará esa sesión.

IR al SUMARIO

Recomendaciones importantes para lograr una defensa profunda

La seguridad en un sistema SCADA no sólo depende del software que se sea capaz de implementar, sino que depende de varios factores que recomendamos su aplicación. Estos factores consisten en tres clases de controles que permiten una “defensa en profundidad” del Sistema SCADA Nacional. Estos controladores son:

- Controles Técnicos.
- Controles Operacionales.
- Controles Administrativos.

Estos controles están compuestos por elementos principales y entre ellos un sistema.

- Subsistema de Detección de Intrusos
- Políticas de Seguridad
- Cifrado de datos (criptografía)
- Sistema de FireWall.
- Mecanismo de tolerancia a fallas, ya que no se debe permitir las interrupciones en el funcionamiento normal del sistema.

Existen otras tareas relacionadas con la seguridad del SCADA, que se destacan por la periodicidad con que se deben realizar y revisar, entre estas recomendamos:

- Evaluación de riesgos y vulnerabilidades.
- Revisión del Sistema de Seguridad.
- Mantenimiento periódico.
- Plan de capacitación y concientización de seguridad.
- Plan de contingencia.

Extensión del módulo

El sistema aún carece de seguridad en cuanto a robos de clave de usuarios o acciones malintencionadas de usuarios que posean permisos para realizar ciertas actividades que puedan comprometer la integridad y buen funcionamiento del sistema.
El sistema cuenta solamente con un método de autenticación (por nombre de usuario y clave) por lo que se desea incorporar un subsistema de autenticación por tarjetas y por parámetros biométricos, logrando así que el mismo sea más completo aún y dando la posibilidad a los usuarios de que se autentiquen por cualquiera de los métodos en cuestión. Tampoco se realizan verificaciones del número de autenticaciones ni de accesos a recursos fallidos o acertados velando que no excedan la cantidad máxima establecida.
En virtud de robustecer la solución presentada, se están desarrollando funcionalidades de alto impacto en este sensible tema del sistema, las que se describen a grandes rasgos a continuación:

- Creación de un Sistema de Detección de Intrusos a fin de evitar ataques malintencionados de usuarios con claves ajenas o con el nivel de seguridad necesario para realizar acciones de importancia crítica en el sistema.
- Ampliar las funcionalidades de la Interfaz de Autenticación para que ésta sea reutilizable para la Autenticación por biométricas y tarjetas.

1. Crear las funcionalidades y métodos necesarios para permitir a los mantenedores la Autenticación en el sistema por tarjetas, brindando una mayor variedad de métodos para validar la pertenencia de un usuario al sistema.
2. Crear las funcionalidades y métodos necesarios para permitir a los mantenedores la Autenticación en el sistema por parámetros biométricos, brindando una mayor variedad de métodos para validar la pertenencia de un usuario al sistema.

Subsistema de Detección de Intrusos.
Es un programa a implementarse y usarse para detectar accesos no autorizados al SCADA, ya sea un computador o la red. Ésto se basa en el análisis pormenorizado del tráfico de red, existiendo diversas maneras de implementarse.

IR al SUMARIO

Ya se están definiendo los nuevos casos de uso que darán cumplimiento a la realización de este subsistema, entre ellos está:

- Verificar accesos multiples

Realiza el proceso de verificación de los accesos múltiples que presenta un usuario a determinado recurso e incluso a un número excesivo de ellos, chequeando que no exceda al número máximo de accesos a un recurso determinado ni a un grupo grande de ellos. Activar una alarma de seguridad para estos casos y registrar en un log detalles de las acciones realizadas por el usuario.

- Verificar autenticaciones múltiples

Este caso de uso describe el proceso de verificación de las autenticaciones múltiples que presenta un usuario, chequea que no exceda al número máximo de autenticaciones permitidas y que dentro de un mismo nodo no tenga ya una autenticación activa o una sesión. Activar una alarma de seguridad para estos casos y registrar en un log detalles de las acciones realizadas por el usuario.

- Verificar evento de tecleo de contraseña

Registrar el tiempo de tecleo que demora un Usuario SCADA en escribir la frase completa de su contraseña. Se deberá activar esta funcionalidad cada vez que un usuario realiza su autenticación usando la contraseña. Activar una alarma de seguridad en caso de no cumplir con el tiempo y registrar en un log detalles de las acciones realizadas por el usuario.

- Cambiar contraseña

Permitir que el sisterma detecte cuándo debe pedir a un usuario, un cambio a una contraseña nueva. Antes deberá realizar la verificación de que la contraseña insertada por el usuario como nueva, no haya sido usada por él anteriormente, además de que cumpla con las políticas de seguridad establecidas como no ser nombres de familiares, ni la fecha de nacimiento, chapas de carros.

Autenticación biométrica

La autenticación biométrica es una funcionalidad que se añadirá al subsistema “Autenticación” del módulo Seguridad del SCADA con el fin de ganar em confidencialidad y seguridad en el sistema, la cual ya se está en definición.

Es una forma de acceder al sistema basado en las características físicas del usuario a autenticar. El reconocimiento de formas, la inteligencia artificial y el aprendizaje son las ramas de la informática que desempeñan el papel más importante en los sistemas de identificación biométricos.

- Autenticar por biometría

La autenticación por parámetros biométricos describe el proceso de identificar positivamente los potenciales usuarios del SCADA Nacional, usando la identificación única del parámetro biométrico suministrado por el usuario. Sobre la base de la información del perfil de Usuario, se le otorga los privilegios correspondientes e inicia una sesión.

- Autenticar por tarjeta de código de barra.

La autenticación por tarjeta de código de barra describe el proceso de identificar positivamente los potenciales usuarios del SCADA Nacional, usando la identificación única del código de barra asignado al usuario. Teniendo en cuenta la información del perfil de Usuario, se le otorga los privilegios correspondientes e inicia una sesión.

En la figura 3 se representan los nuevos casos de uso y su relación y dependencia con los ya desarrollados.

IR al SUMARIO

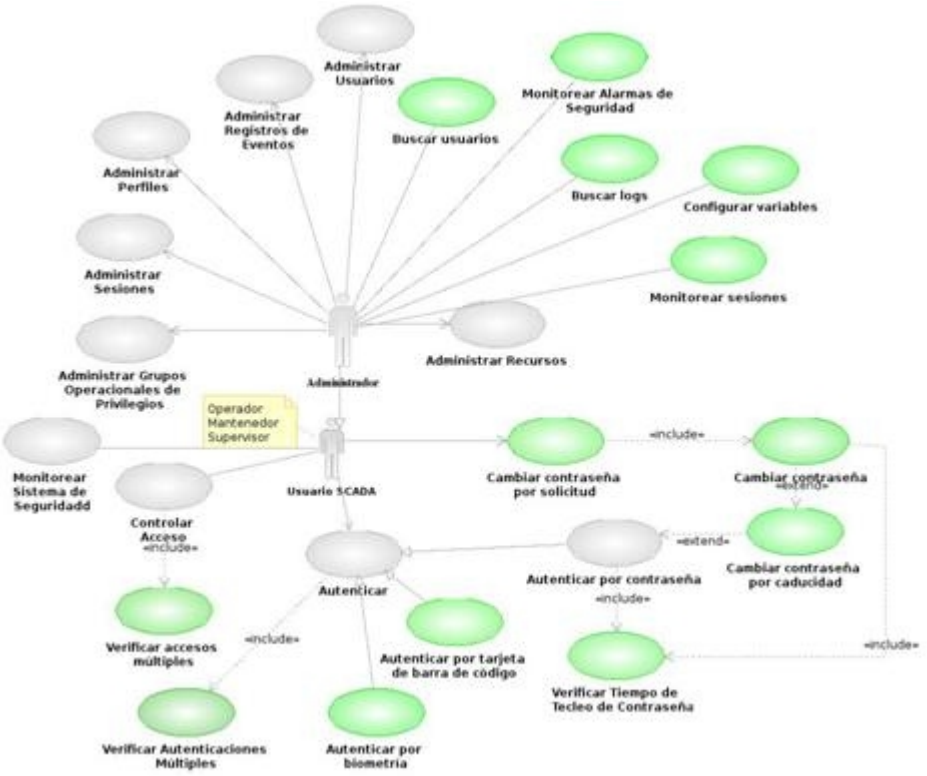

Figura 3. Extensión del diagrama de casos de uso del sistema.

Políticas de seguridad para el módulo Seguridad de un SCADA

Las políticas de seguridad son las reglas y procedimientos que regulan la forma en que una organización previene, protege y maneja los riesgos de diferentes daños. Las definidas por este grupo de trabajo están dirigidas a garantizar una mejor disciplina y menores riesgos al sistema a nivel de autenticación, de seguridad de acceso a la máquina y de restringir la escalabilidad en la red.
En etapas próximas, se harán mejoras técnicas y procedimentales en las políticas de seguridad, además de adicionar otras dirigidas al uso, configuración y funcionamiento de dispositivos de red y la comunicación de la LAN al exterior.
Tanto las políticas como los casos de pruebas de seguridad definidos en el documento, tienen la intención de garantizar que el sistema cumpla con las dimensiones de seguridad siguiente:

- Autenticación: medida por la cual cada interacción en el proceso está privilegiada.
- Acceso: Limitar el acceso o negar todo excepto lo que esté expresamente permitido financieramente y por buenas prácticas.
- Seguridad: garantizar que un proceso no dañe a otros sistemas o procesos, incluso en caso de falla total del mismo.

La política de seguridad definida hasta el momento está dirigida a:

- Protección de los ficheros de almacenamiento de las contraseñas de usuarios y del sistema.
- Evitar uso de contraseñas fáciles de ser adivinadas y vulnerables a ataques de fuerza bruta y diccionarios.
- Evitar que las contraseñas perduren en el tiempo.
- Evitar el uso de contraseñas muy cortas y muy largas.
- No tener puertos de escucha abiertos innecesariamente o servicios activos sin usar.
- Sobre protección a las tuplas de las bases de datos y ficheros que contengas información sencible para el sistema.
- Reglas que fortalezcan la vulnerabilidad del sistema ante ataques de inyección.

IR al SUMARIO

- Pautas para una buena configuración y administración de la red donde está actualmente en desarrollo el sistema y donde será desplegado.

Para la verificación del cumplimiento de algunas de estas medidas y en virtud de analizar y detectar las vulnerabilidades de las funcionalidades implementadas, fueron usadas herramientas libres como el BackTrack, que es una distribución GNU/Linux muy usada para la realización de auditorías de seguridad, que incluye 300 herramientas para este fin.

IR al SUMARIO

Conclusiones

En el trabajo se realizó un análisis de por qué se requiere del uso de herramientas multiplataformas para la realización del módulo Seguridad de un SCADA, así como la ventaja e importancia de las licencias y bibliotecas GPL. Se explica brevemente el análisis y diseño del módulo Seguridad de un SCADA partiendo de las vistas de casos de uso y la lógica y se mencionan las nuevas funcionalidades a adicionar al módulo que ya se está diseñando así como los principios que deben cumplir las políticas de seguridad.

Bibliografía

[1]Herzog Pete, "OSSTMM (Open Source Security Testing Methodology Manual)", fecha de la versión original Lunes 18 de diciembre del 2000, fecha de la versión actual Sábado 23 de agosto del 2003. Versión 2.1.

[2]W. W. Boles y B. Boashash, “A Human Identification Technique Using Images of the Iris and Wavelet Transform”, IEEE TRANSACTIONS ON SIGNAL PROCESSING, Vol. 46, No. 4, Abril 1998.

[3]Sanchez-Avila Carmen y Sanchez-Reillo Raul, “Sistemas de identificación biométrica mediante patrón de iris utilizando representación multiescala e información de fase”.

[4]Daugman John, “How Iris RecognitionWorks” University of Cambridge, The Computer Laboratory, Cambridge CB2 3QG, U.K.

[5]Sitio web de RedIris, última actualización, 2002-07-15. Http://www.rediris.es/cert/doc/unixsec/node14.html

[6]Sánchez Reíllo Raúl. Tesis doctoral “Mecanismos de Autenticación Biométrica Mediante Tarjetas Inteligentes”. Universidad Politécnica de Madrid 2002.

[7]Última actualización, 2008-08-25. Http://www.biometria.gov.ar/index.php/documentos/60-reconocimiento-del-iris-

[8]Ariel Palazzesi. Última actualización, 2007-12-14. Http://www.neoteo.com/biometria-usa-tus-ojos-como-una-llave.neo

[9]Munóx Pérez José. Universidad de Málaga. SISTEMA DE IDENTIFICACIÓN BASADO EN EL IRIS. 2005.

IR al SUMARIO

EVENTOS

Informática 2009
XIII CONVENCIÓN Y FERIA INTERNACIONAL

Estimados colegas:

Del 9 al 13 de febrero de 2009, La Habana acogerá la XIII edición de la Convención y Feria Internacional Informática 2009, que sesionará en el Palacio de Convenciones de La Habana y en el recinto ferial PABEXPO. ¨Las Tecnologías de la Información y las Comunicaciones como soporte para el desarrollo endógeno y la soberanía tecnológica de los pueblos¨, es el tema central que promoverá el evento, y es la fuente de la invitación a la discusión científico tecnológica, a la exposición de proyectos e iniciativas que promuevan los propósitos y acciones que emprenden los países para impulsar el uso de las TIC en el desarrollo de la sociedad.
Informática 2009 estimulará el intercambio entre profesionales, científicos, técnicos, empresarios, representantes gubernamentales, organismos internacionales y público en general, interesados en investigar, promover, analizar y conocer sobre el avance de las tecnologías de la información, las telecomunicaciones, la electrónica y la automática, así como sus aplicaciones actuales en los diversos sectores de la sociedad.
El Comité Organizador de INFORMÁTICA 2009 les reitera la invitación a presentar sus contribuciones profesionales y muestras comerciales con la garantía de que alcanzaremos los objetivos comunes en un clima de amistad y solidaridad.

Dr. Jorge Luis Perdomo Di-Lella
Presidente Ejecutivo del Comité Organizador
Viceministro de la Informática y las Comunicaciones

PDF Explorer 1.5

Por:

Ing. Julio Cesar Camps

Email: camps@tesla.cujae.edu.cu

Ficha Técnica	
Fecha:	Septiembre 30/2005
Nombre:	PDF Explorer
Propiedad:	RTT
Versiones:	PDF Explorer 1.5 Build 43 Beta
Tamaño:	2,946 KB
Plataformas	Windows 95/98/Me/NT/2000/XP.
Idiomas	Inglés
Clasificación	Downloads/file management/organization/
URL	http://rtt.planetaclix.pt/home.htm
Descripción	PDF Explorer es un software de administración de ficheros pdf y una herramienta de extracción de imágenes. Permite de una forma fácil adicionar todos los ficheros pdf que se deseen a una base de datos, almacenando el nombre del fichero, título, asunto y autor, de forma que es posible buscar a través de esos ficheros, verlos, renombrarlos en lote y mucho mas.
Observaciones	Es altamente innovador y brinda las opciones de extraer las imágenes de los ficheros pdf hacia el clipboard. Dichas imágenes pueden ser seleccionadas, intercambiadas, etc. Las propiedades del fichero pdf pueden ser editadas. Y la ayuda se encuentra en el readme.txt
Calificación	Excelente según opiniones y análisis @@@@@

Características

Algunas de las características del PDF Explorer son:

- Rápida y efectiva inclusion en bases de datos de los campos "nombre del fichero", "autor" y "palabras clave" de todos los ficheros .pdf presentes en una carpeta o disco determinado.
- Pueden ser almacenados múltiples discos.
- Búsqueda o filtrado por palabras en los campos almacenados en la base de datos.
- Extracción automática de todas las imágenes contenidos en un fichero pdf, para una mejor manipulación o exportacion, mediante un visualizador interno.
- Herramientas de mantenimiento para el trabajo con la base de datos.

Resumen

El PDF Explorer es pequeño, fácil de usar, no ocupa casi memoria y altamente estable en su comportamiento. Lo cuál lo hace una herramienta altamente recomendable para su uso casi cualquier configuración de hardware. Por último algunas preguntas:

- Posee usted muchos ficheros .pdf?
- Recuerda haber leído algo relacionado con un asunto en especifico, pero no tiene idea de donde pueda estar ese fichero .pdf y menos aún el nombre?
- Posee un fichero .pdf con algunas imagenes que desea usar en otro documento, pero no posee el Adobe Acrobat?

Si su respuesta es “SI” a algunas de las preguntas anteriores, pues entonces el PDF Explorer es lo que necesitas.

NOTICIAS

SOFTWARE

El creador de Linux aprueba Windows 7 — 28/01/2009

En una entrevista con ComputerWorld, Linus Torvalds se refiere al próximo sistema operativo de Microsoft, Windows 7. Torvalds opina que Microsoft ha llegado a la conclusión de que el desarrollo de Vista tomó demasiado tiempo. "Pudiera suponerse que tienen un ciclo de desarrollo de dos años, que considero excesivo", indica Torvalds, acotando que seis meses ha sido el período adecuado para cada versión de Linux, aunque incluso una versión anual puede ser viable.

Fuente: http://www.diarioti.com

SEGURIDAD

Spammers desafían la predicción de Bill Gates — 28/01/2009

Efectivamente, el 24 de enero de 2004, en el World Economic Forum en Davos, Suiza, Bill Gates declaró que el spam sería “cosa del pasado" en dos años. Sin embargo, cinco años después, los expertos de SophosLabs han comprobado que las últimas cifras registradas durante el último trimestre de 2008, demuestran que el spam continua representando una gran amenaza.

Los correos basura ahora son maliciosos y diseñados para infectar los ordenadores a través de sofisticados archivos adjuntos o con enlaces a páginas web infectadas que tienen como fin robar información sensible de los usuarios.

Fuente: http://www.diarioti.com

IR al SUMARIO

SEGURIDAD

Kaspersky lanza prototipo de su antivirus para Windows 7 28/01/2009

Kaspersky Lab anuncia el lanzamiento de un prototipo de Kaspersky Antivirus para Windows 7 que utiliza un nuevo motor antivirus y proporciona a las empresas de todos los tamaños una protección completa frente a la amenaza de los cibercriminales. El prototipo de Kaspersky Antivirus ha sido diseñado para securizar los ordenadores que trabajan con Windows 7. El prototipo será mejorado por las herramientas de administración centralizadas, cuyo desarrollo se ha programado para la fase de test del nuevo sistema operativo.

Fuente: http://www.diarioti.com

INTERNET

Detectan función secreta en beta de Picasa para Macintosh 21/01/2009

La versión beta de Picasa para Mac incorpora una interesante función que permite enviar imágenes directamente a un servicio denominado Google Web Drive. Según información extraoficial, Google Web Drive sería la próxima gran iniciativa de Google para almacenamiento en línea, similar a Microsoft SkyDrive y Microsoft Mesh.

Fuente: http://www.diarioti.com

IR al SUMARIO

HARWARE

LiteOn lanza grabador de 24x con función SmartErase 27/01/2008

Lite-On presentó iHAS324, el grabador de DVD de 24X. iHAS324 representa el grabador de DVD de “nueva generación" con una velocidad máxima de grabación de 24X. La unidad también incluye la función de borrado para discos de CD o DVD. La función de SmartErase ofrece a los usuarios la posibilidad de borrar de forma permanente aquellos discos que contienen datos confidenciales que no deben ser recuperados de ninguna manera. Con SmartErase los usuarios pueden tener la seguridad de saber que sus datos privados y confidenciales pueden borrarse sin que puedan ser recuperados.

Fuente: http://www.diarioti.com

TELEM@TICA

PARA INSCRIBIRSE EN LA REVISTA:

Enviar un mensaje a:

revistatelematica-subscribe@cujae.edu.cu

PARA ANULAR SU INSCRIPCIÓN EN LA REVISTA:

Enviar un mensaje a:

revistatelematica-unsubscribe@cujae.edu.cu

PARA AUTORES QUE DESEEN PUBLICAR EN TELEM@TICA

Para la publicación en nuestra revista los interesados deberán enviar su propuesta escrita indicando claramente: Título del artículo, glosario de términos (No más de media cuartilla), imágenes referenciadas (No más de 200Kb), nombre de los autores, sus fotografías y la institución a la que pertenecen, así como alguna forma de comunicación (teléfono, Fax o correo electrónico). Para una guía más detallada descargue el formato de publicación de la dirección: http://www.cujae.edu.cu/revistas/telematica/Soporte_Tecnico/formato.doc
Su artículo se someterá a revisión por un comité de árbitros que decidirá sobre la publicación del mismo. Deberán acompañar igualmente (en no más de media cuartilla) un glosario, de los términos más importantes utilizados en el artículo. Puede contactarnos a través de nuestro email telematica@revistas.cujae.edu.cu