Universidad de las Ciencias Informáticas

Facultad 5

Título: Subsistema de Seguridad para el SCADA Nacional Guardián del ALBA

Proyecto de tesis para optar por el título de

Ingeniero en Ciencias Informáticas

Autor: Alejandro Manuel Rubinos Carvajal.

Tutor: Ing. Iliana Pérez Pupo.

Co-Tutor: Ing. Amado Espinosa Hidalgo.

Ciudad de la Habana, Mayo, 2009.

Datos de Contacto

Iliana Pérez Pupo:

La tutora Iliana Pérez Pupo es Ingeniero en Ciencias Informáticas, forma parte del Departamento de Sistemas Digitales de la Facultad 5, de la Universidad de las Ciencias Informáticas. Amplios resultados en la producción como parte de la participación en el proyecto SCADA durante 2 años y lo que va del curso 2008-2009.

Amado Espinosa Hidalgo:

Ingeniero Informático y profesor asistente del Departamento de Ingeniería y Gestión de Software de la Facultad 5. Posee 6 años de experiencia en la actividad docente y productiva.

Agradecimientos

Agradezco eternamente a mis padres quienes me formaron, ayudaron y apoyaron incondiconalmente haciendo de mi el hombre que soy hoy.

A mi hermano por ser mi guia, mi amigo, mi segundo padre.

A mi hermana Yudith por siempre estar allí para mi.

A mi novia por su paciencia, comprención y amor acompañandome y apoyandome siempre.

A Kike por trabajar a mi lado todos estos años y ser parte irrefutable de este resultado.

A Amado por sus consejos, ayuda y guía.

A mi tutora Iliana, oponente Alexander y al tribunal especialmente a la profesora Irene.

A mis amigos Adrian, Marcel, Koty y Carlos, ustedes son mis hermanos.

A mi primo Igor por su sonrisa y cariño.

Dedicatoria

A mis padres, mi viejo y mi gordita, no los hay mejores, gracias por estar siempre conmigo.

A mi hermano, siempre te adoraré, gracias por pedirme.

A mis primeros hijos, Lauri y Jorgi, su tio los ama.

A mi abuela por ser mi angel guardián.

A mi flaca linda, que bueno que te encontré.

Síntesis

Desde los primeros pasos en la concepción del “sistema de adquisición, supervisión y control para los pueblos del ALBA”[1] o “SCADA Nacional Guardián del ALBA”, una de las prioridades resultó ser la implantación y utilización de un sistema de Seguridad, capaz de brindar entre otras operaciones la autenticación e identificación de operadores, administradores, supervisores, usuarios en sentido general, así como controlar el acceso a recursos por parte de los mismos dentro del sistema.

La principal razón de ser de esta aplicación es limitar a toda costa los ataques malintencionados por parte de usuarios o terceros, ya sea de modo local o remoto, siendo ésta una de las principales causas de que el paro petrolero ocurrido en el año 2002 pudiera ser llevado a cabo.

El presente documento refleja una investigación sobre las tecnologías usadas para el desarrollo del producto, sus necesidades, tareas, productos y resultados obtenidos que permitieron dotar al SCADA Nacional Guardián del ALBA de la seguridad necesaria para mantener la integridad de un sistema de tal importancia.

PALABRAS CLAVES

Autenticación, Control de acceso, Monitoreo, Perfiles, Usuarios, Grupos Operacionales, Recursos, SCADA, Software Libre.

Tabla de Contenidos

INTRODUCCIÓN

La Universidad de las Ciencias Informáticas (UCI) es un proyecto de la Revolución cuya misión fundamental es “formar profesionales, comprometidos con su Patria, calificados en la rama de la Informática, a partir de un modelo pedagógico flexible, que vincula dinámica y coherentemente el estudio con la producción y la investigación, acorde con las necesidades sociales del país y de otros pueblos hermanos” [2].

En la Universidad la producción se concentra en el desarrollo de proyectos ubicados en variedad de Polos Productivos. El objetivo de los polos es crear un espacio natural para ejecutar proyectos temáticos. Dentro de estos Polos se encuentra el “Polo de Hardware y Automática” de la Facultad 5.

Entre los proyectos de este polo productivo se encuentra el SCADA Nacional Guardián del ALBA, el cual es el resultado de la colaboración de universidades y empresas venezolanas y cubanas, en donde se encuentra enmarcada la solución de este trabajo. El proyecto consta de varios módulos que en su conjunto conforman el sistema. Ellos son desarrollados por distintas líneas de trabajo que a lo largo del proyecto se han ido creando según las necesidades. La línea de desarrollo Seguridad tiene la responsabilidad de garantizar la integración de un Servidor de Seguridad capaz de proveer las funcionalidades de Autenticación, Control de Acceso, Monitoreo de Sesiones de Usuario, Emisión de Alarmas de Seguridad, Detección de Intrusos y ataques al sistema.

La Seguridad en el Control Industrial es un tema novedoso y en desarrollo actual en la rama 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.

Las redes de control, supervisión y adquisiciones de datos industriales se incrementan aceleradamente. Sus aplicaciones en los sectores de la generación de electricidad, extracción y procesamiento de gas natural o petróleo, procesos de refinación de combustibles, extracción y tratamiento de minerales, etc.,

son centro del funcionamiento de programas de desarrollo estratégico de la economía nacional de varias naciones.

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.

El conjunto de decisiones importantes sobre la organización del sistema, la selección de los elementos estructurales que lo forman, sus interfaces, el comportamiento, la composición en subsistemas, además del estilo arquitectural que guía este orden de elementos, son partes ineludibles en la concepción de un sistema.

"Es importante señalar que la arquitectura de la Seguridad se debe basar en el principio de que la prioridad de las tareas en los SCADA, a diferencia de los sistemas informáticos corporativos, es la Disponibilidad, Seguridad y Confiabilidad, minimizando el impacto en el desempeño de las tareas que presentan restricciones de tiempo real"[3].

Análisis Científico Metodológico

El SCADA necesitaba un Sistema de Seguridad capaz de proveer principalmente servicios de identificación-autenticación de los usuarios que en él operan, auditan y trabajan en general, de forma que se pudiera mantener además una diferenciación en cuanto a su capacidad de acceder a los distintos recursos del sistema.

Se requería llevar un control de quiénes y cómo accedían a operaciones sobre los recursos del sistema, en este sentido habrían varios módulos implicados, los que pueden ir desde las capas más bajas a nivel de BDTR(Base de Datos en Tiempo Real), desde la cual se necesitarían enviar comandos o tareas programadas que actuarían sobre uno o varios recursos, haciéndose necesario establecer si la persona que las generó o invocó estaba o no autorizada a hacerlo; hasta las capas de Interfaz de usuario, a través del HMI(Human Machine Interface) para el establecimiento de niveles de visibilidad y operación, restringiendo a cada usuario a lo perpetuado por sus permisos sobre los elementos del sistema.

Se requería además un sistema capaz de monitorizar sesiones de usuarios, “logs” y alarmas propias del sistema de seguridad por parte de administradores, así como acciones preventivas por parte del sistema o sus administradores, que protegieran al mismo de ataques malintencionados o inconscientes.

Ante esta situación, se identificó la necesidad de contar con un mecanismo que limitara el acceso al sistema sólo a los usuarios del mismo, además de que controlara el acceso de los usuarios a los recursos del sistema según su perfil y que realizara chequeos periódicos con el fin de detectar posibles ataques al sistema.

El objetivo principal del trabajo fue:

Desarrollar un módulo de seguridad para el SCADA Nacional Guardián del ALBA que permita la autenticación al sistema, el control de acceso de usuarios a los recursos, el registro de “logs” y revisión de los mismos con el fin de detectar posibles ataques al sistema.

Para dar cumplimiento al objetivo propuesto se formularon las siguientes interrogantes:

¿Cómo lograr que el SCADA Nacional Guardián del ALBA sobre la plataforma GNU/Linux, identificara a los usuarios que en él operan?

¿Cómo lograr que el SCADA Nacional Guardián del ALBA sobre la plataforma GNU/Linux, controle el acceso a recursos por parte de usuarios que en él operan?

¿Cómo lograr que el SCADA Nacional Guardián del ALBA sobre la plataforma GNU/Linux, cuente con herramientas y operaciones que permitan la prevención, reconocimiento y notificación de actividades que atenten contra su integridad?

Para dar respuesta a las interrogantes planteadas se pretende dar cumplimiento a las siguientes tareas:

1. Estudiar e investigar las herramientas y métodos de seguridad de mayor uso a nivel mundial para conocer el estado actual del problema y seleccionar la tecnología y herramientas libres a utilizar.

2. Estudiar los métodos y operaciones existentes para la identificación-autenticación de usuarios.

3. Estudiar los métodos y operaciones existentes para el control de acceso de usuarios a recursos.

4. Estudiar métodos y operaciones existentes para la construcción de un Sistema de Detección de Intrusos (IDS).

5. Establecer políticas de seguridad para el SCADA Nacional Guardián del ALBA.

6. Realizar el análisis y diseño de los componentes o subsistemas para permitir al SCADA Nacional Guardián del ALBA las funcionalidades antes descritas.

7. Implementar los componentes o subsistemas para permitir al SCADA Nacional Guardián del ALBA las funcionalidades antes descritas.

8. Realizar la validación y prueba del sistema aplicando las normas internacionales para garantizar la calidad requerida del producto.

9. Integrar la solución con el SCADA Nacional Guardián del ALBA para que el mismo cuente con las funcionalidades antes descritas.

10. Desarrollar las pruebas de integración de los componentes o subsistemas para validar el desempeño del módulo de seguridad dentro del SCADA Nacional Guardián del ALBA.

11. Elaborar de la documentación necesaria para el mantenimiento y entendimiento del producto.

El trabajo está formado por dos capítulos descritos a continuación:

Capítulo I: Recoge el estado del arte en el que se desarrollará el producto, haciendo referencia a las necesidades, la forma en que los sistemas de seguridad se ven reflejados en los SCADA y la características arquitectónicas que el sistema deberá adoptar de poder ser utilizado en un sistema de control distribuido.

Capitulo 2: Explica la solución elaborada a partir de las necesidades y condiciones reales en las que se desplegaría el producto, los componentes y subsistemas que forman el sistema así como la interacción entre estos y parte de las tecnologías utilizadas.

Capítulo I: Fundamentación teórica

En este capítulo se abordará sobre la tecnología y métodos utilizados como parte de la solución, partiendo de las condiciones y necesidades que conllevaron a la implementación de un módulo de Seguridad.

1.1. Problemas existentes y necesidad de garantizar la seguridad e integridad en los sistemas SCADA.

Una de las características ignoradas durante años en los sistemas SCADA ha sido el tema de garantizar un sistema seguro ante ataques por parte de usuarios o entes malintencionados. Esto se debe principalmente a que se consideraban sistemas aislados, a los cuales no se tenía acceso desde la red de comunicación mundial. Esta característica, aunque garantizaba la seguridad ante ataques externos hacia los sistemas, es muy difícil de actualizar y de interactuar con otros sistemas homólogos; como lo han demostrado hechos irrefutables a lo largo de la historia de este tipo de aplicaciones y que no aplica en las condiciones actuales en que estos sistemas subsisten.

Aún cuando estos sistemas estaban aislados, no se tenía en cuenta el ataque interno provocado por usuarios malintencionados, ya fuere por motivos políticos, morales o personales, que transitan desde un trabajador inconforme como a uno que desea sabotear la instalación en servicio de intereses externos, o por usuarios inexpertos en el tipo de aplicación.

De todo esto se deriva la necesidad de controlar el acceso que usuarios internos, externos y terceras aplicaciones realicen al sistema en cuestión. Este control se realizaría mediante el establecimiento de políticas de seguridad centradas en el reconocimiento de identidad autorizada por parte de los objetos antes mencionados y el control del acceso realizado por estas a los diferentes recursos del sistema mediante el establecimiento de permisos.

1.2 Sistemas de Seguridad en Sistemas SCADA

En la actualidad cualquier sistema informático brinda especial atención e importancia a la acción de garantizar su seguridad, la cual incluye integridad del sistema en general, seguridad de sus recursos, usuarios e instalaciones. De tal modo, se han desarrollado diversos sistemas de seguridad cada uno con herramientas y métodos para garantizar la misma, llevando a cabo principalmente procesos de autenticación, control de acceso, registro de "logs", recuperación ante fallas, redundancia, auditoría y notificación de eventos a administradores y operadores. Los sistemas SCADA no quedan exentos de esta necesidad, de allí que en los primeros pasos de la concepción del SCADA Nacional Guardián del Alba se identificara esta como de total e imprescindible implementación.

El SCADA Nacional Guardián del Alba, como todo sistema de supervisión, control y adquisición necesita salvaguardar la integridad de los elementos que lo componen tomando papel protagónico los recursos que en este se manejan, las acciones sobre ellas y los usuarios que las realizan, más aún cuando la mala manipulación intencionada o no del sistema pudiera llevar a consecuencias catastróficas para el mismo.

Todo ello llevó a identificar varios procesos, o subsistemas que darían solución a la problemática en cuestión.

- ✓ **Subsistema de Autenticación.**

  El proceso de verificación de la identidad del usuario del SCADA Nacional, 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. Basado en la determinación de autenticación, el sistema puede que permita o no el potencial acceso del usuario a los recursos.

Existen varios factores para determinar la autenticidad de una persona, dispositivo o sistema, incluyendo algo que se conozca, algo que tenga o algo que sea. En general, mientras más factores se usen en el proceso de autenticación, más sólido será el proceso. Cuando se usan dos o más factores, el proceso se conoce genéricamente como "*autenticación multi-factor"[3].*

Ejemplos:

Usuario y Contraseña.

Tarjetas inteligentes.

Características biológicas.

Dentro de estos tipos de autenticación, continúa teniendo un gran valor y uso la que se refiere a aquellos datos que sólo son conocidos por el usuario al que estos identifican. Estas cuentan con gran cantidad de documentación y soporte, ya que existen internacionalmente medidas y políticas de seguridad para su uso, que comprenden desde el tamaño de la contraseña utilizada, hasta la variación y combinación de caracteres alfanuméricos y símbolos.

Las tarjetas inteligentes y códigos de barra, entre otras, entran dentro de la gama de autenticaciones a partir de algo que se posee. Éstas son de gran comodidad ya que no precisan del uso de la memoria como el caso de las contraseñas, pero su gran debilidad reside en la incapacidad de garantizar que aquel que usa la tarjeta sea el propietario de la misma, es decir la persona a quien la misma identifica. Es muy común por estas razones la combinación de éstas con el uso de contraseñas o más específico en este caso de códigos

personales, de forma tal que aquel que obtenga una tarjeta que no le pertenece necesitaría conocer el número asociada a la misma por su propietario.

La autenticación por parámetros biométricos ha cobrado singular fuerza en las últimas décadas, entrando en los procesos de autenticación como aquellas realizadas a partir de "algo que eres"[3]. Existen diversas formas de autenticarse a través de parámetros biométricos, entre ellas las más conocidas son: huella dactilar, captura de iris, geometría de la mano, geometría de la cara y reconocimiento de voz. A la hora de seleccionar uno o varios para ser utilizados en una solución los aspectos más tomados en cuenta son: costo, seguridad que brinda, velocidad, facilidad de uso, entre otras.

- ✓ **Subsistema de Control de Acceso.**

Los controles de acceso proporcionan políticas y procedimientos para especificar el uso de los recursos del sistema SCADA Nacional solamente por los usuarios de dicho sistema.

El proceso de conceder o negar peticiones específicas para la obtención y uso de información y servicios de procesamiento relacionados con la información para acceso dentro del ambiente del sistema SCADA.

La autorización es el proceso de determinar, a quién y a qué se le debe permitir el acceso a un recurso particular: control de acceso es el mecanismo para cumplir la autorización.

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.

Las técnicas más actualizadas hoy en día son el establecimiento de niveles de seguridad tanto para usuarios como recursos del sistema, de forma que sólo aquellos usuarios con niveles de seguridad iguales o superiores al que poseen los recursos, podrán acceder y operar sobre éstos. Esta solución tiene como gran inconveniente el no permitir diferenciar en ocasiones aquellos recursos a los que deseamos diferenciar por áreas de trabajo o diferenciar aquellas acciones que se desarrollen sobre ellos, entre otras. Como segunda

variante de más utilización es que prime en las relaciones directas o indirectas de los usuarios a los recursos un permiso que describa las acciones que este pueda o no realizar sobre el mismo. Ésta da la posibilidad además de la creación de contenedores tales como perfiles de usuarios y grupos operacionales de privilegios (contenedores de recursos), permitiendo asignar a un perfil acceso con determinados permisos sólo a aquellos grupos operacionales que se desee, haciendo aún más rápido y configurable el proceso de acceso por parte de usuarios a recursos.

- ✓ **Subsistema Registro de eventos**

Permite registrar todo evento de importancia en forma de “log” de sistema, garantizando así como la auditabilidad y seguimiento del mismo. Permite almacenar evidencias para determinar si el Sistema SCADA salvaguarda sus recursos, mantiene la integridad de los datos y recursos, así como comportamientos por parte de los usuarios que en él intervienen.

Existen muchas formas para el almacenamiento de estos "logs" permitiendo en algunos casos su reciclaje, revisión sistemática y automática, clasificación, etc. Entre ellos son muy utilizados el almacenamiento en bases de datos y en ficheros locales. Estos últimos muy utilizados en el sistema operativo en el que se desplegaría y desarrollaría el SCADA Nacional Guardián del Alba y sus componentes.

- ✓ **Subsistema de Detección de Intrusos**

El término Sistema de Detección de Intrusos (IDS) es utilizado por lo general para referirse a sistemas encargados de vigilar la red analizando cada trama como en el caso de los “sniffer” de red. En el caso del requerido por el SCADA Nacional Guardián del Alba, éste se refiere a aquellas acciones preventivas y de chequeo que permitan descubrir, reconocer y notificar de cualquier posible ataque por parte de usuarios malintencionados, velar por acciones tales como la suplantación de identidad, el acceso inadecuado a recursos en

modo perjudicial para el sistema y múltiples entradas al sistema por parte de un usuario, entre otras.

- ✓ **Subsistema Administración**

  Necesidad de una aplicación capaz de permitir el monitoreo, visualización, búsqueda y administración de componentes tales como usuarios, "logs", alarmas y sesiones de usuario activas. Constituye una herramienta para administradores del sistema, permitiendo salvaguardar el mismo.

1.3 Seguridad como sistema distribuido

En el curso de la historia de los sistemas informáticos, éstos han evolucionado hacia los sistemas distribuidos debido a dos factores fundamentales:

- ✓ Grado de complejidad computacional

Con la versatilidad de la computación, cada día aumentan el número de procesos de la vida real que pueden ser modelados por medio de la computación, algunos de muy alta complejidad, por lo que requieren de grandes niveles de procesamiento que las tecnologías actuales no pueden cubrir, además, es más económico comprar muchas computadoras pequeñas que pocas computadoras grandes.

- ✓ Distribución geográfica de los componentes hardware utilizada o necesidad de compartirlos entre diferentes aplicaciones.

En resumen, los sistemas distribuidos pueden definirse como aplicaciones con una fuerte componente geográfica, donde la ejecución no ocurre en una única estación de trabajo. Entre sus componentes se

encuentra el encargado de gestionar la comunicación entre los diferentes nodos con vistas a garantizar el paso de mensajes y que el sistema responda como un servicio integrado.

El sistema de seguridad para el SCADA Nacional Guardián del Alba deberá adoptar la característica de ser un sistema distribuido ya que éste en sí, lo es. Establecer una comunicación cliente-servidor es de vital importancia, así como asegurar la comunicación del módulo de Seguridad con subsistemas tales como el de Configuración y Bases de Datos Históricas para el registro de eventos antes mencionado, a través del subsistema intercomunicador Middleware.

Capítulo 2: Aporte a la Solución

El trabajo realizado es novedoso en nuestro país, dado que a pesar de que se ha trabajado en temas relacionado con seguridad informática, no así si lo enfocamos en el ambiente específico en que se desarrolló. Esto se refiere a la plataforma y componentes en que se desarrolla GNU/Linux y utilizando bibliotecas provistas y soportadas por la amplia comunidad mundial que existe para el desarrollo de productos de software libre, y como segunda razón el que aunque sea un sistema con altos niveles de portabilidad, o sea que éste puede ser llevado a otros entornos de trabajo y plataformas de despliegue y desarrollo, pues está diseñado para un sistema SCADA, lo cual como había sido mencionado anteriormente es novel en este tipo de sistemas.

Para solventar los requisitos que planteaba el “SCADA Nacional Guardián del ALBA” el autor realizó un trabajo en conjunto con el equipo de Seguridad del proyecto SCADA del Polo de Hardware y Automática para el diseño e implementación de los siguientes insumos divididos en dos anexos, cada uno con duración de 6 meses de trabajo, es por ellos que para nombrarlos se clasificaran por sus respectivos anexos.

- **Primer Anexo:**

    1. Subsistema Autenticación por medio de usuario y contraseña.
    2. Subsistema Control de Acceso.
    3. Subsistema Monitoreo.
    4. Subsistema Registro de Eventos.
    5. Documentación, diseño y pruebas de las funcionalidades.

- **Segundo Anexo**

    1. Subsistema Autenticación por Huellas Dactilares.
    2. Subsistema de Detección de Intrusos.
    3. Documentación, diseño y pruebas de las funcionalidades.

Para ello el equipo de trabajo liderado por el autor se dispusieron al diseño de las funcionalidades para lo cual se separó el trabajo en 4 componentes principalmente, ellos son Base de Datos de Seguridad, Servidor de Seguridad, Cliente de Conexión de Seguridad y Administrador de Seguridad (Security Manager).

2.1 Base de Datos de Seguridad

En función de garantizar la persistencia de los elementos que intervendrán en la aplicación y sus relaciones, se diseñó la Base de Datos de Seguridad. Para ello se utilizó PostgreSQL como sistema de gestión de base de datos relacional orientada a objetos de software libre, publicado bajo la licencia BSD y que cuenta con la característica de ser multiplataforma. Para el trabajo con PostgreSQL en el lenguaje de programación C++, se utiliza la librería pqxx desarrollada en software libre y con amplio soporte en la comunidad.

El diseño se basó principalmente en la creación de 4 entidades: usuarios, recursos, perfiles y grupos operacionales de privilegios. La relación entre ellas permitió al sistema tener una capacidad alta de respuesta inmediata y de extensibilidad. Esto se logra haciendo los perfiles contenedores de usuarios de la misma forma que los recursos dentro de los grupos operacionales de privilegios.

Además, la relación entre los perfiles y grupos operacionales de privilegios, manifiestan el nivel de permiso que tienen los primeros en los segundos, facilitando de esta forma que el acceso de un usuario a un recurso fuera mucho más rápido y sencillo, sin importar si existe o no un número grande de ambos.

El diseño facilita además de una manera sencilla la autenticación de usuarios en el sistema, aunque también puede efectuarse ésta a través de un LDAP(Protocolo Ligero de Acceso a Directorios). La misma cuenta además con las estructuras necesarias para el almacenamiento de "logs" y alarmas, en el caso de los primeros divididos en tablas que permiten su clasificación y reciclaje a partir de tipos y fechas.

2.2 Servidor de Seguridad

El autor desarrolló el Servidor de Seguridad en el que están implementadas todas las funcionalidades que el sistema debe presentar, utilizando una gran cantidad de patrones de diseño e implementación que permitieron garantizar la robustez, rapidez, portabilidad y extensibilidad del mismo. Las funcionalidades más importantes son brevemente explicadas a continuación:

- ✓ Subsistema Autenticación: En este yace la responsabilidad de la identificación del usuario SCADA y la creación de su sesión de trabajo, en la que se verán reflejados sus permisos a los recursos. Cuenta con dos medios para la puesta en marcha del proceso, mediante el uso de usuario y contraseña y a través de su huella dactilar. Cabe agregar que el segundo añade un valor innovador ya que aunque la tecnología existe hace algunos años, no existe un gran desarrollo en la parte de componentes libres para su uso y menos aún para sistemas distribuidos.
- ✓ Subsistema Control de Acceso: A partir de la sesión de usuario creada se encarga de decidir si un usuario puede desarrollar o no, una acción o no, sobre un recurso.

- ✓ Subsistema de Detección de Intrusos: Se encarga del registro y revisión de "logs" en busca de anomalías tales como múltiples accesos a recursos en modo de escritura por parte de uno o varios usuarios, múltiples sesiones creadas por un mismo usuario e intentos de autenticación desde una estación de trabajo ya en uso, generación de alarmas de seguridad y chequeo de validez de contraseña.

El Servidor de Seguridad publica a través del uso del subsistema Middleware las interfaces necesarias para que éstas puedan ser invocadas por cualquier cliente.

Su diseño permitió una gran extensibilidad y la capacidad de reutilizar los componentes y clases implementadas, esto permitió que aunque el trabajo fuese dividido en dos grandes anexos no hubiera la necesidad de reimplementar o rediseñar en el paso de una versión a otra.

2.3 Cliente de Conexión de Seguridad

Al autor se le encomendó la tarea de desarrollar el cliente de seguridad mediante el cual los distintos módulos que requirieran usar las funcionalidades que brinda el módulo de seguridad y que se desarrollan en el Servidor de Seguridad explicado anteriormente. Es una biblioteca que es embebida en dichos módulos, por lo que el acceso se hace rápido y el desarrollo sencillo.

2.4 Administrador de Seguridad (Security Manager)

Aplicación de ayuda, control y administración de elementos de seguridad para administradores que les permite visualizar y administrar alarmas de seguridad y sesiones activas, realizar búsquedas de usuarios y "logs". Desarrollada en GTKmm plataforma para desarrollo de entornos visuales," es capaz de realizar notificaciones al usuario aún cuando la aplicación no está en primer plano o minimizada a través de sonidos y mensajes"[4]. El diseño escogido facilita el cambio de una tecnología a otra, la reutilización de código y la extensibilidad del producto. El Administrador de Seguridad constituye la herramienta que

permite la visualización de los resultados obtenidos a partir del Sistema de Detección de Intrusos, además de que posee los elementos para dar respuesta en caso de que dichos resultados reflejen una violación o ataque o la posible ocurrencia del mismo. Para su comunicación con el Servidor de Seguridad usa el cliente de conexión de seguridad.

2.5 Publicaciones y trabajos relacionados con la Investigación

El trabajo ha sido presentado en varios eventos entre los cuales cobra singular fuerza CITTEL' 08 Congreso Internacional de Telemática y Telecomunicaciones con sede en la Ciudad de La Habana, además el año pasado se presentó dividido en tres trabajos en la jornada científico estudiantil obteniendo la categoría relevante en los tres, ese mismo año se presentó en el evento UCIENCIA.

Como parte del producto SCADA Nacional Guardián del ALBA, ha sido implantado en varias instalaciones de la hermana República Bolivariana de Venezuela, en fase de prueba, principalmente en el patio de tanques situado en el estado Barinas, brindando resultados satisfactorios y meritando diferentes reconocimientos, tales como “Solución más Integral”, en las Primera y Segunda Feria Expositiva de Productos de la UCI en el año 2008, en la primera de las cuales el autor participó como representante del “*stand”* junto a otros compañeros. Obtiene el proyecto Guardián del ALBA del Polo de Automática y Hardware dos premios en el balance de producción 2008 efectuado el viernes 20 de Febrero 2009, otorgado por el Consejo de Dirección de la Universidad: “Premio al Mejor Proceso de Software” y “Premio al proyecto de Mayor Ingreso al País”.

2.6 Ingresos

Hasta la actualidad, por conceptos de ingresos directos, el proyecto ha aportado alrededor de 6 millones de dólares al país, con un reporte de utilidades netas del 90%. El módulo de Seguridad hasta el momento

ha realizado y continúa realizando dos anexos por valor de 187, 920.00 y 335,264.00 respectivamente. El valor del SCADA Nacional Guardián del ALBA va más allá de la parte económica pues ha inspirado entre otros grandes hitos la creación de una empresa mixta entre Cuba y Venezuela cuya primer objetivo es brindar una cobertura para el proceso de informatización de Nuestra América.

CONCLUSIONES

La seguridad de los sistemas informáticos es de gran importancia dado que estos cubren una importante parte de los servicios y empresas a nivel mundial. Gracias al trabajo del autor se presenta una variante de seguridad informática para sistemas distribuidos, críticos y de control tal como el SCADA Nacional Guardián del ALBA.

La solución a la propuesta mostrada en este documento representa el trabajo realizado por el autor y como ésta garantiza y complace con creces los requisitos del cliente. Muestra cómo la solución es innovadora y capaz de competir con sistemas propietarios de este tipo a nivel mundial, mostrando una vez más que el futuro está en el uso de componentes libres más aun para países de nuestra América que son cada día pisoteados por la feroz hambre de poder del capitalismo y sus transnacionales.

Impacto de la Propuesta

La elaboración de la solución permitió, al SCADA Guardián del ALBA:

- ✓ La identificación-autenticación de usuarios en el sistema, de forma tal que proveer el acceso al sistema sólo a aquellos usuarios que estén incorporados al mismo, permitiendo así la creación de sesiones de trabajo en la cual reside la información del usuario.

- ✓ Garantiza el control de acceso a recursos del sistema por parte de los usuarios autenticados en el mismo, así como de aquellas tareas programadas a ejecutarse. Su valor reside en que impide a usuarios sin los permisos requeridos realizar acciones sobre recursos que pudiesen atentar contra su integridad, desde algo tan importante como el envío de un comando en el sistema hasta la simple visualización de una alarma o reporte del mismo.

- ✓ Almacenamiento de "logs" de seguridad que permitan el registro de conductas y operaciones por parte de usuarios.

- ✓ Permite la prevención y notificación de posibles ataques al sistema, mediante revisiones de "logs" de antigüedad, monitoreo de las sesiones activas en el sistema y alarmas propias de seguridad.

- ✓ Permite la visualización de información de usuarios y "logs" del sistema, posibilitando conocer detalles de los mismos para su posterior análisis.
- ✓ Establece entidades de usuarios, perfiles, grupos operacionales de privilegios y recursos, así como sus relaciones y garantiza la persistencia de los mismos.

RECOMENDACIONES

Se recomienda que el producto representado por este trabajo continúe en desarrollo y constante mejora, buscando nuevas herramientas y vías para hacerlo una herramienta de Seguridad aún más potente.

Durante el desarrollo del producto se generaron algunas bibliotecas con utilidad para procesos tales como Encriptación, Acceso a Datos, Validación de cadenas, Gestión de Huellas Dactilares, entre otras, las cuales pueden ser utilizadas por otros productos en desarrollo, a fin de reutilizar componentes autóctonos y que han sido probados en varios ambientes para los cuales la solución fue diseñada.

Aunque la solución actual dio cumplimiento y satisfizo las necesidades actuales del cliente hay una gran cantidad de trabajos que pudieran realizarse a fin de robustecer y enriquecer la misma, haciendo de esta una herramienta a ser utilizada no solo en sistemas de este tipo, tales como vigilancia por cámaras, autenticación por iris, tarjetas inteligentes, código de barra y geometría de la mano y la cara.

Existe una gran cantidad de documentación generada durante el proceso de desarrollo del producto, la que es recomendada para el desarrollo de sistemas de este tipo.

BIBLIOGRAFÍA

1. **Canesto, Kariana.** *Introducción a la arquitectura del Sistema de adquisición supervisión y control para los pueblos del ALBA y descripción de sus módulos.* 2009.

2. **Morell, Melchor Gil.** Carta del Rector. *Portal UCI - Universidad de las Ciencias Informáticas.* [En línea] http://www.uci.cu/?q=node/47.

3. **Valcarcel, Leonardo.** *Documento de Arquitectura del Software "Seguridad".* Mérida: s.n., 2007.

4. **Rubinos Carvajal, Alejandro Manuel.** Especificación de requerimientos de software Seguridad 2.0. Merida 2009

5. **Rubinos Carvajal, Alejandro Manuel.** Descripción General Funcionalidades Seguridad 2.0. Mérida 2009

6. **L. Krutz, Ronald.** Securing SCADA Systems. 2006

7. **Rodríguez Penin, Aquilino.** Sistemas SCADA. Notas de diseño, normativa, seguridad y comunicaciones industriales, primeros pasos con Intouch. 2007

8. **Rodríguez Penin, Aquilino.** Sistemas Scada. 2ª Edición. 2007

GLOSARIO

ALBA: La Alternativa Bolivariana para los Pueblos de Nuestra América o ALBA es una propuesta de integración enfocada para los países de América Latina y el Caribe que pone énfasis en la lucha contra la pobreza y la exclusión social con base en doctrinas de izquierda.

BDTR: Base de Datos en tiempo Real, aplicación usada en el SCADA Nacional Guardian del ALBA.

HMI: Interfaz Hombre-Maquina(Human Machine Interface).

IDS: Intruder Detection System, sistema encargado de detectar ataques o violaciones.

LDAP: Protocolo Ligero de Acceso a Directorios (Lightweight Directory Access Protocol), es un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red. LDAP también es considerado una base de datos (aunque su sistema de almacenamiento puede ser diferente) a la que pueden realizarse consultas.

Licencia BSD: es la licencia de software otorgada principalmente para los sistemas BSD (Berkeley Software Distribution).

Logs: Registros del sistema, se refieren a acciones, comportamientos realizadas por los sistemas o sobre ellos

Middleware: Subsistema de Comunicación del SCADA Nacional Guardián del ALBA

Multiplataforma: es un término utilizado frecuentemente en informática para indicar la capacidad o características de poder funcionar o mantener una interoperabilidad de forma similar en diferentes sistemas operativos o plataformas.

PDVSA: Petróleos de Venezuela, Sociedad Anónima (PDVSA) es una empresa estatal venezolana que se dedica a la explotación, producción, refinación, mercadeo y transporte del petróleo venezolano.

Sistemas de Adquisición de Datos y Control Supervisorio (SCADA): Aplicación de software especialmente diseñada para funcionar sobre computadores en el control de producción, proporcionando comunicación con los dispositivos de campo y controlando el proceso de forma automática desde la pantalla del operador, proveyendo toda la información asociada al proceso.